ACC AMERICA
Association of Corporate Counsel
Northeast Chapter

Nutter

The Corporation as Victim: Cyber Crime, Hacking & Data Breach

ACC Northeast Chapter

Wednesday, June 25, 2014

Nutter McClennen & Fish LLP
Seaport West
155 Seaport Boulevard
Boston, Massachusetts 02210

www.nutter.com | @NutterLaw

ACC America
Association of Corporate Counsel
Northeast Chapter

Nutter

The Corporation as Victim: Cyber Crime, Hacking & Data Breach
ACC – Northeast Program

Wednesday, June 25, 2014

Program Agenda

4:00 – 4:30 pm Registration

4:30 – 6:00 pm **Opening Remarks**

Cathy Mannick
General Counsel and Chief Administrative Officer
AcadiaSoft, Inc.

Panel Discussion

Peter M. Acton, Jr.
Director/Senior Counsel, Global Compliance
EMC Corporation

Adam J. Bookbinder
Assistant US Attorney, Cybercrime Unit
US Attorney's Office, District of Massachusetts

Allison D. Burroughs
Partner, Government Investigations and White Collar Defense
Nutter McClennen & Fish LLP

John T. Martinez
Chief Privacy Counsel
Senior Counsel for Cybersecurity - Intelligence, Information and Services (IIS)
Raytheon Company

Peter T. Trahon
Executive Director
Forensic Technology & Discovery Services
Ernst & Young

Moderated by

Jonathan L. Kotlier
Chair, Government Investigations and White Collar Defense
Nutter McClennen & Fish LLP

6:00 pm **Cocktail Reception & Networking**

ACC America
Association of Corporate Counsel
Northeast Chapter

Nutter

The Corporation as Victim: Cyber Crime, Hacking & Data Breach
ACC – Northeast Program

Wednesday, June 25, 2014

Contents

1. Speaker Biographies

2. Exclusive: FBI Warns Healthcare Sector Vulnerable to Cyber Attacks, by Jim Finkle, *Thomson Reuters*, April 23, 2014

3. Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-20130091, February 12, 2013

4. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technoloy, Feburary 12, 2014

5. Improving Critical Infrastructure Cybersecurity, Incentives Study Analytic Report, Department of Homeland Security, Integrated Task Force, June 12, 2013

6. Under Cyber Attack — Ernst & Young's 2013 Global Information Security Survey, October 2013

7. U.S. States Probe eBay Cyber Attack as Customers Complain, by Jim Finkle and Karen Freifeld, *Thomson Reuters*, May 22, 2014

8. Host Firm Information — Nutter McClennen & Fish LLP

ACC America
Association of Corporate Counsel
Northeast Chapter

Nutter

The Corporation as Victim: Cyber Crime, Hacking & Data Breach
ACC – Northeast Program

Wednesday, June 25, 2014

Speaker Biographies

Peter M. Acton Jr.
Director / Senior Counsel, Global Compliance
EMC Corporation

Adam J. Bookbinder
Assistant US Attorney, Cybercrime Unit
US Attorney's Office, District of Massachusetts

Allison D. Burroughs
Partner, Government Investigations & White Collar Defense
Nutter McClennen & Fish LLP

Jonathan L. Kotlier
Chair, Government Investigations & White Collar Defense
Nutter McClennen & Fish LLP

John T. Martinez
Chief Privacy Counsel
Senior Counsel for Cybersecurity - Intelligence, Information and Services (IIS)
Raytheon Company

Ian D. Roffman
Partner, Securities Enforcement and Litigation
Nutter McClennen & Fish LLP

Peter T. Trahon
Executive Director, Forensic Technology & Discovery Services
Ernst & Young

Peter M. Acton, Jr.
Director/Senior Counsel,
Global Compliance
EMC Corporation

Peter M. Acton, Jr. is the Senior Counsel for Global Compliance at EMC Corporation. Peter, who joined EMC in 2011, is responsible for managing EMC's Global Corporate Compliance program. Prior to joining EMC, Peter was a Partner at McDermott Will & Emery LLP in Boston, where he specialized in white collar investigations and litigation, advising corporate and individual clients in government investigations, internal investigations, *qui tam* and civil litigation. Peter was named a New England Rising Star by *Super Lawyers* magazine from 2009 to 2011. Prior to Joining McDermott, Peter was an attorney at Nutter McClennen & Fish LLP. Peter has served as a panelist on numerous occasions prior to and since joining EMC on various compliance topics, and taught a litigation basics course at Massachusetts Continuing Legal Education for many years.

Peter received his J.D. from Fordham University where he was named the Hon. Milton Pollock Fellow. Peter received his B.A., magna cum laude, from Villanova University where he received numerous honors, including being named to the *Phi Beta Kappa, Phi Kappa Phi*, and *Phi Alpha Theta* honor societies. Peter was also the student body President while at Villanova.

Adam J. Bookbinder
Assistant United States Attorney
Chief, Cybercrime Unit
United States Attorney's Office
for the District of Massachusetts

Adam J. Bookbinder is the chief of the Cybercrime Unit in the U.S. Attorney's Office for the District of Massachusetts. He has been an assistant U.S. Attorney since 1999, spending the past 10 years in the Cybercrime Unit and the previous four in the Economic Crimes Unit. Before joining the U.S. Attorney's Office, he worked as an assistant D.A. in the Essex County D.A.'s Office, an associate at Bingham, Dana, and Gould, and a clerk for Ninth Circuit Judge Stephen Trott. He has a B.A. from Dartmouth College and a J.D. from Harvard Law School.

Nutter McClennen & Fish LLP
Attorneys at Law
www.nutter.com

Allison D. Burroughs **Partner**

Seaport West, 155 Seaport Boulevard, Boston, MA 02210 T: 617.439.2684 F: 617.310.9684 E:aburroughs@nutter.com

Education

University of Pennsylvania Law School, J.D.

Middlebury College, B.A.

Bar Admissions

Massachusetts

Pennsylvania

Honors and Awards

Chambers and Partners, Leading U.S. White-Collar Crime & Government Investigations Litigation Attorney, 2010-2013

Litigation Counsel of America, Fellow

Massachusetts Super Lawyers, 2011-2013

Super Lawyers Business Edition, 2012-2013

The Best Lawyers in America, 2013-2014

2013 Corporate Intl Magazine Legal Award - Business Crime Lawyer of the Year in Massachusetts

2013 International Global Law Experts Awards - Business Crime Lawyer of the Year in Massachusetts

Allison D. Burroughs is a partner in the Litigation Department and a member of the Government Investigations and White Collar Crime practice group. Clients rely on her to represent them in cases and investigations involving federal, state and local law enforcement and regulatory agencies including for internal investigations, grand jury investigations, third party subpoenas and related complex civil litigation. Much of her practice focuses on the life sciences industry, with particular emphasis on off-label and related prosecutions and other False Claims Act cases. She also has extensive experience with the Computer Fraud and Abuse Act and the Stored Communications Act. Allison is an accomplished courtroom lawyer and has successfully tried many federal cases to verdict. She joined the firm from the Boston U.S. Attorney's Office.

Allison's representative transactions include:

- Representing twenty plus engineers involved with complex civil and criminal litigation arising from a major Boston construction project
- Representing a major pharmaceutical company and numerous employees of other pharma companies in various off-label investigations
- Successfully negotiating the dismissal of federal felony charges against an individual charged with offenses arising from a large scale immigration raid
- Defending an individual charged with perjury
- Defending an international shipping company charged with environmental violations
- Regularly represent service providers and universities with issues arising under the Electronic Communications Privacy Act and the Stored Communications Act
- Negotiated pretrial diversion for individual charged civilly and criminally for assault and related civil rights violations
- Represent numerous individuals and companies in federal criminal and civil investigations focused on off-label promotion, kick backs and pricing issues in the pharma and device industries
- Assist clients with internal investigations and, where appropriate, facilitate referrals to law enforcement

Allison's leadership role in the business community includes being a member of the Boston Bar Association's Education Committee and the Steering Committee for the Criminal Justice Section. She was appointed to the BBA's Wrongful Conviction Task Force, as well as the Newton Police Chief Search Committee. She has moderated and participated as a panel member for numerous Bar Association events, including on topics such as computer crime, sentencing, health care and general criminal litigation. Additionally, she was appointed as Special Counsel by the Massachusetts Supreme Judicial Court in 2011 and is currently an appointed member of the First Circuit Rules Advisory Committee.

During her distinguished 16 years with the Department of Justice

in Philadelphia and then Boston, Allison developed expertise in investigating sophisticated white collar and economic crimes, including intellectual property offenses, computer crimes, money laundering, mail and wire fraud, economic espionage, terrorism, telemarketing schemes, FCPA violations and complex RICO prosecutions. At the U.S. Attorney’s Office in Boston, Allison initiated and supervised the computer crime and intellectual property section and managed an outreach program that educated individuals and businesses on preventing and responding to technology related crimes and threats. The Executive Office for United States Attorneys awarded Allison three Director's Awards for Superior Performance as an Assistant United States Attorney for significant prosecutions in the areas of computer crime, international money laundering and organized crime.

Nutter McClennen & Fish LLP
Attorneys at Law
www.nutter.com

Jonathan L. Kotlier

Partner, Chair, Government Investigations and White Collar Defense Practice Group

Seaport West, 155 Seaport Boulevard, Boston, MA 02210 T: 617.439.2683 F: 617.310.9683 E:jkotlier@nutter.com

Education

Boston University School of Law, J.D.

University of Chicago, M.A.

University of Pennsylvania, B.A.

Bar Admissions

Massachusetts

New York

Pennsylvania

Honors and Awards

Chambers and Partners, Leading U.S. White-Collar Crime & Government Investigations Litigation Attorney, 2014

The Best Lawyers in America, 2008-2014

Member, Judicial Nominating Commission, by appointment of Governor Deval L. Patrick (2008 -)

Massachusetts Super Lawyers, 2005-2013

Super Lawyers Business Edition, 2011-2013

Super Lawyers, Corporate Counsel Edition, 2009 & 2010

Boston's Best Lawyers, 2011

Jonathan L. Kotlier is chair of the Government Investigations and White Collar Crime practice group. Jonathan joined the firm in 2004 from the U.S. Attorney's Office where, for eight of his twelve years, he was Chief of the Economic Crimes Unit.

Since joining Nutter, Jonathan has represented several corporations and individuals in white collar criminal and complex civil cases and investigations involving alleged securities fraud, health care fraud, Foreign Corrupt Practices Act violations, environmental crimes, government contracting fraud, and False Claims Act violations. Much of his work has been in the area of defending securities related actions involving accounting fraud issues. He has also conducted internal investigations on behalf of corporations and special litigation committees. He frequently represents individuals and corporations before the Securities and Exchange Commission, FINRA, and the Massachusetts Securities Division.

Jonathan has an outstanding track record of persuading investigative and prosecutive agencies not to bring actions against his clients. Recently, he convinced the SEC not to bring insider trading claims against a client. Similarly, Jonathan successfully argued to a U.S. Attorney's Office that it should not bring a criminal False Claims Act case against a surgeon he represented. Please see "Representative Experience" for more detail.

Jonathan has a long and successful history as a trial attorney. While at the U.S. Attorney's Office, he gained extensive experience prosecuting sophisticated white collar criminal cases involving securities and investor fraud, computer crimes and intellectual property and environmental crimes. He has tried to verdict over 20 jury trials.

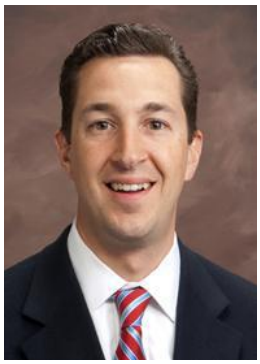
As chief of the Economic Crimes Unit, he worked closely with the Securities and Exchange Commission and the Massachusetts Division of Securities to develop many successful securities fraud prosecutions. He prosecuted, and supervised the prosecution of, numerous securities fraud cases involving accounting fraud, FCPA violations, market manipulation, investment advisor fraud, and insider trading. He served on the Securities and Commodities Fraud Working Group of the Department of Justice.

Jonathan is a past co-chair of the Criminal Justice Section of the Boston Bar Association. As a member of that section, Jonathan moderated several seminar panels on securities fraud topics, including the new SEC cooperation initiative in April 2010. Jonathan is also a member of the Governor's Judicial Nominating Commission.

Recently, he was appointed by the Massachusetts Supreme Judicial Court as special counsel to investigate allegations of improprieties within the judicial system.

John T. Martinez
Chief Privacy Counsel
Senior Counsel for Cybersecurity
Intelligence, Information and Services (IIS)

Raytheon Company
22265 Pacific Blvd.
Rm. 656-R9-2
Sterling, Virginia
20166-6913 USA
571-250-2601



Biography

John Martinez is the Chief Privacy Counsel and Cybersecurity and Special Missions Senior Counsel for Raytheon Intelligence, Information and Services. Previously, he served as Senior Counsel to both the Defense and Civil Mission Solutions and Mission Operations Solutions businesses. Mr. Martinez handles an array of legal issues relating to privacy, cybersecurity, government and commercial contract formation, administration, and compliance as well as issues relating to corporate governance, labor and employment matters, international compliance with FCPA, ITAR and EAR requirements and intellectual property.

Before assuming his current position, Mr. Martinez was the Deputy General Counsel for Intelligence at the Office of the Director of National Intelligence (ODNI). In that role, he supported the Director of National Intelligence in fulfilling his statutory responsibility to ensure Intelligence Community compliance with the U.S. Constitution and laws by providing legal advice to all elements of the ODNI on an array of legal issues including intelligence and national security law, intelligence collection and analysis, covert action, international relations, and litigation.

Prior to joining ODNI, Mr. Martinez was an Associate General Counsel at the Central Intelligence Agency where he was Chief of the Director's Review Group (DRG). The DRG represented Director Panetta on three Executive Order taskforces examining interrogation policy, disposition of Guantanamo Bay detainees, the future detention policy and served as the primary Agency focal point for Department of Justice, House, and Senate investigations into rendition, detention and interrogation matters. Prior to serving as Chief of Director Panetta's Review Group, Mr. Martinez was Chief of the CIA's Counterterrorism Center High-value Detainee Prosecution Taskforce, which was responsible for dealing with classified information issues in terrorism detainee prosecutions, arising in both civilian Article III Courts and the military commission system. Upon joining CIA in 2002, Mr. Martinez served in CIA's Litigation Division where he handled civil and criminal national security cases and later served as an operational lawyer in CIA's Counterterrorism Center.

Before joining CIA in 2002, Mr. Martinez was a litigation associate with the law firm of Greenberg Traurig, LLP in New York City. His practice centered on broker-dealer securities litigation, defending individuals at trial as well as in investigations by the U.S. Securities and Exchange Commission and self-regulatory organizations, such as the NASD (now-FINRA).

Prior to his civil litigation experience in private practice, Mr. Martinez was an Assistant District Attorney in New York County (Manhattan) from 1997 through 2001. He served as a trial attorney concentrating on prosecutions within the Firearms Trafficking, Domestic Violence, and the Sex Crimes Units. In those positions, he prosecuted and brought to trial numerous major felonies such as, attempted murder, kidnapping, sexual violence, weapons and narcotics offenses as well as conducted long-term criminal and grand jury investigations.

Mr. Martinez earned his Juris Doctorate from St. John's University School of Law and a Bachelor of Arts in political science at Pennsylvania State University.

Nutter McClennen & Fish LLP
Attorneys at Law
www.nutter.com

Ian D. Roffman **Partner**

Seaport West, 155 Seaport Boulevard, Boston, MA 02210 T: 617.439.2421 F: 617.310.9421 E:iroffman@nutter.com

Education

University of Chicago Law School, J.D.

University of Chicago, A.B.

Bar Admissions

Massachusetts

Illinois

Honors and Awards

Massachusetts Super Lawyers, 2011-2013

Boston Business Journal's 40 Under 40, 2011

Volunteer Lawyers for the Arts, Fraser Award, 2011

Benchmark Lawyer's Guide "Rising Star," 2011-2013

SEC Chairman's Award, 2002

SEC Enforcement Director's Award, 2007

Ian Roffman is a partner in the Securities Enforcement and Litigation practice group and the Litigation Department. Ian specializes in advising executives, directors, and boards facing SEC and other government investigations and enforcement matters. He has also advised cooperators, witnesses, and victims about their rights before, during, and after government investigations. Prior to joining Nutter, Ian was Senior Trial Counsel in the SEC's Boston office.

Recent representations have included:

- Board Chairman of software company in an SEC accounting fraud investigation
- A State Treasurer in an SEC investigation of municipal bond underwriting
- Portfolio managers in multiple state and federal investigations and litigation relating to collateralized debt obligations and asset-backed securities
- General Counsel of a $20 billion investment advisor in an SEC disclosure and trading investigation
- General Counsel of software company in corporate governance disputes and Delaware litigation
- Multiple executives in insider trading investigations
- Senior executive of a Fortune 500 financial services company in an SEC financial crisis-related investigation
- CFO of a top 10 mutual fund complex in shareholder litigation
- CFO of a multi-national technology company in an FCPA investigation
- CFO of mid-cap public company in an SEC accounting investigation
- Senior executive of Fortune 500 healthcare company in SEC disclosure investigation
- Division head of financial services company in annuity disclosure investigation
- Senior managers of Fortune 500 retail company in SEC disclosure investigation
- Controller of multi-national technology company in SEC accounting investigation
- Hedge fund manager in manipulative trading investigation
- Private equity manager in insider trading investigation
- Mutual fund manager in insider trading investigation

Ian also works with public and private companies, financial services firms, investment advisors, broker-dealers, and other entities in matters involving SEC inquiries, securities litigation, corporate governance disputes, government investigations and complex civil litigation. He conducts internal investigations for boards and management, and represents clients in court, before regulators and law enforcement agencies, in mediations and arbitrations, and in the boardroom.

In 2011, Ian was named as one of the *Boston Business Journal's* "40 under 40." He has been selected for *Massachusetts Super Lawyers* and recognized as a "future star" by the Benchmark lawyer's guide. While at the SEC, Ian received the Enforcement

Director’s Award and the Chairman’s Award for Excellence. In addition, Ian has also represented artists and musicians in various types of matters. His work on their behalf was recognized by the Massachusetts Volunteer Lawyers for the Arts with the Robert B. Fraser Award for pro bono excellence.

Ian is active in a number of non-profit, community and bar organizations. He has been quoted on the SEC and corporate governance by many media outlets and is a frequent speaker and lecturer before bar, industry, and academic organizations.

Biography

Peter Trahon
Executive Director

Contact information
Office: + 1 703.747.1675
Mobile: +1 703.907.9893

peter.trahon@ey.com

Education

B.S., Industrial Technology, Northeastern University

A.S. Computer Engineering, Wentworth Institute of Technology

Certified Forensics Examiner

Certified Information Security Professional

Certified Law Enforcement Instructor

Memberships

SANs

InfaGard

Society of Former Agents

Professional background

Background

Former FBI Special Agent Executive, Cyber Division

Former Director of the National Cyber Investigative Joint Task Force

Led FBI Cyber Division's National Security Section

Supervised the FBI's first Computer Intrusion Squad

Developed Cyber training curriculum for over 1000 global cyber security personnel

Designed, developed and implemented IT business applications

The following is a representative sample of engagements Mr. Trahon has:

Managed national cyber security programs and investigated high risk, complex computer intrusion violations.

Directed the Presidential mandated National Cyber Investigative Joint Task Force. Experienced in leading multi-agency teams to successful outcomes in cyber international investigations involving cyber economic espionage and cyber terrorism.

Directed a team of Special Agents and Computer Forensics Examiners to protect computer systems and networks of the United States Government and private industry by investigating violations of federal statutes in which computer systems and networks are exploited as the targets of terrorist organizations, foreign government sponsored intelligence operations or criminal activities.

Successfully investigated: multi-million dollar Theft of Intellectual Property cases; several criminal computer intrusion cases; foreign intelligence computer intrusion cases; and corporate financial, insurance fraud schemes and public corruption, and internal and external bank fraud schemes.

Managed technical experts to maintain systems performance; designed and developed software programs to ensure successful transitions to new platforms.

EY
Building a better working world

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity.
Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY's Fraud Investigation & Dispute Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the industry sector. With our more than 2,000 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide.

ey.com

Exclusive: FBI warns healthcare sector vulnerable to cyber attacks

BY JIM FINKLE

BOSTON Wed Apr 23, 2014

(Reuters) - The FBI has warned healthcare providers their cybersecurity systems are lax compared to other sectors, making them vulnerable to attacks by hackers searching for Americans' personal medical records and health insurance data.

Health data is far more valuable to hackers on the black market than credit card numbers because it tends to contain details that can be used to access bank accounts or obtain prescriptions for controlled substances.

"The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely," the Federal Bureau of Investigation said in a private notice it has been distributing to healthcare providers, obtained by Reuters.

The notice, dated April 8, did not mention the Obamacare website, Healthcare.gov, which has been criticized by opponents of the Obama administration for security flaws. It urged recipients to report suspicious or criminal activity to local FBI bureaus or the agency's 24/7 Cyber Watch.

FBI spokeswoman Jenny Shearer declined comment on the private industry notification, or PIN. In January the FBI issued a PIN advising retailers to expect more credit card breaches following last year's unprecedented attack on Target Corp.

Details of PINs are typically unclassified, but generally only shared with affected organizations who are asked to keep their contents private.

A series of privately commissioned reports published over the past few years have urged healthcare systems to boost security. Experts applauded the FBI for responding with its own warning.

"I'm really happy to see the FBI doing this. It's nice to see the attention," said Shane Shook, an executive with cybersecurity firm Cylance Inc who helps companies respond to breaches.

Retailers and financial institutions have taken steps to bolster security of financial information after the attack on Target as well as smaller breaches at Neiman Marcus, Michaels and other merchants. Hackers accessed millions of bank card numbers and other customer data.

As those stolen payment card numbers flooded underground markets, the value of that information dropped, leading to "fire sales" by criminals seeking to unload them, said Angel Grant, senior manager for fraud and risk intelligence at EMC Corp's RSA security division.

Demand for medical information, however, remains strong on criminal marketplaces, experts said, partly because it takes victims longer to realize the information has been stolen and report it, and because of the different ways the information can be used.

Cyber criminals were getting paid $20 for health insurance credentials on some underground markets, compared with $1 to $2 for U.S. credit card numbers prior to the Target breach, according cybersecurity firm Dell SecureWorks.

Some criminals use medical records to impersonate patients with diseases so they can obtain prescriptions for controlled substances, Grant said. Several U.S. states, including Massachusetts, have reported a surge in opiate addiction, along with a jump in heroin overdoses that the Obama administration has called a "public health crisis".

Others criminals are purely interested in using the medical data for financial fraud.

"They are harvesting information to make it easier to conduct identity theft, to open new accounts," Grant said.

Pieces of health information are also sometimes combined with other pieces of data into complete packages known as "fullz" and "kitz" on underground exchanges where they can fetch$1,000 or more when bundled with counterfeit documents, according to Dell.

The two-page FBI alert cited a February 2014 report from the non-profit SANS Institute, which trains cybersecurity professionals. SANS had warned the healthcare industry was not well-prepared to fight growing cyber threats, pointing to hundreds of attacks on radiology imaging software, video conferencing equipment, routers and firewalls.

(Reporting by Jim Finkle; Editing by Richard Valdmanis and Mohammad Zargham)

FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

Federal Register
Vol. 78, No. 33
Tuesday, February 19, 2013

Presidential Documents

Title 3—

The President

Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. *Critical Infrastructure.* As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. *Policy Coordination.* Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. *Cybersecurity Information Sharing.* (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the ''Secretary''), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of

Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. *Privacy and Civil Liberties Protections.* (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. *Consultative Process.* The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. *Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.* (a) The Secretary of Commerce shall direct the Director of the National

Institute of Standards and Technology (the ''Director'') to lead the development of a framework to reduce cyber risks to critical infrastructure (the ''Cybersecurity Framework''). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 *et seq.*), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the ''preliminary Framework''). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the ''final Framework'').

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. *Voluntary Critical Infrastructure Cybersecurity Program.* (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the ''Program'').

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. *Identification of Critical Infrastructure at Greatest Risk.* (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. *Adoption of Framework.* (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification

of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. *Definitions.* (a) ''Agency'' means any authority of the United States that is an ''agency'' under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) ''Critical Infrastructure Partnership Advisory Council'' means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) ''Fair Information Practice Principles'' means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) ''Independent regulatory agency'' has the meaning given the term in 44 U.S.C. 3502(5).

(e) ''Sector Coordinating Council'' means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) ''Sector-Specific Agency'' has the meaning given the term in Presidential Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. *General Provisions.* (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater

extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
February 12, 2013.

[FR Doc. 2013–03915
Filed 2–15–13; 11:15 am]
Billing code 3295–F3

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Table of Contents

Executive Summary 1
1.0 Framework Introduction 3
2.0 Framework Basics 7
3.0 How to Use the Framework 13
Appendix A: Framework Core 18
Appendix B: Glossary 37
Appendix C: Acronyms 39

List of Figures

Figure 1: Framework Core Structure 7
Figure 2: Notional Information and Decision Flows within an Organization 12

List of Tables

Table 1: Function and Category Unique Identifiers 19
Table 2: Framework Core 20

Executive Summary

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

To better address these risks, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Executive Order also requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be

used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Use of this voluntary Framework is the next step to improve the cybersecurity of our Nation's critical infrastructure – providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation's critical infrastructure as a whole.

1.0 Framework Introduction

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity," on February 12, 2013.[1] This Executive Order calls for the development of a voluntary Cybersecurity Framework ("Framework") that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk.

Critical infrastructure is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by information technology (IT) and industrial control systems (ICS).[2] This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organization's business, assets, health and safety of individuals, and the environment should be considered. To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of IT and ICS is required. Because each organization's risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Executive Order requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization's approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

---

[1] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] The DHS Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors

To ensure extensibility and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

Just as the Framework is not industry-specific, the common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities. These components are explained below.

- The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core

then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- *Framework Implementation Tiers* ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
- A *Framework Profile* ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2009[3], ISO/IEC 27005:2011[4], National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39[5], and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline[6].

1.3 Document Overview

The remainder of this document contains the following sections and appendices:

- Section 2 describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- Section 3 presents examples of how the Framework can be used.
- Appendix A presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- Appendix B contains a glossary of selected terms.
- Appendix C lists acronyms used in this document.

[3] International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[4] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. http://www.iso.org/iso/catalogue_detail?csnumber=56742

[5] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[6] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

2.1 Framework Core

The *Framework Core* provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in **Figure 1**:

Figure 1: Framework Core Structure

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.
- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”

- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.[7]

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See Appendix A for the complete Framework Core listing.

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

[7] NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at http://www.nist.gov/cyberframework/.

The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

2.2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective. Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination.

The Tier definitions are as follows:

Tier 1: Partial

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation* – An organization may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 2: Risk Informed

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.
- *External Participation* – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

Tier 3: Repeatable

- *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- *External Participation* – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- *External Participation* – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

2.3 Framework Profile

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in the communication of risk within and between organizations. This Framework document does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps can contribute to the roadmap described above. Prioritization of gap mitigation is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.

2.4 Coordination of Framework Implementation

Figure 2 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

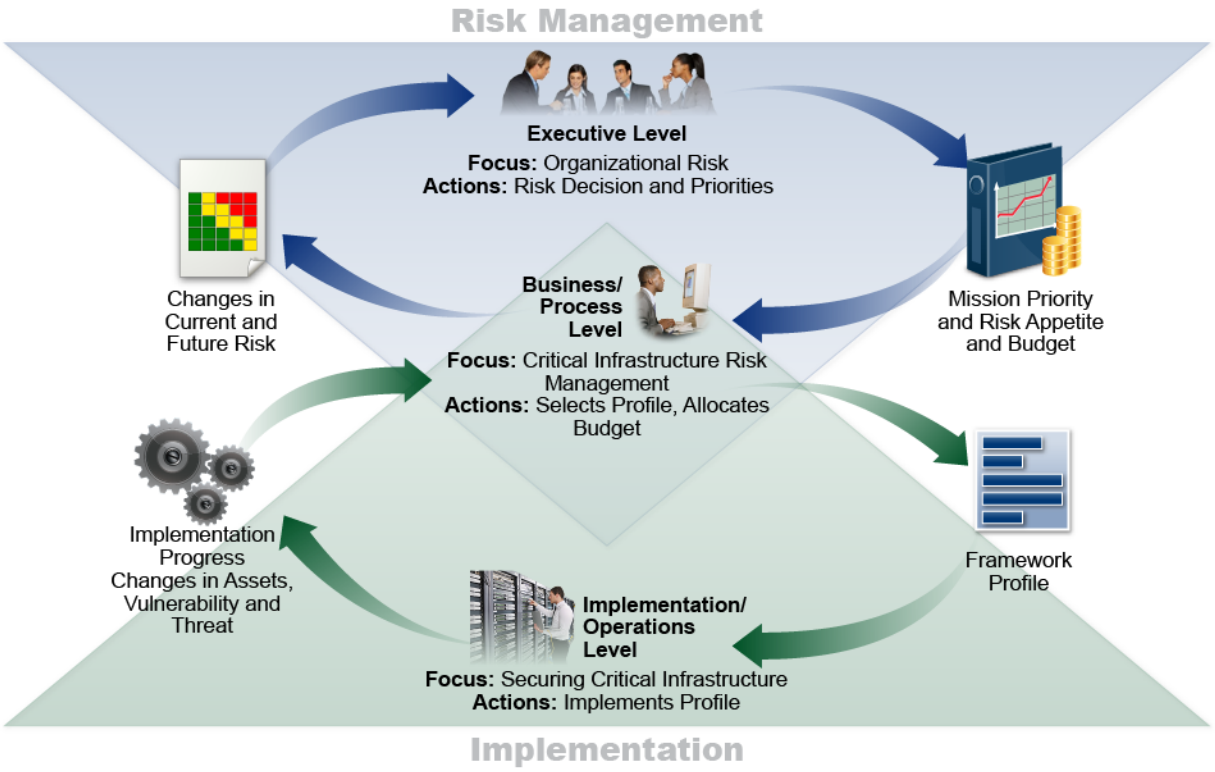


Figure 2: Notional Information and Decision Flows within an Organization

3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The following sections present different ways in which organizations can use the Framework.

3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization's current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired outcomes, thus managing cybersecurity commensurate with the known risk. Conversely, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources to strengthen other cybersecurity practices.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient

step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

3.3 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services. Examples include:

- An organization may utilize a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.

3.4 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

3.5 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology as required by the Executive Order to address individual privacy and civil liberties implications that may result from cybersecurity operations. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program may give rise to these considerations. Consistent with Section 3.4, technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and civil liberties implications may arise when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities. Some examples of activities that bear privacy or civil liberties considerations may include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; cybersecurity mitigation activities that result in denial of service or other similar potentially

adverse impacts, including activities such as some types of incident detection or monitoring that may impact freedom of expression or association.

The government and agents of the government have a direct responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or agents of the government that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.

To address privacy implications, organizations may consider how, in circumstances where such measures are appropriate, their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in Appendix A, the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

Governance of cybersecurity risk

- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements
- Process is in place to assess implementation of the foregoing organizational measures and controls

Approaches to identifying and authorizing individuals to access organizational assets and systems

- Steps are taken to identify and address the privacy implications of access control measures to the extent that they involve collection, disclosure, or use of personal information

Awareness and training measures

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities
- Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies

Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization's anomalous activity detection and cybersecurity monitoring

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities
- Process is in place to conduct a privacy review of an organization's cybersecurity mitigation efforts

Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity,	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7

Function	Category	Subcategory	Informative References
		including privacy and civil liberties obligations, are understood and managed	• **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • **NIST SP 800-53 Rev. 4** PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and	• **COBIT 5** APO12.05, APO13.02

Function	Category	Subcategory	Informative References
		prioritized	• **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	• **CCS CSC** 9 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03

Function	Category	Subcategory	Informative References
			• **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** SC-28
		PR.DS-2: Data-in-transit is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	• **COBIT 5** BAI06.01, BAI01.06 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Protection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-

Function	Category	Subcategory	Informative References
			8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	• **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1,

Function	Category	Subcategory	Informative References
			SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is	• **ISA 62443-2-1:2009** 4.3.3.3.8

Function	Category	Subcategory	Informative References
		monitored to detect potential cybersecurity events	• **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **NIST SP 800-53 Rev. 4** SI-3
		DE.CM-5: Unauthorized mobile code is detected	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1

Function	Category	Subcategory	Informative References
	adequate awareness of anomalous events.		• **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-

Function	Category	Subcategory	Informative References
			5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	• **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents are mitigated	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely	**RC.RP-1:** Recovery plan is executed during or after an event	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5

Function	Category	Subcategory	Informative References
	restoration of systems or assets affected by cybersecurity events.		• **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	• **COBIT 5** EDM03.02
		RC.CO-2: Reputation after an event is repaired	• **COBIT 5** MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References represent a general correspondence and are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

Appendix B: Glossary

This appendix defines selected terms used in the publication.

Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify,

	Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

CCS	Council on CyberSecurity
COBIT	Control Objectives for Information and Related Technology
DCS	Distributed Control System
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
RFI	Request for Information
RMP	Risk Management Process
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Department of Homeland Security Integrated Task Force

Incentives Study Analytic Report

June 12, 2013

Homeland Security

Table of Contents

Table of Contents 1
1. Background 3
1.1. DHS Integrated Task Force and Incentives Working Group 3
1.2. Incentives Study Requirements 4
2. Analysis 5
2.1. Review of Known Cybersecurity Incentive Proposals 6
2.2. Verification of the Initial List of Incentives 9
2.3. Development of the Microeconomic Model 10
2.4. Research 12
2.4.1. Literature Review 13
2.4.2. DHS Incentives Workshop 14
2.4.3. Department of Commerce Notice of Inquiry 15
2.5. Finalization of the List of Incentives 16
2.6. Application of the Microeconomic Model 18
2.6.1. Effectiveness: Does it work? 19
2.6.2. Efficiency: Is there waste? 20
2.6.3. Equity: Who pays and how much? 20
2.6.4. Analytic Summary 21
3. APPENDICES 25
3.1. Literature Review 26
3.1.1. Grants, Rate-Recovery, and Subsidies 26
3.1.2. Insurance 28
3.1.3. Liability and Legal Benefits 30
3.1.4. Prioritized Technical Assistance 30
3.1.5. Procurement 31
3.1.6. Public Recognition 31
3.1.7. Security Disclosure 32
3.1.8. Tax 34
3.2. Bibliography 37
3.3. DHS Incentives Workshop Summary 48
3.3.1. Welcome and Agenda Overview 48
3.3.2. Keynote 1 48

3.3.3. Keynote 2 49
3.3.4. Session I: Regulated Industries 51
3.3.5. Session II: Non-Regulated Industries 54
3.3.6. Session III: Cross-Sector Incentives 58
3.3.7. Session IV: Government Roundtable 59
3.4. Commerce NOI Response Review 61
3.4.1. Grants 62
3.4.2. Insurance, Liability Protections, and Legal Benefits 62
3.4.3. Prioritized Technical Assistance 63
3.4.4. Procurement Considerations 63
3.4.5. Public Recognition 63
3.4.6. Rate-Recovery for Price-Regulated Industries 63
3.4.7. Security Disclosure 64
3.4.8. Streamline Information Security Regulations 64
3.4.9. Subsidies 64
3.4.10. Tax Incentives 65

1. Background

In February 2013, the President signed Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience."[1][2] That same day, President Obama warned in his State of the Union Address:

> America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

The policies set forth in these directives are intended to strengthen the security and resilience of critical infrastructure against evolving threats and hazards, while incorporating strong privacy and civil liberties protections into every cybersecurity initiative. These documents call for an updated and overarching national Framework that reflects the increasing role of cybersecurity in securing physical assets.

Securing critical infrastructure against growing and evolving cyber threats requires a layered approach. The Department of Homeland Security (DHS) actively collaborates with public and private sector partners every day to prevent, protect from, respond to, and coordinate mitigation efforts against attempted disruptions and adverse impacts to the nation's critical cyber and communications networks and infrastructure, as well as a range of additional hazards, including terrorism and natural disasters.

DHS is the Federal Government's lead agency for coordinating the protection, prevention, mitigation, and recovery from cyber incidents. DHS also works regularly with business owners and operators to strengthen their facilities and communities by sharing cyber and other threat information.

1.1. DHS Integrated Task Force and Incentives Working Group

To implement EO 13636 and PPD-21, DHS established an Integrated Task Force (ITF) to lead DHS implementation, coordinate interagency and public and private sector efforts, and ensure effective integration and synchronization of implementation across the homeland security enterprise.

The ITF is currently comprised of eight Working Groups each focused on specific deliverables of implementation. Among these eight Working Groups, the Incentives Working Group was

[1] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
[2] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

established to lead the study of incentives for participating in the voluntary critical infrastructure cybersecurity program.

1.2. Incentives Study Requirements

EO 13636 and PPD-21 are intended to strengthen the security and resilience of critical infrastructure through an updated and overarching national Framework that acknowledges the increased role of cybersecurity in securing physical assets. The government and the private sector have a mutually shared interest in ensuring the viability of critical infrastructure, and the provision of essential services, under all conditions. Critical infrastructure owners and operators are often the greatest beneficiary of investing in their own security, and they have a social responsibility to adopt best practices for cybersecurity. However, the private sector may be justifiably concerned about the return on security investments that may not yield immediately measureable benefits. Effective incentives can help the private sector justify the costs of improved cybersecurity by balancing the short-term costs of additional investment with similarly near-term benefits.

Section 8(d) of EO 13636 includes the following requirement:

> (d) The Secretary [of Homeland Security] shall coordinate establishment of a set of incentives designed to promote participation in the [voluntary cybersecurity] Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

The U.S. Intelligence Community's March 2013 Worldwide Threat Assessment describes increasing risk to U.S. critical infrastructure from cyber attacks, as well as eroding U.S. economic and national security from cyber espionage.[3] Addressing these risks is a top priority for the Federal Government in its responsibility for ensuring the safety and security of the Nation. However, the owners and operators of critical infrastructure often have more immediate business priorities, as well as information gaps, which hinder the adoption of higher levels of cybersecurity.

While some market-based incentives exist to improve the cybersecurity of critical infrastructure, independent of government intervention, the pace of the necessary improvement in cybersecurity needs to be hastened in order to more rapidly counter the increasing risk of cyber attacks and cyber espionage. As such, it is appropriate to consider where government action can provide additional impetus to the market, while acknowledging that there are places where market-based incentives may perform adequately independent of government intervention.[4] The three

[3] Accessed at: www.intelligence.senate.gov/130312/clapper.pdf

[4] Certain industries have already implemented voluntary and mandatory approaches and standards to cyber protection, including bulk electricity transmission through FERC regulations.

independent incentives studies required by EO 13636 seek to make recommendations to accelerate the current levels of cybersecurity by making recommendations to support and expand existing market incentives. Though each of the incentives considered in this study acts by influencing the market for cybersecurity-related products and services, each requires some degree of government intervention to meet the aims of EO 13636.

2. Analysis

Given the requirements in EO 13636, the ITF Incentives Study had three objectives:

1. Recommend a set of incentives designed to promote adoption of the Cybersecurity Framework under development by the National Institute of Standards and Technology (NIST).
2. Evaluate the benefits and relative effectiveness of each of these incentives in promoting adoption of the Framework under development by NIST.
3. Determine which of these incentives require legislation and which can be provided under existing law and authorities.

For the purpose of this study, DHS used the following definition of incentive: ***a cost or benefit that motivates a decision or action by critical infrastructure asset owners and operators to adopt the Cybersecurity Framework under development by NIST.*** For example, this can include grants, insurance, liability considerations, procurement preferences or requirements, public recognition, subsidies, and tax incentives, to name a few.

The scope of the study included the possible incentives that the Federal Government could use—either under existing law and authorities or only through new legislation—to encourage the investment required for adoption of the voluntary Cybersecurity Framework by the owners and operators of critical infrastructure assets within the 16 critical infrastructure sectors defined under PPD-21.

Overall, the study methodology included the following, described in the pages that follow:

1. Review of known cybersecurity incentive proposals
2. Verification of the initial list of incentives
3. Development of the microeconomic model
4. Research
5. Finalization of the list of incentives
6. Application of the microeconomic model

In addition, an initial review of legal feasibility and policy implementation considerations related to incentive adoption was conducted and is described separately along with the DHS recommendations in the DHS Incentives Study report.

2.1. Review of Known Cybersecurity Incentive Proposals

DHS began by conducting an initial review of known cybersecurity incentive proposals to define the range of incentives to be included in the study and to confirm the requirements those incentives were intended to meet. This review included proposals made by academic, advocacy, Federal, and private sector stakeholders. It included a literature review of publicly available proposals, as well as interviews and Working Group meetings with stakeholders. The review yielded the following known government and industry sources of cybersecurity incentive proposals:

1. Cybersecurity Act of 2012, February 14, 2012[5]
2. DHS Blueprint for a Secure Cyber Future, November 2011[6]
3. Recommendations of the House Republican Cybersecurity Task Force, October 2011[7]
4. Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (Green Paper), June 2011[8]
5. Business Software Alliance, the Center for Democracy and Technology, the Internet Security Alliance, TechAmerica, and the U.S. Chamber of Commerce, *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*, March 8, 2011[9]
6. Cross Sector Cybersecurity Working Group (CSCSWG), Incentives Subgroup, *Incentives Recommendations Report*. September 2009.[10]
7. President's Cyberspace Policy Review, May/June 2009[11]
8. Internet Security Alliance, *Issue Area 3: Norms of Behavior—Hathaway Questions*, March 24, 2009[12]

Collectively, these sources contained a set of 14 broad categories of both remunerative and coercive incentives, which served as an initial focus of inquiry. The list below was simply intended to represent the initial descriptive cataloging of the major incentive categories contained within the eight sources listed above, and does not represent either the recommendations or the economic or legal analyses required by EO 13636.

1. Expedited Security Clearance Process: establish a procedure to expedite the provision of security clearances to appropriate personnel employed by critical infrastructure owners and operators under the Framework.

---

[5] Accessed at: http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105
[6] Accessed at: http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
[7] Accessed at: http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf
[8] Accessed at: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf
[9] Accessed at: http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/cybersecurity_white_paper_publicprivatepartnership.ashx
[10] Obtained from White House National Security Staff
[11] Accessed at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[12] Accessed at: http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20ISSUE%20AREA%203%20-%20NORMS%20OF%20BEHAVIOR---HATHAWAY%20QUESTIONS.pdf

2. Grants: direct federal funding for investment in cybersecurity products and services that would allow adoption of the Framework; alternatively, condition existing grant programs to adoption of Cybersecurity Framework.
3. Include Cybersecurity in Rate Base: allow rate recovery of cybersecurity investments in the rates charged for services provided by Framework adopters.
4. Information Sharing: implement a procedure for ensuring that Framework adopters are provided with relevant near real-time cyber threat information.
5. Insurance: promote cybersecurity insurance through related incentives and/or federal reinsurance programs to help underwrite the development of cybersecurity insurance programs.
6. Liability Considerations: capped liability in exchange for improved cybersecurity or increased liability for the consequences of poor security.
7. New Regulation/Legislation: for example, a combination of insurance requirements and liability protections for organizations that adopt the Framework.
8. Prioritized Technical Assistance: ensure Framework owners and operators receive prioritized cybersecurity technical assistance
9. Procurement Considerations: offer preferential consideration in the procurement process for Framework owners and operators and/or requiring Framework adoption by federal goods/services providers.
10. Public Recognition: create an award for companies that adopt the Framework and/or best practices; voluntary certification/accreditation for Framework adoption.
11. Security Disclosure: require public notification of disclosures to encourage owners and operators to take care to avoid breaches.
12. Streamline Information Security Regulations: create unified compliance model for similar requirements and eliminate overlaps among existing laws (e.g. Sarbanes-Oxley, the Health Insurance Portability and Accountability Act of 1996, or HIPAA, and Gramm-Leach-Bliley).
13. Subsidies: fund direct purchase of cybersecurity products and services for Framework owners and operators.
14. Tax Incentives: provide tax credits and/or deductions for Framework adopters.

Table 1 below illustrates the distribution of these incentives among the eight sources.

Table 1. Distribution of Incentive Categories by Source

	Incentive Description	CSA 2012	DHS Blueprint 2011	House Republican Task Force 2011	Commerce Green Paper 2011	BSA, CDT, ISA, TA, Chamber of Commerce 2011	CSCSWG 2009	President's CSPR 2009	ISA 2009
1	Expedited Security Clearance Process	X							
2	Grants		X	X		X	X		X
3	Include Cybersecurity in Rate Base								X
4	Information Sharing	X			X				
5	Insurance			X	Y	X	Y		X
6	Liability Considerations	X	X	X	Y	X		X	X
7	New Regulation/Legislation					X	Y	X	X
	(e.g. Cyber SAFETY Act)					X	Y		X
8	Prioritized Technical Assistance	X							
9	Procurement Considerations	X					X	X	X
10	Public Recognition	X					Y		X
11	Security Disclosure				X				
12	Streamline Information Security Regulations			X		X	X		X
13	Subsidies		X				X		X
14	Tax Incentives		X	X		X	X	X	X

Key

X indicates that the incentive was recommended by the source

Y indicates that the incentive was discussed by the source but not formally recommended

2.2. Verification of the Initial List of Incentives

To review, refine, and expand the preceding list of incentives, the list was presented to (1) a meeting of the full ITF on March 8, 2013, (2) the interagency representatives of the ITF Incentives Working Group on March 20, 2013, and (3) interagency and industry stakeholders—including representatives from both the Partnership for Critical Infrastructure Security and the Cross Sector Cybersecurity Working Group—at the Incentives Working Group on March 27, 2013.

At each of these presentations, representatives were asked to review the list and to offer any additional incentive categories, or sub-categories to the existing broadly defined categories, that the Federal Government should consider. Based on feedback received from the March 27, 2013 Working Group meeting, the additions highlighted in bold below were made to six of the 14 incentives.

- Expedited Security Clearance Process: expedite the provision of security clearances to appropriate personnel employed by CI owners and operators under the Framework, **as well as expedited Sensitive Compartmented Information Facility (SCIF) sponsorship**.

- Liability Considerations **and Legal Benefits**: reduce liability in exchange for improved cybersecurity or increased liability for the consequences of poor security; **full indemnity, higher burdens of proofs, or limited penalties; case consolidations; case transfers to a single federal court; creation of a federal legal privilege that also preempts State litigation discovery law and applies to owners and operators that undertake cybersecurity self-assessments so that those assessments would not be discoverable in subsequent litigation and/or used as evidence in court.**

- Security Disclosure: require public notification of disclosures to encourage owners and operators to take care to avoid breaches; **preemption of state notice requirements.**

- Streamline Information Security Regulations: create unified compliance model for similar requirements and eliminate overlaps among existing laws (e.g. Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley); **streamline differences between U.S. and international law (perhaps through treaties); allow equivalent adoption (so that companies wouldn't need to adopt the Framework if they're already doing something equivalent); reduce the audit burden; move to the head of the line with prioritized permitting.**

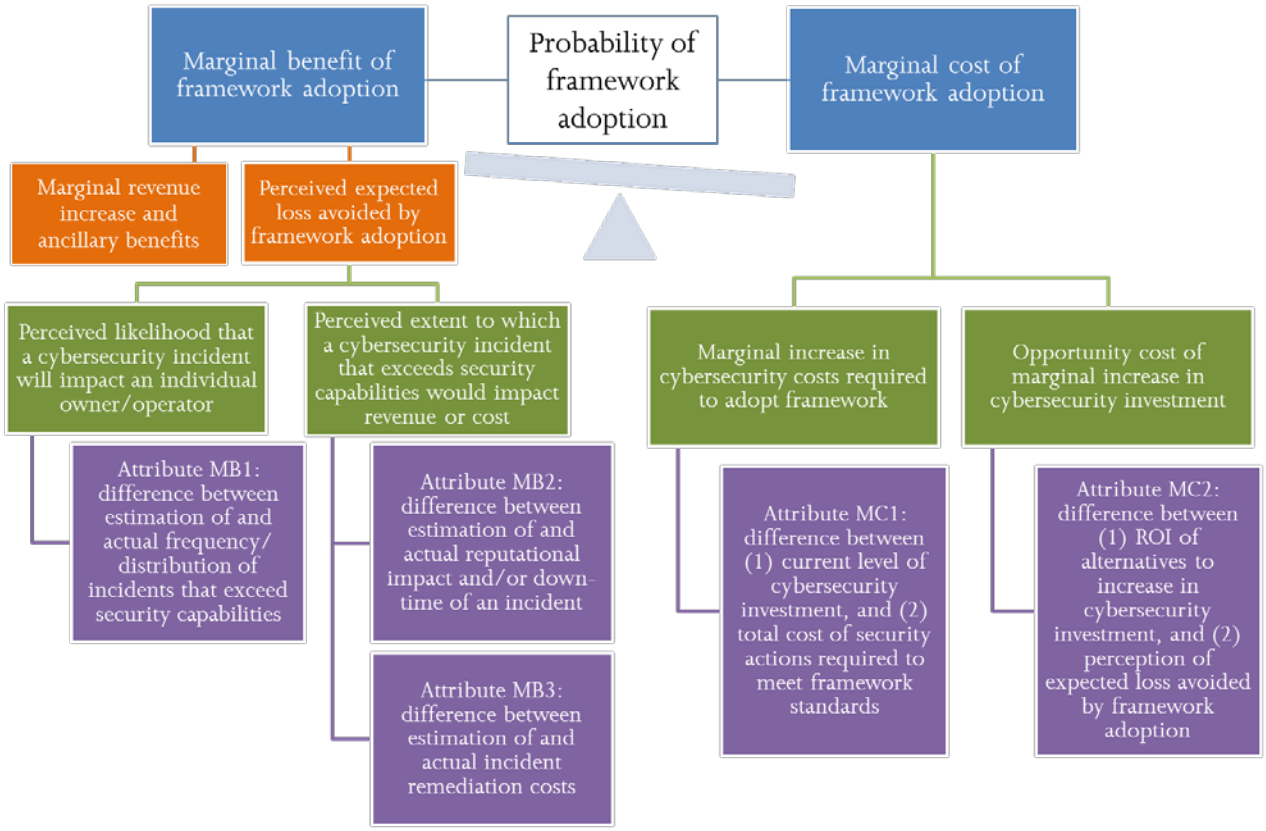
- Subsidies: fund direct purchase of cybersecurity products and services for Framework owners and operators; **low-interest financing options or loans.**

- Tax Incentives: provide tax credits or deductions for Framework owners and operators; **decreased rate on capital gains for investors in companies adopting the Framework.**

2.3. Development of the Microeconomic Model

As noted above, given the requirements set forth in EO 13636, the core analytic objective for this study is to evaluate the benefits and relative effectiveness of each of these incentives in promoting adoption of the voluntary Cybersecurity Framework. While the incentives study is required within 120 days of the date of EO 13636 (June 12, 2013), the preliminary version of the Cybersecurity Framework is required within 240 days of the date of the EO 13636 (October 10, 2013). Therefore, since the set of standards, methodologies, procedures, and processes that will comprise the Cybersecurity Framework are unknown at the time of this writing, the incentives that are intended to promote its adoption must be assessed prospectively, in terms of the likelihood that they will motivate organizations to adopt the Cybersecurity Framework in the future. More specifically, the core analytic question that this study seeks to inform is: to what extent would each of the incentives considered affect the probability that critical infrastructure asset owners and operators will adopt the Cybersecurity Framework under development by NIST? To answer this question, DHS developed the conceptual microeconomic model in Figure 1.

Figure 1. Microeconomic Model



The conceptual microeconomic model presented in Figure 1 is designed to consider the probability of Framework adoption in terms of its marginal benefit and marginal cost for each prospective organization. Marginal cost-benefit analysis is appropriate because it assesses only the changes in benefits and costs associated with Framework adoption, rather than the full benefits

and costs associated with all of the cybersecurity standards, methodologies, procedures, and processes within the Framework irrespective of whether some have already been adopted. For example, some prospective adopters may have adopted very few, if any, of the cybersecurity standards, methodologies, procedures, and processes that will be in the Framework. Others with high levels of technological sophistication may have adopted cybersecurity standards, methodologies, procedures, and processes that exceed the Framework in all respects. In each case, the probability of Framework adoption will be a function of the marginal benefit of only those cybersecurity standards, methodologies, procedures, and processes that prospective organizations would apply as they adopt the Framework.

More specifically, the marginal benefit of Framework adoption is composed of (1) marginal revenue increase and ancillary benefits, and (2) the perceived expected loss avoided by Framework adoption. Marginal revenue increases could be associated with tangible financial gains such as Federal procurement or public recognition incentives. Ancillary benefits could be associated with incentives that lower business expenses, such as streamlining existing information security regulations by providing reductions in non-Framework adoption costs (e.g. consolidating audit requirements).

Another set of benefits is related to the perceived expected loss, or perceived risk, avoided by Framework adoption. This is, in turn, composed of two elements:

1. The perceived likelihood that a cybersecurity incident will impact an individual owner or operator. This perceived likelihood is presumably lowered by Framework adoption. This is defined by attribute MB1, the difference between estimation of and actual frequency and distribution of incidents that exceed security capabilities.
2. The perceived extent to which a cybersecurity incident that exceeds security capabilities would impact revenue or cost. This is defined by attribute MB2, the difference between estimation of and actual reputational impact and/or down-time of an incident, and attribute MB3, the difference between estimation of and actual incident remediation costs.

Risk avoidance is qualified as *perceived* expected loss avoidance because information about the likelihood and impact of cybersecurity incidents is interpreted and characterized by individuals and organizations in ways that are not simply based on fact, but is also related to the degree to which it the risk is observable or known and uncontrollable or dreaded.[13] The growing field of behavioral economics, rooted in the work of Kahneman and Tversky, has much to offer on the importance of considering perceived loss.[14] Incentives that increase the perceived expected loss avoided by Framework adoption include Bundled Insurance Requirements, Liability Protections, and Legal Benefits; Prioritized Technical Assistance; and Security Disclosure. These all can be

[13] See, for example, Slovic, Fischhoff, and Lichtenstein, "Why Study Risk Perception?" Risk Analysis, Vol. 2, No. 2. 1982.
[14] Kahneman and Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, Vol. 47, No. 2. (Mar., 1979), pp. 263-292.

categorized as benefits as they lower the perceived losses related to cybersecurity incidents and, therefore, enhance a business' bottom line.

On the other side of the microeconomic model is the marginal cost of Framework adoption. The marginal cost increase of Framework adoption is composed of two elements. The first is the marginal increase in cybersecurity costs required to adopt the Framework, defined by attribute MC1, the difference between the current level of cybersecurity investment and the total cost of security actions required to meet Framework standards. The second is the opportunity cost of the marginal increase in cybersecurity investment, defined by attribute MC2, the difference between the return on investment of alternatives to an increase in cybersecurity investment and the perception of expected loss avoided by Framework adoption. The incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing include grants, rate-recovery for price-regulated industries, subsidies, and tax incentives. These have the potential to make it more cost effective for owners and operators to adopt the Framework.

To assess the probability of Framework adoption for each incentive in absolute rather than relative terms, quantitative estimates for each of the elements within each attribute would be required for each prospective organization in order to compare the marginal benefit to the marginal cost for each incentive. These estimates could then be aggregated across all prospective organizations to inform an overall assessment of the absolute probability of Framework adoption for each incentive. Unfortunately, this is not possible due to incomplete and imperfect data. The attributes that define the marginal benefit of Framework adoption are uncertain. Many of the elements within each attribute are currently unknown and many, to some extent, are unknowable. As noted by the National Science and Technology Council's Subcommittee on Networking and Information Technology Research and Development (NITRD), "Secure practices must be incentivized if cybersecurity is to become ubiquitous…The projected benefits must be quantified to demonstrate that they outweigh the costs incurred by the implementation of improved cybersecurity measures."[15] For these reasons, to apply the microeconomic model described above, evidence was gathered through systematic research to consider the relative effectiveness of each of the incentives through empirical evaluation of relevant voluntary non-cybersecurity incentives.

2.4. Research

Until better data become available, it is not yet possible to quantify the benefits of the Cybersecurity Framework. And until the Framework has been developed, it is similarly not yet possible to estimate the costs of implementing the Framework. Moreover, there are no empirical evaluations of the effectiveness of incentives in promoting the adoption of the Framework,

[15] National Science and Technology Council's Subcommittee on Networking and Information Technology Research and Development, "Trustworthy Cyberspace: Strategic Plan for the federal Cybersecurity Research and Development Program," accessed at http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

because the Framework is still under development, and the incentives intended to promote its eventual adoption do not yet exist. As a result, the methodology for analyzing the effectiveness of the incentives under evaluation for EO 13636 relies on secondary research of evaluations of voluntary non-cybersecurity programs and largely qualitative methods to assess the relative effectiveness of the incentives. To complement the literature review, stakeholder interviews and workshops were conducted, and responses to the Department of Commerce Notice of Inquiry were reviewed.

2.4.1. Literature Review

Empirical evaluations of voluntary government incentive programs in the literature were considered the primary sources of the secondary research. Since a government incentive program for the adoption of a voluntary Cybersecurity Framework does not yet exist, the literature obviously does not yet include research or evaluations of voluntary cybersecurity incentive programs. One exception is the growing body of research on cybersecurity insurance as an incentive for the promotion of cybersecurity in general, independent of a voluntary Cybersecurity Framework. DHS has recently contributed to the work examining obstacles that hinder the development of the cybersecurity insurance market, having hosted an all-day workshop on cybersecurity insurance in October 2012.[16] Based on stakeholder input during that workshop, DHS held a cybersecurity insurance roundtable in May 2013 that focused on how organizations should build more effective cyber risk cultures. DHS plans to continue this dialogue with stakeholders going forward as the continued development of the cybersecurity insurance market could have significant benefits for future cybersecurity efforts.

For the remaining incentive categories, there exists literature that contains evaluations of those incentives applied to investment in non-cybersecurity voluntary programs that is informative for the analysis and recommendations required by EO 13636. For example, while there are no current tax incentives for cybersecurity investment, there is an extensive literature on the use of tax credits for increasing expenditures on research and development, as well as the effects of tax incentives on tangible, depreciable investments, especially those in equipment. There is also an extensive literature evaluating the use of rate recovery in the form of price cap regulation for electric distribution and transmission networks and telecommunications. Such evaluations of incentives for investment in non-cybersecurity voluntary programs are assumed to be relevant to the study of cybersecurity voluntary programs, though identical results are not assumed.

To scope this effort, the literature review was limited to studies examining relevant incentives. Relevant studies assessed incentives to promote participation in voluntary government programs, and focused upon voluntary investment decisions made by organizations (e.g. rather than individuals or households), wherever available. Studies and research were assessed for quality to inform conclusions about differences among evaluations within incentive categories. For example, articles published in peer-reviewed journals received a high assessment of quality, while

[16] See http://www.dhs.gov/publication/cybersecurity-insurance

anecdotal evidence that is not necessarily representative or generalizable received a low assessment of quality.

Interviews with stakeholders, Working Group meetings and Workshops with industry representatives, and responses to the Commerce Notice of Inquiry were used to complement the findings from the literature review, and to help inform conclusions about differences among evaluations as well as about evaluations that are inconclusive.

The literature review was completed with research support from the White House Council of Economic Advisers, the Department of the Treasury's Tax Policy and Federal Insurance Offices, and the Homeland Security Studies and Analysis Institute. The resulting reviews of 144 peer-reviewed journal articles, law review articles, conference papers, working papers, government reports, dissertations, and book chapters are reviewed in Appendix 3.1, and the references are listed in Appendix 3.2.

2.4.2. DHS Incentives Workshop

To complement this research, on Friday, April 19, 2013, DHS hosted an Incentives Workshop. The all-day workshop included two keynote addresses and four panel sessions with time allotted for audience questions and discussion. Approximately 80 interagency and industry participants attended. This section offers a brief summary of the Workshop, and a more detailed summary is included in Appendix 3.3. Workshop participants focused on the following questions:

- How likely is your sector or firm to adopt the voluntary Framework in the absence of new incentives?
- What kinds of incentives are most likely and least likely to promote adoption of the voluntary Framework and why?
- What examples of incentives have worked well for your sector or firm, what types have not worked well, and why?
- Can you think of additional incentive categories the Federal Government should consider?
- What are the likely impacts of the incentives under consideration on your sector or firm?
- What barriers prevent you from taking steps to better address cybersecurity?

The workshop began with keynote addresses from Bruce McConnell, DHS's Acting Deputy Undersecretary for Cybersecurity, and Larry Clinton, President and CEO of the Internet Security Alliance.

Bruce McConnell began by noting that America's national security and economic prosperity are increasingly dependent upon the cybersecurity of critical infrastructure. Because the vast majority of U.S. critical infrastructure is owned and operated by private companies, reducing the risk to these vital systems requires a strong partnership between government and industry. EO 13636 represents an opportunity for the government and the private sector to collaborate in promoting the cybersecurity of the nation's critical infrastructure. Input provided at the Incentives Workshop will represent an essential step toward ensuring that critical infrastructure owners and operators

adopt the appropriate security measures to provide essential services to the American people under all conditions.

Larry Clinton outlined the adaptation of other incentives models to cybersecurity, and offered a series of "Incentivization Principles," including that in order to be effective incentives must: be powerful enough to affect corporate investment behavior; be calibrated to match the level of additional investment required to adopt the Framework; vary not just from sector to sector but business to business and thus a menu of incentives will be needed; recognize that regulation that does not include full cost recovery is not a substitute for incentives; and that cost not compensated through incentives will either be passed on to consumers or reduce investment in critical infrastructure.

Session I focused on regulated industries, with panelists from the Federal Energy Regulatory Commission, the American Public Power Association, the National Association of Regulatory Utility Commissioners, the American Gas Association, and the Financial Services sector. Moderated by the President of the Information Technology and Innovation Foundation, panelists discussed a range of issues, including incentives to share information, whether Smart Grid assistance will help utilities with cybersecurity, and rate recovery as an incentive for Framework adoption.

Session II reviewed incentives-related issues specific to non-regulated industries. Moderated by DHS, panelists included the Internet Security Alliance, Dickstein Shapiro LLP (a law firm that advises SAFETY Act applicants), Verizon, and Boeing. Panelists discussed questions related to the current environment in non-regulated sectors, whether research and development tax credits accessible to regional clusters and patent protection would be effective incentives, and how a risk-based approach should operate within the Framework.

Session III's cross-sector incentives panelists answered questions about their views on creating a competitive advantage for organizations seen as good stewards of cybersecurity, as well as how the Framework should address "signature-less" attacks. This panel was moderated by DHS and included panelists from SAIC, DHS, the General Services Administration, Northrop Grumman, and General Electric.

Session IV, the concluding government roundtable, provided participants with an opportunity to hear from the Federal representatives responsible for drafting the incentives studies for their respective Government departments. It consisted of DHS, the Department of Commerce, and the Department of the Treasury.

2.4.3. Department of Commerce Notice of Inquiry

On March 28, 2013, the Department of Commerce issued a 30-day Notice of Inquiry (NOI) entitled, "Incentives to Adopt Improved Cybersecurity Practices."[17] "Comments on Incentives to

[17] Docket number 130206115-3115-01: http://www.ntia.doc.gov/federal-register-notice/2013/notice-inquiry-incentives-adopt-improved-cybersecurity-practices

Adopt Improved Cybersecurity Practices NOI" were posted on April 29, 2013, and included 45 comments from the following 45 respondents:[18]

Advanced Cybersecurity Center, American Association for Laboratory Accreditation, American Fuel and Petrochemical Manufacturers, American Gas Association, American Insurance Association, American Petroleum Institute, American Public Power Association, atsec, Booz Allen Hamilton, Bryan Rich, Business Software Alliance, CACI, Covington & Burling/Chertoff Group, DCS Corp, Donald Edwards, Dong Liu, Edison Electric Institute, Electric Power Supply Association, Emmanuel Adeniran, Encryptics, Federal Communications Commission, Financial Services Sector Coordinating Council, Gary Fresen, Honeywell, Internet Infrastructure Coalition, Internet Security Alliance, IT SCC, Los Angeles Department of Water and Power, Marsh, Microsoft, Monsanto, National Cable and Telecommunications Assoc., NCTA- The Rural Broadband Association, National Electrical Manufacturers Association, National Rural Electric Cooperative Association, Robin Ore, San Diego Gas & Electric and Southern California Gas Company, Sasha Romanosky, Southern California Edison, Telecommunications Industry Association, Terrence August & Tunay Tunca, U.S. Chamber of Commerce, US Telecom Association, Utilities Telecom Council, and Voxem Inc.

As noted above, responses to the Commerce NOI were reviewed as a complement to the findings from the literature review, and to help inform conclusions about differences among evaluations as well as evaluations that are inconclusive. Similar to the DHS Incentives Workshop, the evaluation of NOI responses focused on the following questions:

- Are there additional incentive categories, or sub-categories, that should be considered?
- Which incentives are most likely and least likely to promote adoption of the voluntary Framework and why?

Appendix 3.4 provides both a brief summary of the 45 responses to the Commerce NOI as well as a table that indicates which of the incentives considered were recommended, discussed, or neither discussed nor recommended by each of the respondents.

2.5. Finalization of the List of Incentives

Based on information and feedback obtained through the literature review, the DHS Incentives Workshop, and the Commerce NOI, the initial list of incentives was refined prior to conducting the analysis. Table 2 below summarizes both the initial list of incentives described above and the finalized list of refined incentive categories that were used as the primary units of analysis.

[18] The full responses can be accessed at: http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi

Table 2. Finalization of the List of Incentives

	Initial Incentive Category		Final Incentive Category
1	Expedited Security Clearance Process	→	Remove due to existing DHS efforts
2	Grants		No Change
3	Include Cybersecurity in Rate Base	→	"Rate-Recovery for Price-Regulated Industries"
4	Information Sharing	→	Remove due to EO Section 4
5	Insurance	→	Remove as independent category and include in "Bundled Insurance Requirements, Liability Protections, and Legal Benefits"
6	Liability Considerations and Legal Benefits	→	Remove as independent category and include in "Bundled Insurance Requirements, Liability Protections, and Legal Benefits"
7	New Regulation/Legislation (e.g. "Cyber SAFETY Act")	→	Limit to "Bundled Insurance Requirements, Liability Protections, and Legal Benefits"
8	Prioritized Technical Assistance		No Change
9	Procurement Considerations		No Change
10	Public Recognition		No Change
11	Security Disclosure		No Change
12	Streamline Information Security Regulations		No Change
13	Subsidies		No Change
14	Tax Incentives		No Change

Expedited Security Clearance Process was removed from consideration due to existing DHS efforts to provide expedited clearances independent of adoption of the Cybersecurity Framework. More specifically, the DHS Critical Infrastructure Private Sector Clearance Program was developed in 2007 to facilitate the processing of security clearance applications for private sector partners. The DHS Office of Infrastructure Protection is implementing an improved process to streamline the clearance process and to meet the requirement in EO 13636 Section 4(d): "The Secretary… shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order." In doing so, DHS believes that national security should be the principal criteria for expediting clearances. Similarly, information sharing was removed as an incentive that would have been contingent upon adoption of the Framework due to the requirements in EO 13636 Section 4, which was interpreted to indicate that information sharing should occur independent of adoption of the Cybersecurity Framework.

The initial incentive, "Include Cybersecurity in Rate Base" was more clearly defined as "Rate-Recovery for Price-Regulated Industries," since price-regulated industries are the only industries to which rate-recovery of cybersecurity costs is able to be applied.

Both "Insurance" and "Liability Considerations and Legal Benefits" were removed as independent categories and were included in a bundle of insurance requirement, liability protections, and legal benefits, which would likely require legislation. DHS believes it is important to treat these incentives as a package, with each component an essential piece of a potential incentive structure. DHS believes that insurance is an important incentive independent of government intervention, and existing cybersecurity insurance markets may ultimately have the effect of promoting adoption of the Cybersecurity Framework outside of government intervention. For example,

critical infrastructure owners and operators who adopt the Framework are likely to have lower levels of cybersecurity risk given their use of the standards, methodologies, procedures, and processes that will comprise the Cybersecurity Framework. If cybersecurity insurance premiums reflect the reduction in risk associated with Framework adoption, then the Framework and the cybersecurity insurance markets are likely to be mutually reinforcing: insurance will be more affordable for Framework adopters, and thus the probability of Framework adoption will be greater for those owners and operators who seek such affordable insurance policies. The incentive provided by lower premiums requires no government intervention beyond the planned development of the Cybersecurity Framework, and so there are no insurance actions to recommend within the scope of this report independent of the bundled incentive composed of insurance requirements, liability protection, and legal benefits. Nonetheless, market-based incentives like insurance can be encouraged via government policy, including policy that promotes sustained stakeholder dialogue about enhancing their viability. These incentives are encouraged through the bundled incentive requirements considered for this study: that owners and operators carry insurance in order to receive its liability protections.

2.6. Application of the Microeconomic Model

EO 13636 requires DHS to include an analysis of the benefits and relative effectiveness of the incentives considered. As described above, effectiveness is defined in terms of the probability of Framework adoption. To help distinguish between areas where incentives are assessed to have similar relative effectiveness, DHS also assessed each incentive in terms of two additional criteria that include benefits beyond the extent to which the incentive promotes adoption of the Framework: efficiency and equity. In general terms, each of these criteria answer the following questions:

- Effectiveness: Does it work?
- Efficiency: Is there waste?
- Equity: Who pays and how much?

To assimilate the broad range of information sources gathered in our research in an integrated analysis, each incentive was qualitatively assessed in terms of its relative effectiveness, efficiency, and equity. The incentives were then assessed in relative terms against each of these criteria using the following simple tiering heuristic:

- Top tier incentive, relative to other incentives, against each criterion
- Second tier incentive, relative to other incentives, against each criterion
- Insufficient evidence to merit either a top tier or a second tier assessment, relative to other incentives, against each criterion.

The efficiency criterion was only applied to the cost-sharing incentives.

2.6.1. Effectiveness: Does it work?

As described above, effectiveness is defined by the extent to which an incentive affects the probability of Framework adoption. Recall that the attributes in the microeconomic model that define the marginal benefit of Framework adoption are uncertain: Increasing unknown, and to some extent unknowable, benefits could increase the probability of adoption for some Framework adopters, while reducing Framework implementation costs that will occur with certainty increases the probability of Framework adoption for all Framework adopters. Additionally, marginal revenue increases would apply only to the subset of organizations that both adopt the Framework and sell goods and services to the Federal Government through the procurement process.

For these reasons, other things being equal, incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing are more likely to promote the adoption of the Framework than incentives that increase the perceived expected loss avoided by Framework adoption and/or that increase marginal revenue or ancillary benefits. As a result, effectiveness judgments are principally driven by Framework cost sharing, though expected loss avoidance, marginal revenue increase, and ancillary benefits also contribute to a lesser extent.

The incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing include:

- Grants,
- Rate-recovery for price-regulated industries,
- Subsidies, and
- Tax incentives.

Of these four categories, two incentives are assessed to be in the top tier of incentive categories for cost-sharing, and thus the top tier of incentive categories for the probability of Framework adoption: grants to non price-regulated industries, and rate-recovery for price-regulated industries. Subsidies and tax incentives are assessed to be in the second tier for cost-sharing and thus the second tier for the probability of Framework adoption.

This is in part due to the temporal nature of the cost-sharing provided by each of these incentives. Both grants and price-caps are able to help offset the costs of Framework adoption before those costs are incurred. Tax incentives would provide either full or partial reimbursement for costs that have already been incurred. For those organizations for which operating cash flows are insufficient to support non-operating costs, offering reimbursement for costs incurred to adopt the Cybersecurity Framework may be insufficient to spur the required investment. However, grants, subsidies, and tax incentives create a potential moral hazard where taxpayers fund cyber security improvements for privately owned critical infrastructure, potentially for the long-term.

A recent study summarized the existing research on the effectiveness of R&D tax incentives and reported that, "while there is substantial evidence that R&D tax incentives increase the level of [measured] R&D," there is "scarce evidence, however, that even the most successful innovation

tax incentives are cost-effective." For example, they cite a benefit-cost ratio of between 0.293 and 2.0 and remark that any particular incentive could have widely varying effects, depending on firm size, the time frame, and other factors. A separate study found a price elasticity of 3 to 4 for changes in state R&D tax incentives, and GAO found that the gains in R&D spending were only a fraction of the cost of the credit.

Subsidies in the form of payments for reported expenses would provide either full or partial reimbursement for costs that have already been incurred. In the case of an interest subsidy, the costs could be offset temporarily in the form of a subsidized loan before the Framework costs are incurred. Additionally, an interest rate subsidy could create an unintended incentive for owners and operators to take on debt.

Due to the volume of the literature reviewed, a summary of the literature on effectiveness is contained in Appendix 3.1 and the relevant references are listed in Appendix 3.2.

2.6.2. Efficiency: Is there waste?

Efficiency was applied to cost sharing incentives, and consists of both moral hazard and adverse selection. Moral hazard in this context exists because of differences in the degree to which techniques for adopting the Framework are cost-effective, and can be thought of as allowing owners and operators to choose techniques that are not cost-effective. Adverse selection in this context exists due to differences in the cost of adoption among owners and operators within and across sectors, and can be thought of as over-paying "lost cost" owners and operators that are already near the frontier of sophistication.

The efficiency criterion was only applied to the four categories of cost-sharing incentives: grants to non price-regulated industries, and rate-recovery for price-regulated industries, subsidies, and tax incentives. Of these, based on both economic theory and evidence in the literature, the following two incentives are assessed to be in the top tier for efficiency because they address both moral hazard and adverse selection: grants to non price-regulated industries, and rate-recovery for price-regulated industries.

As noted in the previous section, due to the volume of the literature reviewed, a summary of the literature on efficiency is contained in Appendix 3.1 and the relevant references are listed in Appendix 3.2.

2.6.3. Equity: Who pays and how much?

Each of the incentives was also assessed in terms of (1) whether government, industry, or consumers would pay for the cost of Framework adoption and/or the administration of the incentive, and (2) whether they would pay all/most of the cost of Framework adoption and/or the administration of the incentive, a moderate amount, or none/least.

The incentives for which the government or taxpayers would bear none or the least cost for Framework adoption and administration of the incentive are: rate-recovery for price-regulated

industries, prioritized technical assistance, procurement considerations, and streamlining information security regulations. From a policy-making perspective these incentives are considered more equitable. Due to programmatic costs associated with administering the incentives, government and taxpayers would bear a moderate portion of the cost of the Bundled Insurance Requirements, Liability Protections, and Legal Benefits; Public Recognition; and Security Disclosure. Grants to price-regulated industries, subsidies, and tax incentives would require government and taxpayers to pay most or all of the cost of Framework adoption.

By definition, industry would bear none or the least cost for Framework adoption for the four categories of cost-sharing incentives: grants to price-regulated industries, rate-recovery for price-regulated industries, subsidies, and tax incentives. Industry would bear a moderate portion of the cost of Framework adoption for the Bundled Insurance Requirements, Liability Protections, and Legal Benefits: its insurance requirements and application process would impose some level of transaction costs, while the risk transfer it provides through insurance and liability protections would help to offset expected losses incurred by cybersecurity incidents. Industry would bear all or most of the costs of Framework adoption for the remaining incentives: prioritized technical assistance, procurement considerations, public recognition, security disclosure, and streamlining information security regulations.

Finally, consumers of the products and services provided by owners and operators (as distinct from the general class of taxpayers) would bear none or the least cost for Framework adoption for grants to price-regulated industries, prioritized technical assistance, public recognition, streamlining information security regulations, subsidies, and tax incentives. Consumers would bear a moderate portion of the cost for the Bundled Insurance Requirements, Liability Protections, and Legal Benefits, procurement considerations, and security disclosure, since the cost of insurance premiums, procurement requirements, and security disclosures are likely to be passed on to consumers through the price of the goods and services consumed. By definition, consumers would bear all or most of the cost of rate-recovery for price-regulated industries.

2.6.4. Analytic Summary

Figure 2 below summarizes the analysis of each of the incentives against the criteria above.

Figure 2. Analytic Summary

	Incentive	Effectiveness				Efficiency		Equity		
		Probability of Framework Adoption	Framework Cost Sharing	Expected Loss Avoided	Marginal Revenue Increase and Ancillary Benefits	Moral Hazard	Adverse Selection	Government/ Taxpayer Cost	Industry Cost	Consumer Cost
1	Grants	●	●			●	●		●	●
2	Rate-Recovery for Price-Regulated Industries	●	●			●	●	●	●	
3	Bundled Insurance Requirements, Liability Protections, and Legal Benefits	○		●				○	○	○
4	Prioritized Technical Assistance			○				●		●
5	Procurement Considerations	○			●			●		○
6	Public Recognition							○		●
7	Security Disclosure							○		○
8	Streamline Information Security Regulations				○			●		●
9	Subsidies	○	○				●		●	●
10	Tax Incentives	○	○				●		●	●

Key

●	Indicates a top tier incentive, relative to other incentives, against the criterion defined *within* each column.
○	Indicates a second tier incentive, relative to other incentives, against the criterion defined *within* each column.
	Indicates insufficient evidence to merit either a top tier or a second tier assessment, relative to other incentives, against the criterion defined *within* each column.
	Indicates the criteria were not applied to the incentive.

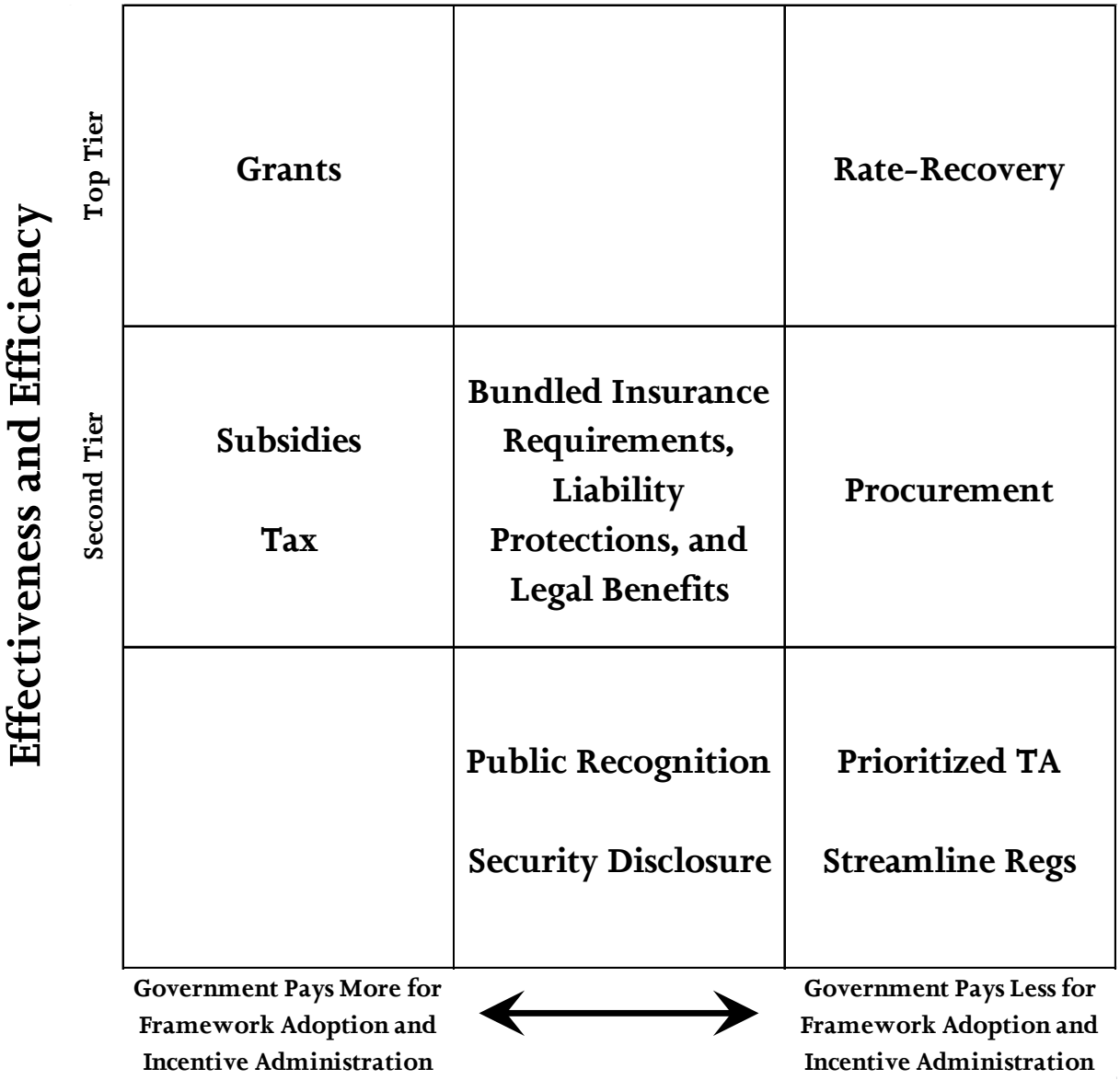
The analysis of effectiveness, efficiency, and equity summarized in Figure 2 includes nine dimensions of economic criteria, and three tiers of assessment for each of ten incentive categories, resulting in 78 data points. Since the purpose of this analysis is to help inform the decision about which incentives to implement to promote adoption of the Cybersecurity Framework, a method for applying this analysis in a way that synthesized the 78 data points was needed to generate meaningful findings that allowed for consideration of the tradeoffs that reflected the decision to be informed. The method that was selected was to reduce the dimensionality of the criteria through two consolidations.

First, as noted in Section 2.6.2, the efficiency criterion was only applied to the four cost-sharing incentives: grants to non price-regulated industries, rate-recovery for price-regulated industries, subsidies, and tax incentives. Of these, the top tier for both effectiveness and efficiency included the same two incentives: grants to non price-regulated industries, and rate-recovery for price-regulated industries. The second tier for both effectiveness and efficiency similarly included the same two incentives: subsidies and tax incentives. As a result, the effectiveness and efficiency criteria were consolidated as follows: for those incentives for which efficiency was applied, the top and second tiers for the consolidated criteria were the same as either criterion individually. For those incentives for which efficiency was not applied, all tiers for the consolidated criteria were assessed to be the same as the effectiveness criteria alone.

Second, it was assumed that an important decision point for the selection of the incentives for implementation will be the degree to which new government funding is available. Accordingly, the dimensions for the equity criteria were reduced from three to one by focusing the equity analysis only on government/taxpayer costs.

The analytic application of these consolidations resulted in the three-by-three matrix shown in Figure 3 below, with the consolidated tiering assessment for effectiveness and efficiency on the y-axis. The x-axis represents a range, from left to right, from government/taxpayers pay more for Framework adoption and incentive administration to government/taxpayers pay less for Framework adoption and incentive administration.

Figure 3: Consolidated Analysis



3. APPENDICES

3.1. Literature Review[19]

3.1.1. Grants, Rate-Recovery, and Subsidies

The question of how to best incentivize investment in cyber security falls into the broader study of how to design effective economic incentive mechanisms. The most effective incentives overcome both moral hazard and adverse selection – which arise from information asymmetry. This section reviews economic literature related to common economic incentive mechanisms.

Moral Hazard. A variety of techniques exist to incentivize firms to achieve cyber security standards. The firms responsible for critical infrastructure are in the best position to determine which techniques are most cost-effective since costs depend on a host of factors specific to individual firms. Moreover, even if the government knew the best techniques to achieve its cyber security standard, it may be difficult or costly to monitor those chosen by each firm. This problem is called "moral hazard" and arises from information asymmetry – meaning the firms know more about the costs of meeting the cyber security standard than the government.

The presence of moral hazard calls for policy incentives that enable firms to profit from taking cost-saving actions. For example, the government could provide fixed grants contingent upon a firm meeting its cyber security standard. Since the grant would depend only on meeting the standard and not on the techniques used to meet it, the firm would have a powerful incentive to find the most efficient techniques.

This basic principle has been applied in numerous settings including the regulation of public utilities, government contracting and various research prizes:

Since the 1980s, government regulation of public utilities has increasingly moved from traditional "rate-of-return" regulation to "price cap" regulation. Under rate-of-return regulation, the price a firm is permitted to charge consumers varies positively with the firm's cost. This guarantees firms a fixed rate of return and provides little incentive to save on costs. In contrast, price cap regulation sets a fixed price for consumers, enabling firms to increase profits by reducing costs. Price cap regulation is common in the context of electric distribution and transmission networks (Joskow, 2013) and telecommunications (Sappington, 2003) – see Vogelsang (2002) for more examples. Joskow (2013) shows empirical evidence that the introduction of price caps led to substantial cost reductions in the electric distribution and transmission networks of the United Kingdom.

In addition to public utilities, similar policy incentives exist in government grants. The government grants process has seen an increased use of performance-based [as opposed to cost-based] procurement arrangements. A recent variant is the "pay for success" model of delivering social services. In the pay-for-success model, a government agency commits funds to pay for a

[19] As noted in Section 2.4.1, the review of the relevant literature was supported by the White House Council of Economic Advisers, the Department of the Treasury's Office of Tax Policy and Federal Insurance Office, and the Homeland Security Studies and Analysis Institute.

specific outcome achieved within a given period of time. The financial capital to cover the operating costs of achieving the outcome is provided by independent investors – however, the government disperses payment of the funds contingent on the specified results. Similar to price cap regulation, investors have an incentive to provide a successful program at the lowest cost. The pay-for-success model is being tried in several states and has been included in the last three of the President's Budgets. Mulgen, et. al. (2011) provides an extensive discussion of the principles behind, and the nuances in implementing, pay-for-success programs. Notably, they require careful and objective measurements of success.

Lastly, various research prizes, such as those recently offered by the X-Prize Foundation, have been successful in spurring innovation in socially desirable directions. Kremer and Williams (2010) discuss these prizes, including the recent $1.5 billion pilot Advance Market Commitment (AMC) mechanism for a pneumococcus vaccine. Under an AMC, the sponsor legally commits—in advance of product development and licensure—to underwrite a guaranteed price for a vaccine. Vaccines are eligible if a committee deems that they fulfill a set of technical specifications laid out in advance.

Unobserved Heterogeneity of Costs. Even with the most efficient techniques, there are wide disparities between firms within and across industries in terms of the cost of meeting the standard. The government may not know the full extent of these cost disparities when it issues incentives, which makes it difficult to tailor them to appropriate firms. For example, if the government could anticipate how much it would cost each firm to achieve the standard, it could tailor the incentives to cover only the cost of achievement. This would ensure the standard's adoption by all firms at the lowest cost to taxpayers. The only way to induce widespread adoption of the standard when cost disparities are unknown is to offer incentives generous enough to cover the highest-cost firms. It is likely that the incentive will exceed the amount needed to cover low-cost firms, consequently wasting public funds. This problem is known as "adverse selection" and like moral hazard, arises from asymmetric information.

If the government could observe the cost of adopting cyber security standards after each firm had incurred its expenses, then a potential solution to adverse selection is a cost-sharing system. Under a cost-sharing system, the government only pays for costs incurred by firms to reach the standard. Examples include subsidies and tax credits based on a firm's reported cyber expenses. Such policies are equivalent to the rate-of-return regulation discussed previously in the context of regulated utilities. Both policies suffer the same problem: while they avoid over-paying low cost firms, they blunt the incentive to take cost-saving actions –which is necessary for overcoming moral hazard. It may also be difficult to determine which of a firm's expenses were necessary to meet the standard and which would have been made regardless. For example, tax credits and subsidies end up paying for work that would have been done anyway. For these reasons, a cost-sharing system is not the recommended approach.

Various approaches to solving the trade-off between moral hazard and adverse selection have been advanced in both theory and practice. Laffont and Tirole (1986) argue that the tradeoff can be solved by offering firms a "menu" of incentive schemes. While the exact nature of the optimal

menu is complex, Rogerson (2003) shows that the idea can be implemented by offering firms a choice between a cost-reimbursement contract and a fixed-price contract. A low-cost firm is likely to choose the fixed-price contract with the concomitant incentive to choose efficient techniques. A high-cost firm is likely to choose cost-reimbursement.

The most common approach in the context of utility regulation is to choose a price cap based on historical or constructed data that firms cannot manipulate by incurring unnecessary costs (Joskow, 2013; Vogelsang (2002). The goal is to choose a firm-specific price cap that leaves as little profit for the firm as possible while not depending on the behavior of the firm itself. If the price cap depends on a firm's behavior, (i.e., if this year's price cap depends on last year's realized cost) firms have an incentive to distort their behavior to raise their realized cost. A common approach begins with a historical base-line cost and then adjusts annually for: inflation, some "x-factor" reflecting efficiency improvements, and a "y-factor" accounting for changes in input prices beyond the firm's control. Another approach is known as "yardstick competition," whereby each firm's price cap depends on the cost of its competitors.

A third option would be to rely on gradations of performance and tie incentives to cyber-security improvements. It goes without saying that any scheme tying incentives to compliance must be monitored to verify that a firm has complied with the standard. Ideally, the monitor would measure gradations of compliance, rather than using binary measure (compliant or not). Examples of this include Energy Star ratings and DHS SAFETY Act certifications/designations. Similar to the "pay for success" model, the payment firms receive could escalate with improvements in cyber-security.

Such an approach could go a long way toward solving the adverse selection problem. Under a program that rewards only full compliance, a high-cost firm would require a large payment before it would be willing to make an effort. The same firm would be more likely to make an effort if it were rewarded for improvements. By the same token, low cost firms would likely begin the program with high grades and thus be able to obtain only limited payments for improvement before hitting full compliance (though one may want to incorporate some penalty for backsliding).

Regulated Firms. Many of the critical infrastructure sectors identified as "lifeline" sectors (i.e. electricity, water, transportation, and communications/IT) involve price-regulated firms, so that the adoption of a cyber-security standard can be grafted onto existing incentive regulation. A firm operating under a price cap already faces a high-powered incentive to minimize costs. If the government also wanted the firm to adopt a cyber-security standard using the lowest-cost technique, this could be accomplished by raising the price cap, contingent on the firm improving (or meeting the standard), by an amount that would be sufficient to cover additional cost.

3.1.2. Insurance

Cybersecurity insurance transfers risk from individuals and organizations to insurance carriers. It can help mitigate losses due to data breaches, network damage, or cyber extortion. However, risk

managers recommend that a risk transfer strategy be pursued only after other risk management strategies (i.e., risk acceptance, risk mitigation, and risk avoidance) have been exhausted (DHS, 2012). In addition to general insurance problems such as moral hazard—in which the availability of insurance protection increases risky behavior—the literature suggests certain challenges faced by the use of insurance to promote cybersecurity. Moore (2010) and Lelarge and Bolot (2009) cite the current (when their articles were written) lack of data for cyber damages as a specific difficulty for cyber insurance implementation; without reliable estimates of incident damage, appropriate insurance premiums cannot be determined to properly align incentives. At a Department of Homeland Security (DHS) Cybersecurity Insurance Workshop held in October 2012, an IT professional stated that the data needed by insurers to understand the risks and economics of this threat are in short supply, limiting the availability and breadth of policies. However, another workshop participant responded that this data exists but "few [companies] have interpreted that data to clarify their potential losses and corresponding insurance needs," in part because they do not know that affordable and attractive cybersecurity insurance policies exist and also because of their reluctance to share cyber incident data with the public. Moore (2010) also points out entities' lack of awareness of cyber-risk as an issue, but insurers suggest mandatory security breach disclosure legislation to help overcome this.

That said, insurance can offer incentives for firms or individuals to invest in cybersecurity by providing lower premiums for those entities that take the appropriate precautions. Hahn and Layne-Farrar (2006) "see cyber insurance as an extremely promising route to solving the identified market failures in software security."

In 2002, Kunreuther established that there is a "lack of interest by insurers, reinsurers and investors in providing funds for protection against terrorist attacks." With the passage of the Terrorism Risk Insurance Act of 2002, the United States established a public-private partnership in which the government provides no-cost reinsurance to insurers. Michel-Kerjan and Raschky (2011) use empirical evidence to shows that government intervention in this market has impacted insurers' behavior, finding "tentative evidence for moral hazard caused by the government backstop under TRIA."

Due to the limited academic literature on cyberinsurance, we are unable to determine the effectiveness of cyberinsurance as an incentive to induce firm behavior. However, research attempts to determine if insurance affects internet security. For example, Lelarge and Bolot (2009) study the benefits of using insurance to manage internet risks. They conclude that insurance can increase the level of self-protection and overall security of the internet. This stands in sharp contrast to the claims of Sheety, Schwartz, Felegyhazi, and Walrand (2010), who also seek to determine the effects of cyber insurance; their model concludes that while insurance improves user welfare in general, it fails to improve network security. Beyond cybersecurity, insurance is a tool that can be used to induce risk-mitigating behavior. Landry and Li (2012) conduct a study focused on factors contributing to the adoption of a hazard mitigation project, as reflected in Community Rating Systems participation, which offers flood insurance discounts based on management activities. They find empirical evidence that previous flood experience increases

participation; however, results were mixed for the impact of flood events when looking across time.

3.1.3. Liability and Legal Benefits

Legal incentives can be used to motivate socially optimal behavior (through "carrot" incentives like liability protections) and deter harmful behaviors (through "stick" incentives like liability standards). The research suggests that legal incentives can be an effective policy tool for environmental programs, but their degree of effectiveness varies by firm- and industry-specific factors.

For example, Alberini et al. and Turvani (2005) and Wernstedt, Meyer, and Alberini (2006) find that real-estate developers with potential interest in brownfield properties value liability relief as an incentive, refuting earlier claims (Urban Institute et al, 1997) that developers do not value liability relief as an incentive. Both Alberini et al. (2005) and Wernstedt et al. (2006) find that inexperienced developers are more responsive to liability relief than other forms of incentives, although this may only apply to the subpopulation of inexperienced developers that are reasonably likely to consider investing in brownfield projects. Alberini et al. (2005) also find that developers who sell their development projects, as opposed to using them, appear to value liability relief even more highly.

Alberini and Frost (2007) suggest that economic theory is ambiguous on predicting the response of a firm handling hazardous waste in a state with a strict liability standard. Shavel (1984) finds that "strict liability forces a firm to internalize pollution damage and choose [to take greater care] against accidental releases" but only if damages of pollution do not exceed the firm's assets. However, Beard (1990) finds that "when the damage exceeds the firm's assets or the firm can escape prosecution, it will take less precaution." Alberini and Austin (1999) find empirical evidence that "strict liability may, in fact, increase [emphasis added] the frequency of accidental releases of toxic pollutants" for firms holding specific types of chemicals, but state that further research is needed to understand why this occurs.

Tietenberg (1989) suggests that it appears the effects of liability laws vary with the scale and the assets of the firm that generates waste. Alberini and Austin (1999) find evidence that smaller firms find shelter from liability laws due to their limited assets (i.e., they avoid "wealth targeting" by regulatory agencies), and as a result, they are disproportionately responsible for spills or accidents in states imposing strict liability on polluters.

3.1.4. Prioritized Technical Assistance

Research identified limited literature on prioritized technical assistance as an incentive to induce firm behavior; therefore, its effectiveness as an incentive remains unclear. However, the two studies cited below point to its potential ineffectiveness.

Johnston (2005) studies the Strategic Goals Program, a voluntary environmental program for job shop metal finishers, and finds that direct technical assistance "was insufficient to enlist large

numbers of the important middle tier firms." However, the study suggests that technical assistance provided value to smaller firms by offering knowledge that increased profitability.

The Malaysian government introduced three incentives, including a fast track approval process, to encourage developers to implement a new housing delivery system, Build Then Sell (BTS). Yusof, Abu-Jarad, and Badree (2012) find that these "incentives are ineffective to influence the implementation of BTS."

3.1.5. Procurement

The government can use preferential consideration in the procurement process to promote participation by disadvantaged enterprises, such as small or minority owned businesses. In general, the literature appears to suggest that procurement preference can motivate firm behavior. For example, Myers and Chan (1996) and Chatterji, Chay, and Fairlie (2013) examine the effectiveness of preferential treatment for minority businesses. Myers and Chan find that preferential treatment increased the number of bids submitted by minority businesses; this corresponds with a reduction in their success rates as the total number of bids did not increase. Similarly, Chatterji et al. note an increase in African-American business ownership rates after implementation of a preferential program. Kranokutskaya and Seim (2011) look at preferential treatment of small bidders in highway procurement auctions and its effect on their incentives to participate in government procurement. They find that the bid preference "has significant implications for [small bidders'] participation and bidding behavior" and the program has been successful in promoting participation by disadvantaged enterprises. However, this preferential treatment comes at a cost to the government as allocation of bids moves away from the lowest cost competitors in the market.

In addition to procurement considerations for minority groups, the government uses preferential treatment to promote environmentally responsible firms. After assessing green public procurement (GPP) as a policy tool, Brannlund, Lundberg, and Marklund (2009) find that "even if firm type tailored criteria would be allowed, the possibility for GPP to work as a cost-efficient environmental policy tool is still negligible in practice;" therefore, other tools, such as taxes, are preferable.

3.1.6. Public Recognition

The literature is inconclusive on the effectiveness of public recognition to induce firm behavior. However, public recognition offered by voluntary programs can be attractive to potential participants as a signal of quality to the marketplace. For example, Videras and Alberini (2000), Arora and Cason (1996), and Brouhle and Harrington (2010), find that public recognition is an important component of participation in voluntary environmental programs. Specifically, Videras and Alberini (2000) note that "firms who wish to show consumers about their environmental performance progress and who do so by publishing environmental reports" are more likely to participate. Arora and Cason (1996) find that larger firms, those with greatest toxic releases, and those with higher advertising expenditures are more likely to participate. Gugerty (2009)

examines motivations of non-profits for joining voluntary accountability and standard-setting programs. He indicates that "club theory and the economics of certification suggest that such programs have the potential to provide a signal of quality by setting high standards and fees and rigorously verifying compliance." Karamos's (1999) study on identifying the characteristics and incentives that induce company participation in Voluntary Environmental Agreements (VEAs) provides a literature review indicating that public recognition is one of the two most prevalent incentives linked to participation in the Department of Energy's Climate Challenge Program (CCP).

Brouhle and Harrington (2010) find evidence that firms use participation in voluntary environmental programs to signal to investors and regulators but not to consumers. Using survey data for a sample of S&P 500 firms, Khanna and Anton (2002) conclude that public recognition of firms who adopted environmental management systems allows differentiation from other firms. Additionally, market pressures by consumers, investors, and competitors create greater incentives for adoption than other instruments such as the threat of liability or mandatory regulation.

Banerjee and Solomon (2003) study the effectiveness of five energy-labeling programs, including government and private sector initiatives. They find that "[g]overnment support to a labeling program not only increases its credibility and recognition, but also improves financial stability, legal protection and long-term viability" and that "[s]imple seal-of-approval logos and labels have generally affected consumer behavior more than the complex information-disclosure labels."

3.1.7. Security Disclosure

Security disclosure in the cybersecurity field could encourage companies to better secure the personal information they hold about individuals and take steps to prevent the breaches that cause them. While security disclosure may indeed promote such benefits, for the purpose of this study effectiveness was evaluated as the ability to promote adoption of the Framework. Security disclosure as an incentive for Framework adoption could be implemented in one of two ways: (1) apply disclosure laws to any organization that is the victim of a security disclosure breach, or (2) require owners and operators that do not adopt the Framework to disclose security breaches, and do not require owners and operators that do adopt the Framework to disclose security breaches.

Under the first method, to avoid the negative reputational effects that security disclosure would impose, owners and operators would be motivated to adopt those portions of the Framework that would mitigate future security breaches. Since the extent to which the Framework will address security breaches is unknown, it is unclear whether this would constitute a large or small portion of the overall Framework. Under the second method, adverse selection would encourage those firms most likely to have security breaches to adopt the Framework, and the resultant perverse incentive would be greater adoption of the Framework among those "breach-likely" firms and underreporting of breaches and perhaps their mitigation. For these reasons, security disclosure is not assessed to be in one of the top tiers of effectiveness for Framework adoption.

Nonetheless, if security disclosure were considered independent of Framework adoption, the review of the relevant literature that follows indicates that, overall, disclosure can be an effective

motivator of firm behavior across various regulated industries. In some industries, government bodies have been able to create incentives for companies to protect citizens simply by providing greater disclosure of practices. For example, a meta-analysis conducted by Weil, Fung, Graham, and Fagotto (2006) assess the effectiveness of what they call "regulatory transparency systems" (mandatory disclosure of information by private or public institutions with a regulatory intent) in restaurant hygiene, nutritional labeling, workplace hazard communication, and five other diverse systems in the U.S. Their two main conclusions indicate:

- "transparency systems alter decisions only when they take into account demanding constraints by providing pertinent information that enables users to substantially improve their decisions with acceptable costs." The presence of this phenomenon is referred to as "user embeddedness."
- "highly effective transparency policies … cause users to systematically incorporate new responses into their decision making that in turn change disclosers' decision calculations." The presence of this phenomenon is referred to as "discloser embeddedness."

Disclosure mechanisms are used in a variety of industries, with varying levels of influence on firm behavior. On restaurant hygiene, Jin and Leslie (2003) find that hygiene grade cards displayed in restaurant windows caused restaurants in Los Angeles County to improve hygiene quality and led to "possibly a 20 percent decrease in food-related hospitalizations." A similar study by Simon et al. (2005) determines there was a 13 percent decrease in the number of foodborne disease hospitalizations in L.A. County in 1998, the year following the implementation of the hygiene grade program. Findings by Jin and Leslie (2009) support the view that "reputation can cause firms to provide safe products."

The literature suggests that disclosure mandated by legislation can induce socially optimal effects. For example, Bennear and Olmstead's (2008) study suggests the 1996 Amendments to the Safe Water Drinking Act, which mandated that community drinking water suppliers issue annual consumer confidence reports (CCRs) to customers, resulted in a reduction of "total violations between 30% and 44% … and reduced the more severe health violations by 40%-57%" for larger utilities required to mail CCRs directly to customers. Konar and Cohen (1997) find that on the day following the issue of toxic release inventory (TRI) data to the public "firms with the largest stock price decline … subsequently reduced emissions more than their industry peers.…[This] is consistent with the view that financial markets may provide strong incentives for firms to change their environmental behavior."

A study by Blackman, Darley, Lyon, and Wernstedt (2010) on Oregon's voluntary clean-up programs (VCPs) finds that public disclosure of contaminated sites spurs voluntary remediation by responsible parties. Chatterji and Toffel (2010) find that firms "shamed" by low KLD ratings—the most widely used rating of corporations' environmental activities and capabilities—were "most 'able' to seize low-hanging fruit [to] show the most improvements in environmental performance."

However, impact on consumer behavior due to nutrition labeling is less clear. Moorman (1998) finds that food companies strategically reacted to this new requirement by adding low-fat, low-sodium product choices, but not eliminating traditional unhealthy options. Research in this area indicates "positive results on public health are less clear (Derby and Levy, 2001)." Weil et al. (2006) find that the following disclosure systems produced moderate or low effectiveness: toxic releases, workplace hazards, patient safety, and plant closing notification.

Dalley's (2007) examination of regulators' use of disclosure schemes rather than substantive regulation over the past several decades to achieve regulatory goals leads him to conclude that "only when one understands the mechanism by which the disclosure system will operate (i.e. accounting for how firms and individuals process and react to information) can one assess the likelihood that it will in fact achieve its goal and what the true costs of the disclosure requirement are."

3.1.8. Tax[20]

The following literature review presents a short description and bibliography of attempts within the professional literature to measure the effectiveness of two major types of tax incentives. This listing is not intended to be comprehensive. The first section discusses findings regarding the credit for increasing expenditures on research and development (R&D). The second section reviews papers that have estimated the effects of tax incentives on tangible, depreciable investments, especially those in equipment.

3.1.8.1. The Research Credit

Using a cost of capital approach in a multi-country regression analysis, Bloom and van Reenen (2002) find a short-run price elasticity for R&D activity of about -0.1, but a long-run elasticity of just under -1.0. They find that the variation between firms in the effectiveness of the credit depends on their different tax positions. The authors cite Baily and Lawrence (1992), Hall (1993), Hines (1994), and Mamuneas and Nadiri (1996) as also finding price elasticities of at least unity. They also cite Mansfield (1986) and Griffith, Sandler, and van Reenen (1995) as being perhaps more skeptical concerning the sensitivity of R&D to its user cost. Among other things, they refer to the possibility that taxpayers may be simply relabeling expenditures as R&D, as opposed to actually conducting greater R&D activities.

In a recent paper, Graetz and Doud (2012) summarize the existing research on the effectiveness of R&D tax incentives. They report that, "while there is substantial evidence that R&D tax incentives increase the level of [measured] R&D," there is "scarce evidence, however, that even the most successful innovation tax incentives are cost-effective." For example, they cite a benefit-cost ratio of between 0.293 (McCutchen (1993)) and 2.0 (Hall (1993)), and remark that any particular incentive could have widely varying effects, depending on firm size, the time frame, and other

[20] As noted in Section 2.4.1, the review of the relevant tax literature was conducted by the Department of the Treasury's Office of Tax Policy, and is reproduced here in Appendix Section 3.1.8. as provided by that office.

factors. Wilson (2009) finds a price elasticity of 3 to 4 for changes in state R&D tax incentives, but Graetz and Doud also cite the Bloom and van Reenen (2002) paper, as well as U.S. GAO (1998), which found that the gains in R&D spending were only a fraction of the cost of the credit.

Graetz and Doud question whether R&D incentives lead to increased output overall, or whether they simply shift R&D among regions. They cite a few conflicting studies in this regard. Cantwell and Mudambi (2000) suggest that incentives do not affect location decisions, but their study is limited to U.K. data only. Hines and Jaffe (2000) found evidence to suggest that domestic and foreign R&D are complements, while Wilson (2009) found the opposite result. Graetz and Doud also raise the possibility that companies reclassify expenditures to qualify for the incentives.

Finally, these authors report on several studies that have evidence concerning whether R&D has spillover effects or otherwise increases productivity. Lychagin et al. (2010) find positive effects in nearby locations, but that these effects decay rapidly with distance. Griffith, Redding, and van Reenen (2001) found that an R&D tax credit increases productivity, but that the increase is not cost effective in the short-run. The long-run could yield the opposite conclusion. Machin and van Reenen (1998) found that increased R&D increases the demand for skilled workers, while Goolsbee (1998a) found that incentives tend to increase the salaries of R&D workers rather than increase the volume or quality of R&D performed. Additional studies in this vein include Thomson and Jensen (2011) and Aerts (2008), which imply that incentives shift resources toward the employment of skilled workers and increase relatively the salaries of those already employed.

More recently, Rao (2013) has found a short-run user cost elasticity of about unity for qualified R&D spending (as a percent of sales), with larger effects in the long-run. Her work, however, suggests that much of the response may be due to a reallocation of spending between nonqualified and qualified research spending.

3.1.8.2. Investment Incentives

Most investment tax incentives aim to lower the user cost of new capital outlays and thereby increase the demand for investment. Hassett and Hubbard (2002) provide a history of theoretical and empirical developments in this area. After citing work by Auerbach and Hassett (1991), Caballero, Engel and Haltiwanger (1995), Cummins, Hassett and Hubbard (1994, 1996), and Goolsbee (2000), they conclude that empirical studies had "reached a consensus that the elasticity of investment with respect to the tax-adjusted user cost of capital is between 0.5 and 1.0." They also cite a finding by Goolsbee (1998b) of a significant response of capital goods prices to investment subsidies, concluding that capital goods manufacturers largely capture the benefits of investment tax incentives. However, the opposite conclusion is found in Hassett and Hubbard (1998), who find that local investment tax credits have had a negligible effect on (world) prices paid for capital goods.

Other work, including Eisner (1969), Summers (1981), Bernanke, Bohn, and Reiss (1988), and Chirinko, Fazzari, and Meyer (1999) has been less sanguine regarding the effects of tax variables on business investment. For example, using micro data, Chirinko, Fazzari and Meyer found a user-

cost elasticity for equipment of -0.25. This may be compared to the -0.66 elasticity found by Cummins, Hassett, and Hubbard.

Hines(1998) argues that tax incentives for equipment investment could lower the pre-tax returns of such capital, reducing the payoffs to bondholders in case of bankruptcy, and that bondholders should demand that firms pay them higher interest rates to compensate for this risk. Hines found evidence consistent with this mechanism in studying the Tax Reform Act of 1986. Thus, it is possible that aggregate investment could fail to rise, even as favored assets are substituted for assets not so favored by the tax incentive. Other mechanisms may also affect both the micro and macro responses to the introduction of a major tax incentive.

Plummer (2000) looked at firm-specific forecasts of capital expenditures published before and after relevant tax legislation dates. She found the investment tax credit's incentive effects were concentrated primarily among low-debt firms and firms with positive taxable income.

Desai and Goolsbee (2004) found evidence of a larger responsiveness of investment to tax parameters. Consistent with the "new view" of dividend taxation, they also found that dividend taxes failed to influence incentives for making investments.

More recent estimates have focused on the reaction of equipment investment to temporary tax incentives, such as increased first-year write-offs (expensing). Such incentives have been in place for much of the past decade, but always on a temporary basis, with supposed known ending dates. The amount of increased expensing (when it has been in force) has varied between 30 percent, 50 percent, and 100 percent of an investment's cost. The main purpose of a temporary incentive is to alter the timing of investment over time – stealing from the future, so to speak, in order to generate aggregate demand currently. Desai and Goolsbee (2004) found that the effect of 30 percent partial expensing was too small to have a large impact. Cohen and Cummins (2006) found only a small response to the earliest expensing provision. Knittel (2007) found evidence that firms with losses and loss carryovers tended not to use the credit; the incentive of a faster write-off of investment cost was certainly lower for such firms. Also, a substantial number of states refused to align their income taxes with the federal system with regard to the expensing provision, creating a disincentive for taxpayers to use the expensing provision. A more recent study, House and Shapiro (2008), using the same data as Cohen and Cummins, found large differences in investment response across asset types that were differentially affected by the temporary expensing incentive.

Edgerton (2010) focused on the interactions of tax incentives with individual tax characteristics of firms, finding that financing constraints and tax carrybacks and carryforwards are important determinants of the effectiveness of investment tax incentives. His most salient finding was the importance of a company's cash flow on its ability to take advantage of tax incentives.

3.2. Bibliography

Aerts, K. 2008. "Who writes the pay slip? Do R&D subsidies merely increase researcher wages? Katholieke Universitiert Leuven, 33.

Alberini, Anna and Kathleen Segerson. 2002. "Assessing Voluntary Programs to Improve Environmental Quality." Environmental and Resource Economics, 22: 157-184.

Alberini, Anna, and David H. Austin. 1999. "Strict Liability as a Deterrent in Toxic Waste Management: Empirical Evidence from Accident and Spill Data." Journal of Environmental Economics and Management, 38(1): 20-48.

Alberini, Anna, and Shelby Frost. 2007. "Forcing Firms to Think About the Future: Economic Incentives and the Fate of Hazardous Waste." Environmental & Resource Economics, 36(4): 451–474.

Alberini, Anna, et al. 2005. "The role of liability, regulation and economic incentives in brownfield remediation and redevelopment: Evidence from surveys of developers." Regional Science and Urban Economics, 35(4): 327-351.

Alderson, David and Kevin Soo Hoo. 2004. "The Role of Economic Incentives in Securing Cyberspace." Center for International Security and Cooperation (CISAC) Report, Stanford.

Armstrong and Sappington. 2007. "Recent Developments in the Theory of Regulation." Handbook of Industrial Organization. Volume 3.

Arora, Seema, and Timothy N. Cason. 1996. "Why Do Firms Volunteer to Exceed Environmental Regulations? Understanding Participation in EPA's 33/50 Program." Land Economics, 72(4): 413-432.

Attanasio, Meghir, and Santiago. 2011. "Education Choices in Mexico: Using a Structural Model and a Randomized Experiment to Evaluate PROGRESA." The Review of Economic Studies. Volume 79: 37-66.

Auerbach, A.J. and K.A. Hassett (1991), "Recent U.S. investment behavior and the Tax Reform Act of 1986: a disaggregate view," Carnegie-Rochester Conference Series on Public Policy 35:185-215.

Aurora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang. 2009. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure." Information Systems Research, 21(1): 115–132.

Baily, M., and R. Lawrence, (1992), "Tax incentives for R&D: what do the data tell us?" Study commissioned by the Council on Research and Technology, Washington, DC.

Bakshi and Gans. 2009. "Securing the Containerized Supply Chain: Analysis of Government Incentives for Private Investment." Management Science. Volume 56: 219-233.

Banerjee, Abhijit, and Barry D. Solomon. 2003. "Eco-labeling for energy efficiency and sustainability: a meta-evaluation of US Programs." Energy Policy, 31(2): 109-123.

Barnett, S.A. and P. Sakellaris (1998), "Nonlinear response of firm investment to Q: testing a model of convex and nonconvex adjustment costs," Journal of Monetary Economics (October 1998):261-288.

Bennear, Lori S., and Shelia M. Olmstead. 2008. "The impacts of the "right to know": Information disclosure and the violation of drinking water standards." Journal of Environmental Economics and Management, 56(2): 177-130.

Bernanke, B., H. Bohn, and P. Reiss, (1988), "Alternative non-nested specification tests of time series investment models." Journal of Econometrics, 37(2):293–326.

Bisogni, Fabio, Simona Cavallini, and Sara di Trocchio. "Cybersecurity at European Level: The Role of Information Availability." Communications & Strategies, 81: 105-124.

Blackman, Allen, Sarah Darley, Thomas P. Lyon, and Kris Wernstedt. 2010. "What Drives Participation in State Voluntary Cleanup Programs? Evidence from Oregon." Land Economics, 86 (4): 785-799.

Bloom, N., R. Griffith, and J. van Reenen, (2002) "Do R&D tax credits work? Evidence from a panel of countries 1979-1997." Journal of Public Economics 85, 1-31.

Böhme, Rainer, and Galina Schwartz. 2010. "Modeling Cyber-Insurance: Towards A Unifying Framework." Working paper presented at the Workshop on the Economics of Information Security, Harvard University.

Bolot, Jean, and Marc Lelarge. 2008. "Cyber Insurance as an Incentive for Internet Security." Paper presented at the Workshop on the Economics of Information Security, Hanover, NH.

Branco, Manuel Castelo and Lúcia Lima Rodrigues. 2006. "Corporate Social Responsibility and Resource-Based Perspectives." Journal of Business Ethics, 69(2): 111-132.

Brännlund, Runar, Sofia Lundberg, and Per-Olov Marklund. 2009. "Assessment of green public procurement as a policy tool: Cost-efficiency and competition considerations." Umea Economic Studies (Working Paper) No 775.

Brouhle, Keith, and Donna Ramirez Harrington. 2010. "GHG Registries: Participation and Performance Under the Canadian Voluntary Climate Challenge Program." Environmental and Resource Economics, 47 (4): 521-548.

Brown, Jeffrey R., and J. David Cummins, Christopher M. Lewis and Ran Wei. 2004. "An empirical analysis of the economic impact of federal terrorism reinsurance." Journal of Monetary Economics, 51: 861-898.

Bryden, Anna, et al. 2013. "Voluntary agreements between government and business—A scoping review of the literature with specific reference to the Public Health Responsibility Deal." Health Policy, 110(2-3): 186-197.

Burby, Raymond J. 2006. "Hurricane Katrina and the Paradoxes of Government Disaster Policy: Bringing About Wise Governmental Decisions for Hazardous Areas." The ANNALS of the American Academy of Political and Social Science, 604: 171-191.

Caballero, R.J., E.M.R.A. Engel and J.C. Haltiwanger (1995), "Plant-level adjustment and aggregate investment dynamics," Brookings Papers on Economic Activity 2:1-54.

Cambini, Carlo, and Laura Rondi. 2010. "Incentive regulation and investment: evidence from European energy utilities." Journal of Regulatory Economics, 38(1): 1-26.

Cantwell, J. and R. Mudambi, (2000), "The location of MNE R&D activity: The role of investment incentives," 40 Management International Revue, 127.

Chatterji, Aaron K., and Michael W. Toffel. 2010. "How Firms Respond to Being Rated" Strategic Management Journal, 31(9): 917-945.

Chatterji, Aaron K., Kenneth Y. Chay, and Robert W. Fairlie. 2013. "The Impact of City Contracting Set-Asides on Black Self-Employment and Employment." Forthcoming in Journal of Labor Economics.

Chirinko, R.S., S. M. Fazzari, and A.P. Meyer, (1999), "How responsive is business capital formation to its user cost?: An exploration with micro data." Journal of Public Economics, 74(1):53–80.

Cohen, D. and J. Cummins (2006), "A Retrospective Evaluation of the Effects of Temporary Partial Expensing," Finance and Economics Discussion Series #2006-19, Divisions of Research and Statistics and Monetary Affairs, federal Reserve Board, Washington D.C.

Cordes, J. 2011. An Overview of the Economics of Cybersecurity and Cybersecurity Policy. George Washington University Cybersecurity Policy and Research Institute. Report GW-CSPRI-2011-6.

Cummins, J.G., K.A. Hassett and R.G. Hubbard (1994), "A reconsideration of investment behavior using tax reforms as natural experiments," Brookings Papers on Economic Activity 2:1-74.

Cummins, J.G., K.A. Hassett and R.G. Hubbard (1996), "Tax reforms and investment: a cross-country comparison," Journal of Public Economics 62:237-273.

Cyber Data Risk Managers. 2013. 2013 Data Privacy, Information Security and Cyber Insurance Trends.

Dalen, Dag Morten, Espen R. Moen, and Christian Riis. 2006. "Contract renewal and incentives in public procurement." International Journal of Industrial Organization, 24: 269-285.

Dalley, Paula J. 2007. "The Use and Misuse of Disclosure as a Regulatory System." Florida State University Law Review, 34(4): 1089–1131.

Delmas, Magali, Maria J. Montes-Sancho, and Jay P. Shimshack. 2010. "Information Disclosures Policies: Evidence from the Electricity Industry." Economic Inquiry, 48(2): 483-498.

Department of Homeland Security. 2012. Cybersecurity Insurance Workshop Readout Report.

Desai, M.A. and A.D. Goolsbee, (2004), "Investment, Overhang, and Tax Policy," Brookings Papers on Economic Activity, no. 2 (Fall 2004), 275-328.

Dourado, E. 2012. Internet Security without Law: How Service Providers Create Order Online. Mercatus Center at George Mason University. Working Paper No. 12-19

Dourado, E., and Brito, J. 2012. Is There a Market Failure in Cybersecurity? Mercatus Center at George Mason University. Mercatus on Policy No. 106.

Dynes, Scott, Eric Goetz, and Michael Freeman. 2008. "Cybersecurity: Are Economic Incentives Adequate?" IFIP International Federation for Information Processing, 253: 15-27.

Edgerton, J., (2010), "Investment incentives and corporate tax asymmetries," Journal of Public Economics, 94 (December 2010), 936-952.

Eeten, M. and Bauer, J. 2008. Economics of Malware: Security Decisions, Incentives and Externalities. Organisation for Economic Co-operation and Development (OECD), Directorate for Science, Technology, and Industry (STI). STI Working Paper 2008/1

Égert, Balázs. 2009. "Infrastructure Investment in Network Industries: The Role of Incentive Regulation and Regulatory Independence." CESifo (Center for Economic Studies and Ifo Institute for Economic Research) working paper, No. 2642.

Eisner, R., (1969), "Tax policy and investment behavior: comment." American Economic Review, 59(3): 379–388.

Etzioni, A. Fall 2011. Cybersecurity in the Private Sector. Issues in Science and Technology, pp. 58-62.

Fiszbein, et. al. 2009. "Conditional Cash Transfers: Reducing Present and Future Poverty." World Bank.

Gal-Or, Esther, and Anindya Ghose. 2005. "The Economic Incentives for Sharing Security Information." Information Systems Research, 16(2): 186-208.

Goetz, Kimberly S. 2010. "Encouraging sustainable business practices using incentives: a practitioner's view." Management Research Review, 33(11): 1042-1053.

Goolsbee, A.D. (2000), "Taxes and the quality of capital," Mimeograph (University of Chicago).

Goolsbee, A.D., (1998a), "Does government R&D policy mainly benefit scientists and engineers? 88 American Economic Revue, 298.

Goolsbee, A.D., (1998b), "Investment tax incentives and the price of capital goods," Quarterly Journal of Economics, 113:121-148.

Gordon, L. A. and M. P. Loeb, Managing Cybersecurity Resources: A Cost-Benefit Analysis (McGraw-Hill, Inc.), 2006.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn. 2003. "Sharing Information on Computer Systems Security: An Economic Analysis." Journal of Accounting and Public Policy, 22(6): 461-485.

Graetz, M. and R. Doud, (2012), "Technological innovation, international competition, and the challenges of international income taxation." Columbia Law Review, 113, 347-446.

Graham, Mary, and Catherine Miller. 2001. "Disclosure of Toxics Releases in the United States." Environment: Science and Policy for Sustainable Development, 43(8): 8–20.

Greene, Mark R. 1979. "A Review and Evaluation of Selected Government Programs to Handle Risk." Annals of the American Academy of Political and Social Science, 443: 129-144.

Griffith, R., D. Sandler, and J. van Reenen, (1995), "Tax incentives for R&D," Fiscal Studies 16 (2), 21–44.

Griffith, R., S. Redding, and J. van Reenen, (2001), "Measuring the cost effectiveness of an R&D tax credit for the UK," 22 Fiscal Studies, 375.

Gugerty, Mary Kay. 2009. "Signaling Virtue: Voluntary Accountability Programs among Nonprofit Organizations." Science Policy, 42(3): 243-273.

Hahn, Robert W., and Anne Layne-Farrar. 2006. "The Law and Economics of Software Security." Harvard Journal of Law and Public Policy, 30(1): 283-353.

Hall, B., (1993), "R&D tax policy during the 1980s: success or failure?" in Poterba, J., ed., Tax Policy and the Economy, 29, 1–35.

Hassett, K.A. and R.G. Hubbard (1998), "Are investment incentives blunted by changes in the price of capital goods?" International Finance 1:103-126.

Hassett, K.A. and R.G. Hubbard, (2002), "Tax policy and business investment," in Auerbach A. and M. Feldstein, Handbook of Public Economics (Elsevier, Amsterdam).

Hausken, Kjell. 2006. "Income, interdependence, and substitution effects affecting incentives for security investments." Journal of Accounting and Public Policy, 25(6): 629-665.

Hausken, Kjell. 2007. "Information sharing among firms and cyber attacks." Journal of Accounting and Public Policy, 26(6): 639-688.

Hines, J. and A. Jaffe, (2000), "International taxation and the location of inventive activity," in Hines, J.R., ed., International Taxation and Multinational Activity 201.

Hines, J., (1994). "No place like home: tax incentives and the location of R&D by American multinationals." Tax Policy and the Economy 8, 65–104.

Hines, J., (1998). "Is it investment ramifications of distortionary tax subsidies." Working Paper 6615 (National Bureau of Economic Research).

House, C. and M. Shapiro (2008), "Temporary Investment Tax Incentives: Theory with Evidence from Bonus Depreciation," American Economic Review 98 No. 3 (June, 2008): 737- 768.

Jaffee, Dwight M., and Thomas Russell. 1997. "Catastrophe Insurance, Capital Markets, and Uninsurable Risks." The Journal of Risk and Insurance, 64(2): 205-230.

Jin, Ginger Zhe, and Phillip Leslie. 2003. "The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards." The Quarterly Journal of Economics, 118(2): 409-451.

Jin, Ginger Zhe, and Phillip Leslie. 2009. "Reputational Incentives for Restaurant Hygiene." American Economic Journal: Microeconomics, 1(1): 237-267.

Johnston, Jason Scott. 2005. "The Promise and Limits of Voluntary Management-Based Regulatory Reform: An Analysis of EPA's Strategic Goals Program." U of Penn, Inst for Law & Econ Research Paper No. 05-17; U of Penn Law School, Public Law Working Paper No. 06-05.

Joskow, Paul. 2013. "Incentive Regulation in Theory and Practice: Electricity Distribution and Transmission Networks."

Karamanos, Panagiotis. 1999. "Voluntary environmental agreements for the reduction of greenhouse gas emissions: Incentives and characteristics of electric utility participants in the climate challenge program." Dissertations and Theses; Thesis (Ph.D.)--Indiana University.

Khanna, Madhu, and William Rose Q. Anton. 2002. "Corporate Environmental Management: Regulatory and Market-Based Incentives." Land Economics, 78(4): 539-558.

Khanna, Madhu, Patricia Koss, Cody Jones, and David Ervin. 2007. "Motivations for Voluntary Environmental Management." Policy Studies Journal, 35(4): 751–772.

Khanna, Madhu, Wilma Rose H. Quimio, and Dora Bojilova. 1998. "Toxics Release Information: A Policy Tool for Environmental Protection." Journal of Environmental Economics and Management, 36(3): 243–266.

Knittel, M. (2007), "Corporate Response to Accelerated Tax Depreciation: Bonus Depreciation for Tax Years 2002-2004," Office of Tax Analysis Working Paper 98, U.S. Department of the Treasury.

Kobayashi, B. 2011. An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods. George Mason University School of Law, Law and Economics Working Paper Series.

Kobayashi, Bruce H. 2005. "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goods." Law and Economics Working Paper Series.

Konar, Shameek, and Mark A. Cohen. 1997. "Information as Regulation: The Effect of Community Right to Know laws on Toxic Emissions." Journal of Environmental Economics and Management, 32(1): 109–124.

Krasnokutskaya, Elena, and Katja Seim. 2011. "Bid Preference Programs and Participation in Highway Procurement Auctions." The American Economic Review, 101(6): 2653-2686

Kremer and Williams. 2010. "Incentivizing Innovation: Adding to the Tool Kit." Innovation Policy and the Economy. Volume 10

Kunreuther, Howard C., Mark V. Pauly, and Stacey McMorrow. 2013. Insurance and Behavioral Economics: Improving Decisions in the Most Misunderstood Industry. New York, NY: Cambridge University Press.

Kunreuther, Howard. 2002. "The role of insurance in managing extreme events: Implications for terrorism coverage." Business Economics, 37(2): 6-16.

Kunreuther, Howard. 2008. "Reducing Losses from Catastrophic Risks through Long-Term Insurance and Mitigation." Social Research, 75(3): 905-930, 1033.

Laffont, Jean-Jaques and Jean Tirole. 1993. A Theory of Incentives in Procurement and Regulation, Massachusetts Institute of Technology Press.

Landry, Craig E., and Jingyuan Li. 2012. "Participation in the Community Rating System of NFIP: Empirical Analysis of North Carolina Counties." Natural Hazards Review, 13(3): 205–220.

Lelarge, M., and Bolot, J. 2009. Economic Incentives to Increase Security in the Internet: The Case for Insurance. IEEE INFOCOM 2009 proceedings.

Lelarge, Marc, and Jean Bolot. 2009. "Economic Incentives to Increase Security in the Internet: The Case for Insurance." INFOCOM 2009, IEEE. 1494-1502.

Lesk, M. November/December 2011. Cybersecurity and Economics. IEEE Security & Privacy.

Lychagin, S. et al., (2010), "Spillovers in space: does geography matter?" Center For Economic Performance, Discussion Paper No. 991.

Machin S. and J. van Reenen, (1998), "Technology and changes in skill structure: Evidence from seven OECD countries," 113 Quarterly Journal of Economics, 1215.

Mamuneas, T., and M. Nadiri, (1996), "Public R&D policies and cost behaviour of the U.S. manufacturing industries." Journal of Public Economics 63, 57–81.

Mansfield, E., (1986). "The R&D tax credit and other technology policy issues." American Economic Association Papers and Proceedings 76, 190–194.

Mazurek, Janice. 2002. "Government-sponsored voluntary programs for firms: An initial survey." New Tools for Environmental Protection: Education, Information, and Voluntary Measures. The National Academies Press, National Academy of Sciences: 219-234.

McCutchen, W.W. Jr. (1993), "Estimating the impact of the R&D tax credit on strategic groups in the pharmaceutical industry, 22 Res. Policy, 337.

Michel-Kerjan, Erwann, and Paul Raschky. 2011. "The Effects of Government Intervention on The Market for Corporate Terrorism Insurance." University of Pennsylvania, Wharton School working paper # 2011-05.

Miller, Steven R., Abdul O. Abdulkadri, Sandra S. Batie, and Satish V. Joshi. 2012. "Motivation, Barriers and Incentives for the Participation of Livestock Operations in MAEAP." Dept. of Agricultural, Food, and Resource Economics Staff Paper Series.

Moon, Seong-gin. 2008. "Corporate Environmental Behaviors in Voluntary Programs: Does Timing Matter?" Social Science Quarterly, 89(5): 1102–1120.

Moore, T. 2010. Introducing the Economics of Cybersecurity: Principles and Policy Options. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. pp. 3-23. National Research Council.

Moore, Tyler, and Richard Clayton. 2011. "The Impact of Public Information on Phishing Attack and Defense." Communications & Strategies, 81: 45-68.

Moore, Tyler. 2010. "The economics of cybersecurity: Principles and policy options." International Journal of Critical Infrastructure Protection, 3(3-4): 103-117.

Mulgan, et. al., 2011. "Social Impact Investment: the challenge and opportunity of Social Impact Bonds." The Young Foundation

Mulligan, Deirdre K., and Fred B. Schneider. 2011. "Doctrine for Cybersecurity." Daedalus, 140(4): 70-92.

Myers, Samuel L., and Tsze Chan. 1996. "Who Benefits from Minority Business Set-Asides? The Case of New Jersey." Journal of Policy Analysis and Management, 15(2): 202-226.

Plummer, E., (2000), "Incentive effects of the investment tax credit: Evidence from analysts' forecasts," in (ed.) 12 (Advances in Taxation, Volume 12), Emerald Group Publishing Limited, 127-171.

Post, Joseph, Michael Wells, James Bonn, and Patrick Ramsey. 2011. "Financial Incentives for NextGen Avionics." Ninth USA/Europe Air Traffic Management Research and Development Seminar.

Rao, N. (2013), "Do tax credits stimulate R&D spending? The effect of the R&D tax credit in its first decade," (The Wagner School, New York University).

Rue, R., and Pfleeger, L. July/August 2009. Making the Best Use of Cybersecurity Economic Models. IEEE Security & Privacy.

Sappington, David E. 2003. "The Effects of Incentive Regulation on Retail Telephone Service Quality in the United States." Review of Network Economics. Volume 2, Issue 4: 355-375.

Sappington, David E. M., and Dennis L. Weisman. 1994. "Designing superior incentive regulation: Accounting for all." Fortnighty, 132(4): 12-15.

Segerson, Kathleen ed. 2002. Economics and Liability for Environmental Problems. Aldershot, UK and Burlington, VT: Ashgate Publishing Co.

Segerson, Kathleen, and Thomas J. Miceli. 1998. "Voluntary Environmental Agreements: Good or Bad News for Environmental Protection?" Journal of Environmental Economics and Management, 36(2): 109-130.

Segerson, Kathleen. 2006. "Chapter 10: An Assessment of Legal Liability as a Market-Based Instrument" in Moving to Markets in Environmental Regulation: Lessons from Twenty Years of Experience. Oxford Scholarship Online.

Shapiro & Rabinowitz. "Voluntary Regulatory Compliance in Theory and Practice: The Case of OSHA." Administrative Law Review Volume 52: 97-155.

Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. 2010. "Competitive Cyber-Insurance and Internet Security." Economics of Information Security and Privacy, 229-247.

Simon, Paul, et al. 2005. "Impact of Restaurant Hygiene Grade Cards on Foodborne-Disease Hospitalizations in Los Angeles County." Journal of Environmental Health, 67(7): 32–36.

Stahl, Michael M. 1994. "Promoting Voluntary Compliance: A Valuable Supplement to Environmental Enforcement."

Summers, L., (1981), "Taxation and corporate investment: A Q-theory approach." Brookings Papers on Economic Activity, 1:67–140.

Thomson, R. and Jensen, J. (2011), "The Effects of public subsidies on R&D employment, evidence from OECD Countries, (Intellectual Property Research Institute of Australia, Working Paper No. 2/11).

U.S. Department of Commerce, Internet Policy Task Force, "Cybersecurity, Innovation, and the Internet Economy" (Green Paper), June 2011

U.S. Department of Homeland Security, Cross Sector Cyber Security Working Group, Incentives Subgroup. September 2009. Incentives Recommendations Report.

U.S. Department of Homeland Security. November 2012. Cybersecurity Insurance Workshop Readout Report.

U.S. Government Accountability Office, (1989), "Tax policy and administration: The research tax credit has stimulated some additional research spending."

U.S. House of Representatives, House Republican Cybersecurity Task Force. October 2011. Recommendations of the House Republican Cybersecurity Task Force.

U.S. National Research Council. 2010. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy.

Verma, Kiran, Barry M. Mitnick, and Alfred A. Marcus, 1999. "Making Incentive Systems Work: Incentive Regulation in the Nuclear Power Industry." Journal of Public Administration Research and Theory: J-PART, 9(3): 395-436.

Videras, Julio, and Anna Alberini. 2000. "The appeal of voluntary environmental programs: which firms participate and why?" Contemporary Economic Policy, 18(4): 449-460.

Vogelsang, Ingo. 2002. "Incentive Regulation and Competition in Public Utility Markets: A 20-Year Perspective." Journal of Regulatory Economics. Volume 22: 5-27.

Weil, David, Archon Fung, Mary, Graham, and Elena Fagotto. 2006. "The Effectiveness of Regulatory Disclosure Policies." Journal of Policy Analysis and Management, 25(1): 155-181.

Wernstedt, Kris, Peter B. Meyer, and Anna Alberini. 2006. "Attracting Private Investment to Contaminated Properties: The Value of Public Interventions." Journal of Policy Analysis and Management, 25(2): 347-369.

White House. n.d. "Cyber-Insurance Metrics and Impact on Cyber-Security." Undated policy white paper. Accessed April 25, 2013.

Wilson, Daniel J., (2009), "Beggar thy neighbor? The in-state, out-of-state, and aggregate effects of R&D tax credits," 91 Revue of Economics and Statistics, 431.

Yusof, Nor'Aini, Ismael Younis Abu-Jarad, and Mohd Hasanal Badree. 2012. "The Effectiveness of Government Incentives to Facilitate an Innovative Housing Delivery System: The Perspective of Housing Developers." Theoretical and Empirical Researches, 7(1): 55-68.

Zhang, Yichen. 2009. "Incentives for Poultry Integrators to Contract Bio-Secure Producers and Implication for Government Indemnification Program." Master's Thesis, Mississippi State University, Department of Agricultural Economics.

3.3. DHS Incentives Workshop Summary

Incentives Working Group
Workshop Notes

Date: April 19, 2013
Location: 1110 N. Glebe Road, Arlington, VA 22201, Executive Briefing Facility

In addition to the panelists listed below, participants in the workshop included the following Federal Government departments and agencies: Department of Agriculture, Department of Commerce, Department of Defense, Department of Education, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of State, Department of Transportation, Department of the Treasury, Environmental Protection Agency, Federal Communications Commission, Federal Deposit Insurance Corporation, Food and Drug Administration, General Services Administration, National Guideline Clearinghouse, National Institute of Standards and Technology, National Security Staff, and the Office of the Director of National Intelligence.

Industry and nongovernmental participants included representatives from AIG, American Fuel and Petrochemical Manufacturers, American Gas Association, American Public Power Association, Association of Metropolitan Water Agencies, BNY Mellon, Boeing, Booz Allen Hamilton, CSC, Deloitte, Dickstein Shapiro, Fire Eye, General Dynamics, General Electric, Homeland Security Studies and Analysis Institute, Information Technology & Innovation Foundation, International Legal Technology Association, Internet Security Alliance, Juniper Networks, Lockheed Martin, LSB Industries, National Association of Regulatory Utility Commissioners, National Defense Industrial Association, NERC, Northrup Grumman, Praxair, Sacramento Municipal Utility District, SAIC, Securities Industry and Financial Markets Association, U.S. Chamber of Commerce, USAA, Utilities Telecom Council, Verizon, and Worldwide Insight.

3.3.1. Welcome and Agenda Overview

Bob Kolasky described ITF's role. It is important that the work on incentives is done well and transparently. A principle goal is including perspective of critical infrastructure community.

3.3.2. Keynote 1

Acting Deputy Under Secretary McConnell began with recognition of the tragic Boston bombings. He noted that there is, today, a strategic moment for cybersecurity; we are lucky that there has not yet been a loss of life due to cyber attacks, but that likely is coming. Today, we are putting in place part of a larger effort to create a partnership to stop the growth of these problems. We are here to explore the art of the possible with respect to what the public-private partnership can be and can achieve.

There is significant interconnection between cybersecurity and infrastructure. PPD 21 has a broader focus than just protection, and takes a holistic and strategic view of things. There are three key elements to the EO: (1) privacy and civil liberties and rights, (2) information sharing, and (3) Cybersecurity Framework. This will be a voluntary Framework, and no other aspects of the Executive Order (EO) rely on adoption of the Framework.

The Framework will be the result of the extensive and collaborative effort conducted by the National Institute of Standards and Technology (NIST). The Framework will reference technical controls, but it will be more than that. It will be a risk management Framework, including resilience and not just focused on protection. The Framework will not only be for the technical community, but will be brought to corporate boards and leadership. It will have words understandable to such audiences, and include potential investments that need to be made within a risk management Framework.

The Framework is due by mid-February 2014, and will allow stakeholders tell DHS if they will utilize the voluntary program.

PS-Prep is one example of a voluntary incentive program. Though three organizations (AT&T, the American Bar Association, and RASGAS) are now certified, this is not a resounding uptake (later in the workshop it was noted that a fourth organization has recently completed its conformity assessment and will be eligible to receive its certification soon). So it seems that PS-Prep is not using the right incentives. That is why we are holding this meeting. We want to know: how can we get it right? What are the right incentives? Currently, there is also fiscal restraint, making some incentives harder to institute than others. We may require many incentives, including regulations and legislation. But, we have a great set of people working on this.

3.3.3. Keynote 2

Larry Clinton, President and CEO of the Internet Security Alliance, began by noting that government and industry have aligned, but not identical security goals. Hope to fill in the gap today. Business interests reflect business requirements. We are thinking about cyber all wrong. It is not just a tech issue, but an enterprise issue. The problem is people, not technology. Just because you are breached, you (firms) are not necessarily negligent. There are two types of companies, those who know they were attacked and those who don't know. Perimeter defense is outmoded. This is not just like seatbelts; is not a consumer product safety issue. Systems are not bad, but they are under attack, and there are many incentives to attack them. It is not true that industry does not want to spend on cyber. Spending has doubled (from $40 to 80 billion) in recent years.

This is more than the $59B spent each year for all DHS. The notion of perimeter defense is a thing of the past, as it possible to defend systems even if you have been breached. Billions for eHealth records and standards in recent funding (stimulus, etc.); but, health sector is among worst – Johns Hopkins University study, PriceWaterhouseCoopers (PwC) study.

It is inappropriate to focus on regulation, as they are static, U.S.-specific, often set ceilings when we really need floors, don't necessarily work (can be bad for security as they may push too much focus on compliance – which can be anti-security), and hard to make work.

Incentives are as important to cybersecurity as is technology, but the incentives favor the attackers (cheap and easy to access, and normally one generation ahead of defenders, and few prosecutions), government and industry have different jobs and see "risk" differently (with the private sector often more risk tolerant than government), often the risk taker is not the damage sufferer, with irresistible incentives often promoting insecurity. For example, the cloud, modern supply chains, and other aspects of modern systems are inherently insecure and prevalent because they make business easier.

There are massive economic incentives to be insecure. People have been moving from traditional telephony to voice over Internet Protocol (VoIP); international supply chain; cloud computing – PwC study – 62% had little or no faith in cloud, including 48% that had already done that. Standards can lead to insecurity; suggest pen testing is reduced from quarterly to annually for compliance with the Framework.

There is a long and successful history of government/industry partnerships using economic incentives, e.g., the power grid and telephone network. However, if cyber is a big problem, a big deal is required. How should this be done?

Again, many sectors are involved here; thus, we may require a menu of incentives, even within sectors. In fact, incentives must apply at the corporate level, not the sector level

A century ago – hot technology was power and phone – U.S. government guaranteed rate of return to utilities so that they would invest in less profitable, rural areas.

What are the goals of the Framework? Adopt the Framework (what is the Framework?), prevent catastrophic attacks (including acts of war, which would be a federal job), protect personally identifiable information (PII) or IP? Maybe best to incentivize innovation, but not compliance (can use large public sector players with economies of scale to assist smaller players)?

Acts of war are supposed to be prevented by national government, are private sector companies supposed to now? If so, 900% spending increase. Is program going to lead to greater security? Didn't with healthcare or federal Information Security Management Act (FISMA).

Incentives are best viewed through a series of principles, including that in order to be effective incentives must be: powerful enough to affect corporate investment behavior, calibrated to match the level of additional investment required to adopt the Framework, vary not just from sector to sector but business to business and thus a menu of incentives will be needed, recognize that regulation that does not include full cost recovery is not a substitute for incentives, and that cost not compensated through incentives will either be passed on to consumers or reduce investment in critical infrastructure - there is no free lunch to be had.

3.3.4. Session I: Regulated Industries

Session I featured five panelists from regulated industries: Anna Cochrane of the Federal Energy Regulatory Commission, Will Coffman of the American Public Power Association, Miles Keogh of the National Association of Regulatory Utility Commissioners, Jim Linn of the American Gas Association, and Karl Schimmeck of the Financial Services sector. Moderated by Rob Atkinson of the Information Technology and Innovation Foundation, questions from the first session included the following:

- What incentives are there to share information?
- Does cost recovery work as an incentive?
- Will the smart grid help utilities with cybersecurity?
- Is rate recovery enough of an incentive to adopt the Framework if it is deemed a prudent investment?

Rob Atkinson: One approach to handling cybersecurity is legislation. There is no cost to the government and appears to provide security. The other extreme, often supported by business is to subsidize private sector cybersecurity while also providing them the freedom to fashion their own security. But, it's obvious that funding for subsidies is extremely unlikely. What is needed is a middle ground that changes behavior but doesn't cost too much.

Karl Schimmeck (Financial Services): The Financial Services (FS) Sector seeks to create trust in dealing with the problem of cybersecurity which it sees as a real threat to the industry. While FS already uses incentives, the sector wants to see others adopt incentives. We suggest using limited federal investment in the right places. It's uncertain whether the Framework will make us safer, so is the idea that the Framework is the right path a correct assumption? Because the Framework has not been developed, there is nothing to incentivize as yet.

There are two threats: a national threat and a threat to business. The goal should be to set the appropriate level of response to each. We need to also consider disincentives, for example, the current system allows hackers get away with their actions; this needs to be addressed. We need standardization and harmonization of the Framework with international rules. Finally, industry has a concern about regulatory backlash, that is, how to encourage sharing of information in the face of the fear that the government might then use to information to regulate the sharers.

Incentives: Use the limited available money to fund R&D and provide grants to ISACs; if a certain level of security is reached, then the owner/operator can received incentives from the Government; share information across sectors, but protect the sharers from liability; and, accelerate security clearances for sharing of classified information.

Miles Keogh (NARUC): All regulation is some sort of incentive, either a carrot or a stick. The trick is assuring that an apparent incentive isn't actually a stick, i.e., an orange stick. While cybersecurity is a new issue for State Public Utility Commissions (PUCs) to weigh in overseeing utility investments, it is not too exotic in the sense that any investment must be seen to be prudent, or a prudent cybersecurity investment is a prudent investment. However, PUCs need to

be educated in cybersecurity, so they can ask the right questions concerning investments and understand the responses. A utility needs to construct a strategy to determine what a PUC expects from a rate case and educate the PUC. A risk management approach to cybersecurity is preferable to regulation in that prudent investments are what we want from utilities and the PUC system looks at prudence. A utility can increase spending on cybersecurity but it must be certain that the investment yields an increase in security.

Resilience – the utilities and PUCs need to agree on what this means before they can share a common understanding of what an investment in resilience is for. The value of any investment needs to be shown. The question then is: how do you create value via an investment?

Anna Cochran (FERC): FERC has mandatory cybersecurity standards to assure the reliability of the grid. FERC rules allow rate increase and a reasonable rate of return. There is some increased flexibility where extraordinary cost is incurred by a utility, e.g., a surcharge might be allowed after a hurricane. This is not an incentive, but a means to recover costs beyond the operator's control.

Incentives: Congress provided incentives to encourage transmission facilities to increase reliability through increased recovery of costs of investment. Because companies recover costs in different ways, some may be stronger competitively or have higher levels of security. Accordingly, non-rate based incentives would be preferable.

Jim Linn (AGA): Expedite clearances? The Energy Sector has this already. Information sharing? This should be done already, too. However, disclosure of information could make a company a larger target. Sharing of information describing the means of a cyber-attack could expose info on the system and needs protection. An approach that singles out a company based on expertise could also make the company a target.

Will Coffman (American Public Power Association - APPA): For the Electricity Sector, which already is regulated through FERC, design the Framework to reflect the existing FERC cyber standards rather than penalizing a company for participating in the program. Good incentives for the Electricity Sector: encouraged information sharing; increased numbers of clearances to access classified information, and certification programs. Adherence to these might result in lower insurance premiums. Finally, encourage companies to pass on cyber information they receive by providing liability protection.

Question: what are the differences in the regulatory sphere vs. the non-regulated sphere?

Karl Schimmeck: Because FS is already held to standards, the Framework should include those standards that are being met. This would prevent them from potentially being regulated again, despite meeting standards. The Framework should go beyond standards, like providing liability protection for information sharing.

Miles Keogh: Regulation is necessary for utilities to assure reliability, so the Framework could provide pressure for utilities to use best practices. Going beyond compliance with standards might

be a seen as a disincentive. However, this concern can be mitigated by PUCs recognizing prudent investments in cost recovery decisions.

Question: what incentives are there to share information?

Karl Schimmeck: many companies worry that regulators will misuse information provided voluntarily. Also, removing liability for information sharing would encourage the practice.

Miles Keogh: One would want to change the culture of utilities, e.g., by educating managers in cybersecurity, training employees, and replacing a check-box mentality with a systems approach. First figure out how to incentivize this behavioral change, then information sharing should be straight-forward.

Anna Cochran: Can a safe-harbor be created for information-sharers? There is a provision in the FERC rules for this.

Jim Linn: If shared information was divulged, it exposes a company's security positions.

Question: Would an EPA Energy Star approach work, i.e., would providing a seal of approval as a cyber-secure company be a factor that would attract investors?

Jim Linn: No. It is preferable not to raise a company's profile. Investors might be guided by a seal, but that's a lesser concern than the increased targeting. There is no competitive advance to the seal and, moreover, we would prefer to have all companies at the same level of security.

Karl Schimmeck: Here are two types of R&D efforts: fund universities or DHS Centers to develop advanced cybersecurity technology; and encourage companies to put leading edge technology into use, but provide liability protection in case the company is sued because the technology wasn't adequately tested.

Anna Cochran: Recovery of R&D and installation of advanced technology costs are recoverable to utilities.

Question: Does cost recovery work as an incentive?

Miles Keogh: A prudent investment in cybersecurity is recoverable from PUCs if it is a sound, risk-based mechanism. If the mechanism is prudent, it will be approved.

Audience: Voluntary consensus standards are best practices. These might be the basis of the Framework. The Framework might give companies an incentive to undertake adoption and certification. Do industries adhere to best practices?

Miles Keogh: Don't certify, but instead incentivize companies to adopt best practices as the goal.

Question: Will the Smart Grid help utilities with cybersecurity?

Miles Keogh: The Grid's greater connectivity will create vulnerabilities, but greater resilience and cyber capacity will also be created, which might improve security.

Larry Clinton: It is important not to equate resilience and security.

Question: Should a PUC be overruled if it doesn't treat cybersecurity expenditures as a priority for political reasons, such as consumer resistance to higher bills?

Miles Keogh: A prudent investment will be approved. Will compliance with the Framework be deemed a prudent investment? FERC has mandatory standards, which are defined as prudent investments. If the Framework is well designed, but badly implemented or doesn't lead to prudent decision-making, then expenditures won't be approved.

Question: Is rate recovery enough of an incentives to adopt the Framework, if it is deemed a prudent investment?

Miles Keogh: There might be other factors than rate recovery, e.g., economic considerations.

Jim Linn: The Gas Industry will be taking steps to assure cybersecurity in any case.

Caller (AIG): What is the value of a Framework if we don't understand the risk?

Panel summary: Three incentives: (1) liability protection for information sharing; (2) innovation creates risks, so protection is needed for innovation; and (3) improve R&D with liability protection.

3.3.5. Session II: Non-Regulated Industries

Session II reviewed incentives-related issues specific to non-regulated industries. Moderated by Roberta Stempfley of DHS, the panel included the Internet Security Alliance's Clinton, Brian Finch (Dickstein Shapiro LLP, a law firm that advises SAFETY Act applicants), Marc Sachs (Verizon), and John Toomer (Boeing). Questions from the second session included the following:

- What is the current environment in non-regulated sectors like from your viewpoint?
- Can other programs that rely on social behavior be adapted to incentivize the Framework?
- How about research and development tax credits accessible to regional clusters and patent protection as incentives?
- If the Framework had a risk-based approach, how would it work?

Question: What is the environment in non-regulated sectors from your viewpoint?

John Toomer (Boeing): Boeing has two components, the defense component that is part of the DIB and the commercial which is regulated. Cybersecurity is a given in all aspects of the business and in the companies that support Boeing. As a result, incentives won't affect us. Information sharing, however, is very important. The company wants to share best practices and has been doing so. Boeing is involved with eight sector ISACs. Cybersecurity is integral to the business and management is well aware of the issue and involved.

Boeing supports the Framework in general, but will wait so see what it looks like when developed. The Framework will need to address company suppliers which range from large to very small companies. There will need to be a variety of incentives for these.

Marc Sachs (Verizon): The Communications Sector has five components: wire, wireless, cable, broadcast, and satellite. Each is unique in that some have physical infrastructure, such as cables, while other deal more in the invisible aspects of communications. Some aspects of the industry are regulated.

The Communications Sector has three key elements: availability is critical to communications so there is a heavy emphasis to assure resilience; integrity must be there to assure that information is not compromised; and confidentiality is more of a customer issue, since they need to take steps if this is important, whereas the carrier simply delivers the information. The industry is highly targeted by cyber-attacks.

Brian Finch (Dickstein Shapiro LLP): Does the SAFETY Act apply to cyber-attacks? The Framework is just the latest exercise in partnership, starting with the NIPP, followed by PS-PREP. Just as those partnerships needed incentives, such as liability protection, to gain partners, so does the Framework. The SAFETY Act could provide this incentive. Consider that over 700 technologies have been approved by DHS under the Act. The Act establishes affirmative liability protection for users of approved technology if sued. The Act denies awarding of punitive damages, but, more importantly, certifies a presumption of non-liability to third parties. If a party certified against third-party liability sells the technology to another party, the purchaser is also immune under the Act. Any technology that has a security purpose is included under the broad scope of the Act.

Why hasn't the Act been used in the cases of cybersecurity technology? First, most people are unaware of its potential applicability because it has been used solely for physical security. Second, over the 10 years since 9/11, we've suffered terrorism fatigue, causing us to downplay the importance of terrorism attacks.

Is more than applying the Act to cybersecurity needed? Perhaps, change phrasing so that the Act applies to more than "acts of terrorism," and that it applies to cyber terrorism and cyber technology. Because the Secretary of DHS makes determinations under the Act, these changes should be easy to make.

Larry Clinton (ISA): Do companies want subsidies? No, this is not an incentive. They understand the government's fiscal constraints and the need for pragmatism. If a program has value, it will be adopted. The Framework is too fuzzy right now. Industry has spent considerable sums on cybersecurity already and understands value. But does more need to be done? The Framework needs to get business to do more.

We don't know what the Framework will look like, but it should include language about risk-management. Also, it should address probabilities, consequences, and economics to make sense to business. Because senior managers are not savvy about digital information, taking cybersecurity

out of the IT realm and putting it into the enterprise risk management realm will improve their understanding.

The Framework seems aimed at rudimentary attacks. Since attackers try this first, then raise the sophistication of the attack if this fails, the Framework needs to address progressive response to attacks. Also, consider cascading attacks, since not just one business is attacked, but connected businesses, both large and small, too. The Framework needs to cascade its protections down to these, too.

Question: Can other programs that rely on social behavior be adapted to incentivize the Framework?

John Toomer: There are large and small players, so recognize information sharing among large businesses for their benefit and then use the government to push out the information to the small businesses or create products for small businesses for adoption via incentives.

Over-compliance caused by duplicative federal, state, local agency, and customer audits of compliance result in duplication and diverting resources from cybersecurity. Create a central compliance audit to streamline the audit process to one audit. A good performer could be excused from follow-on audits.

Brian Finch: Amend the SAFETY Act to allow certification of international standards and practices that have proven effective. Since effectiveness is a sliding scale, create a sliding scale of incentives.

Marc Sachs: Industry needs assurance that liability from customer suits will be avoided if they take protective actions. If DHS wants industry to abandon what it is now doing under National Institute of Standards and Technology (NIST) standards to undertake the Framework, incentives will be needed. Because cyber-attacks do not respect political boundaries, if DHS wants businesses to adopt the Framework and come under federal oversight, then preempt states and localities.

From a financial perspective, tax credits and R&D provide too little incentive, but litigation and audits are very expensive and incentives in these areas would be attractive to large businesses.

Unknown party: The FTC (FCC?) rules of conduct to protect against botnets contain an appendix that details the barriers to adoption of the code of conduct and ways to circumvent the barriers that might be useful to the Framework incentives effort.

John Toomer: We want incentives for innovator companies. The threat is evolving, so we want protections to evolve, too. One approach would be an open innovation forum where ideas could be shared without fear of barriers and penalties. The government should encourage rather than inhibit this type of openness in order to engender trust and encourage those highly motivated enterprises.

Brian Finch: We have a cyber-problem, but who will benefit if the Framework is established? Probably not the large businesses. Figure out how to structure the Framework to get the best

results. Litigation is very expensive. The SAFETY Act covers reasonable behavior if government-approved processes were used, as evidence of reasonable behavior.

Question: How about R&D tax credits accessible to regional clusters and patent protection as incentives?

Marc Sachs: For the Communications Sector, innovation is made by integration, processes, and systems rather than by things, so patent issues aren't applicable here.

Rob Yellen (AIG): Create incentives around enterprise risk management.

Larry Clinton: You need a menu of innovations for small companies, too.

John Toomer: Boeing has a number of small companies who aren't integrated into the general business so that they can be agile. Accelerating and streamlining patents would be helpful.

Brian Finch: Tax credits won't work. R&D and innovation work now without incentives, that is, new products have no problem enticing investors and customers. Instead, give resources for R&D and innovation through DHS centers and other entities. Maybe, large companies can get procurement advantage with government if they assist smaller companies with cybersecurity.

Larry Clinton: The government does many other things than allow tax incentives that should be explored.

Question: What definition of cyber incident should be used to trigger the SAFETY Act?

Brian Finch: Not sure, but it should be as broad as the definition of a terrorism incident under the Act. The definition should not be narrowed so that supply chain security involving compromised parts would be covered. Perhaps, "any damaging electronic attack" is about right

Question: If the Framework had a risk-based approach, how would it work?

Marc Sachs: What does "risk" mean? The Executive Order is based on consequence only. This is an important distinction and needs to be discussed in the EO context.

Larry Clinton: Risk means something different to government than to business. The government view of risk will not build partnership unless it recognizes business's concerns, such as economics.

John Toomer: It's all about brand, so that customers will want to use your products. Reputation is important in considering risk, but there is an economic component, too. The government needs to understand what business does.

Brian Finch: How bad will losses from stolen intellectual property and trade secrets be? This needs to be explored. More needs to be done to protect this investment.

3.3.6. Session III: Cross-Sector Incentives

Session III's Cross-sector Incentives panelists answered questions about their views on creating a competitive advantage for organizations seen as good stewards of cybersecurity, as well as how the Framework should address "signature-less" attacks. This panel was moderated by Bob Kolasky (DHS) and included Kevin Bonnette (SAIC), Tom Finan (DHS), Emile Monette (Government Services Administration), Don Perkins (Northrop Grumman), and Christine Ricci (General Electric).

Kevin Bonnette (SAIC): SAIC is prepared to embrace the Cybersecurity Framework and assist its clients with solutions to implement the Framework as well. Consider the shrinking budgets for the government and private industry in reviewing the regulations and requirements each organization is expected to follow. The challenge going forward will be to understand the cost involved to meet expectations within the Framework.

Tom Finan (DHS): Mr. Finan supports Strategy and Policy within the Office of the Assistant Secretary for Infrastructure Protection National Protection and Programs Directorate (NPPD/IP). NPPD/IP is in a unique position to provide impact on the cybersecurity market. While DHS cannot offer a solution to fix everything, it is a likely organization to start the discussion between industry and the government.

Emile Monette (GSA): General Services Administration (GSA) has a Joint Working Group on Improving Cybersecurity and Resilience through Acquisition. The primary focus of the WG is Executive Order 13636 section 8(e), which requires a report on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. WG members include DHS, NIST, the Department of Defense, and the Office of Management and Budget (OMB). On April 25, a Request for Information (RFI) will be published in the federal Register. The RFI has three categories: feasibility, commercial practice, and steps that can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity. While the RFI will be left open for public comment for 30 days, GSA would prefer comments by May 15 so the feedback can be incorporated into the final document.

Don Perkins (Northrop Grumman): Northrop Grumman is currently dealing with the competition for risk security and rigor that comes through providing products and services. Like other organizations, it has developed practices through lessons learned. Ongoing dialogue between industry and government has also helped the organization create a multi-tiered approach to its incentives. Government should consider a similar multi-tied approach to pass along information. In addition, a lexicon to list common definitions and recognized standards would ensure that all who support cybersecurity are using the same terminology.

Private Sector Representative: Agreed with Mr. Perkins on the utility of a lexicon as there are individuals who do not understand what cybersecurity means. Similarly, some departments will define cybersecurity differently and it is important to have a similar understandings.

After the panelists provided an overview of their thoughts on cross-sector incentives, the following questions were posed to the group:

Question: In thinking about procurements, what are your thoughts about providing competing companies with a competitive advantage if their organization is seen as a good steward of cybersecurity?

Private Sector Representative: My primary concern with the approach would be within the details of the requirements. International companies will need to have enhanced levels of requirements. Additionally, several attendees of the workshop brought up ways this competitive advantage for companies could lead to disadvantages for the Federal Government. For example, it is unclear whether all the requirements can be measurable, which could lead to murky rulings that some businesses could deem unfair or the competitive advantage could largely favor big businesses that have the capital to meet all of the demands of the Framework.

Question: How will the recommendations harmonize with other existing requirements? Will it address "signature-less" attacks?

Kevin Bonnette: While correct in the need to harmonize the cybersecurity Framework with other existing requirements and legislation, it is important to note that this document is not expected to encompass everything for all departments and agencies. The Cybersecurity Framework will not be a one-size-fits-all recommendation.

Question: A private sector representative cautioned the Incentives Working Group on using the wording "secure product device" in lieu of calling a particular company secure. It is important the language dictate an understanding of the difference, because it will be possible to follow the Framework and not be secure.

Bob Kolasky: The Framework will be silent on a lot of these questions. At the moment, the definition for each incentive is being developed outside of the Framework.

3.3.7. Session IV: Government Roundtable

Session IV, the concluding Government roundtable, provided participants with an opportunity to hear from the Federal representatives responsible for drafting the incentives studies for their respective Government departments. It consisted of Tony Cheesebrough (DHS), Suzanne Lightman (Commerce Department, representing Ari Schwartz), and Leigh Williams (Treasury Department).

Tony Cheesebrough (DHS): Mr. Cheesebrough is the Chief Economist for the Integrated Task Force and the DHS National Protection and Programs Directorate. He provided an overview of the fourteen proposed incentives including the source documents from which each incentive was either recommended or discussed. For more information, review the slide deck titled "DHS Incentives Study: Objectives, Scope, Methodology, and Microeconomic Framework."

Emile Monette (GSA): GSA has a Joint Working Group on Improving Cybersecurity and Resilience through Acquisition. The primary focus of the WG is Executive Order 13636 section 8(e). Considering it is an interagency effort, WG members include DHS, NIST, DoD, and OMB.

On April 25, the Request for Information (RFI) will be published in the federal Register, visit http://www.regulations.gov. Submit comments via the federal eRulemaking portal by searching for "Notice-OERR-2013-01." Select the link "Submit a Comment" that corresponds with "Notice-OERR-2013-01." Follow the instructions provided at the "Submit a Comment" screen. Please include your name, company name (if any), and "Notice-OERR-2013-01" on your attached document by May 15.

Leigh Williams (Treasury): Treasury will review incentives based on four focus areas: (1) focus; (2) fair; (3) flexible; and (4) consistent. Treasury received some specific requirements within the EO to look at benefits and other items. Additionally, Treasury will want to ensure their work is integrated into the interagency deliverables appropriately.

Suzanne Lightman (NIST and Department of Commerce): Commerce will release a draft paper for public comment.

Question: How will incentives be analyzed?

Samara Moore: Incentives will be analyzed per the guidance in Section 9 of the EO, which addresses identifying cyber-dependent infrastructure.

Question: Will there be another look at incentives after the Framework is developed?

Tony Cheesebrough: We have received approval to amend our report based on feedback received during the incentives peer-review process, and so it is also possible that the incentives may be re-evaluated after the Framework is developed.

Question: What are some of the lessons from today's workshop that you will take back with you to your respective organizations?

Suzanne Lightman: Think carefully about how each incentive is defined and what ought to be considered an incentive.

Tony Cheesebrough: Liability protections were widely endorsed. Also, not only based on feedback today, but due to existing DHS efforts on expediting clearances as well as EO Section 4's requirements on information sharing, these two are not likely to be included in our recommendations.

Leigh Williams: Consider a multi-tiered approach to incentives.

3.4. Commerce NOI Response Review

On March 28, 2013, the Department of Commerce issued a 30-day Notice of Inquiry (NOI) entitled, "Incentives to Adopt Improved Cybersecurity Practices."[21] "Comments on Incentives to Adopt Improved Cybersecurity Practices NOI" were posted on April 29, 2013, and included 45 comments from the following respondents:[22]

Advanced Cybersecurity Center, American Association for Laboratory Accreditation, American Fuel and Petrochemical Manufacturers, American Gas Association, American Insurance Association, American Petroleum Institute, American Public Power Association, atsec, Booz Allen Hamilton, Bryan Rich, Business Software Alliance, CACI, Covington & Burling/Chertoff Group, DCS Corp, Donald Edwards, Dong Liu, Edison Electric Institute, Electric Power Supply Association, Emmanuel Adeniran, Encryptics, Federal Communications Commission, Financial Services Sector Coordinating Council, Gary Fresen, Honeywell, Internet Infrastructure Coalition, Internet Security Alliance, IT SCC, Los Angeles Department of Water and Power, Marsh, Microsoft, Monsanto, National Cable and Telecommunications Assoc., NCTA- The Rural Broadband Association, National Electrical Manufacturers Association, National Rural Electric Cooperative Association, Robin Ore, San Diego Gas & Electric and Southern California Gas Company, Sasha Romanosky, Southern California Edison, Telecommunications Industry Association, Terrence August & Tunay Tunca, U.S. Chamber of Commerce, US Telecom Association, Utilities Telecom Council, Voxem Inc.

As noted in Section 2.4.3, responses to the Commerce NOI were reviewed as a complement to the findings from the literature review, and to help inform conclusions about differences among evaluations as well as evaluations that are inconclusive. Similar to the DHS Incentives Workshop, the evaluation of NOI responses focused on the following questions:

- Are there additional incentive categories, or sub-categories, that should be considered?
- Which incentives are most likely and least likely to promote adoption of the voluntary Framework and why?

A summary of the 45 responses is provided below. Instead of a list detailing each response, a synopsis of responses is included for each category discussed in this report, as well as notable suggestions of particular interest. Additionally, Table 3 below indicates which of the incentives considered were recommended, discussed, or neither discussed nor recommended by each of the respondents.

[21] Docket number 130206115-3115-01: http://www.ntia.doc.gov/federal-register-notice/2013/notice-inquiry-incentives-adopt-improved-cybersecurity-practices

[22] The full responses can be accessed at: http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi

3.4.1. Grants

Respondents noted that significant costs could be associated with implementing the Cybersecurity Framework, depending on its final content and requirements. Several respondents suggested that grants could offset the investment required to implement new cybersecurity architecture, as well as to fund subsequent assessments to evaluate Framework adoption and associated impacts on system and network security. Respondents further noted the potential effectiveness of cross-sector grants to guide uniform maturity among critical-infrastructure owners and operators. For example, one respondent cited the potential for grant funds to enable information sharing and analysis centers to coordinate Framework adoption among member organizations, promoting economies of scale and minimizing the cost imposed on any individual entity. However, respondents also noted that the conditions for obtaining grants must not outweigh the estimated benefits from grant receipt.

3.4.2. Insurance, Liability Protections, and Legal Benefits

Numerous respondents suggested the potential value of various aspects of liability protection or a more robust cybersecurity insurance market. Notably, several respondents also mentioned a cybersecurity-specific SAFETY Act that could integrate several incentives to encourage Framework adoption and broaden cybersecurity investment. A common suggestion among respondents was the need for indemnity, at some level, from liability for security breaches if organizations adopting cybersecurity measures as defined in the Framework. Several respondents framed such indemnity as "safe-harbor protection", in which DHS or a third party would accredit an organization as making reasonable efforts to adopt the Framework, thereby triggering indemnity against certain legal claims. A respondent from the financial sector further noted that Framework adoption should entitle "protection from liability for FTC or State attorney general actions arising out of events or breaches relating to these practices, as such compliance constitutes sufficiently responsible and reasonable 'due care' behavior." However, other respondents noted that previous legislative attempts to codify some indemnity for adoption of cybersecurity best practices were insufficient to change the behavior of target organizations. Similarly, some respondents reported that a predictable process for validating Framework adoption is essential for the effectiveness of any indemnity regime, as organizations will require assurance that they are in fact covered under any such program before investing in Framework adoption. However, several respondents did note that the connection between a security breach and potential negligence may be fallacious in the current risk environment, as a highly adaptable threat implies that a certain number of breaches are inevitable regardless of cybersecurity measures.

Respondents further noted the potential importance of the cybersecurity insurance market to encourage adoption of appropriate security measures. The Cybersecurity Framework could provide a basis for a "standard of care" to support the issuance of cybersecurity insurance. As noted by one respondent, "cyber liability insurance represents both a financial incentive (i.e., protects an organization against loss, protects shareholder value) and a hidden penalty (i.e., over time insurance guidelines will establish higher standards of due care that will create costs for companies)" to encourage Framework adoption. A respondent also noted the relevance of the Terrorism Risk Insurance Act (TRIA) in providing coverage

for losses attributable to a cybersecurity incident with a terrorism nexus, and the possibility of expanding TRIA criteria to encompass losses associated with other cyber malefactors.

Certain respondents also noted the application of the existing SAFETY Act in the context of Framework adoption. DHS does not believe, however, that is feasible without modifications to the Act.

3.4.3. Prioritized Technical Assistance

Several respondents noted the potential benefit of prioritized technical assessment for entities adopting the Cybersecurity Framework. Such assistance was suggested in three contexts: prioritized response from technical teams such as the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) after a cybersecurity incident, preferred entry in cybersecurity training programs, and increased availability of vulnerability assessments, including on-site red-teaming and penetration testing. One respondent also suggested that DHS could assist adopters in securing priority Internet and telecommunications access during major incidents that result in service disruption.

3.4.4. Procurement Considerations

The potential benefits of incorporating Framework adoption into DHS or Federal procurement standards was suggested as a potentially low-cost, high-impact incentive. Respondents suggested that procurement considerations could allow the Framework to serve as a market differentiator, and increase the baseline cybersecurity of participants (a stated goal of the Framework). However, respondents also noted that procurement considerations would only affect the sub-set of critical infrastructure owners and operators that bid for Federal contracts. Furthermore, respondents emphasized that procurement considerations require a technology-neutral approach to cybersecurity, implying that such neutrality should be a foundational precept of the Framework if procurement is to be used as a viable incentive. This matches the Executive Order's requirement for the Framework to be technology-neutral.

3.4.5. Public Recognition

Public recognition was not frequently cited by respondents as a potentially effective incentive for encouraging adoption of the Framework. However, certain respondents did suggest existing recognition programs that could be applicable to Framework adoption. For example, a respondent noted that the Federal Government could establish a certification program to publicize that implementing entities have adopted the Framework, similar to the Payment Card Industry Data Security Standard certification. Another respondent noted the potential benefit of a "cybersecurity excellence" award in which participants could demonstrate their adherence to the Framework, which would then be evaluated by DHS or a third-party and could be reward by a qualifying moniker. A similar suggestion included authorizing certified organizations to use a particular image or logo on publicity materials to demonstrate the commitment of the awardee to cybersecurity.

3.4.6. Rate-Recovery for Price-Regulated Industries

The potential benefit of rate-recovery for cybersecurity costs for price-regulated industries was noted by several respondents. A common observation was the inability of price-regulated industries to invest in

cybersecurity controls without the ability to pass on associated costs to a customer base. A utility trade association noted the potential effectiveness of directing the Federal Energy Regulatory Commission (FERC) to develop a cost recovery mechanism "allowing companies to go before the Commission to recover prudently incurred costs as a result of complying with federal cybersecurity mandate." Presumably such an approach could be used for other price-regulated industries, as well.

3.4.7. Security Disclosure

Mandated security disclosure was generally discussed by respondents as a disincentive for adopting the Framework. A respondent in the telecommunications sector noted: "The public disclosure of such attacks will do little – if anything – to compel such owners and operators to avoid security breaches, since they already have substantial incentives to do so. In fact, rather than act as an incentive, the public disclosure of such breaches would only serve to educate the attackers and increase the risk." Rather, respondents suggested that disclosure of security breaches should be encouraged as a voluntary best practice to promote information sharing on significant threats and vulnerabilities, but that barriers to disclosure such as potential liability should be resolved. Respondents further explained that breach disclosure, if encouraged or mandated, should be directly connected with a recommended cybersecurity mitigation to incentivize appropriate investment; otherwise such disclosures may be ineffective or encourage misallocation of resources.

3.4.8. Streamline Information Security Regulations

Respondents repeatedly cited inconsistent, overlapping, and duplicative information security regulations and guidelines as limiting standardized and measurably effective cybersecurity, and encouraged the government to reduce both the number and complexity of such requirements. A respondent suggested that owners and operators could be given credit for Framework adoption if they can demonstrate adopting similarly stringent standards recommended by their particular sector. Similarly, another respondent suggested a "Good Actor" benefit in which entities that pass an audit or review under one standard would be granted a time-defined exemption from similar reviews under duplicative regulations. Respondents also encouraged the preemption of state and local regulations, including privacy, tort, and contract laws that may impose obligations duplicating or conflicting with the Cybersecurity Framework. Respondents further suggested that the Framework should align existing regulations that artificially distinguish between sectors to ensure that entities providing functions across multiple sectors will be held accountable to a single standard.

3.4.9. Subsidies

Several respondents reported that costs are one of the most significant barriers to sufficient investment in effective cybersecurity, and that directing federal funding toward specific, Framework-compliant solutions could provide an incentive for Framework adoption. One respondent noted that "Federal subsidies and grants have been used successfully in other contexts in order to achieve important public policy goals when the conditions for obtaining such subsidies do not discourage their use, and their application in the cybersecurity environment could be appropriate." Notably, respondents did not differentiate between subsidies and grants in most cases, instead discussing all government transfer

payments under a single category. DHS' research does make the distinction, however, and finds it meaningful.

3.4.10. Tax Incentives

Respondents also noted the use of tax incentives in encouraging behavioral changes, such as the residential energy tax credit and the first-time home buyer credit, and the potential effectiveness of such incentives in reducing the fixed costs associated with cybersecurity investment. Among suggested tax incentives were the accelerated depreciation of cybersecurity-related hardware and software, as well as tax credits and deductions for cyber-related personnel, and capital investment for organizations choosing to adopt the Cybersecurity Framework. A respondent from the financial sector suggested tax incentives based upon Statement of Position 98 of the Financial Accounting Standards Board, which provides guidance in accounting for the costs of computer software. Under this model, costs associated with Framework adoption could be tax deductible or amortized over a specific period of time. Uniquely, a respondent also suggested that tax incentives be provided to non-critical infrastructure businesses that contract with Framework adopters, providing a market incentive to further encourage Framework adoption among critical infrastructure owners and operators. Another respondent suggested a "Capital Gains Tax Incentive for Cyber Assurance that would reward shareholders with a lower capital gains tax rate on the sale of assets (stocks and bonds) of corporations that voluntarily adopt the NIST Cybersecurity Framework."

Table 3. Commerce Notice of Inquiry Responses by Incentive Category

Key

- ● Indicates the incentive was recommended by the respondent
- ○ Indicates the incentive was discussed but not recommended by the respondent
- ☐ Indicates the incentive was neither discussed nor recommended by the respondent

Commerce NOI Respondent		Grants to Unregulated Industries	Rate-Recovery for Price Regulated Industries	Insurance	Liability Considerations and Legal Benefits	New Legislation: Cyber SAFETY Act	Prioritized Technical Assistance	Procurement Consideration	Public Recognition	Security Disclosure	Streamline Information Security Regulations	Subsidies	Tax Incentive
1	Advanced Cybersecurity Center	●		●									
2	American Association for Laboratory Accreditation								○				
3	American Fuel and Petrochemical Manufacturers	○	○	●	●	○						○	○
4	American Gas Association	●	●		●								
5	American Insurance Association			○					●		○		
6	American Petroleum Institute				○		○				○		
7	American Public Power Association				●						○		
8	atsec							○			○		○
9	Booz Allen Hamilton	○		●	○				●		○		
10	Bryan Rich												
11	Business Software Alliance			●									●
12	CACI				○			●			●		

	Commerce NOI Respondent	Grants to Unregulated Industries	Rate-Recovery for Price Regulated Industries	Insurance	Liability Considerations and Legal Benefits	New Legislation: Cyber SAFETY Act	Prioritized Technical Assistance	Procurement Consideration	Public Recognition	Security Disclosure	Streamline Information Security Regulations	Subsidies	Tax Incentive
13	Covington & Burling/Chertoff Group				●	●		●			○		○
14	DCS Corp			●									
15	Donald Edwards								●				
16	Dong Liu			○	●				●			●	
17	E8dison Electric Institute				●								○
18	Electric Power Supply Association		●										
19	Emmanuel Adeniran	○			●		●					○	
20	Encryptics			●								●	
21	FCC				○						○		●
22	Financial Services Sector Coordinating Council	●			●						●		●
23	Gary Fresen				●								
24	Honeywell				●		●						●
25	Internet Infrastructure Coalition				●						●		
26	Internet Security Alliance	○	○	○	●	○	○	○	○	○	○	○	○
27	IT SCC				○							○	
28	Los Angeles Department of Water and Power	●		●	●		●					●	
29	Marsh			●									
30	Microsoft			●				●			●		
31	Monsanto				○								

	Commerce NOI Respondent	Grants to Unregulated Industries	Rate-Recovery for Price Regulated Industries	Insurance	Liability Considerations and Legal Benefits	New Legislation: Cyber SAFETY Act	Prioritized Technical Assistance	Procurement Consideration	Public Recognition	Security Disclosure	Streamline Information Security Regulations	Subsidies	Tax Incentive
32	National Cable and Telecommunications Assoc.				●			●			●		○
33	National Electrical Manufacturers Association				●			●					
34	National Rural Electric Cooperative Association			●	●	●							
35	NCTA- The Rural Broadband Association				●								
36	Robin Ore	●		○	○								○
37	San Diego Gas & Electric and Southern California Gas Company		●		●			●		●			
38	Sasha Romanosky			●	○					○		○	●
39	Southern California Edison										●		
40	Telecommunications Industry Association			●	●								●
41	Terrence August & Tunay Tunca				●				○			●	
42	U.S. Chamber of Commerce				●	●		●			●		
43	US Telecom Association	●	○		●	○	○			○	●	●	
44	Utilities Telecom Council				●						●		●
45	Voxem Inc.												●

Insights on governance, risk and compliance

October 2013

Under cyber attack

EY's Global Information Security Survey 2013

EY

Building a better working world

Contents

Today's cyber realities

You could be under cyber attack — now! 2

A significant percentage of executives reading this report will soon learn that hackers have breached the security perimeter of their organization.

Improve

Awareness of cyber threats propels improvements 3

Our survey suggests that many more organizations recognize the extent and depth of the threats they face and that they are making improvements to protect themselves. Yet, despite the progress they are making, organizations need to do more — and quickly — to combat cyber risks that are increasing exponentially in number and complexity.

Expand

Leading practices to combat cyber threats 9

Although organizations have made great strides in improving their information security programs, our findings suggest that there are 10 specific areas that leading organizations should take to expand on these improvements.

Innovate

To survive, innovation must power transformation 14

We asked respondents to rank 13 emerging technologies according to importance, familiarity and confidence in capabilities. The results show that organizations are placing more emphasis on what is in front of them and what they know and not nearly enough on what may be just around the corner or appearing on the horizon.

Conclusion

Combating cyber attacks requires leadership and accountability 20

The pace of technology evolution will only accelerate in the years to come — as will the cyber risks. Addressing these risks requires proactive thinking with tone-from-the-top support. Not considering risks until they arise gives cyber attackers the advantage.

Welcome

Paul van Kessel
EY Global RISK Leader

Ken Allan
EY Global Information Security Leader

Welcome to *Under cyber attack: EY's Global Information Security Survey 2013*.

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless and often politically motivated. When one tactic fails they will try another until they breach an organization's defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services and the collection/analysis of big data.

In addition, regulators are seeing this threat and are putting pressure on businesses to comply with rules and regulations, to admit to cyber breaches publicly, and to submit to detailed examinations. Businesses should not allow themselves to fall into the regulatory trap; leaders should look to what they need to do to manage their residual risks and fully understand where they stand.

Organizations must be prepared to combat against and manage and mitigate cyber attacks that can occur anytime, anywhere.

Our 16th annual information security survey explores three levels of response to cyber risk in an environment where cyber attacks are numerous, constant and increasingly complex:

1. **Improve** – Improvements and challenges: the improvements organizations are making to address the cyber threats they currently face and the challenges that still need more work
2. **Expand** – Leading practices: the steps leading organizations are taking to stretch or expand current improvements to more proactively address new threats
3. **Innovate** – Innovation in security: the solutions organizations need to develop to address technologies that are just around the corner or may be soon appearing on the horizon

Our survey explores the experiences of more than 1,900 client organizations and how they are responding to today's cyber threats. In addition to our survey, we interviewed a number of senior executives representing organizations that in EY's experience demonstrate leading practices in addressing cyber risks. We have also used analyses from EY security professionals and secondary research to provide depth and context to our survey findings.

We would like to extend a personal note of thanks to all of our survey participants. We appreciate the time they took to share their experiences with us.

We welcome the opportunity to discuss in greater detail the implications of these findings and look forward to hearing from you.

Paul van Kessel
EY Global RISK Leader

Ken Allan
EY Global Information Security Leader

Today's cyber threats

You could be under cyber attack — now!

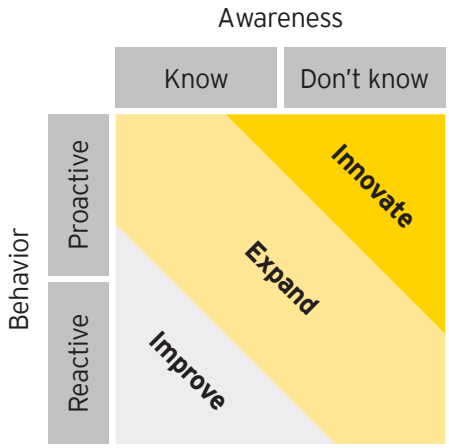
Cybersecurity attacks have increased exponentially in the last few years. Every day, as the rapid-fire evolution of technology marches forward, new, more complex cyber risks emerge, threatening significant harm to an organization's brand and bottom line. Everyone and every organization is a target.

In the time it takes to review this report, a significant percentage of readers will learn of an attack that will have breached their organizations' security. The infiltration could have occurred days, weeks or even months ago — and they don't even know it. When the knowledge and magnitude of the breach does surface, the associated costs to the organization may be staggering. We need only to think of the high-profile attacks on well-known brands and organizations that appear in the world press daily, and consider the number of data records lost and the financial and reputation costs, to understand the impact.

In our Global Information Security Survey 2012 report, titled *Fighting to close the gap*, we addressed the notion of a widening gap between the current state of an organization's information security program versus where it needs to be to successfully defend the more insidious cyber attacks the majority of organizations face. In our Global Information Security Survey 2013 report we find that organizations are moving in the right direction, but more still needs to be done — urgently.

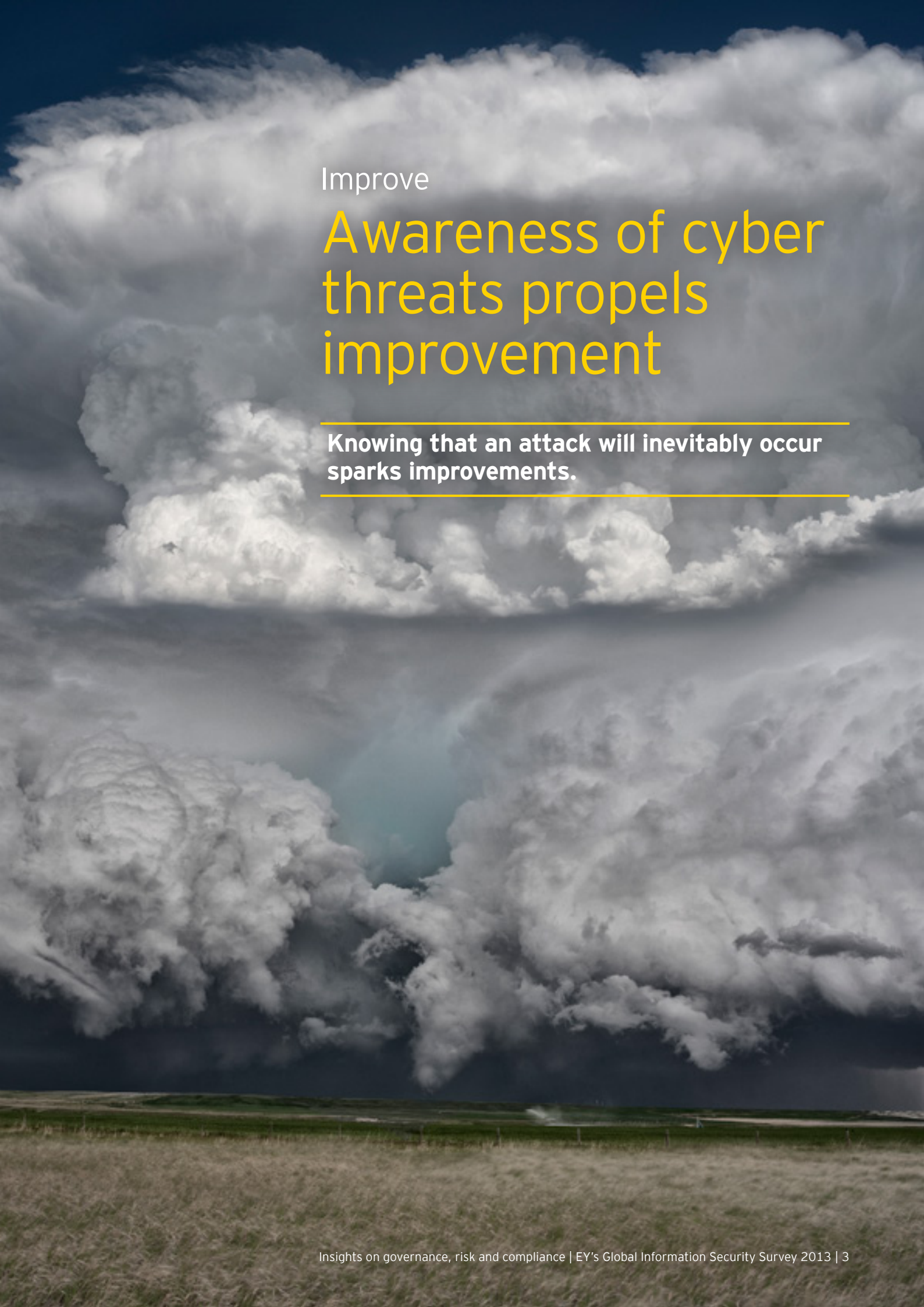
We have structured our Global Information Security Survey 2013 report to explore three areas:

1. **Improve.** For many organizations, this is the current state. Over the past year, organizations have made substantial progress in improving their defenses against cyber attacks. Yet their position remains reactive, addressing the threats they know, but not seeking to understand the threats that may be just around the corner.
2. **Expand.** Leading organizations are taking bolder steps to combat cyber threats. They are more proactive in determining both the known and unknown risks within their security programs. However, there remains room to expand security measures.



3. **Innovate.** Organizations aspiring to be information security innovators need to set their sights on new frontiers. These organizations need to continuously review, rethink and potentially redesign their entire information security framework in order to be better prepared. In many cases, innovating may require a fundamental transformation of the information security program to proactively fortify against both the known and the unknown risks in the cyber risk environment.

In the pages that follow, we explore the actions organizations have taken to address current threats, how leading organizations are looking beyond today's threats in an effort to prepare for the cyber risks that may be on the horizon, and how new technologies and new ideas can help organizations proactively prepare for a future that is certain to challenge even the most sophisticated and robust information security programs and functions.



Improve

Awareness of cyber threats propels improvement

Knowing that an attack will inevitably occur sparks improvements.

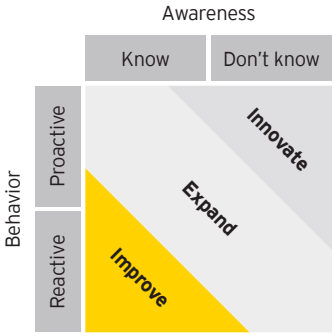
70%

of organizations indicate that information security policies are owned at the highest organizational level

76%

of organizations conduct self-assessments or commission an independent external assessment of the information security measures taken by third parties with data access

Awareness of cyber threats propels improvement



Our survey indicates that many organizations recognize the extent and depth of the threats they face – from the top of the organization to the shop floor. For nearly three- quarters of organizations surveyed, information security policies are now owned at the highest organizational level.

In 10% of organizations the information security function reports directly to the CEO. Information security professionals in 35% of the organizations we surveyed present information security to the board and those at the top of the governing structure on a quarterly basis; a little more than 1 in 10 report monthly. In our Global Information Security Survey 2012 the percentage of information security professionals who reported to senior executives monthly was zero.

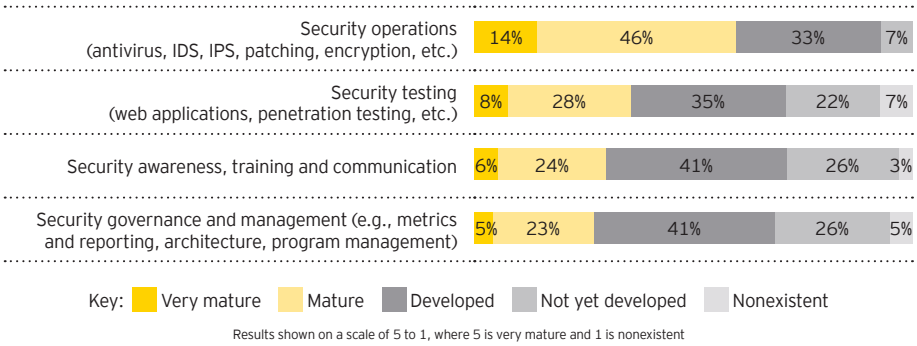
Information security is now seen as vital to the ongoing health and success of the organization. Formal security operations (antivirus, IDS, IPS, patching, encryption, etc.) are mature in a majority of organizations.

Data protection is no longer being treated as another line item in a contract or something that organizations simply assume third parties do. Three-quarters of respondents indicate that their organizations mandate self-assessments, or commission an independent external assessment, of the information security measures performed by external partners, vendors or contractors who have access to their data.

However, although organizations have made strides in the right direction, there remains room for improvement. Many organizations are increasing investment in information security, yet many information security professionals continue to feel that their budgets are insufficient to address mounting cyber risks.

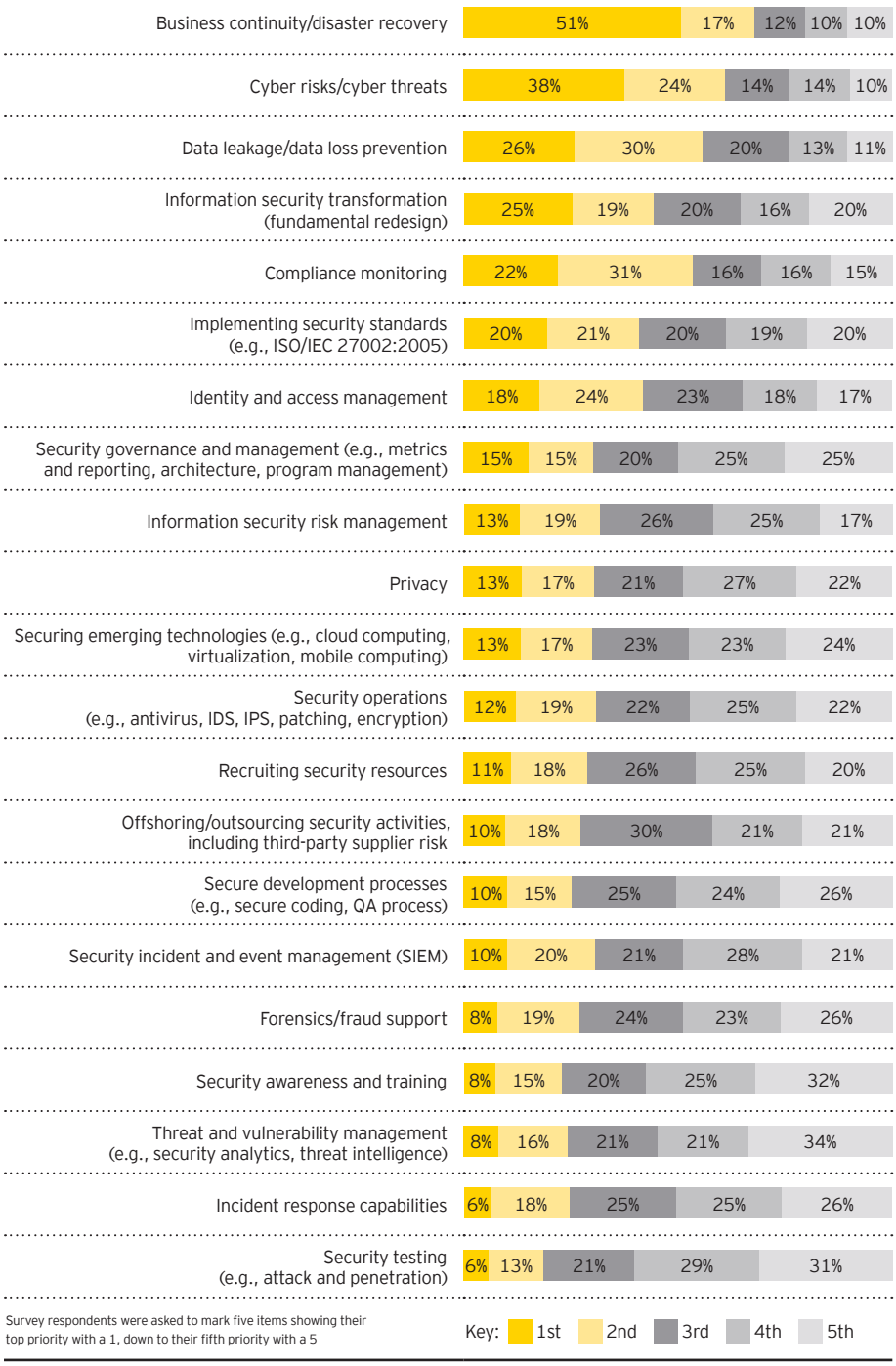
Similarly, although organizations feel they are addressing the right priorities, many indicate that they do not have the skilled resources to support their needs. Even though the trend is shifting focus away from "keeping the lights on" and toward improvement and innovation, many organizations are still leaving themselves exposed. Furthermore, a lot of organizations with technologies installed and running (antivirus, IDS, IPS, etc.), still find that the configuration and the processes around them (e.g., patch management, threat intelligence) are not adapted to today's needs. It's not surprising that many organizations feel that some aspects of their security management processes are not yet fully mature.

Maturity of information security management processes in surveyed organizations



Results shown on a scale of 5 to 1, where 5 is very mature and 1 is nonexistent

Which information security areas do you define as "top priorities" over the coming 12 months?



Survey respondents were asked to mark five items showing their top priority with a 1, down to their fifth priority with a 5

35%

of organizations have their information security professionals present information security to the board or members of the top governing structure quarterly

Based on findings from our Global Information Security Survey 2013, the following pages show the leaps forward that organizations are making in the fight against cyber crime; these are placed alongside the steps that they still need to make in today's environment.

The leaps that organizations are making

68%

of respondents state business continuity and disaster recovery as their top two priorities

Organizations are making moves to focus more on the right priorities

Generally, organizations name business continuity and disaster recovery as their top information security priority for the next 12 months. Cyber risks and cyber threats, data leakage and data loss prevention, information security transformation, and compliance monitoring round out the top five.

Financial institutions place even greater emphasis on cyber risk and cyber threats. It is also a concern for any organizations with US$1 billion or more in revenue.

43%

of organizations indicate that information security budgets are on the rise

Organizations are investing more in information security

Overall, 43% of survey respondents indicate that their budgets are on the rise.

Within the government and public sectors, some respondents reported budget increases, but a majority indicate that their budgets have stayed the same as last year.

Small businesses with a turnover of less than US$10m or businesses located in rapid-growth markets report the highest increases as a percentage of their budgets.

46%

of spend will be directed toward security improvement, expansion and innovation in the next 12 months

Organizations are shifting their focus from operations and maintenance to improving and innovating

Although security operations and maintenance remains important, it is less of a focus for the next year than for the year before.

Respondents' attention is shifting toward security improvement, expansion and innovation. In the year to come, 46% of spend will be directed to these initiatives.

46%

of organizations align their information security strategy to the organization's business strategy

Organizations demonstrate alignment among strategies and drivers

Nearly half of the organizations we interviewed align their information security strategy with the organization's business strategy; more than half align their information security strategy with their IT strategy.

Financial services organizations exhibit the strongest strategy alignment.

This suggests a consolidation of organizational strategies and drivers, as well as an increased understanding of the imperative for an information security strategy, regardless of an organization's size or industry.

68%

of organizations say their information security function partially meets organizational needs

Efforts to improve cybersecurity programs are growing

Since 2012 there has been a small drop (6% versus 8%) in the number of organizations saying that their information security function does not meet organizational needs, and a slight increase in those who say that it fully meets their needs.

At the same time, 68% believe that their information security function partially meets organizational needs and that improvements are underway. Among financial services organizations, this number rises to 74%.

Overall, information security functions are making the right improvements to more effectively meet the needs of the business and create value for the organization.

The steps that organizations still need to take

Information security departments continue to struggle with a lack of skilled resources, executive awareness and support

Although information security is focusing on the right priorities, in many instances, the function doesn't have the skilled resources or executive awareness and support needed to address them. In particular, the gap is widening between supply and demand, creating a sellers' market. Fifty percent of recipients cite a lack of skilled resources as a barrier to value creation. Similarly, where only 20% of previous survey participants indicated a lack of executive awareness or support, 31% now cite it as an issue.

As a result, although the information security department itself is making great strides toward improvement, support from the rest of the organization appears to lag behind.

50%

of respondents cite a lack of skilled resources as a barrier to value creation

Information security departments are still feeling the pinch

Although budgets are on the rise, information security functions continue to feel that budget constraints are their biggest obstacle to delivering value to the business. Sixty-five percent cite an insufficient budget as their number one challenge to contributing to the levels the business expects; among organizations with revenues of US$10 million or less this figure rises to 71%.

Information security's number one obstacle to success mirrors the business's perception of their value. Although 17% of respondents indicate that information security fully meets the needs of their organization, 68% continue to feel that the department only partially meets organizational needs, with improvements underway.

Information security organizations need to make a better job of articulating and demonstrating the value of investments in security.

65%

of respondents cite budget constraints as their number one obstacle to delivering value to the business

Despite the security improvements organizations have made, many remain exposed

Nearly one-third of organizations still do not have a threat intelligence program, and slightly more than one-third have an informal program. In terms of vulnerability identification, nearly one in four has no program.

Financial services are the most mature of the industries we interviewed, although organizations of US$1 billion in revenue or more also reported higher levels of maturity in their cybersecurity programs.

However, organizations, regardless of industry or size; should be concerned by the overall lack of maturity and rigor in a number of security areas. These critical issues must improve. In many cases, organizations will need to urgently invest more to improve and innovate. After all, the cost of a breach can be far more costly.

35%

of respondents feel they are leaders or pioneers in security programs

A lack of alignment in other critical areas is still too common

Although there have been improvements in alignment to business and IT strategies (for example, threat modeling needs to actively identify all areas of risk and move from a technology-led activity to a business-focused activity), many organizations have made no moves to improve their alignment with the organization's risk appetite or with today's risk environment. Financial services organizations are more aligned, while organizations in rapid-growth markets are less aligned.

This lack of alignment suggests that when setting budgets or determining resource requirements, too few organizations consider the cyber risks they are prepared to accept or must defend against at all costs, and far too many organizations only look inward to satisfy themselves that they are adequately protected against cyber risks – a view that may be costly when an attack occurs.

62%

of organizations have not aligned their information security strategy to their risk appetite or tolerance

Threats are growing too, often at a faster pace

Thirty-one percent of respondents say the number of security incidents within their organization has increased over the last 12 months by at least 5%.

When taking action to improve their information security function, organizations need to determine whether the improvements they are making will address the expected volume and frequency of existing and emerging threats, and whether they can implement them fast enough to keep pace with the threat landscape. Very specifically, organizations need to understand how effectively these actions will help to protect their business processes.

59%

of organizations cite an increase in external threats

31%

of respondents say the number of security incidents have increased over the previous 12 months

32%

of respondents say that phishing has most changed their risk exposure

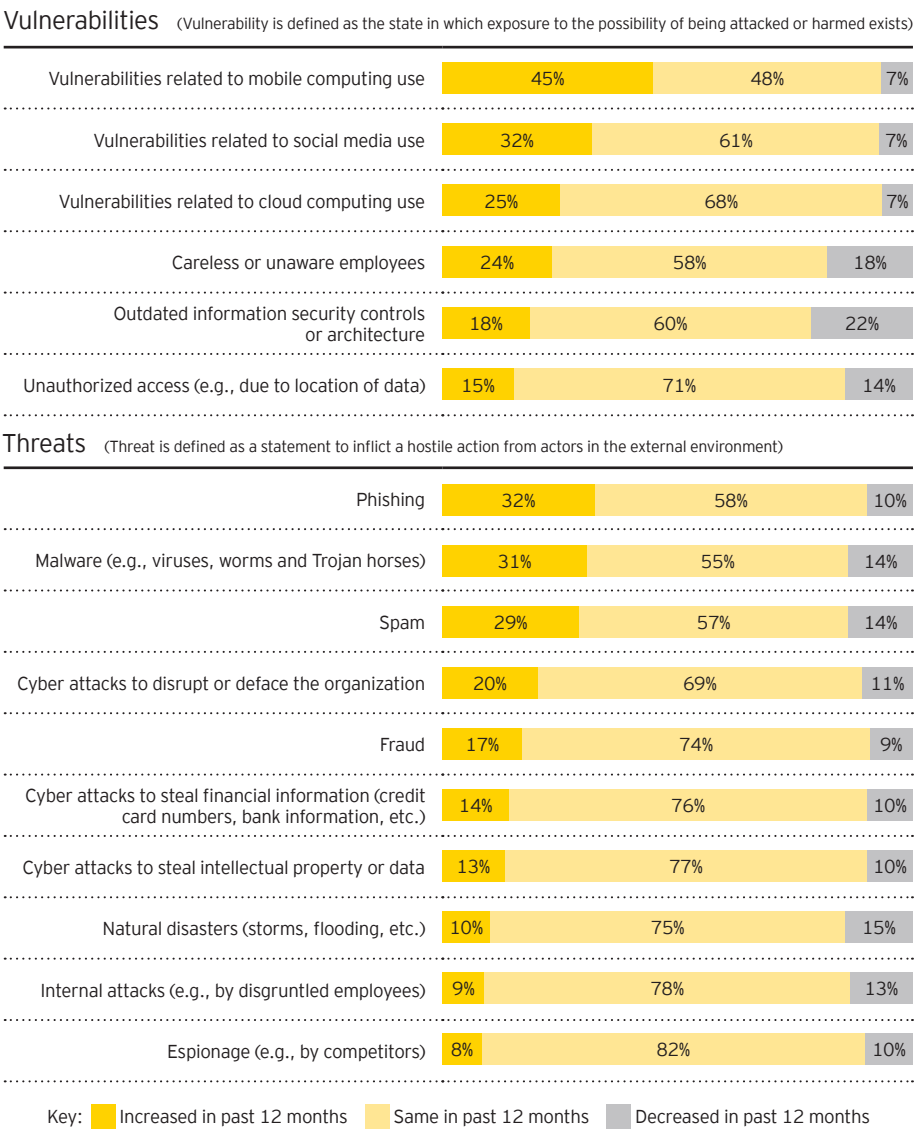
45%

of respondents say mobile computing has most changed their risk exposure

Despite the efforts organizations have made over the course of the last 12 months to improve their information security programs, much more still needs to be done. Only 23% of respondents rated security awareness and training – a key component of continuous improvement activities – as their number one or two priority; 32% ranked it last. The only security area rated a lower priority by more respondents was threat and vulnerability management, an activity for which 31% of respondents had no program; this is surprising, as without it organizations have little visibility into where the cyber threats are and where a cyber attack may be coming from.

For as much progress as organizations have made, many organizations still have a long way to go. As the rate and complexity of cyber attacks continue to increase, organizations need to act quickly to avoid leaving themselves exposed to a costly and brand-damaging security incident that shakes the confidence of consumers and shareholders.

Based on actual incidents, these threats and vulnerabilities have most changed respondents' risk exposure over the last 12 months

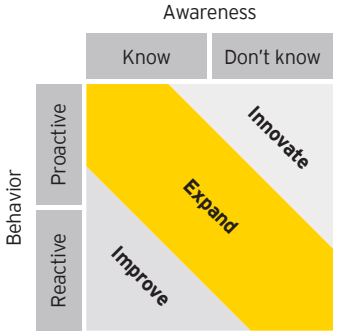


Expand

Leading practices to combat cyber threats

Organizations must signal support from the top to be proactive and ready for the unknown. Those that are satisfied with merely being reactive may not survive the next attack.

Leading practices to combat cyber threats



For the most part, organizations have improved their information security programs over the last 12 months. However, our findings suggest that leading organizations take improvements one step further. In particular, there are 10 areas that we have grouped into four categories where we see leading companies expanding improvement opportunities. See diagram on pages 12-13.

Commitment from the top

- **Board support.** Organizations need executive support to establish a clear charter for the information security function and a long-term strategy for its growth.

Organizational alignment

- **Strategy.** Information security must develop strong, clearly defined relationships with a wide range of stakeholders across the business and establish a clearly defined and formalized governance and operating model.
- **Investment.** Organizations need to be willing to invest in cybersecurity.

People, processes and technology to implement

- **People.** Today's information security function requires a broad range of capabilities with a diversity of experiences. Technical IT skills alone are no longer enough.
- **Processes.** Processes need to be documented and communicated, but information security functions also need to develop change management mechanisms to quickly update processes when opportunities for improvement arise.
- **Technology.** To gain the most value from a technology solution, information security functions must supplement their technology deployment efforts with strategic initiatives that address proper governance, process, training and awareness.

Operational enablement

- **Continuous improvement.** Organizations must establish a framework for continuously monitoring performance and improving their information security programs in the areas of people, process and technology.
- **Physical security.** Organizations should ensure that all their information security technology is physically secure, especially with consideration for access to Wi-Fi. A security operations center (SOC) can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.
- **Analytics and reporting.** Signature and rule-based tools are no longer as effective in today's environment. Instead, information security functions may wish to consider using behavior-based analytics against environmental baselines.
- **Environment.** Information security requires an environment that includes a well-maintained enterprise asset management system (which includes criticality of supported business processes) to manage events associated with business priorities and assess the true risk or impact to the organization.

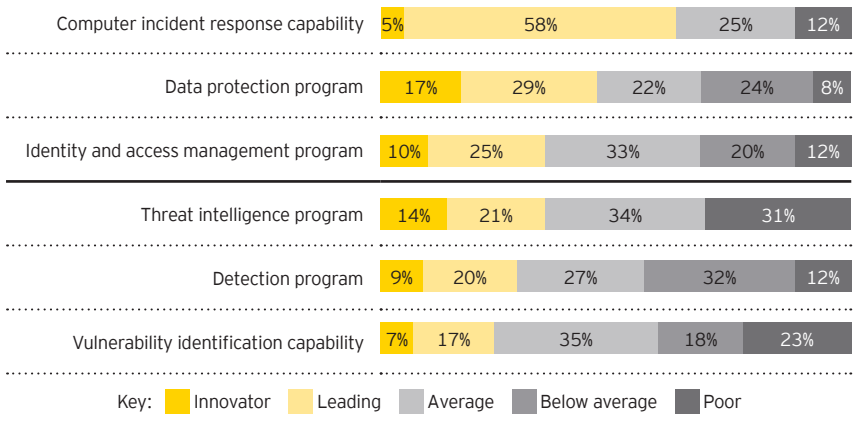
In addition to our survey findings, this year we elected to interview a select number of executives from organizations that, based on our experience in information security, we believe are more successfully protecting their organization from cyber risks and threats by being proactive and focused on the unknown.

We considered these interview responses within the context of our survey findings. We then augmented these results by drawing on the knowledge of our information security professionals and our considerable experience serving our clients. By layering the survey data, client experience and EY knowledge, we developed a clear understanding of the cascading, cumulative effect each improvement area identified has within the four expanded improvement categories. Ultimately, if an organization does not embark on its journey from the beginning (i.e., seek to make improvements at the "commitment from the top" stage), then it cannot achieve lasting change, or expand on previous successes, in any of the categories that follow.

Information security program maturity scale

In our survey, we asked respondents to rank the maturity of their information security programs in six key areas.

The responses to well-established information security approaches, such as identity and access management program, are below what is needed, and more recent approaches, such as threat intelligence and vulnerability identification, are less mature and need more attention.



We have taken the responses and ranked them from innovator to poor. Organizations are innovators if they have an advanced program and poor if they have no program at all.

> Executives at the highest level of an organization need to commit to strive for information security maturity – and be accountable for achieving it. Without it, none of the other improvements the information security function seeks to implement will realize their intended benefits.

On the following pages we have captured the leading practices we noted during our one-on-one interviews with clients. Implementing one or more of these leading practices in isolation will help; it will improve the status quo of your information security. However, implementing leading practices in each of the 10 focus areas in concert will result in a significant expansion of your cyber threat responses and in a step change in your information security level.

The leading practices that enable improvement

Commitment from the top

Organizational alignment

"Our information security solution has changed from the traditional architecture of protecting the business practices itself to protecting the services that can complete the overall business practices. This turns the closely business coupled model into a relatively flexible loosely coupled model, providing security functions by means of services, packaging security services to release into the system."

Financial services organization

"From our point of view, the most successful practice within information security was the changing of the idea: from considering issues solely on the operational level in the past, to the new approach, which is risk-oriented. Analysis, reporting, presentation and other methods are used to spot potential problems, and these problems are communicated and solved together with the business departments now in a more active way, which was rather passive in the past."

Technology organization

"We drive the self-optimization process of information security management system through internal/external monitoring, including internal audit, internal information security risk assessment, internal security checking, external information technology audit, external compliance checking, etc."

Financial services organization

"It's important to have skilled professionals with business vision. The biggest challenge in today's security market is to find professionals who are capable to innovate and adapt to the changes in the required speed."

Mining and metals organization

Executive and board support

- Articulate risk appetite to provide clear, unambiguous direction
- Incentivize timely remediation of security issues, e.g., via internal audit or information security functions
- Measure information security performance and the criteria for success
- Foster an information security culture throughout all levels of the organization
- Understand how security events can impact the business, its services and its products
- Integrate information security insights directly into management decision-making processes
- Translate information security threats into their impact on the P&L and balance sheet

Strategy

- Identify and involve all relevant stakeholders
- Establish an organization-wide SOC, including comprehensive threat intelligence and vulnerability monitoring
- Align security strategy with overall business strategy
- Determine which security functions sit in-house versus outsourced and in the cloud
- Increase business and stakeholder confidence through use of trusted standards (ISO, COSO, COBIT, etc.) and consider alignment or formal certification
- Conduct independent third-party assessments – then get a second, independent opinion
- Define what is considered to be a "secure" organization; define KRI and KPI to monitor success
- Leverage the expertise of partners and vendors
- Build an information security organization and operating model that anticipates rather than reacts

Investment

- Identify who pays for cybersecurity
- Define a holistic risk framework to evaluate the increasing risk landscape
- Prioritize security initiatives to drive security investment
- Categorize expected benefits, e.g., brand protection, risk reduction, improved compliance and cost reduction
- Decrease the spend on maintenance and incidents; increase the spend on improvement and innovation

Every business is a potential target for a cyber attack. The motives, methods and opportunities may differ, but we have found that organizations at any one of the following stages in their life cycle are even more at risk:

- **Major organizational or structural change.** Although new technologies are driving marketing and customer-oriented initiatives, accompanying information security measures are not necessarily keeping up the pace. Marketing and development functions are not always as aware of – or prepared to respond to – the risks and threats that come with new technologies. Organizations can also disconnect and distract employees, causing them to forget or discard tested security measures and protocols.
- **Mergers and acquisitions.** New systems, policies, procedures and safeguards can create gaps in information security systems, measures and protocols. Mergers and acquisitions also often come with headcount reductions, activating many highly motivated disgruntled ex-employees familiar with their organizations' systems, processes and security measures.
- **Entering new markets.** New markets usually means new processes, vendors, buyers, systems – even new languages and cultures. All of these factors come with varying levels of security risk and threat awareness. Unfamiliar governmental regulations on privacy, communications and data security further complicate the security environment.
- **Headline grabbers.** Hackers and cyber attackers often use public relations disruptions to target companies whose attention is focused elsewhere. Employees and shareholders can act erratically and unpredictably, straining the organization's ability to identify and address an increased volume of threats on a variety of platforms. Reactive "emergency" actions designed to solve a short-term problem run the risk of actually creating openings and issues that can pose long-term risks

People, processes and technology to implement

Operational enablement

People

- Raise employee awareness of their security responsibilities and appropriate use of organization's assets, IP, data and technology
- Screen and hire the right people with the right skills and competencies, including those in high-risk roles
- Make information security part of the performance assessment of employees
- Know and control who holds elevated privileges
- Cultivate "security knowledge champions" in the business

Processes

- Use tested, enforceable contract clauses to make partners and vendors responsible and accountable for information security
- Describe information security processes to gain an understanding of rules and procedures and get everyone speaking the same language
- Align to a recognized information security standard, e.g., ISO 27001
- Ensure information security is an integral part of the GRC (risk management) function of the organization, not a stand-alone function
- Establish ongoing assurance monitoring of controls within outsourced third-party services
- Differentiate between compliance and regulatory requirements and defining the threat landscape
- Involve the business in the risk management process to improve key risk identification and increase security awareness
- Implement cyber governance into the business and business processes
- Anticipate potential security breaches and build adequate incident response and communications approach

Technology

- Build clear relationships among information technology, operational technology and information security
- Balance the technology choices with the threats and vulnerabilities the technology brings
- Ensure information security is an integral part of IT projects; as a result new information systems are secure from the start
- Understand the inventory of technologies you rely on and develop specific standards for them
- Develop the capability to monitor technology assets hosting sensitive data and critical business services in real time
- Routinely test security at an application level as well as an infrastructure level
- Align your information security efforts to the safety of your product, the robustness of your services and/or the customer experience
- Make information security part of your product/service offering

Continuous improvement

- Leverage intelligence from industry bodies, law enforcement agencies, peer organizations, regulatory authorities and professional advisers
- Continually reassess new technologies and the threat landscape to confirm focus is on the right priorities
- Establish a security simulation sandbox or capability to test security from a hacker's perspective
- Always remain vigilant; listen to what is going on in the market, understand new trends in information security and new threats, and adjust the risk assessment accordingly
- Implement an innovation function within the information security function to anticipate information security issues in new technologies

Functional security

- Understand the link between physical security and network security in light of wireless devices
- Effective prevention requires close cooperation between information security, human resources, IT and legal
- Improve coordination between physical, IT security and information security
- Systematically perform risk analysis on emerging technologies

Analytics and reporting

- Commission independent assessments from multiple parties within and outside the organization to assess the effectiveness of GRC and the information security function
- Build a holistic capability to correlate seemingly unconnected events and to detect behavioral anomalies using analytical tools and models
- Establish a dedicated security assurance reporting capability in order to measure security vulnerability and compliance improvements
- Investigate and assess current external threat level, then provide early warnings to IT and the business and establish crisis response teams
- Present to the board the impact of cybersecurity threats on the P&L, balance sheet, reputation and brand
- Coordinate with service providers and certification bodies to exchange information and leading practices

Environment

- Align first, second and third lines of defense to re-confirm responsibilities and reduce overlap in duties
- Effective prevention requires close cooperation between information security and IT
- Know critical assets and their vulnerabilities; monitor attacks on infrastructure level closely

"Key to successful practices is comprehensibility and applicability. People prefer practical hands-on in contrast to complex theoretical approaches. You need to identify the information-related risks across the business process using straightforward, standardized questions and challenge the received information by verification, then use this information to identify your 'crown jewels' and consider all relevant stakeholders. Then you can outline the business impact and the risk assessment, in combination with proposed measures to mitigate the risk."

Oil and gas organization

"Partnership with third parties has enabled us to design an information security strategy and associated improvement program with external market knowledge and expertise, as well as to flex resource requirements to help with surges in demand for security architecture and design, security testing and security incident response and investigation. Co-sourcing/outsourcing is viewed as much if not more as a capability enhancement play than it is for cost reduction."

Financial services organization

"It's vital to have the right players lined up in the 'Core Command Center' – the right functions (coordination among info sec, IT, line of business leaders, communications and marketing, physical security people. You need all the names in advance of the people who know all the right connections to all aspects of the business. And the right 'seniority' level has to 'be in the room' – i.e., people with decision-making authority in real time."

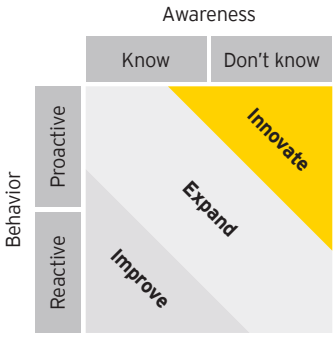
Financial services organization

Innovate

To survive, innovation must power transformation

Innovative information security solutions can protect organizations against known cyber risks and prepare them for a great unknown: the future.

Over the course of the last year, many organizations have made improvements to their current information security programs to better protect themselves from known cyber risks. Leading organizations have expanded the opportunities for improvement to more proactively anticipate both known and unknown cyber risks. However, to be a cyber threat innovator, organizations need to reach well beyond the 10 leading practices in four key categories that we have articulated. Innovators must constantly scan the horizon, searching for the vulnerabilities in each opportunity emerging technology brings.

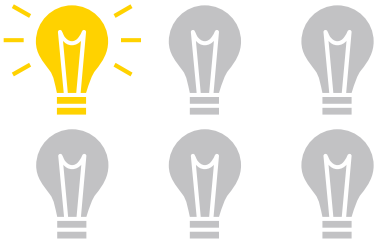


Budget allocations toward security innovation are inching their way up, enabling organizations to channel more resources and effort toward innovating solutions that can protect them against the great unknown: the future.

However, many organizations still feel that their budgets are insufficient to become innovating pioneers. As such, it is critical to focus time and effort when assessing new technologies to not only understand the benefits, but also the critical knowledge gaps and associated cyber risks: that is, an organization's familiarity with a technology and how capable it is to address these risks. Once the unknown becomes known, the organization can then prioritize and address the risks in order of importance.

50%

of respondents indicate that their budgets will increase anywhere from 5% to 25% or more in the next 12 months



14%

of spend in the coming 12 months will be on security innovation (emerging technology)

Emerging technologies and trends

In our survey, we ask respondents to rank by level of importance the following 13 emerging technologies and trends. We have grouped these technologies and trends into three categories: current, around the corner and on the horizon.

Current technologies

Current technologies have been on many organizations' radar for several years now and in many cases have already been implemented. These include:

- **Digital devices**, which includes the security and risk considerations for:
  - Smartphones and tablets
  - Software applications
  - Web-based applications (HTML5) and website design to fit mobile screens
- **Social media** in the context of a digital business enabler and network facilitator

Around the corner

Technologies around the corner have been a focus of consideration for a short while and may be close to broader implementation or adoption. These technologies include:

- **Big data**, which we describe as the exponential volume and complexity of data under management
- **Enterprise application store**, which encompasses associated costs versus increased productivity of employee requests for applications
- **Supply chain management**, in the context of how external assets (customers, suppliers, vendors, contractors and partners) impact security
- **Cloud service brokerage** as it pertains to how brokers manage cloud security, privacy and compliance issues
- **Bring your own cloud**, including personal cloud infrastructures that can be owned, managed and operated by an organization, third party or a combination of both, and may exist on or off the premises or concern data and applications access that only cloud owners manage

On the horizon

Technologies on the horizon are moving away from the concept or idea phase and one day may become reality. These technologies include:

- **In-memory computing**, which involves data storage in the main random access memory instead of complicated databases, allowing real-time analyses of high-volume data
- **Internet of things** (for example, embedded sensors, image recognition technologies), which are used in security programs but more often will be applied to our day-to-day lives
- **Digital money** and the associated regulations and legislation needed to address fraud and money laundering issues relating to mobile money services
- **Cyber havens**, where countries provide data hosting without onerous regulations

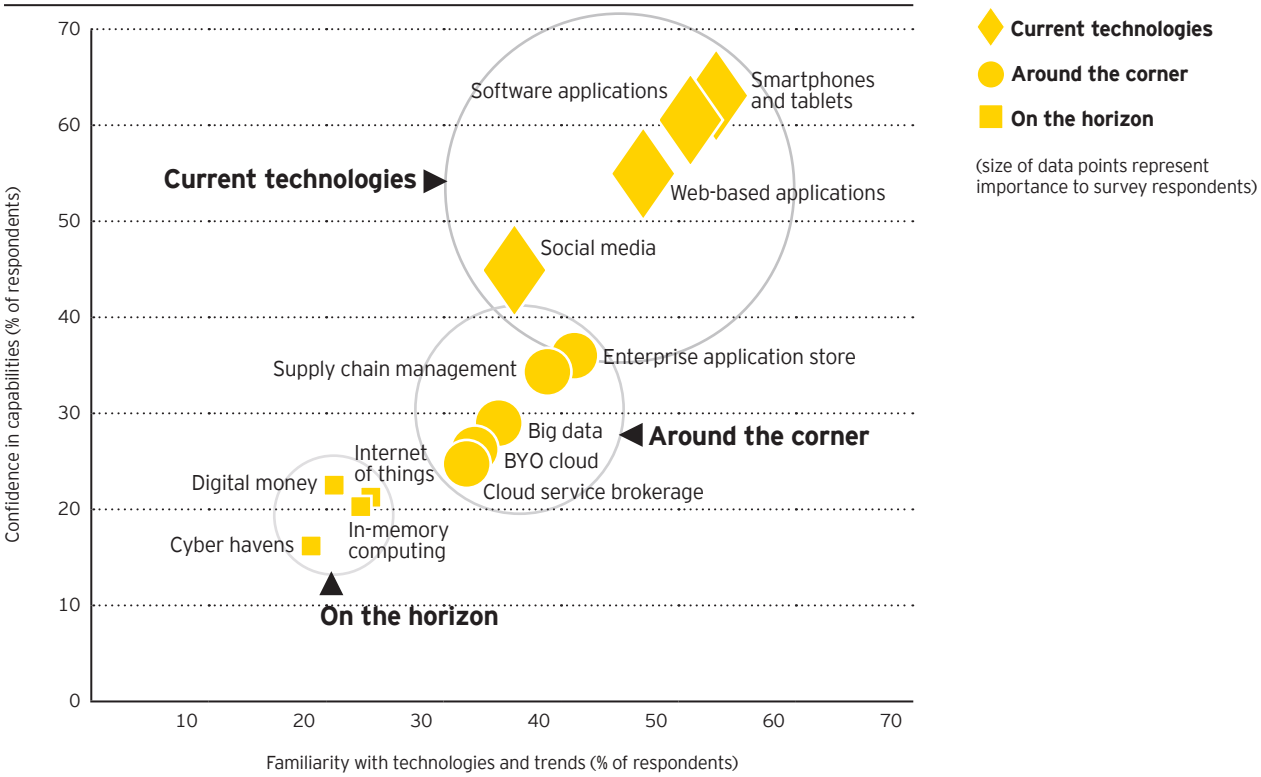
In addition to asking respondents to rank emerging technologies and trends based on their level of importance, we asked them to rank their level of familiarity with each, and then their confidence in being able to address the implications of these new technologies.

- **Familiar:** Are the emerging technologies known?
- **Capability:** Are we able to deal with the security implications of emerging technologies?
- **Importance:** How much focus do we put on emerging technologies threats?

We also asked our interviewees for their perspectives on emerging technologies and trends, like bring your own cloud. From these results, and the observations of our security professionals, we have developed a correlation diagram that ranks level of importance against the level of familiarity and capabilities.

The horizontal axis depicts familiarity, while the size of the circle indicates level of importance. Unsurprisingly there is a correlation between how familiar an organization is to how important it considers that technology to be. The vertical axis plots how confident an organization feels today in its capabilities to defend against cyber threats and minimize vulnerabilities.

Emerging technologies and trends

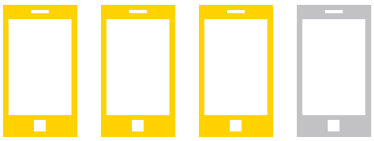


26%

say BYO cloud is important

19%

say in-memory computing is important



70%

find security of smartphones and tablets important

71%

find security of software applications important

High rankings for current technologies

As demonstrated in the "Emerging technologies and trends" correlation diagram (page 17), current technologies and trends carry the most weight in terms of level of importance, familiarity and confidence in capabilities. For the most part, organizations are aware of these technologies and in many instances have already adopted them.

However, although we expected a high score for digital devices, a score of 70% for smartphones and tablets is not high enough given the devices' ubiquity. A few years ago, organizations could not imagine employees using their personal smartphones and tablets for work purposes. In fact, bring your own device (BYOD) only entered the market in 2009; widespread adoption of BYOD has only occurred recently.

Yet, as we continue to hear about sensitive or confidential security breaches by those using smartphones and tablets, the question becomes: Who is responsible for the smartphone's data – employer or employee? And how often is the smartphone being updated and security notifications appearing?

As current technologies become further entrenched in an organization's network and culture, organizations need to keep in mind how employees use the devices, both in the workplace and in their personal lives. This is especially true when it comes to social media. Survey findings suggest that this continues to be an area where organizations still don't feel confident in their capability to address risks.

If organizations still don't have a high level of confidence after four years of mobile device use in the workplace, how will they face the challenge of managing and defending against personal and hosted clouds? Moreover, if organizations are putting all their energy into addressing current technology issues, how will they protect themselves against technologies that are just around the corner or are about to appear on the horizon?

Organizations need to be more forward-looking. As we see with digital devices and social media, organizations should have been preparing for current technologies as they were appearing on the horizon. If resources are still working to improve capabilities for technologies that are right in front of them or already behind them then they will have no time to prepare a defense that proactively protects the organization from technologies that are just around the corner.

Leading practice recommendations from some of our respondents:

- "If you have fallen behind, have two-way discussions with the business and IT – not to roadblock, or own or control, but to get things moving and make things happen." – *Retail and wholesale organization*
- "Privacy, security and fraud functions need to integrate. What customers and employees see as private information will have to change." – *Financial services organization*
- "The weakest element in information security is the human factor. As a result, we are constantly improving the awareness programs and introducing new security instruments." – *Financial services organization*
- "We see the threats and risks rising in the application landscape. Whereas we used to protect the network and the exposed systems, we now need to protect all systems – at application level – throughout the whole network, including the content of information used in applications (e.g., emails and attachments)." – *Retail and wholesale organization*

Average importance for technologies and trends that are just around the corner

Respondents rank technologies categorized as being around the corner (i.e., those that have been on organizations' radar for a period of time but may not yet be implemented or widely adopted) as average in terms of level of importance, familiarity and confidence in their capabilities to address related cyber risks.

Organizations typically view these technologies as offering opportunities to improve their performance and create competitive advantage. This is where familiarity and confidence in capabilities needs to increase today, as the importance of these technologies is likely to grow significantly in the near future.

The terms big data, supply chain management and enterprise application store (sometimes known as shadow IT) have already entered the corporate lexicon. Bring your own cloud and cloud service brokerage are as close to being adopted within organizations as BYOD was just a year ago. Organizations need to know now the cyber risks associated with these technologies, the organization's vulnerabilities to these risks and how they can mitigate them. Determining the cyber threats at the time of adoption is simply too late.

More attention needed on technologies and trends on the horizon

With so much effort focused on what is right in front of them, organizations are not giving enough consideration to technologies and trends categorized as being on the horizon — for now. As the speed at which technologies emerge and are adopted accelerates, the future may be closer than we think.

Mature organizations are already beginning to consider these technologies. They are reviewing, rethinking and, in some cases, completely redesigning their information security programs to prepare for future technologies and to capture the potential benefits of innovation.

If organizations want to get ahead of cyber threats — or at least keep pace — they need to be proactive not only about the known and unknown risks associated with technologies just around the corner, but also about those just beginning to appear on the horizon. Organizations need to devote resources now to understanding both the opportunities and the threats — and to act on their findings. Organizations also need to be prepared to fundamentally transform their information security programs where necessary. Otherwise, the gap between an organization's information security program and the cyber threats it faces will only continue to grow.

When considering technologies appearing around the corner, respondents share these observations:

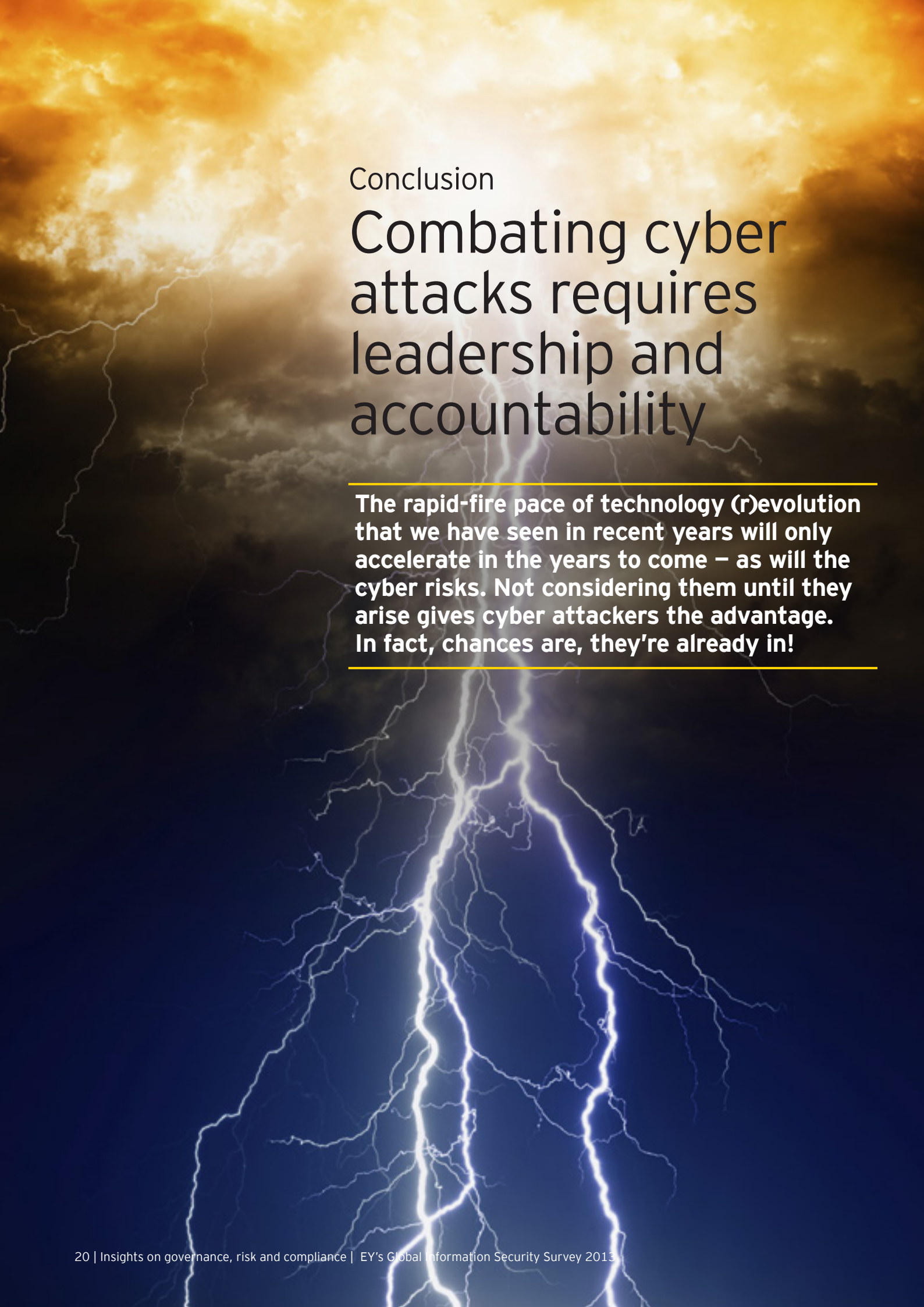
"Plan to close the gap through partnership or co-sourcing. Strengthen the monitoring capabilities; exploit existing tools and technologies. Increase due diligence of service providers; produce more robust incident management processing and establish threat intelligence."
— Financial services organization

"Security intelligence is the key to the future. … We need big data techniques to find the bad guys."
— Financial services organization

Respondents considering technologies and trends on the horizon share the following observations:

"You can never say that you are fully successful in information security; this would be complacent. It is a continuous fight to close any potential gaps between threats and security measures. To this end, we 'get out of the box': we try to listen to the market, understand new trends in information security, to identify new threats and how we can deal with them. One must always be vigilant. The most important thing is to take a holistic view, be open-minded and open to discussion and collaboration. Not only within the boundaries of the organization, but also across organizations."
— Financial services organization

"New technologies will create new issues you have to think about in advance."
— Professional services organization



Conclusion

Combating cyber attacks requires leadership and accountability

The rapid-fire pace of technology (r)evolution that we have seen in recent years will only accelerate in the years to come – as will the cyber risks. Not considering them until they arise gives cyber attackers the advantage. In fact, chances are, they're already in!

Organizations are making good progress in improving how they manage the risks they already know. However, with only 17% of respondents indicating that their information security function fully meets the needs of the company, they still have a long way to go.

And they are running out of time. The volume of cyber risks that organizations don't know, particularly when it comes to emerging technologies that are just around the corner or appearing on the horizon, is growing at a rate too fast for many organizations to keep up with.

New technologies now drive marketing and customer-oriented initiatives, while information security chases associated cyber threats from behind. Mergers or acquisitions, structural changes within the organization or entering new markets all place additional stress on the information security function to provide adequate protection.

As our survey findings indicate, organizations need to place more emphasis on improving employee awareness, increasing budgets and devoting more resources to innovating security solutions. These efforts need to be championed by executives at the highest level of the organization, who need to be aware that 80% of the solution is non-technical — it's a case of good governance.

Cyber attacks aren't going to stop!

In the past 12 months, more than twice as many respondents indicate that the frequency of attacks has gone up compared to those who indicate that they've decreased. If they succeed in infiltrating an organization's security perimeter, the consequences are distracting at the least, paralyzing at the worst. Security breaches can derail key objectives; undermine the confidence of shareholders, analysts and consumers; damage your brand reputation; and cause significant financial harm.

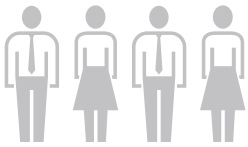
Too frequently, information security is perceived as a compliance necessity and a cost burden to the business. Executives need to view information security as an opportunity that can truly benefit the company and its customers. They need to look at the leading practices outlined in this report and consider how they can be applied to their business. However, with respondents indicating that they are devoting only 14% of their budget spend on innovating new security solutions in the next 12 months, the possibility of hackers wreaking havoc on organizations becomes not only likely, but inevitable.

> "Cyber crime is the greatest threat for organizations' survival today."

Ken Allan
EY Global Information Security Leader

Survey methodology

Profile of participants



1,909
respondents

64
countries worldwide

25
industry sectors

EY's Global Information Security Survey was conducted between June 2013 and July 2013. More than 1,900 respondents across all major industries and in 64 countries participated.

For our survey, we invited CIOs, CISOs, CFOs, CEOs and other information security executives to take part. We distribute a questionnaire to designated EY professionals in each country practice, along with instructions for consistent administration of the survey process.

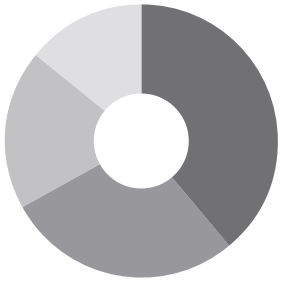
The majority of the survey responses were collected during face-to-face interviews. When this was not possible, the questionnaire was conducted online.

If you wish to participate in future EY Global Information Security Surveys, please contact your EY representative or local office, or visit www.ey.com/giss and complete a simple request form.

Respondents by industry sector

Aerospace and defense	47
Airlines	12
Asset management	42
Automotive	66
Banking and capital markets	361
Chemicals	35
Cleantech	5
Consumer products	116
Diversified industrial products	128
Government and public sector	128
Health care	37
Insurance	125
Life sciences	47
Media and entertainment	57
Mining and metals	39
Oil and gas	43
Power and utilities	61
Private equity	3
Professional firms and services	73
Provider care	12
Real estate	69
Retail and wholesale	98
Technology	179
Telecommunications	72
Transportation	54

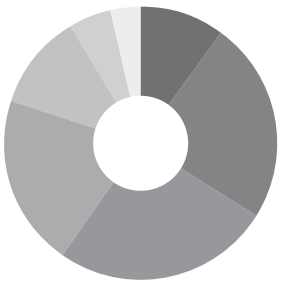
Respondents by area (1,909 respondents)



Key:

EMEIA	39%
Americas	28%
Asia-Pacific	19%
Japan	14%

Respondents by total annual company revenue



Key:

US$10–US$50 billion	196
US$1–US$10 billion	455
US$100 million–US$1 billion	492
US$10–US$100 million	388
Less than US$10 million	217
Government, nonprofit	96
Not applicable	65

Additional thought leadership resources

EY regularly publishes **Insights on governance, risk and compliance**, including thought leadership on information security topics. These perspectives are designed to help clients by offering timely and valuable insights that address issues of importance for C-suite executives. Please visit www.ey.com/GRCinsights

Beating cybercrime. Security Program Management from the Board's perspective.

Most organizations struggle to keep pace with the breakneck velocity of these changing technologies and threats, creating hazardous gaps between the true risks that threaten their viability and their ability to respond and mitigate these risks effectively. Organizations can benefit from an objective assessment of their information security programs and structures via EY's Security Program Management approach.

www.ey.com/spm

Cybersecurity: considerations for the audit committee

Cybersecurity is not just a technology issue; it's a business risk that requires an enterprise-wide response. Boards of directors are starting to take note, particularly members of the audit committee, who now list cybersecurity among their top concerns.

http://www.ey.com/Publication/vwLUAssets/Cybersecurity_Considerations_for_the_audit_committee/$FILE/Cybersecurity_considerations_for_the_audit_committee_GA0001.pdf

Security Operations Centers against cyber crime. Top 10 considerations for success.

Understanding that security information attacks can never be fully prevented, companies should advance their detection capabilities so they can respond appropriately. A well-functioning Security Operations Center (SOC) is at the heart of all such efforts. We explore the top 10 considerations critical to the success of your SOC.

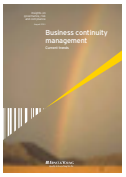
www.ey.com/soc

Identity and access management (IAM): beyond compliance

IAM is evolving into a risk-based program with capabilities focused on entitlement management and enforcement of logical access controls, leveraging new technologies to transform from a compliance-based program into a true business enabler.

www.ey.com/iam

Business continuity management



Approximately 50% of companies neglect to take steps to safeguard their businesses in the event of a disaster, which could potentially threaten their existence. Disasters and the resulting non-availability of resources can be devastating, and leading companies have increasing awareness of the need to develop, maintain and sustain effective business continuity management programs.

www.ey.com/bcmtrends

Privacy trends: the uphill climb continues

As the privacy landscape continues to evolve and mature, trends are forming around how market conditions are impacting organizations' privacy decisions. Our report highlights the three megatrend categories playing increasingly large roles as we enter a new era in privacy protection: governance, technology and regulation.

www.ey.com/privacy2013

Key considerations for your internal audit plan: enhancing the risk assessment and addressing emerging risks

The internal audit risk assessment and the ongoing refresh processes are critical to identifying and filtering the activities that internal audit can perform to provide measurable benefit to the organization. The processes begin by identifying these emerging risks and focus areas and their corresponding practical, value-based audits.

www.ey.com/iaplan

Please also see this book on cybersecurity published by EY and ISACA: http://www.ey.com/US/en/Newsroom/News-releases/News_Five-Things-Every-Organization-Should-Know-about-Detecting-and-Responding-to-Targeted-Cyberattacks

EY's risk services

We have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance, as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our clients' applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

The leaders of our RISK practice are:

Global RISK Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area RISK Leaders		
Americas		
Jay Layman	+1 312 879 5071	jay.layman@ey.com
EMEIA		
Jonathan Blackmore	+44 20 795 11616	jblackmore@uk.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Shohei Harada	+81 3 3503 1100	harada-shh@shinnihon.or.jp

The information security leaders within our RISK practice are:

Global Information Security Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Information Security Leaders		
Americas		
Jose Granado	+1 713 750 8671	jose.granado@ey.com
EMEIA		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Mike Trovato	+61 3 9288 8287	mike.trovato@au.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business having the right advisors on your side can make all the difference. Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

EYG no. AU1885

1304-1063727 EC
ED 0114.

www.ey.com/giss

U.S. states probe eBay cyber attack as customers complain

BY JIM FINKLE AND KAREN FREIFELD

BOSTON/NEW YORK Thu May 22, 2014

(Reuters) - EBay Inc came under pressure on Thursday over a massive hacking of customer data as three U.S. states began investigating the e-commerce company's security practices.

Connecticut, Florida and Illinois said they are jointly investigating the matter. New York Attorney General Eric Schneiderman requested eBay provide free credit monitoring for everyone affected.

Details about what happened are still unclear because eBay has provided few details about the attack. It is also unclear what legal authority states have over eBay's handling of the matter.

The states' quick move shows that authorities are serious about holding companies accountable for securing data following high-profile breaches at other companies, including retailers Target Corp, Neiman Marcus and Michaels and credit monitoring bureau Experian Plc.

Congress and the Federal Trade Commission are investigating the Target breach, which resulted in the firing of the company's chief executive and its chief information officer.

"There is definitely a climate shift," said Jamie Court, president of the advocacy group Consumer Watchdog. "The departure of the Target CEO over the problem signals inside the board room and in the halls of government that these are betrayals of customers and that they won't be tolerated."

EBay shares fell 0.7 on Nasdaq, compared with a 0.6 increase in the Nasdaq CompositeIndex.

The investigation by the states will focus on eBay's measures for securing data, circumstances that led to the breach and the company's response, said Jaclyn Falkowski, a spokeswoman for Connecticut Attorney General George Jepsen.

EBay spokeswoman Amanda Miller declined to comment on the states' actions, but said the company was working with authorities around the globe.

"We have relationships with and proactively contacted a number of state, federal and international regulators and law enforcement agencies," she said. "We are fully cooperating with them on all aspects of this incident."

COMPLAINTS

Some customers complained on eBay Community forums that they had not received much information about the breach from eBay and have yet to get notifications by email, which the company has promised to do.

"This is all over the news - Nothing from EBay," sfbay111 said in one post on an eBay forum.

Several security experts said the best practices would be to have a message pop up when users log in, telling them about the breach and forcing password changes.

As of Thursday afternoon, eBay did not have information on the attack visible on its market home page, www.ebay.com.

"That's really poor incident response," said David Kennedy, a cyber forensics expert who is CEO of TrustedSEC LLC. "EBay should be held to a higher standard."

Kathryn Higa, a Honolulu-based entrepreneur and longtime eBay user, said she was "disappointed" with eBay's response to the breach.

She would like the company to post notices on its marketplace, www.ebay.com. They are currently on its corporate site, www.ebayinc.com.

"They have not exercised all the vehicles available to them to protect their customers," she told Reuters via telephone.

The company addressed delays in notification in a Tweet on Thursday afternoon: "Just to let everyone know, it will take some time for every eBay user to get our reset email. You can still go to eBay to change password."

INVESTIGATION

A spokesman for the FBI's San Francisco office said multiple agents were working on the case, but declined to comment on the likelihood of apprehending the culprits.

Even though the criminals have yet to surface, that has not prevented others from trying to profit from their work.

Someone posted a batch of emails, scrambled passwords, phone numbers and addresses of more than 12,000 people on the Internet, saying it was a sample of data stolen from eBay and offering to sell the full batch for 1.453 bitcoin, or a little more than $750.

EBay's Miller said the information was not authentic.

Reuters spoke to six people whose phone numbers were included in that batch. While only four said they had eBay accounts, all of them said the data was correct, which suggests they may have been victims of another data breach.

(Additional reporting by Mark Hosenball in Washington, Soham Chatterjee, Supantha Mukherjee and Subrat Patnaik in Bangalore, Joseph Menn in San Francisco; Editing by Dan Grebler)

Nutter
Nutter McClennen & Fish LLP
ATTORNEYS AT LAW

OVERVIEW OF THE FIRM

Quality

Clients come to Nutter to work with top quality lawyers who are results-driven, accountable and provide highly responsive service. The firm serves a diverse blue chip roster of clients including major U.S. and global corporations and financial institutions, research universities, high technology and emerging companies, investors, developers, foundations and families. Nutter has a long track record of exceeding the most demanding expectations of clients, with depth in many industries including medical devices, pharmaceuticals, banking and financial services, real estate, energy and various high technology sectors.

Experience

In continuous practice for 135 years and one of the top-ranked firms in Boston, Nutter provides clients with a broad multidisciplinary platform of sophisticated legal expertise and resources, including depth in handling very complex litigation, transactions, and other legal counseling. The practice is organized into legal departments from which lawyers with the appropriate expertise and levels of experience are assembled to address each client's unique situation:

- Business and Finance
- Intellectual Property
- Litigation
- Real Estate
- Labor and Employment
- Tax
- Trusts and Estates

Efficiency

The firm's service model is based on right-sized legal teams working closely with clients to accomplish their goals. It has long been our experience that lean staffing and close partner involvement in managing legal work result in efficiencies that contain cost for the client.

Values

Nutter takes it as a fundamental responsibility to understand a client's business, objectives and definition of value. All attorneys and staff are guided by core commitments and practices that we believe determine the excellence of our clients' experience:

- Work hard to deliver the value and efficiency clients deserve
- Respect the clients and be accountable to them
- Be passionate and innovative about getting the best result for the client
- Be exceptionally responsive and proactive about communicating with the client

- Contribute legal solutions that create long-term value for the client's organization

Making a Difference to Our Clients

Resources

- One of New England's largest law firms
- Over 150 Lawyers
- Network of relationships
- Platform of multiple practice areas serving clients in a range of industries

Experience

- Continuous record of client service and achievement for over a century

Client-centered approach

- Driven by respect for our clients and dedicated to their needs
- Known for close partner involvement and responsiveness

Deep roots

Nutter has a distinguished pedigree as the firm that was founded by Louis D. Brandeis -- who later became one of the most renowned US Supreme Court justices of the twentieth century -- and his classmate Samuel D. Warren, member of a prominent Boston family. They founded the firm in 1879 (originally as Warren and Brandeis), two years after they graduated from Harvard Law School and eleven years before they published their landmark law review article "The Right to Privacy," which first addressed the idea of a right to privacy in a legal context in the United States and continues to be cited and studied around the world. The firm rapidly achieved success, trying cases before the Supreme Court, handling international patent filings and representing some of the major industries that were burgeoning in New England at the time. The founding partners' rich legacy continues to inspire and set an example for the firm, and we uphold the same standard of focused dedication, innovation and unwavering commitment that they established.

Pro Bono

Nutter is a founding member and challenge participant in the Pro Bono Institute's Law Firm Pro Bono Project and is deeply committed to giving back and to making a meaningful contribution to society and our community. The majority of the firm's attorneys actively participate in the pro bono program, providing representation on political asylum/immigration cases; in housing court providing eviction defense; on family law for battered women; through programs that support healthy kids, veterans and seniors; and many others. Our co-founder Louis Brandeis is widely recognized as one of the first lawyers in the country to pioneer pro bono service, and we proudly continue in that tradition.

More information

For more detailed information about our services and expertise, we invite you to visit our website at www.nutter.com or m.nutter.com or contact us.

Nutter McClennen & Fish LLP
Attorneys at Law
www.nutter.com

Government Investigations and White Collar Defense

What matters most?

Clients facing an investigation or enforcement action by the government need help quickly. Every step or misstep can have an irreversible impact on the outcome. Whether it's the U.S. Attorney's Office, the SEC, the IRS, or another federal or state agency or a self-regulatory organization, an investigation can be serious, alarming and potentially damaging. Knowing what direction to take, what strategy to pursue, what to communicate when and to whom -- indeed knowing what to do every step of the way -- is critical.

What matters most is having the right team in your corner – legal counsel who are:

- Experienced both as prosecutors and trial lawyers
- Creative and practical at problem-solving
- Responsive and proactive
- Committed to understanding your business
- Dedicated to providing the highest quality of service
- Cost-sensitive
- Driven to win

Our proven and trusted team

Led by former high-ranking prosecutors and seasoned trial lawyers, the Nutter team is a tightly-knit group of dedicated attorneys who work together on strategies to solve clients' problems. Highly experienced partners share their expertise and insight to optimize each client's case, in a collaborative approach that benefits the client with their combined knowledge and the strength of their collective commitment. We give each client an exceptional degree of direct partner attention, together with the consistent support of talented litigation associates who concentrate in government investigations and white collar defense work.

Together, our white collar defense attorneys have more than 50 years of combined experience as federal prosecutors in Boston and Philadelphia. Clients have the advantage of their extensive state and federal experience together with their broad range of experience handling criminal, civil and administrative matters for companies, institutions and individuals.

Allison D. Burroughs was an Assistant U.S. Attorney in the District of Massachusetts for ten years, for most of which she prosecuted white collar crime and oversaw the office's Computer Crime and Intellectual Property program. She also served as the office's Senior Litigation Counsel and received the Department of Justice's Director's Award for Superior Performance three times. She is a highly experienced trial lawyer with over 20 cases tried to verdict.

Jonathan L. Kotlier served for twelve years in the U.S. Attorney's Office for the District of Massachusetts, during eight of which he was Chief of the Economic Crimes Unit. He worked closely with the Securities and Exchange Commission and the Massachusetts Division of Securities on securities fraud cases, and has conducted internal investigations and represented numerous high level corporate officers in investigations by the SEC and Department of Justice. A seasoned trial lawyer, he has tried over 20 cases to verdict.

Ian D. Roffman is a former Senior Trial Counsel in the Enforcement Division of the Securities and Exchange Commission in Boston, where he received both the Chairman's Award for Excellence and the Enforcement

Director’s Award.

John R. Snyder, who has extensive securities litigation experience, defending broker-dealer firms and associated persons before arbitrators and regulatory agencies and in federal and state courts. John has in-depth knowledge of the securities industry, broker-dealer operations, supervisory and compliance systems, and the laws and regulations that govern the industry.

Who we represent

The Nutter white collar defense team represents companies and institutions, corporate management and employees, and a variety of other individuals who have included board members, chief executives and other top officers. Clients come from a wide range of industries and fields, including:

- Pharmaceuticals and other life sciences sectors
- Banking and other financial services
- High technology
- Manufacturing
- Major educational and medical institutions

Our clients range from Fortune 500 companies to world-renowned universities to employee groups to smaller businesses, who have turned to the firm for representation on the full spectrum of criminal and civil matters, regulatory proceedings, compliance efforts, internal investigations and other interactions with the state and/or federal governments.

What we do

The services we provide include:

- Helping clients avoid running afoul of the government by advising them on corporate compliance and conducting internal investigations and audits as necessary
- Vigorously defending the rights of clients who are targets, subjects or witnesses in governmental investigations and civil, criminal and regulatory actions
- Representing clients in False Claims Act cases and qui tam investigations
- Handling grand jury investigations, subpoena responses, hearings, negotiations, trials, appeals and all other aspects of litigation with the government
- Drawing on extensive experience and substantive knowledge in a variety of specialty areas that are important to our clients, including:
  - Health care
  - Securities fraud and insider trading
  - Computer fraud and abuse
  - The Foreign Corrupt Practices Act (FCPA)
  - Banking issues including suspicious transactions and money laundering
  - Sarbanes–Oxley Act compliance
  - Other issues facing the financial services sector

Some examples of our success

Successes the Nutter team has achieved for clients include:

- Winning acquittal in a high-profile federal trial for the general counsel of a publicly traded software company

charged with securities fraud and false statements

- Winning acquittal for a pharmaceutical company manager after a nationally watched three-month federal trial on conspiracy and health care fraud charges
- Representing a multi-national health care provider in a government investigation with potentially extensive criminal exposure which resulted in relatively modest civil fine and closure of the government investigation
- Representing the target of an IRS criminal enforcement matter involving over $10 million of prime real estate in which the individual was not charged and ultimately received a tax refund
- Representing a mutual fund company in a Massachusetts Division of Securities investigation; no suit was filed
- Obtaining a non-prison time sentence after a multi-day sentencing hearing for the chief in-house lawyer of a large construction company; the attorney had been charged in a multi-million dollar workers' compensation fraud and the government sought a substantial prison term
- Convincing the government not to bring criminal charges against an officer of a major health care company who had received a target letter from the government; the other officers who received target letters were all criminally charged
- Representing a financial institution that had failed to file currency transaction reports for over $50 million in cash deposits; the U.S. Treasury Department ultimately took no enforcement action

Our areas of expertise

Health Care Fraud and Abuse
Nutter's government enforcement defense attorneys have been involved in virtually every major health care fraud case in New England over the past decade, including actions brought under the anti-kickback statute and the newest wave of cases challenging the off-label promotion of pharmaceutical products. Our group represents corporations, medical institutions and individuals in federal and state civil and criminal health care enforcement actions.

Securities Enforcement
Our attorneys have extensive experience with all types of federal and state, criminal and civil, SEC, and FINRA investigations and enforcement actions, including those regarding insider trading, accounting issues, and mutual fund late trading and market timing. Our group also conducts internal investigations into corporate governance and breach of fiduciary duty issues. Ian Roffman is a former senior counsel at the SEC, and Jonathan Kotlier worked extensively with the SEC, FINRA, and Massachusetts Division of Securities during his 12 years at the US Attorney's Office; he also served on the Department of Justice's Securities and Commodities Fraud Working Group.

False Claims Act and Government Contracts
Nutter has broad experience representing private and non-profit entities, and individuals, who have been sued for submitting allegedly false claims to government agencies. Nutter has also represented individuals whose work on government contracts has led to criminal charges. Our extensive work in the area covers industries ranging from military procurement to import/export firms, hospitals and medical devices.

Internal Investigations
Handling internal investigations is an integral part of the legal services we provide. Our attorneys extend expert legal advice, identify potential exposures at the earliest possible point, and assist clients in developing and adopting a plan to address these issues internally or negotiate a resolution with the regulator involved.

Compliance Programs
Our attorneys evaluate client needs, industry standards, regulatory guidance and the Federal Sentencing Guidelines to develop and implement optimal compliance programs that reflect a client's unique requirements. In addition, the team conducts "refresher" courses to maintain the client's awareness of both new and old regulations, as well as to highlight legal developments that may affect a client's business.

Computer Crime

Nutter attorneys have deep expertise in the issues surrounding the investigation, prosecution and defense of complex computer crime and intellectual property offenses, including theft of trade secrets, violations of the Computer Fraud and Abuse Act and other issues related to computer intrusions and the unauthorized use of electronic information. We also advise companies on compliance with state and federal disclosure obligations related to identity theft and the misuse of personal information.

General Regulatory Enforcement

Nutter has experience defending criminal and civil government enforcement actions in a wide range of areas beyond those described above. Our work, however, is not limited to defense; our attorneys also have extensive experience as special prosecutors and in representing victims of fraud in their efforts to recoup lost assets.

We’re inspired. We’re committed. We’re Nutter.

The Nutter of today has grown through several generations of lawyers from an illustrious beginning in Boston in 1879. Two young Harvard Law School graduates -- Samuel D. Warren, scion of one of the city’s elite families, and Louis D. Brandeis, who would later become one of the most famous lawyers in modern history – co-founded the firm a few years after they graduated first and second in their class. The firm, originally called Warren & Brandeis, quickly became very successful, and a strong foundation was laid which has endured for 135 years and counting of continuous practice.

We celebrate the legacy and example our founder Louis D. Brandeis, who practiced law here for over 35 years before beginning a long and distinguished term on the Supreme Court of the United States in 1916. Brandeis was a man of great accomplishment and conviction, deeply dedicated to his clients and recognized as a brilliant advocate. A pioneer of privacy rights and the *pro bono* tradition, he left a legacy of service and commitment that inspires lawyers to this day. We are proud of our DNA as a firm and appreciate that it provides us a strong platform on which to serve as legal counsel to our clients today.

Nutter McClennen & Fish LLP
Attorneys at Law
www.nutter.com