Cybersecurity: Data, Statistics, and Glossaries

Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739)

View Key Policy Staff

May 7, 2015 (R43310)

Jump to Main Text of Report

Related Author

- Rita Tehan

Related Policy Issue

- Cybersecurity

Contents

Tables

Summary

This report describes data and statistics from government, industry, and information technology (IT) security firms regarding the current state of cybersecurity threats in the United States and internationally. These include incident estimates, costs, and annual reports on data security breaches, identity thefts, cybercrimes, malwares, and network securities.

For information on cybersecurity-related issues, including authoritative reports by topic, see CRS Report R42507,*Cybersecurity: Authoritative Reports and Resources, by Topic*, by Rita Tehan. For information on legislation, hearings, and executive orders, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.

Cybersecurity: Data, Statistics, and Glossaries

Data and Statistics[1]

This section describes data and statistics from government, industry, and information technology (IT) security firms regarding the current state of cybersecurity threats in the United States and internationally. These include incident estimates, costs, and annual reports on data security breaches, identity thefts, cybercrimes, malwares, and network securities.

Table 1. Data and Statistics: Cyber Incidents, Data Breaches, Cybercrime

Title	Date	Source	Pages	Notes
Web Hacking Incidents Database	Ongoing	Breach Security, Inc.	N/A	The web hacking incident database project dedicated to maintaining a li application-related security incident WHID's purpose is to serve as a too awareness of the web application s problem and provide information for analysis of web application security Unlike other resources covering we security, which focus on the technic the incident, the WHID focuses on t the attack. To be included in WHID must be publicly reported, be assoc web application security vulnerabilit an identified outcome.
Significant Cyber Incidents Since 2006	Ongoing	Center for Strategic and International Studies (CSIS)	15	This timeline records significant cyb since 2006. It focuses on successfu government agencies, defense and companies, or economic crimes wit more than a million dollars.
Overview of Current Cyber Attacks (logged by 180 Sensors)	Ongoing	Deutsche Telekom	N/A	Provides a real-time visualization ar cyberattacks detected by a network sensors placed around the world.
Digital Attack Map	Ongoing	Arbor Networks	N/A	The map is powered by data fed fro customers worldwide who have agr network traffic and attack statistics. displays global activity levels in obs traffic, which it is collected anonymo does not include any identifying info about the attackers or victims involv particular attack.
Real-Time Web Monitor	Ongoing	Akamai	N/A	Akamai monitors global Internet con around the clock. The map identifie regions with the greatest attack traf
Regional Threat Assessment: Infection Rates and Threat Trends by Location Regional Threat Assessment: Infection Rates and Threat Trends by Location (Note: Select "All Regions" or a specific country or region to view threat assessment reports)	Ongoing	Microsoft Security Intelligence Report (SIR)	N/A	Data on infection rates, malicious w threat trends by regional location, w
ThreatWatch	Ongoing	NextGov	N/A	ThreatWatch is a snapshot of the d intrusions against organizations and globally, on a daily basis. It is not an authoritative list, because many co are never reported or even discover information is based on accounts pu outside news organizations and res
McAfee Research & Reports (multiple)	Ongoing	McAfee	N/A	Links to reports by the company on cybersecurity threats, malware, cyb spam.
Cyber Power Index	Ongoing	Booz Allen Hamilton and	N/A	The index of developing countries' a withstand cyber attacks and build s

		the Economist Intelligence Unit		economies, rates the countries on t regulatory frameworks, economic a issues, technology infrastructure, ar The index puts the United States in spot, and the United Kingdom in no
Data Breaches	Ongoing	Identity Theft Resource Center (ITRC)	N/A	The ITRC breach list is a compilatio breaches confirmed by various med and notification lists from state gove agencies. This list is updated daily a each Tuesday. To qualify, breaches include personally identifiable inform could lead to identity theft, especial Security numbers. ITRC follows U.S guidelines about what combination information comprises a unique indi exposure of this information constitu breach.
Cytherthreat: Real-Time Map	Ongoing	Kaspersky Labs	N/A	Kaspersky Labs has launched an in cyberthreat map that lets viewers se cybersecurity incidents as they occu world in real time. The interactive m malicious objects detected during o on-demand scans, e-mail and web a detections, and objects identified by and intrusion detection sub-systems
Global Botnet Map	Ongoing	Trend Micro	N/A	Trend Micro continuously monitors network activities to identify comma control (C&C) servers and help incr protection against botnet attacks. T map indicates the locations of C&C victimized computers they control th discovered in the previous six hours
HoneyMap	Ongoing	Honeynet Project	N/A	The HoneyMap displays malicious a they happen. Each red dot on the m represents an attack on a computer represent honeypots, or systems se record incoming attacks. The black bottom gives the location of each at Honeynet Project is an internationa profit security research organizatior to investigating the latest attacks ar open source security tools to impro security.
The Cyberfeed	Ongoing	Anubis Networks	N/A	Provides real-time threat intelligenc worldwide.
2015 Data Breach Investigations Report (DBIR)	April 14, 2015	Verizon	70	A full three-quarters of attacks sprea first victim to the second in 24 hours more than 40% spread from the firs second in under an hour. On top of with which attackers compromise m victims, the useful lifespan of share can sometimes be measured in hou Researchers also found that of the observed in current information sha only 2.7% were valid for more than the number dwindles from there. Da information sharing has to be good effective.
HIPAA breaches: The list keeps growing	March 12, 2015	Healthcare IT News	N/A	More than 41 million people have h protected health information compre Health Insurance Portability and Ac

				Act (HIPAA) privacy and security br Using data from the Department of Human Services, which includes HI breaches involving more than 500 i reported by 1,149 covered entities a associates, the website compiled a searchable list.
Federal Information Management Security Act (Annual Report to Congress)	February 27, 2015	Office of Management and Budget (OMB)	100	The number of actual cybersecurity reported by federal agencies to the decreased last year. Data show the number of incident reports sent by t agencies to US-CERT going up by during FY2014 from the year before two significant categories from that removed— non-cybersecurity incide "other"— the number actually show of about 6%. Non-cybersecurity inci the mishandling of personality ident information, but without a cybersecu component, meaning the data brea occurred through a misplaced pape Incidents classified as "other" are th scans, blocked attempts at access a miscellaneous events. Reported inc actual serious cybersecurity issues, malware, suspicious network activit improper usage, declined last year. that did increase in recorded numbe social engineering, unauthorized ac denial-of-service attacks.
2014 Global Threat Intel Report	February 6, 2015	CrowdStrike	77	This report summarizes CrowdStrik daily scrutiny of more than 50 group threat actors, including 29 different sponsored and nationalist adversar findings explain how financial malw the threat landscape and point of sa became increasingly prevalent. The profiles a number of new and sophis adversaries from China and Russia Hurricane Panda, Fancy Bear, and Bear.
Incident Response/Vulnerability Coordination in 2014	February 2015	ICS/CERT Monitor	15	In FY2014, the Industrial Control Sy Emergency Response Team (ICS-C received and responded to 245 inci reported by asset owners and indus The Energy sector led all others ag with the most reported incidents. IC continuing partnership with the Ene provides many opportunities to shar and collaborate on incident respons Also noteworthy in 2014 were the in reported by the Critical Manufacturi some of which were from control sy equipment manufacturers.
Business Email Compromise	January 22, 2015	Internet Crime Complaint Center	N/A	The Business Email Compromise (B sophisticated scam targeting busine work with foreign suppliers and bus regularly perform wire transfer paym thieves stole nearly $215 million fro businesses in the past 14 months, u that starts when business executive

				employees have their email accoun
CISCO 2015 Annual Security Report (free registration required)	January 20, 2015	Cisco	53	Government agencies worldwide, c banks and many other companies, able to cope when the inevitable da occurs, according to the study on ac cybersecurity. About 43% of the pul falls into the "highly sophisticated" s posture segment. The best security be found within the telecommunicat energy sectors, tied at 47%.
The Cost of Malware Containment	January 20, 2015	Ponemon Institute		According to the study, organization received nearly 17,000 malware ale which pose a taxing and costly end those alerts, only 3,218 were consid actionable and only 705 (or 4%) we investigated. An average of 395 hou weekly investigating and containing to false positives or false negatives, participating organizations an estim million yearly in average value of lo
2014 Global Report on the Cost of Cybercrime	October 8, 2014	HP Enterprise Security and Ponemon Institute	31	The 2014 global study of U.S.-base spanning seven nations, found that course of a year, the average cost o for companies in the United States more than 9% to $12.7 million up fr million in the 2013 study. The avera resolve a cyberattack is also rising, 45 days from 32 days in 2013.
Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015	September 30, 2014	Pricewaterhouse Coopers (PwC)	31	The Global State of Information Sec (GSISS), on which the report is bas more than 9,700 respondents world detected that the number of cyber in increased at a compound annual ra since 2009. As the frequency of cyb have risen so too has the reported c managing and mitigating them. Glol estimated average financial loss fro incidents was $2.7 million, a 34% in 2013. Big losses have also been mo with the proportion of organizations financial hits in excess of $20 millio doubling. Despite greater awarenes cybersecurity incidents, the study fo global information security budgets decreased 4% compared with 2013
How Consumers Foot the Bill for Data Breaches (infographic)	August 7, 2014	NextGov.com	N/A	In 2013, there were more than 600 breaches, with an average organiza more than $5 million. But in the end customers who are picking up the ta higher retail costs to credit card reis
Is Ransomware Poised for Growth?	July 14, 2014	Symantec	N/A	Ransomware usually masquerades "wheel clamp" for the victim's comp example, pretending to be from the enforcement, it might suggest the v been using the computer for illicit pu to unlock it the victim would have to often between $100 and $500. Ran escalated in 2013, with a 500% (six increase in attack numbers betweer and end of the year.
Critical Infrastructure: Security	July 2014	Unisys and	34	Unisys and Ponemon Institute surv

Preparedness and Maturity		Ponemon Institute		600 IT security executives of utility, manufacturing organizations. Overa finds organizations are simply not p deal with advanced cyber threats. C companies have actually deployed programs and, according to the surv threat actually stems from negligent
The Value of a Hacked Email Account	June 13, 2013	Krebs on Security	N/A	One prominent credential seller in th underground peddles iTunes accou and Fedex.com, Continental.com, a United.com accounts for USD $6. G accounts fetch $5, while $4 buys ha credentials at registrar and hosting Godaddy.com, as well as wireless p Att.com, Sprint.com, Verizonwireles Tmobile.com. Active accounts at Fa Twitter retail for just $2.50 apiece... crime shops go even lower with the hacked accounts, charging between for active accounts at dell.com, ove walmart.com, tesco.com, bestbuy.c target.com, etc.
Online Trust Honor Roll 2014	June 11, 2014	Online Trust Alliance	N/A	Out of nearly 800 top consumer we evaluated, 30.2% made the Honor R distinguishes them in best practices safeguarding data in three categorie domain/brand protection, privacy, a Conversely, nearly 70% did not qua Honor Roll, with 52.7% failing in at l the three categories.
Net Losses: Estimating the Global Cost of Cybercrime	June 2014	CSIS and McAfee	24	This report explores the economic i cybercrime, including estimation, re variances, IP theft, opportunity and costs, and the future of cybercrime. costs the global economy up to $57 annually, with the United States tak billion hit, the largest of any country up to 0.8% of the global economy. F United States, the estimated $100 m means 200,000 lost jobs, and is alm the total loss for the G-8 group of W countries.
2014 U.S. State of Cybercrime Survey	May 29, 2014	PwC, *CSO Magazine*, the U.S. Computer Emergency Readiness Team (CERT) Division of the Software Engineering Institute at Carnegie Mellon University, and the U.S. Secret Service	21	The cybersecurity programs of U.S. organizations do not rival the persis tactical skills, and technological pro potential cyber adversaries. This ye four (77%) respondents to the surve security event in the past 12 months than a third (34%) said the number incidents detected increased over th year.
The Target Breach, by the Numbers	May 6, 2014	Krebs on Security	N/A	A synthesis of numbers associated Target data breach of December 19 number of records stolen, estimated to credit unions and community ban of money Target estimates it will sp

				upgrading payment terminals to sup and-PIN enabled cards).
2014 Cost of Data Breach: Global Analysis	May 5, 2014	Ponemon Institute/IBM	28	The average cost of a breach is up 2014, with U.S. firms paying almost more than the global average. In the States, a data breach costs organiz average $5.85 million, the highest o nations analyzed, up from $5.4 milli Globally, the cost of a breach is up to $3.5 million. The United States lik the highest cost per record stolen, a from $188 last year. The country als terms of size of breaches recorded: companies averaged 29,087 record compromised in 2014.
Website Security Statistics Report	April 15, 2014	WhiteHat Security	22	WhiteHat researchers examined the assessment results of the more tha websites under WhiteHat Security r to measure how the underlying prog languages and frameworks perform The report yields findings to specific that are most prone to specific class attacks, for how often and how long determination as to whether popula languages and frameworks yield sin in production websites. The popular complexity of .Net, Java, and ASP r potential attack surface for each lan larger; as such, 31% of vulnerabilitie observed in .Net, 28% were found i 15% were found in ASP.
More online Americans say they've experienced a personal data breach	April 14, 2014	Pew Research Center	N/A	Findings from a January 2014 surve 18% of online adults have had impo personal information—such as Soci numbers, credit cards, or bank acco stolen. That is an increase from the online adults who reported persona theft in July 2013 and 21% who said email or social networking account or taken over without their permissio number reported this experience in survey.
2014 Internet Security Threat Report	April 8, 2014	Symantec	98	In 2013, there were 253 data breac exposed more than 552 million sets data, according to the annual repor number of data breaches was up 62 previous year and nearly 50 more th previously dubbed by Symantec "ye breach." In addition, eight mega-bre exposed more than 10 million identi eightfold increase from one the yea nearly double the five in 2011.
Advanced Threat Report 2013	February 27, 2014	FireEye	22	The report analyzes more than 40,0 attacks across the globe to map out trends in advanced persistent threa attacks. The United States topped t countries targeted by APT activity, w FireEye defines as online attacks th "likely directly or indirectly supporte state." American institutions were a by many more APT malware familie

				of malware that share significant an code with each other) than anywher
State of the Internet Report, 3rd Quarter 2013	January 28, 2014	Akamai	40	Akamai maintains a distributed set unadvertised agents deployed acro Internet that log connection attempt company classifies as attack traffic. the data collected by these agents, able to identify the top countries fro attack traffic originates, as well as t targeted by these attacks. Overall, concentration of attacks declined du quarter of 2013, with the top 10 cou originating 83% of observed attacks with 89% in the second quarter. Ch Indonesia, however, continued to o than half of all observed attack traff
Cisco 2014 Annual Security Report	January 16, 2014	Cisco	81	The report offers data on and insigh security concerns, such as shifts in trends in vulnerabilities, and the res distributed denial-of-service (DDoS report also looks at campaigns that specific organizations, groups, and and the growing sophistication of th attempt to steal sensitive informatio concludes with recommendations fo security models holistically and gai across the entire attack continuum– during, and after an attack. (Free re required.)
McAfee Labs 2014 Threats Predictions	January 7, 2014	McAfee	6	In 2013, the rate of growth in the ap new mobile malware, which almost targets the Android platform, was fa than the growth rate of new malwar PCs. In the last two quarters report malware growth was nearly flat, wh appearances of new Android sampl 33%.
Trends in Incident Response in 2013	October-December 2013	ICS-CERT Monitor	14	In 2013, ICS-CERT responded to 2 reported either directly from asset o through other trusted partners. The these incidents were initially detect business networks of critical infrast organizations that operate industria systems (ICS). Of the 256 reported 59%, or 151 incidents, occurred in t sector, which exceeded all incident other sectors combined.
ENISA Threat Landscape 2013 – Overview of Current and Emerging Cyber-Threats	December 11, 2013	European Union Agency for Network and Information Security	70	The report is a collection of top cyb have been assessed in the reportin within 2013). ENISA has collected reports regarding cyber threats, risk agents. ETL 2013 is a comprehens compilation of the top 15 cyber thre assessed.
Emerging Cyber Threats Report 2014	November 14, 2013	Georgia Institute of Technology	16	The report highlights cloud security issues involving the 'Internet of Thi to the notion that the increase of Int capable devices could create oppo remote hacking and data leakage. everything from home automation t smartphones and other personal de

				becoming connected to the Internet devices will capture more real-world and could permit outside parties, co and governments to misuse that inf (From the annual Georgia Tech Cyl Summit 2013.)
2013/2014 Global Fraud Report	October 23, 2013	Kroll/Economist Intelligence Unit	N/A	The Annual Global Fraud Survey, c by Kroll and carried out by the Econ Intelligence Unit, polled 901 senior worldwide from a broad range of ind functions in July and August 2013. of companies suffering external cyb designed to steal commercial secre 2012-2013 compared with the previ year.
2013 Cost of Cyber Crime Study	October 8, 2013	HP and the Ponemon Institute	28	The study found the average compa U.S. experiences more than 100 su cyberattacks each year at a cost of That is an increase of 26% from las Companies in other regions fared b experienced significant losses. This annual study was conducted in the States, United Kingdom, Germany, Japan, and France and surveyed ov organizations.
Illicit Cyber Activity Involving Fraud	August 8, 2013	Carnegie Mellon University Software Engineering Institute	28	Technical and behavioral patterns w extracted from 80 fraud cases—67 13 external—that occurred betweer the present. These cases were use insights and risk indicators to help p industry, government, and law enfo more effectively prevent, deter, dete investigate, and manage malicious activity within the banking and finan
FY2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002 (FISMA)	March 7, 2013	White House/OMB	63	More government programs violate security law standards in 2012 than previous year, and at the same time security costs have increased by m billion. Inadequate training was a la the reason all-around FISMA adher slipped from 75% in 2011 to 74% in Agencies reported that about 88% c with system access privileges recei security awareness instruction, dow in 2011. Meanwhile, personnel expe accounted for the vast majority—90 $14.6 billion departments spent on technology security in 2012.
Linking Cybersecurity Policy and Performance: Microsoft Releases Special Edition Security Intelligence Report	February 6, 2013	Microsoft Trustworthy Computing	27	Introduces a new methodology for e how socioeconomic factors in a cou impact cybersecurity performance, measures such as use of modern te mature processes, user education, enforcement and public policies rela cyberspace. This methodology can that will help predict the expected c performance of a given country or r
SCADA [Supervisory Control and Data Acquisition] and Process Control Security Survey	February 1, 2013	SANS Institute	19	SANS Institute surveyed profession with SCADA and process control sy Seventy percent of the nearly 700 r said they consider their SCADA sys

				high or severe risk. One-third of the that they have been already been ir
Blurring the Lines: 2013 TMT Global Security Study	January 8, 2013	Deloitte	24	Report states that 88% of companie believe that they are vulnerable to a cyber threat, even though more tha those surveyed have experienced a incident in the last year. Companies mistakes by their employees as a to 70% highlighting a lack of security a a vulnerability. Despite this, less tha companies (48%) offer even genera related training, with 49% saying tha budget was making it hard to impro
Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online	December 20, 2012	Organisation for Economic Cooperation and Development (OECD)	94	This report provides an overview of and statistics in fields of informatior privacy, and the protection of childre highlights the potential for the devel better indicators in these respective showing in particular that there is ar underexploited wealth of empirical d mined and made comparable, will e current evidence base for policymal
State Governments at Risk: a Call for Collaboration and Compliance	October 23, 2012	National Association of State Chief Information Officers and Deloitte	40	Assesses the state of cybersecurity nation and found that only 24% of c information security officers (CISOs confident in their states' ability to gu against external threats.
2012 NCSA/Symantec National Small Business Study	October 2012	National Cyber Security Alliance	18	This survey of more than 1,000 sma midsize businesses found that 83% respondents said they do not have for protecting their companies agair cyberattacks, while 76% think they hackers, viruses, malware, and cyb breaches.
McAfee Explains The Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim	August 3, 2012	Forbes.com	N/A	In August 2012, NSA director Keith quoted a statistic from antivirus firm the cost of worldwide cybercrime ar $1 trillion a year. "No, the statistic w made up. Yes, it's just a 'ballpark fig 'unscientific' one, the company adm despite Pro Publica's criticisms and rather fuzzy math, the company sta trillion-dollar conclusion as a (very) estimate."
Does Cybercrime Really Cost $1 Trillion?	August 1, 2012	ProPublica	N/A	In a news release from computer se McAfee announcing its 2009 report Economies: Protecting Vital Informa company estimated a trillion dollar g cybercrime. That number does not a report itself. McAfee's trillion-dollar questioned by the three independer researchers from Purdue University McAfee credits with analyzing the ra which the estimate was derived. An of their origins by ProPublica has fo grounds to question the data and m to generate these numbers, which M Symantec say they stand behind.
Measuring the Cost of Cybercrime	June 25, 2012	11th Annual Workshop on	N/A	This report states that in total, cybe earnings might amount to a couple

		the Economics of Information Security		citizen per year. But the indirect cos defense costs are very substantial (times that). The authors conclude th basis of the comparative figures col study, we should perhaps spend les anticipation of computer crime (on a firewalls etc.) but we should certain awful lot more on catching and puni perpetrators."
The Risk of Social Engineering on Information Security: A Survey of IT Professionals	September 2011	Check Point	7	The report reveals 48% of large cor 32% of companies of all sizes surve been victims of social engineering, 25 or more attacks in the past two y businesses anywhere from $25,000 $100,000 per security incident. Phis social networking tools are the mos sources of socially engineered threa
Revealed: Operation Shady RAT: an Investigation of Targeted Intrusions into 70+ Global Companies, Governments, and Non-Profit Organizations During the Last 5 Years	August 2, 2011	McAfee Research Labs	14	A comprehensive analysis of victim a five-year targeted operation that p government and other organizations them in the United States, and copi from military secrets to industrial de
A Good Decade for Cybercrime: McAfee's Look Back at Ten Years of Cybercrime	December 29, 2010	McAfee	11	A review of the most publicized, per costly cybercrime exploits from 200

Note: Statistics and other information are from the source publications and have not been independently verified by the Congressional Research Service (CRS).

Cybersecurity: Glossaries, Lexicons, and Guidance

Table 2 contains descriptions of and links to glossaries of useful cybersecurity terms, including those related to cloud computing and cyber warfare.

Table 2. Glossaries, Lexicons, and Guidance Pertaining to Cybersecurity Concepts

Title	Source	Date	Pages	Notes
Hacker Lexicon	Wired.com	Ongoing	N/A	Hacker Lexicon is WIRED's explainer series that seeks to de-mystify the jargon of information security, surveillance, and privacy.
Global Cyber Definitions Database	Organization for Security and Co-operation in Europe (OSCE)	November 2014	N/A	A compilation of definitions of cybersecurity (or information security) terms. The website also includes a submission form to share new or additional definitions.
Compilation of Existing Cybersecurity and Information Security Related Definitions	New America	October 2014	126	"Broadly, the documents analyzed for this report fall into one of five categories: national strategies and documents by governments, documents from regional and global intergovernmental organizations, including member state submissions to the United Nations General Assembly (UNGA), and international private and intergovernmental standards bodies as well as dictionaries."
Glossary of Key Information Security Terms, Revision 2	National Institute of Standards and Technology (NIST)	May 2013	222	Besides providing some 1,500 definitions, the glossary offers a source for each term from either a NIST or Committee for National Security Systems (CNSS) publication. The

				committee is a forum of government agencies that issues guidance aimed at protecting national security systems.
NIST Cloud Computing Reference Architecture	NIST	September 2011	35	Provides guidance to specific communities of practitioners and researchers.
Glossary of Key Information Security Terms	NIST	May 31, 2013	211	The glossary provides a central resource of terms and definitions most commonly used in NIST information security publications and in CNSS information assurance publications.
CIS Consensus Security Metrics	Center for Internet Security	November 1, 2010	175	Provides recommended technical control rules/values for hardening operating systems, middleware and software applications, and network devices. The recommendations are defined via consensus among hundreds of security professionals worldwide. (Free registration required.)
Joint Terminology for Cyberspace Operations	Chairman of the Joint Chiefs of Staff	November 1, 2010	16	This lexicon is the starting point for normalizing terms in all DOD cyber-related documents, instructions, CONOPS, and publications as they come up for review.
Department of Defense Dictionary of Military and Associated Terms	Chairman of the Joint Chiefs of Staff	November 8, 2010 (as amended through September 15, 2013)	547	Provides joint policy and guidance for Information Assurance (IA) and Computer Network Operations (CNO) activities.
DHS Risk Lexicon	Department of Homeland Security (DHS) Risk Steering Committee	September 2010	72	The lexicon promulgates a common language, consistency and clear understanding with regard to the usage of terms by the risk community across the DHS.

Source: Highlights compiled by CRS from the reports.

Key Policy Staff

The following table provides names and contact information for CRS experts on policy issues related to cybersecurity bills currently being debated in the 114th Congress.

Legislative Issues	Name/Title	Phone	Email
Legislation in the 114th Congress	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Critical infrastructure protection	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Chemical industry	Dana Shea	7-6844	dshea@crs.loc.gov
Defense industrial base	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Electricity grid	Richard J. Campbell	7-7905	rcampbell@crs.loc.gov
Financial institutions	N. Eric Weiss	7-6209	eweiss@crs.loc.gov
Industrial control systems	Dana Shea	7-6844	dshea@crs.loc.gov
Cybercrime			
Federal laws	Charles Doyle	7-6968	cdoyle@crs.loc.gov
Law enforcement	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
Cybersecurity workforce	Wendy Ginsberg	7-3933	wginsberg@crs.loc.gov
Cyberterrorism	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Cyberwar	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Data breach notification	Gina Stevens	7-2581	gstevens@crs.loc.gov
Economic issues	N. Eric Weiss	7-6209	eweiss@crs.loc.gov

Espionage			
Advanced persistent threat	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Economic and industrial	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
Legal issues	Brian T. Yeh	7-5182	byeh@crs.loc.gov
State-sponsored	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Federal agency roles	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Chief Information Officers (CIOs)	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov
Commerce	John F. Sargent, Jr.	7-9147	jsargent@crs.loc.gov
Defense (DOD)	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Executive Office of the President (EOP)	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Homeland Security (DHS)	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Intelligence Community (IC)	John Rollins	7-5529	jrollins@crs.loc.gov
Justice (DOJ)	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
National Security Agency (NSA)	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Science agencies (NIST, NSF, OSTP)	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Treasury and financial agencies	Rena S. Miller	7-0826	rsmiller@crs.loc.gov
Federal Information Security Management Act (FISMA)	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Federal Internet monitoring	Richard M. Thompson II	7-8449	rthompson@crs.loc.gov
Hacktivism	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
ormation sharing	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Antitrust laws	Kathleen Ann Ruane	7-9135	kruane@crs.loc.gov
Civil liability	Edward C. Liu	7-9166	eliu@crs.loc.gov
Classified information	John Rollins	7-5529	jrollins@crs.loc.gov
Freedom of Information Act (FOIA)	Gina Stevens	7-2581	gstevens@crs.loc.gov
Privacy and civil liberties	Gina Stevens	7-2581	gstevens@crs.loc.gov
International cooperation			
Defense and diplomatic	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Law enforcement	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
National strategy and policy	Eric A. Fischer	7-7071	efischer@crs.loc.gov
National security	John Rollins	7-5529	jrollins@crs.loc.gov
Public/private partnerships	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Supply chain	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Technological issues	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Botnets	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Cloud computing	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov
Mobile devices	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov
Research and development (R&D)	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov

Footnotes

[1]. For information on selected authoritative reports and resources on cybersecurity, see CRS Report R42507, *Cybersecurity: Authoritative Reports and Resources, by Topic*, by Rita Tehan. For lists of legislation and hearings in the 112th-114th Congresses, executive orders, and presidential directives, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.