ISSUES BEFORE CONGRESS ▾ REPORTS ▾ EVENTS ▾ RESOURCES ▾ ABOUT CRS ▾ MY CRS ▾ PLACE A REQUEST

CRS.gov

CRS REPORTS & ANALYSIS PRINT

Cybersecurity: Data, Statistics, and Glossaries

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

February 5, 2015 (R43310)

Jump to Main Text of Report

Related Author

- Rita Tehan

Related Policy Issue

- Cybersecurity

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.

Contents

Tables

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
Significant Cyber Incidents Since 2006	Ongoing	Center for Strategic and International Studies (CSIS)	15	A list of significant cyber events since 2006. The report states, "Significance is in the eye of the beholder, but we focus on successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars."
Overview of Current Cyber Attacks (logged by 180 Sensors)	Ongoing	Deutsche Telekom	N/A	Provides a real-time visualization and map of cyberattacks detected by a network of 180 sensors placed around the world.
Digital Attack Map	Ongoing	Arbor Networks	N/A	The map is powered by data fed from 270+ ISP customers worldwide who have agreed to share

				network traffic and attack statistics. The map displays global activity levels in observed attack traffic, which it is collected anonymously, and does not include any identifying information about the attackers or victims involved in any particular attack.
Real-Time Web Monitor	Ongoing	Akamai	N/A	Akamai monitors global Internet conditions around the clock. The map identifies the global regions with the greatest attack traffic.
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 websites, and threat trends by regional location, worldwide.
ThreatWatch	Ongoing	NextGov	N/A	ThreatWatch is a snapshot of the data breach intrusions against organizations and individuals, globally, on a daily basis. It is not an authoritative list, because many compromises are never reported or even discovered. The information is based on accounts published by outside news organizations and researchers.
McAfee Research & Reports (multiple)	Ongoing	McAfee	N/A	Links to reports by the company on cybersecurity threats, malware, cybercrime, and spam.
Data Breaches	Ongoing	Identity Theft Resource Center (ITRC)	N/A	The ITRC breach list is a compilation of data breaches confirmed by various media sources and notification lists from state governmental agencies. This list is updated daily and published each Tuesday. To qualify, breaches must include personally identifiable information that could lead to identity theft, especially Social Security numbers. ITRC follows U.S. federal guidelines about what combination of personal information comprises a unique individual. The exposure of this information constitutes a data breach.
Global Botnet Map	Ongoing	Trend Micro	N/A	Trend Micro continuously monitors malicious network activities to identify command-and-control (C&C) servers and help increase protection against botnet attacks. The real-time map indicates the locations of C&C servers and victimized computers they control that have been discovered in the previous six hours.
HoneyMap	Ongoing	Honeynet Project	N/A	The HoneyMap displays malicious attacks as they happen. Each red dot on the map represents an attack on a computer. Yellow dots represent honeypots, or systems set up to record incoming attacks. The black box on the bottom gives the location of each attack. The Honeynet Project is an international 501c3 non-profit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security.
The Cyberfeed	Ongoing	Anubis Networks	N/A	Provides real-time threat intelligence data worldwide.
Business Email Compromise	January 22, 2015	Internet Crime Complaint Center	N/A	The Business Email Compromise (BEC) is a sophisticated scam targeting businesses that work with foreign suppliers and businesses that regularly perform wire transfer payments. Cyber

				thieves stole nearly $215 million from businesses in the past 14 months, using a scam that starts when business executives or employees have their email accounts hijacked.
CISCO 2015 Annual Security Report (free registration required)	January 20, 2015	Cisco	53	Government agencies worldwide, compared with banks and many other companies, are better able to cope when the inevitable data breach occurs, according to the study on advances in cybersecurity. About 43% of the public sector falls into the "highly sophisticated" security posture segment. The best security stances can be found within the telecommunications and energy sectors, tied at 47%.
The Cost of Malware Containment	January 20, 2015	Ponemon Institute		According to the study, organizations typically received nearly 17,000 malware alerts weekly, which pose a taxing and costly endeavor. Of those alerts, only 3,218 were considered to be actionable and only 705 (or 4%) were investigated. An average of 395 hours is wasted weekly investigating and containing malware due to false positives or false negatives, costing participating organizations an estimated $1.27 million yearly in average value of lost time.
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.-based companies, spanning seven nations, found that over the course of a year, the average cost of cybercrime for companies in the United States climbed by more than 9% to $12.7 million up from $11.6 million in the 2013 study. The average time to resolve a cyberattack is also rising, climbing to 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 Security Survey (GSISS), on which the report is based, surveyed more than 9,700 respondents worldwide and detected that the number of cyber incidents increased at a compound annual rate of 66% since 2009. As the frequency of cyber incidents have risen so too has the reported costs of managing and mitigating them. Globally, the estimated average financial loss from cyber incidents was $2.7 million, a 34% increase over 2013. Big losses have also been more common, with the proportion of organizations reporting financial hits in excess of $20 million, nearly doubling. Despite greater awareness of cybersecurity incidents, the study found that global information security budgets actually 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 data breaches, with an average organization cost of more than $5 million. But in the end, it is the customers who are picking up the tab, from higher retail costs to credit card reissue fees.
Is Ransomware Poised for Growth?	July 14, 2014	Symantec	N/A	Ransomware usually masquerades as a virtual "wheel clamp" for the victim's computer. For example, pretending to be from the local law enforcement, it might suggest the victim had been using the computer for illicit purposes and to unlock it the victim would have to pay a fine —often between $100 and $500. Ransomware

				escalated in 2013, with a 500% (six-fold) increase in attack numbers between the start and end of the year.
Critical Infrastructure: Security Preparedness and Maturity	July 2014	Unisys and Ponemon Institute	34	Unisys and Ponemon Institute surveyed nearly 600 IT security executives of utility, energy, and manufacturing organizations. Overall, the report finds organizations are simply not prepared to deal with advanced cyber threats. Only half of companies have actually deployed IT security programs and, according to the survey, the top threat actually stems from negligent insiders.
The Value of a Hacked Email Account	June 13, 2013	Krebs on Security	N/A	One prominent credential seller in the underground peddles iTunes accounts for $8, and Fedex.com, Continental.com, and United.com accounts for USD $6. Groupon.com accounts fetch $5, while $4 buys hacked credentials at registrar and hosting provider Godaddy.com, as well as wireless providers Att.com, Sprint.com, Verizonwireless.com, and Tmobile.com. Active accounts at Facebook and Twitter retail for just $2.50 apiece... [S]ome crime shops go even lower with their prices for hacked accounts, charging between $1 and $3 for active accounts at dell.com, overstock.com, walmart.com, tesco.com, bestbuy.com and target.com, etc.
Online Trust Honor Roll 2014	June 11, 2014	Online Trust Alliance	N/A	Out of nearly 800 top consumer websites evaluated, 30.2% made the Honor Roll, which distinguishes them in best practices for safeguarding data in three categories: domain/brand protection, privacy, and security. Conversely, nearly 70% did not qualify for the Honor Roll, with 52.7% failing in at least one of the three categories.
Net Losses: Estimating the Global Cost of Cybercrime	June 2014	CSIS and McAfee	24	This report explores the economic impact of cybercrime, including estimation, regional variances, IP theft, opportunity and recovery costs, and the future of cybercrime. Cybercrime costs the global economy up to $575 billion annually, with the United States taking a $100 billion hit, the largest of any country. That total is up to 0.8% of the global economy. For the United States, the estimated $100 million cost means 200,000 lost jobs, and is almost half of the total loss for the G-8 group of Western 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 persistence, tactical skills, and technological prowess of their potential cyber adversaries. This year, three in four (77%) respondents to the survey detected a security event in the past 12 months, and more than a third (34%) said the number of security incidents detected increased over the previous year.
The Target Breach, by the Numbers	May 6, 2014	Krebs on Security	N/A	A synthesis of numbers associated with the Target data breach of December 19, 2013 (e.g., number of records stolen, estimated dollar cost to credit unions and community banks, amount

				of money Target estimates it will spend upgrading payment terminals to support Chip-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 worldwide in 2014, with U.S. firms paying almost $1.5 million more than the global average. In the United States, a data breach costs organizations on average $5.85 million, the highest of the 10 nations analyzed, up from $5.4 million in 2013. Globally, the cost of a breach is up 15% this year to $3.5 million. The United States likewise had the highest cost per record stolen, at $201, up from $188 last year. The country also led in terms of size of breaches recorded: U.S. companies averaged 29,087 records compromised in 2014.
Website Security Statistics Report	April 15, 2014	WhiteHat Security	22	WhiteHat researchers examined the vulnerability assessment results of the more than 30,000 websites under WhiteHat Security management to measure how the underlying programming languages and frameworks perform in the field. The report yields findings to specific languages that are most prone to specific classes of attacks, for how often and how long, as well as a determination as to whether popular modern languages and frameworks yield similar results in production websites. The popularity and complexity of .Net, Java, and ASP mean that the potential attack surface for each language is larger; as such, 31% of vulnerabilities were observed in .Net, 28% were found in Java, and 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 survey show that 18% of online adults have had important personal information—such as Social Security numbers, credit cards, or bank accounts—stolen. That is an increase from the 11% of online adults who reported personal information theft in July 2013 and 21% who said they had an email or social networking account compromised or taken over without their permission. The same number reported this experience in a July 2013 survey.
2014 Internet Security Threat Report	April 8, 2014	Symantec	98	In 2013, there were 253 data breaches that exposed more than 552 million sets of personal data, according to the annual report. The number of data breaches was up 62% from the previous year and nearly 50 more than in 2011, previously dubbed by Symantec "year of the breach." In addition, eight mega-breaches exposed more than 10 million identities each, an eightfold increase from one the year before and nearly double the five in 2011.
Advanced Threat Report 2013	February 27, 2014	FireEye	22	The report analyzes more than 40,000 advanced attacks across the globe to map out the latest trends in advanced persistent threat (APT) attacks. The United States topped the list of countries targeted by APT activity, which FireEye defines as online attacks that were "likely directly or indirectly supported by a nation state." American institutions were also targeted by many more APT malware families (collections of malware that share significant

				amounts of code with each other) than anywhere else.
State of the Internet Report, 3rd Quarter 2013	January 28, 2014	Akamai	40	Akamai maintains a distributed set of unadvertised agents deployed across the Internet that log connection attempts, which the company classifies as attack traffic. Based on the data collected by these agents, Akamai is able to identify the top countries from which attack traffic originates, as well as the top ports targeted by these attacks. Overall, the concentration of attacks declined during the third quarter of 2013, with the top 10 countries originating 83% of observed attacks, compared with 89% in the second quarter. China and Indonesia, however, continued to originate more than half of all observed attack traffic.
Cisco 2014 Annual Security Report	January 16, 2014	Cisco	81	The report offers data on and insights into top security concerns, such as shifts in malware, trends in vulnerabilities, and the resurgence of distributed denial-of-service (DDoS) attacks. The report also looks at campaigns that target specific organizations, groups, and industries, and the growing sophistication of those who attempt to steal sensitive information. The report concludes with recommendations for examining security models holistically and gaining visibility across the entire attack continuum—before, during, and after an attack. (Free registration required.)
McAfee Labs 2014 Threats Predictions	January 7, 2014	McAfee	6	In 2013, the rate of growth in the appearance of new mobile malware, which almost exclusively targets the Android platform, was far greater than the growth rate of new malware targeting PCs. In the last two quarters reported, new PC malware growth was nearly flat, while appearances of new Android samples grew by 33%.
Trends in Incident Response in 2013	October-December 2013	ICS-CERT Monitor	14	In 2013, ICS-CERT responded to 256 incidents reported either directly from asset owners or through other trusted partners. The majority of these incidents were initially detected in business networks of critical infrastructure organizations that operate industrial control systems (ICS). Of the 256 reported incidents, 59%, or 151 incidents, occurred in the energy sector, which exceeded all incidents reported in 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 cyber threats that have been assessed in the reporting period (i.e., within 2013). ENISA has collected over 250 reports regarding cyber threats, risks, and threat agents. ETL 2013 is a comprehensive compilation of the top 15 cyber threats assessed.
Emerging Cyber Threats Report 2014	November 14, 2013	Georgia Institute of Technology	16	The report highlights cloud security and security issues involving the 'Internet of Things,' referring to the notion that the increase of Internet-capable devices could create opportunities for remote hacking and data leakage. With everything from home automation to smartphones and other personal devices becoming connected to the Internet, these devices will capture more real-world information

				and could permit outside parties, companies, and governments to misuse that information. (From the annual Georgia Tech Cyber Security Summit 2013.)
2013/2014 Global Fraud Report	October 23, 2013	Kroll/Economist Intelligence Unit	N/A	The Annual Global Fraud Survey, commissioned by Kroll and carried out by the Economist Intelligence Unit, polled 901 senior executives worldwide from a broad range of industries and functions in July and August 2013. The number of companies suffering external cyberattacks designed to steal commercial secrets doubled in 2012-2013 compared with the previous financial year.
2013 Cost of Cyber Crime Study	October 8, 2013	HP and the Ponemon Institute	28	The study found the average company in the U.S. experiences more than 100 successful cyberattacks each year at a cost of $11.6 million. That is an increase of 26% from last year. Companies in other regions fared better, but still experienced significant losses. This year's annual study was conducted in the United States, United Kingdom, Germany, Australia, Japan, and France and surveyed over 230 organizations.
Illicit Cyber Activity Involving Fraud	August 8, 2013	Carnegie Mellon University Software Engineering Institute	28	Technical and behavioral patterns were extracted from 80 fraud cases—67 insider and 13 external—that occurred between 2005 and the present. These cases were used to develop insights and risk indicators to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage malicious insider activity within the banking and finance sector.
2013 Data Breach Investigations Report	April 23, 2013	Verizon	63	This annual report cited 621 confirmed data breaches last year, and more than 47,000 reported "security incidents." The victims spanned a wide range of industries. Thirty-seven percent of breached companies were financial firms; 24% were retailers and restaurants; 20% involved manufacturing, transportation and utility industries; and 20% of the breaches affected organizations that Verizon qualified as "information and professional services firms." (The totals exceed 100% because of rounding.)
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 violated data security law standards in 2012 than in the previous year, and at the same time, computer security costs have increased by more than $1 billion. Inadequate training was a large part of the reason all-around FISMA adherence scores slipped from 75% in 2011 to 74% in 2012. Agencies reported that about 88% of personnel with system access privileges received annual security awareness instruction, down from 99% in 2011. Meanwhile, personnel expenses accounted for the vast majority—90%—of the $14.6 billion departments spent on information 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 examining how socioeconomic factors in a country or region impact cybersecurity performance, examining measures such as use of modern technology, mature processes, user education,

				law enforcement and public policies related to cyberspace. This methodology can build a model that will help predict the expected cybersecurity performance of a given country or region.
SCADA [Supervisory Control and Data Acquisition] and Process Control Security Survey	February 1, 2013	SANS Institute	19	SANS Institute surveyed professionals who work with SCADA and process control systems. Seventy percent of the nearly 700 respondents said they consider their SCADA systems to be at high or severe risk. One-third of them suspect that they have been already been infiltrated.
Blurring the Lines: 2013 TMT Global Security Study	January 8, 2013	Deloitte	24	Report states that 88% of companies do not believe that they are vulnerable to an external cyber threat, even though more than half of those surveyed have experienced a security incident in the last year. Companies rated mistakes by their employees as a top threat, with 70% highlighting a lack of security awareness as a vulnerability. Despite this, less than half of companies (48%) offer even general security-related training, with 49% saying that a lack of budget was making it hard to improve security.
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 existing data and statistics in fields of information security, privacy, and the protection of children online. It highlights the potential for the development of better indicators in these respective fields showing in particular that there is an underexploited wealth of empirical data that, if mined and made comparable, will enrich the current evidence base for policymaking.
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 across the nation and found that only 24% of chief information security officers (CISOs) are very confident in their states' ability to guard data against external threats.
2012 NCSA/Symantec National Small Business Study	October 2012	National Cyber Security Alliance	18	This survey of more than 1,000 small and midsize businesses found that 83% of respondents said they do not have a written plan for protecting their companies against cyberattacks, while 76% think they are safe from hackers, viruses, malware, and cybersecurity 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 Alexander quoted a statistic from antivirus firm McAfee that the cost of worldwide cybercrime amounted to $1 trillion a year. "No, the statistic was not simply made up. Yes, it's just a 'ballpark figure' and an 'unscientific' one, the company admits. But despite Pro Publica's criticisms and its own rather fuzzy math, the company stands by its trillion-dollar conclusion as a (very) rough estimate."
Does Cybercrime Really Cost $1 Trillion?	August 1, 2012	ProPublica	N/A	In a news release from computer security firm McAfee announcing its 2009 report, "Unsecured Economies: Protecting Vital Information," the company estimated a trillion dollar global cost for cybercrime. That number does not appear in the report itself. McAfee's trillion-dollar estimate is questioned by the three

				independent researchers from Purdue University whom McAfee credits with analyzing the raw data from which the estimate was derived. An examination of their origins by ProPublica has found new grounds to question the data and methods used to generate these numbers, which McAfee and Symantec say they stand behind.
Measuring the Cost of Cybercrime	June 25, 2012	11th Annual Workshop on the Economics of Information Security	N/A	This report states that in total, cyber-crooks' earnings might amount to a couple of dollars per citizen per year. But the indirect costs and defense costs are very substantial (at least 10 times that). The authors conclude that "on the basis of the comparative figures collected in this study, we should perhaps spend less in anticipation of computer crime (on antivirus, firewalls etc.) but we should certainly spend an awful lot more on catching and punishing the 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 companies and 32% of companies of all sizes surveyed have been victims of social engineering, experiencing 25 or more attacks in the past two years, costing businesses anywhere from $25,000 to over $100,000 per security incident. Phishing and social networking tools are the most common sources of socially engineered threats.
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 profiles from a five-year targeted operation that penetrated 72 government and other organizations, most of them in the United States, and copied everything from military secrets to industrial designs.
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, pervasive, and costly cybercrime exploits from 2000 to 2010.

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
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."
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.
Glossary of Key Information Security Terms, Revision 2	National Institute of Standards and	May 2013	222	Besides providing some 1,500 definitions, the glossary offers a source for each term from either a

	Technology (NIST)			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 113th Congress.

Legislative Issues	Name/Title	Phone	Email
Legislation in the 113th 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
Information 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-113th Congresses, executive orders, and presidential directives, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.

Site index □

ISSUES BEFORE CONGRESS

Agriculture

Appropriations and Budget

Defense

Economy, Finance, and Recovery

Education, Employment, and Income

Emergencies and Disasters

Energy, Environment, and Resources

Federal Government

Foreign Policy

Health

Homeland Security and Terrorism

Housing

Law and Justice

Science and Technology

Social Policy

Tax

Trade

Transportation

REPORTS

Overview

Recent Reports

Find an Analyst

Constitution Annotated

Congressional Operations

Insights

Legal Sidebar

In Focus

EVENTS

All Events

Appropriations and Budget

Federal Legal Research

Legislative Process

Programs for District Offices

Orientations

Policy and Legal seminars

View/Cancel Registrations

Recorded Events

Training & Program Descriptions

RESOURCES

Overview

Tools for Staff

Legislative Reference Sources

Grants & Federal Assistance

Tracking Federal Funds

Congressional Liaison Offices

CQ's American Congressional Dictionary

ABOUT CRS

Overview

Contact us

CRS History

Leadership

Organization

Research Areas

Using CRS.gov

Legal / Credits

QUICK LINKS

Appropriations Status Table

Congressional Operations

Constitution Annotated

Events

Recent Reports

CRS Videos

New to Congress

District/State Staff

Services to Interns

Legislative Information System (LIS)

Feedback

Contact us....

EXTERNAL RESOURCES

Congress.gov

LC Net

Library of Congress Book Loan

CRS TEL: 7-5700