CRS Reports & Analysis

Cybersecurity: Data, Statistics, and Glossaries
July 16, 2018 (R43310)
Jump to Main Text of Report
Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739)
View Key Policy Staff

Related Author

- Rita Tehan

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, malware, and network securities.

Much is written on this topic, and this CRS report directs the reader to authoritative sources that address many of the most prominent issues. The annotated descriptions of these sources are listed in reverse chronological order, with an emphasis on material published in the last several years. Included are resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources.

The following reports comprise a series of authoritative reports and resources on these additional cybersecurity topics:

- CRS Report R44405, *Cybersecurity: Overview Reports and Links to Government, News, and Related Resources*, by Rita Tehan
- CRS Report R44406, *Cybersecurity: Education, Training, and R&D Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44408, *Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44410, *Cybersecurity: Critical Infrastructure Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44417, *Cybersecurity: State, Local, and International Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44427, *Cybersecurity: Federal Government Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan

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

(Continuously updated reports are listed in alphabetical order by source, followed by reports in reverse-chronological order)

Title	Date	Source	Pages	Notes
Real-Time Web Monitor (Global Attack Traffic) - Map	Continuously Updated	Akamai	N/A	Akamai monitors global internet conditions around the clock and identifies the global regions with the greatest attack traffic, cities with the slowest web connections (latency), and geographic areas with the most web traffic (traffic density).
The Cyberfeed	Continuously Updated	Anubis Networks	N/A	Provides real-time threat intelligence data worldwide.
Digital Attack Map	Continuously Updated	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 is collected anonymously, and does not include any identifying information about the attackers or victims involved in any particular attack.
Cyber Power Index	Continuously Updated	Booz Allen Hamilton and the Economist Intelligence Unit	N/A	The index of developing countries' ability to withstand cyberattacks and build strong digital economies rates the countries on their legal and regulatory frameworks, economic and social issues, technology infrastructure, and industry. The index puts the United States in the no. 2 spot, and the United Kingdom in no. 1.
Web Hacking Incidents Database	Continuously Updated	Breach Security, Inc.	N/A	The web hacking incident database (WHID) is a project dedicated to maintaining a list of web application-related security incidents. Its purpose is to serve as a tool for raising awareness of the web application security problem and provide information for statistical analysis of web application security incidents. Unlike other resources covering website security, which focus on the technical aspect of the incident, the WHID focuses on the impact of the attack. To be included in WHID an incident must be publicly reported, be associated with web application security vulnerabilities, and have an identified outcome.

Significant Cyber Incidents Since 2006	Continuously Updated	Center for Strategic and International Studies (CSIS)	15	This timeline records significant cyber events since 2006. It focuses on successful attacks on government agencies and defense and high tech companies, and economic crimes with losses of more than $1 million.
Cybersecurity Market Report	Continuously Updated	Cybersecurity Ventures	N/A	The quarterly report covers the business of cybersecurity, including market sizing and industry forecasts from research by IT analyst firms, emerging trends, employment, the federal sector, hot companies on the Cybersecurity 500 list, notable mergers and acquisitions, investment and initial public offering (IPO activity), and more.
Breaches Affecting 500 or More Individuals	Continuously Updated	Department of Health and Human Services	N/A	As required by Section 13402(e)(4) of the HITECH Act, the Secretary of Health and Human Services must list breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the breaches. Additionally, this new format includes brief summaries of breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary.
IMPACT - Information Marketplace for Policy and Analysis of Cyber-Risk & Trust	Continuously Updated	Department of Homeland Security (DHS) Science & Technology Directorate, Cybersecurity Division	N/A	IMPACT supports global cyber risk research & development by coordinating, enhancing, and developing real world data, analytics and information sharing capabilities, tools, models, and methodologies.
Overview of Current Cyber Attacks (logged by 180 Sensors)	Continuously Updated	Deutsche Telekom	N/A	Provides a real-time visualization and map of cyberattacks detected by a network of 180 sensors placed around the world.
Advanced Threat Report (annual reports)	Continuously Updated	FireEye	N/A	FireEye gathers and publishes threat intelligence gathered from millions of virtual machines in customer deployments. Expert analysts monitor, interpret, and package the data to better arm the public against cyber attackers. These annual threat reports include global and regional

				threat intelligence on industry trends as well as detailed malware analyses.
HoneyMap	Continuously Updated	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 501(nonprofit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve internet security.
Data Breaches	Continuously Updated	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.
World's Biggest Data Breaches (visualization)	Continuously Updated	Information is Beautiful	N/A	Selected data losses greater than 30,000 records.
Cytherthreat: Real-Time Map	Continuously Updated	Kaspersky Labs	N/A	Kaspersky Labs has launched an interactive cyberthreat map that lets viewers see cybersecurity incidents as they occur around the world in real time. The interactive map includes malicious objects detected during on-access and on-demand scans, email and web antivirus detections, and objects identified by vulnerability and intrusion detection sub-systems.
McAfee Research & Reports (multiple)	Continuously Updated	McAfee	N/A	Links to reports by the company on cybersecurity threats, malware, cybercrime, and spam.
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)	Continuously Updated	Microsoft Security Intelligence Report (SIR)	N/A	Data on infection rates, malicious websites, and threat trends by regional location, worldwide.

ThreatWatch	Continuously Updated	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.
DataLossDB	Continuously Updated	Open Security Foundation	N/A	The Open Security Foundation's DataLossDB gathers information about events involving the loss, theft, or exposure of personally identifiable information (PII). DataLossDB's dataset, in current and previous forms, has been used in research by numerous educational, governmental, and commercial entities, which often have been able to provide statistical analysis with graphical presentations.
Chronology of Data Breaches, Security Breaches 2005 to the Present	Continuously Updated	Privacy Rights Clearinghouse	N/A	These U.S.-only data breaches have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. The list is not a comprehensive compilation of all breach data. Reported incidents affecting more than nine individuals from an identifiable entity are included.
Global Botnet Map	Continuously Updated	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.
Timeline of Federal Civilian Cybersecurity Incidents	April 2018	Belfer Center (Harvard) in partnership with the Carnegie Endowment for International Peace	2	A list of federal civilian cybersecurity incidents, excerpted from the Appendix of the *Understanding Federal Cybersecurity* report (pages 46-47)
2018 Internet Security Threat Report	March 29, 2018	Symantec	89	"Targeted attack sector continues its

				expansion, including a 600% increase in IoT attacks; Cryptojacking explodes by 8,500%, stealing resources and increasing vulnerability; Ransomware shifts from big score to commodity, lowering prices while increasing variants; Malware implants grow by 200%, exploiting the software supply chain; Mobile malware continues to spread: variants increase by 54%."
The Economic Impact of Cybercrime --No Slowing Down	February 21, 2018	Center for Strategic & International Studies	28	The report concludes that close to $600 billion, nearly 1% of global GDP, is lost to cybercrime each year, which is up from a 2014 study that put global losses at about $445 billion. The report attributes the growth over three years to cybercriminals quickly adopting new technologies and the ease of cybercrime growing as actors leverage black markets and digital currencies.
The Cost of Malicious Cyber Activity to the U.S. Economy	February 2018	Council of Economic Advisers	62	The U.S. economy loses between $57 billion and $109 billion per year to malicious cyber activity (i.e., between 0.3% and 0.6% of the value of all the country's goods and services). The total loss figure is based primarily on analyzing the effects of data breaches and other cyber incidents on companies' stock prices. As a result, the data skews toward larger companies.
Internet Organised Crime Threat Assessment (IOCTA) 2017	October 2017	Europol	80	This year's report highlights how cybercrime continues to grow and evolve, taking new forms and directions, as demonstrated in some of the attacks of unprecedented scale of late 2016 and mid-2017. It further highlights the progressive convergence of cyber and serious and organised crime, supported by a professional underground service economy. The report goes on to list a number of key recommendations to address the phenomenon of cybercrime and identifies several priority topics to inform the definition of operational actions for EU law enforcement in the framework of the EU Policy Cycle. These include concrete actions under EC3's [European Cybercrime Centre] three main mandated areas - child sexual exploitation online, cyber-dependent crime, and payment fraud, as well as cross-cutting crime enablers.
The Equifax Data Breach: What to	September 8,	Federal Trade	NA	FTC information on what to do after the

Do	2017	Commission		Equifax data breach, including information how to set up a credit freeze and/or fraud alert.
Counting the Cost: Cyber Exposure Decoded	July 10, 2017	Lloyd's of London	56	Lloyd's estimates that the global cyber market is worth between $3 billion and $3.5 billion. Despite this growth, insurers' understanding of cyber liability and risk aggregation is an evolving process as experience and knowledge of cyber-attacks grows. Lloyd's of London warns that a serious cyber-attack could cost the global economy more than $120bn (£92bn) – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy.
2017 Cost of Data Breach Study: Global Overview	June 28, 2017	IBM and Ponemon	35	The average total cost of data breaches for the 419 companies participating in this research decreased from $4.00 to $3.62 million. The average cost for each lost or stolen record containing sensitive and confidential information also significantly decreased from $158 in 2016 to $141 in this year's study. However, despite the decline in the overall cost, companies in this year's study are having larger breaches. The average size of the data breaches in this research increased 1.8%.
2016 Internet Crime Report	June 21, 2017	Internet Crime Complaint Center's (IC3)	23	IC3 is a joint project of the National White Collar Crime Center and the FBI. In 2016, IC3 received a total of 298,728 complaints with reported losses in excess of $1.3 billion. This past year, the top three crime types reported by victims were nonpayment and nondelivery, personal data breach, and payment scams. The top three crime types by reported loss were Business Email Compromise (BEC), romance and confidence fraud, and non-payment and nondelivery scams.
What the Public Knows About Cybersecurity	March 22, 2017	Pew Research Center	18	Most Americans lack a basic understanding of online security measures. Although most of the people responding to the survey were able to identify string passwords from a list and knew that public Wi-Fi is not safe, just one-third knew what HTTPS is and just one-tenth were able to identify two-factor authentication. The survey of 1,055 American adults consisted of a 13-question online quiz. The median score was 5.5.

IBM X-Force Threat Intelligence Index 2017: The Year of the Mega-Breach (registration required)	March 2017	IBM Security	30	In 2016, more than 4 billion personal records were leaked worldwide, exceeding the combined total from the two previous years. The leaked documents comprised the usual credit cards, passwords, and personal health information, but the report also notes a shift in cybercriminal strategies, finding a number of significant breaches were related to unstructured data, such as email archives, business documents, intellectual property, and source code.
In 2017, The Insider Threat Epidemic Begins	February 2017	Institute for Critical Infrastructure Technology	52	The report offers a comprehensive analysis of the Insider Threat Epidemic, including research on (1) Characterizing Insider Threats (the insider threat cyber "kill chain," nonmalicious insider threats, malicious insider threats); (2) The Insider Threat Debate; (3) Policies, Procedures, and Guidelines to Combat Insider Threats; (4) Non-Technical Controls; and (5) Technical Controls.
Emerging Cyber Threats, Trends, and Technologies for 2017	December 2016	Georgia Institute of Technology Institute for Information Security and Privacy	20	The report discusses emerging cyber threats, trends and technologies for the year 2017. The report is broken down into several sections that discuss emerging threats and trends, such as the privacy technology nexus, e-voting systems, ransomware, global information manipulation, health care fraud, and dual-use technologies. The report offers solutions to the topics that are derived from experts in the field.
2016 Norton Cybersecurity Insights Report	November 23, 2016	Symantec	9	Researchers surveyed 20,907 consumers in 21 markets, 76% of respondents said they know they should actively protect their information online, but still engaged in risky behaviors, including sharing passwords. The report found that globally, 35% of people said they have at least one unprotected device, vulnerable to ransomware and phishing attacks, and that within the last year, 689 million people in 21 countries experienced a cybercrime.
The 2016 Cyber Resilient Organization (Executive Summary)	November 16, 2016	Ponemon Institute and IBM	5	Cyber resilience is an organization's ability to maintain its core purpose and integrity in the face of cyberattacks. The global survey features insight from more than 2,400 security and IT professionals from around the world, including the United States, United Kingdom, France, Germany, United Arab Emirates, Brazil,

				and Australia. Only 32% of IT and security professionals say their organization has a high level of cyber resilience—down slightly from 35% in 2015. The 2016 study also found that 66% of respondents say their organization is not prepared to recover from cyberattacks.
Q3 State of the Internet/Security Report	November 15, 2016	Akamai	40	Akamai says it confronted 19 "mega attacks" in the third quarter of this year, including the two biggest it has ever encountered in history. The prime targets for the 19 mega attacks, which Akamai defines as those that reach over 100 Gbps, were media and entertainment companies, even though gaming and software firms were also hit. The two record-breaking attacks, reaching 623 Gbps and 555 Gbps, were directed at security blogger Brian Krebs. The attacks succeeded in taking down Krebs' website until Jigsaw, a unit of Google's parent company Alphabet GOOG, deployed its Project Shield service to deflect the attack.
Building Confidence: Facing the Cybersecurity Conundrum	November 1, 2016	Accenture	8	A survey of 2,000 security officers representing large enterprises worldwide reveals that "on average, an organization will face more than a hundred focused and targeted breach attempts every year, and respondents say one in three of these will result in a successful security breach."
Examining the Costs and Causes of Cyber Incidents	October 10, 2016	RAND	15	Researchers found that the typical cost of a breach was about $200,000 and that most cyber events cost companies less than 0.4% of their annual revenues. The $200,000 cost was roughly equivalent to a typical company's annual information security budget.
Measuring the Financial Impact of IT Security on Businesses	September 13, 2016	Kaspersky Lab	N/A	The survey reveals that on average, a single cybersecurity incident now costs large businesses a total of $861,000. Meanwhile, small and medium businesses (SMBs) pay an average of $86,500. To assess the state of the security landscape in the United States and across the world, Kaspersky Lab looked at the attitudes toward security, the cost of data breaches and the losses incurred from incidents. According to the survey results, nearly half (49%) of U.S. businesses, and over half globally (52%), assume that their IT security will be compromised at some

				point.
Examining the Costs and Causes of Cyber Incidents	August 25, 2016	Journal of Cybersecurity	15	The research seeks to examine the composition and costs of cyber events, and attempts to address whether there are incentives for firms to improve their security practices and reduce the risk of attack. "Specifically, we examine a sample of over 12 000 cyber events that include data breaches, security incidents, privacy violations, and phishing crimes. First, we analyze the characteristics of these breaches (such as causes and types of information compromised). We then examine the breach and litigation rate, by industry, and identify the industries that incur the greatest costs from cyber events. We then compare these costs to bad debts and fraud within other industries."
Legal Issues in Cybersecurity and Data Privacy [Infographic]	August 24, 2016	Labyrinth Law	N/A	The infographic displays data breach statistics, legal responsibility information, a brief list of regulatory enforcement actions, and mitigating threat suggestions.
2016 Internet Security Threat Report | Government	April 8, 2016	Symantec	98	Public-sector data breaches exposed some 28 million identities in 2015, but hackers were responsible for only one-third of those compromises, according to new research. Negligence was behind nearly two-thirds of the exposed identities within government agencies. In total, the report suggests 21 million identities were compromised accidentally, compared with 6 million by hackers.
2016 Data Breach Investigations Report (annual)	April 2016	Verizon	85	This report covers 100,000+ incidents, including 2,260 analyzed breaches across 82 countries. "In 93% of cases, it took attackers minutes or less to compromise systems. Organizations, meanwhile, took weeks or more to discover that a breach had even occurred—and it was typically customers or law enforcement that sounded the alarm, not their own security measures."
Data Breach Digest: Scenarios from the Field	March 3, 2016	Verizon	84	The report is a set of 18 case studies chosen to represent the most common and destructive types of incidents seen over the past eight years. For each incident, the report reveals the events leading up to the breach, details of the investigation, and the how Verizon helped the organization recover. The incidents include a water

				utility at which intruders managed to manipulate water treatment processes and flow, a developer who outsourced his work to China, and pirates (the seafaring variety) who used information stolen from a shipping company's computers to target specific containers on vessels they boarded.
Emerging Cyber Threats Report 2016	November 2015	Georgia Institute of Technology Cybersecurity Summit 2015	20	Nearly two dozen cybersecurity experts from Georgia Tech, business, government and defense, share their observations about emerging trends in a more connected world. Key findings included the privacy tug-of-war between individuals and organizations has become a tug with no war; exponential growth in the Internet of Things over the past two years creates a larger cyberattack surface; the digital economy is growing more complex while a lack of highly trained security workers persists worldwide; and cyber espionage shows no sign of abating.
2015 Global Report on the Cost of Cybercrime	October 8, 2015	HP Enterprise Security and Ponemon	30	The study found that a benchmark sample of U.S. organizations experienced an average cost of cybercrime of $15 million. The study shows that since 2009, the average cost of cybercrime per organization per year increased by 82%. This year the range was anywhere between $1.9 million and $65 million each year per company. While annualized cost increases as organizational size increases, small organizations incur more than double the per-capita cost than large organization, experiencing $1,571 in costs per seat compared with a larger organization's $667 per seat.
Follow the Data: Dissecting Data Breaches and Debunking Myths	September 22, 2015	Trend Micro	N/A	Trend Micro's Forward-Looking Threat Research (FTR) Team has taken 10 years of information on data breaches in the United States from the Privacy Rights Clearinghouse (PRC) (from 2005 through 2015) and subjected it to detailed analysis to better understand the real story behind data breaches and their trends. The study identifies a number of deeper trends such as (1) hacking or malware attacks account for the single greatest cause of data loss with portable device loss a close second, (2) PII is the data most likely stolen with financial data second, and (3) credentials are not the most commonly stolen data, but the most likely data to lead to additional types of data loss.

E-mail Account Compromise (EAC)	August 27, 2015	FBI Internet Crime Complaint Center (IC3)	N/A	The FBI warned about a significant spike in victims and dollar losses stemming from an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers. According to the FBI, thieves stole nearly $750 million in such scams from more than 7,000 victim companies in the United States between October 2013 and August 2015.
Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes	June 23, 2015	FBI Internet Crime Complaint Center (IC3)	N/A	Between April 2014 and June 2015, the CryptoWall ransomware cost Americans more than $18 million. The money was spent not only on ransoms, which range from $200 to $10,000 apiece, but also on "network mitigation, network countermeasures, loss of productivity, legal fees, IT services, or the purchase of credit monitoring services for employees or customers."
2015 Cost of Data Breach: Global Analysis	May 27, 2015	Ponemon Institute/IBM	31	According to the study of 350 companies spanning 11 countries, the average consolidated total cost of a data breach is $3.8 million, representing a 23% increase since 2013.The study also found that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased 6% from a consolidated average of $145 to $154. Health care emerged as the industry with the highest cost per stolen record with the average cost for organizations reaching as high as $363. Additionally, retailers have seen their average cost per stolen record jump dramatically from $105 last year to $165 in this year's study.
2015 Data Breach Investigations Report (DBIR)	April 14, 2015	Verizon	70	A full three-quarters of attacks spread from the first victim to the second in 24 hours or less, and more than 40% spread from the first victim to the second in under an hour. On top of the speed with which attackers compromise multiple victims, the useful lifespan of shared information can sometimes be measured in hours. Researchers also found that of the IP addresses observed in current information sharing feeds, only 2.7% were valid for more than a day, and the number dwindles from there.

HIPAA Breaches: The List Keeps Growing	March 12, 2015	Healthcare IT News	N/A	More than 41 million people have had their protected health information compromised in Health Insurance Portability and Accountability Act (HIPAA) privacy and security breaches. Using data from the Department of Health and Human Services, which includes HIPAA breaches involving more than 500 individuals, reported by 1,149 covered entities and business associates, the website compiled a sortable, 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 incidents reported by federal agencies to the DHS decreased last year. Data show the total bulk number of incident reports sent by the largest 24 agencies to US-CERT going up by about 16% during FY2014 from the year before. But when two significant categories from that data set are removed—"non-cybersecurity incidents" and "other"—the number actually shows a decrease of about 6%. Noncybersecurity incidents involve the mishandling of personality identifiable information, but without a cybersecurity component, meaning the data breach likely occurred through a misplaced paper document. Incidents classified as "other" are things such as automated network scans, blocked attempts at access, and miscellaneous events. Reported incidents of actual serious cybersecurity issues, such as malware, suspicious network activity, and improper usage, declined last year. Real threats that did increase in recorded number include social engineering, unauthorized access, and denial-of-service attacks.
2014 Global Threat Intel Report	February 6, 2015	CrowdStrike	77	This report summarizes CrowdStrike's year-long daily scrutiny of more than 50 groups of cyber threat actors, including 29 different state-sponsored and nationalist adversaries. Key findings explain how financial malware changed the threat landscape and point of sale malware became increasingly prevalent. The report also profiles a number of new and sophisticated adversaries from China and Russia, including Hurricane Panda, Fancy Bear, and Berserk Bear.
Incident Response/Vulnerability Coordination in 2014	February 2015	ICS/CERT Monitor	15	In FY2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received and responded to 245

				incidents reported by asset owners and industry partners. The energy sector led all others again in 2014 with the most reported incidents. ICS-CERT's continuing partnership with the energy sector provides many opportunities to share information and collaborate on incident response efforts. Also noteworthy in 2014 were the incidents reported by the critical manufacturing sector, some of which were from control systems equipment manufacturers.
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 challenge. 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 has risen so too have 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% 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, 2014	Krebs on Security	N/A	From the blog, "One prominent credential seller in the underground peddles iTunes accounts for $8, and Fedex.com, Continental.com, and United.com accounts for $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 billion 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 (US-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. In 2013, 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	Cybersecurity expert Brian Krebs synthesizes 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, and amount of money Target estimates it will spend upgrading payment terminals to support Chip-and-PIN enabled cards).
Website Security Statistics Report	April 15, 2014	WhiteHat	22	WhiteHat researchers examined the

		Security		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.
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.
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 cybercrimes from 2000 to 2010.

Source: Highlights compiled by CRS from the reports.

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

(Continuously updated reports are listed in alphabetical order by source, followed by reports in reverse-chronological order)

Title	Source	Date	Pages	Notes
Sideways Dictionary	*Washington Post* and Jigsaw	Ongoing	N/A	Defines cyber and technology terms using nontechnical analogies.
Codex -Building Blocks	Wilson Center	Ongoing	N/A	Definitions and examples of computer security terms.
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.
Cybersecurity Style Guide	Bishop Fox	February 15, 2018	92	This guide is designed for security researchers. It provides advice on which words to use in reports, how they should look in the middle of a sentence, and how to pronounce them out loud. Since the terms are listed alphabetically, you'll find serious usage advice right next to playful entries about internet culture.
Global Cyber Definitions Database	Organization for Security and Co-operation in Europe (OSCE)	November 2014	N/A	A compilation of definitions of cybersecurity and 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 four 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	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.
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.
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 Concept of Operations (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.

Author Contact Information

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

Key Policy Staff

See CRS Report R42619, *Cybersecurity: CRS Experts*, by Eric A. Fischer for the names and contact information for CRS experts on policy issues related to cybersecurity.

Footnotes

1.

For lists of legislation and hearings in the 112th-115th Congresses, executive orders, and presidential directives, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.