4

Cybersecurity

Wolters Kluwer | BAKER BOTTS

Cybersecurity Introduction

Cyber-attacks have become a serious security concern for any company that touches Big Data. In just the third quarter of 2016, 18 million new malware samples were captured.[1] More than 4,000 ransomware attacks have occurred every day since the beginning of 2016, which is a 300% increase from 2015, where 1,000 ransomware attacks were seen per day.[2] 2016 also saw a high-profile, subversive incident which occurred in the run-up to the 2016 U.S. presidential election. A joint investigation by the U.S. Department of Homeland Security and Federal Bureau of Investigation concluded that two groups of Russia's intelligence services were responsible for the attack.[3]

A cyber-attack can spread quickly and breach the security of computer systems in multiple countries. For example, on May 12, 2017, the WannaCry ransomware attack targeted computers running the Microsoft Windows operation system and infected more than 230,000 computers in over 150 countries within the first day.[4] The victims included not only individuals but also multinational companies like FedEx,[5] Nissan,[6] and Telefónica.[7]

The costs associated with protecting against and recovering from cyber-attacks can be substantial. Steve Langan, chief executive at Hiscox Insurance, estimated that in 2016, cybercrime cost the global economy over $450 billion,[8] and this number is projected to reach $2 trillion by 2019.[9]

---

1 *Cybercrime Reaches New Heights in the Third Quarter,* Panda Security (Oct. 20, 2016), *http*://www.pandasecurity.com/mediacenter/pandalabs/pandalabs-q3/.

2 *How to Protect Your Networks from Ransomware,* Department of Justice (*https*://www.justice.gov/criminal-ccips/file/872771/download (last visited Oct. 31, 2017).

3 *Grizzly Steppe – Russian Malicious Cyber Activity,* United States Computer Emergency Readiness Team (Dec. 29, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

4 Abhijit Ahaskar, *New wave of malware attacks and how you can tackle them,* live mint (Oct. 28, 2017), http://www.livemint.com/Leisure/R1J9RJhZv6niz2l9DhyOgJ/New-wave-of-malware-attacks-and-how-you-can-tackle-them.html.

5 Jackie Wattles, *Who got hurt by the ransomware attack*, CNN Tech (May 14, 2017), http://money.cnn.com/2017/05/13/technology/ransomware-attack-who-got-hurt/index.html.

6 *Id.*

7 Shona Ghosh and Rob Price, *A massive cyberattack using leaked NSA exploits has hit 99 countries, and it's still spreading,* Business Insider (May 12, 2017), http://www.businessinsider.com/telefonica-and-other-firms-have-been-infected-by-wannacry-malware-2017-5.

8 Luke Graham, *Cybercrime costs the global economy $450 billion: CEO,* CNBC (Feb. 7, 2017), https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

9 Steve Morgan, *Cyber Crime Costs Projected to Reach $2 Trillion by 2019,* Forbes (Jan 17, 2016), https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#331218ae3a91.

Information-Security Challenges and Threats

COMMON ATTACKS

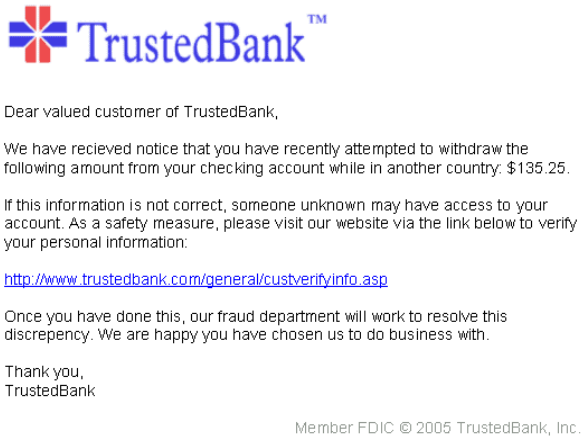
PHISHING

Phishing is an attempt to acquire sensitive information or install malicious software by masquerading as a trustworthy entity in an electronic communication. According to the Anti-Phishing Working Group ("APWG"), the total number of phishing attacks in 2016 exceeded 1.2 million, which was the highest number of attacks recorded to date.[10] In a June 14, 2016, announcement, the FBI warned that cyber scammers attempted to steal $3.1 billion between October 2013 and May 2016 from 22,143 victims.[11]

The figure below shows a typical phishing email, disguised as an official email from a bank. The sender is attempting to deceive the recipient into revealing confidential information by falsely "confirming" it at the phisher's website. Although the web address of the bank's webpage appears to be legitimate, the hyperlink would actually direct the recipient to the phisher's webpage. Other common phishing attacks include requesting that the communication recipient call a telephone number to receive a refund or requesting that the recipient click a hyperlink to update and verify his or her information.

[10] *Unifying the Global Response to Cybercrime,* APWG (Feb. 23, 2017), http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf.

[11] *Business E-Mail Compromise: The 3.1 Billion Dollar Scam,* Federal Bureau of Investigation (Jun. 14, 2016), https://www.ic3.gov/media/2016/160614.aspx.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Phishing email

Among different phishing scams, spear phishing, an email directed at specific individuals or companies, has been one of the most successful techniques.[12] The cybersecurity firm FireEye conducted a survey that found that 84% of organizations had experienced a successful spear-phishing attack in 2015. The survey further found that the average impact of a successful spear-phishing attack was $1.6 million.[13] According to FireEye, some victims of spear-fishing attacks saw their stock price drop by as much as 15% after a phishing attack.[14]

MALWARE

Malware is software intended to damage, disable, or otherwise misuse computer systems (e.g., computer viruses, worms, trojan horses, ransomware, spyware, and adware). The security firm Symantec discovered more than 430 million new unique pieces of malware in 2015, up 36 percent from the year before.[15]

In 2016, ransomware became one of the top malware threats for businesses.[16] Ransomware blocks access to the victim's data or threatens to publish or delete it until a ransom is paid. Nearly 400 variants of ransomware were detected in the last quarter of 2016.[17] CryptoLocker, one of the most successful ransomware attacks, infected over 500,000 victims and extorted an estimated $3 million before it was taken down by authorities.[18] In May 2017, the

---

12 Debbie Stephenson, *Spear Phishing: Who's Getting Caught?*, Firmex (May 30, 2013), https://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught/.

13 *Spear-Phishing Attacks,* FireEye, https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (last visited Oct. 31, 2017).

14 *Id.*

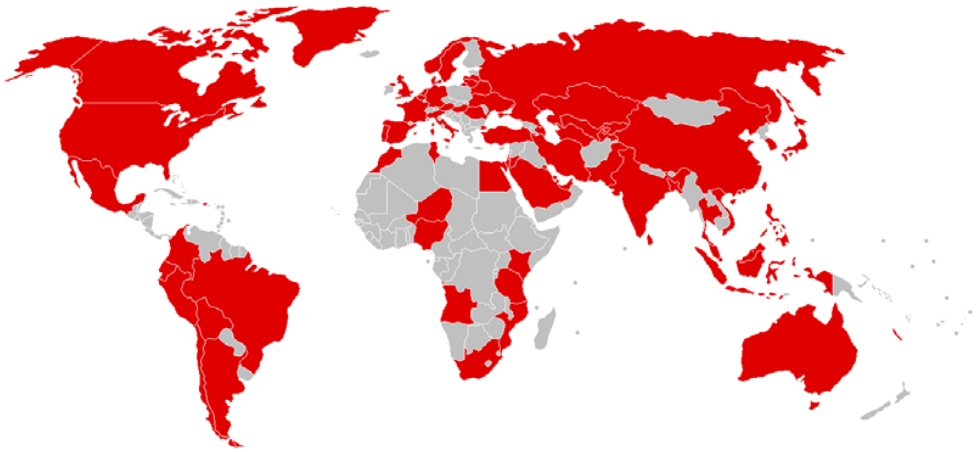
15 *Internet Security Threat Report,* Symantec (Apr. 2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

16 *State of Malware Report,* Malwarebytes (2017), https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf.

17 *Id.*

18 Mark Ward, *Cryptolocker victims to get files back for free,* BBC (Aug. 6, 2014), http://www.bbc.com/news/technology-28661463.

WannaCry attack affected more than 200,000 victims and infected more than 300,000 computers.[19] The figure below shows the countries affected by WannaCry in the first few hours of the attack.



Map of the countries initially affected by WannaCry[20]

Ad fraud malware is another common cybersecurity threat. Ad fraud, also called click fraud or click spam, is a practice wherein dubious advertising networks use automated programs to interact with advertisements online.[21] The programs attempt to generate fraudulent internet traffic or advertisement clicks by simulating legitimate user activity,[22] which can be used to generate profits for the website or service hosting the advertisement.[23] For example, in May 2017, Google removed more than 40 apps from of its Play store after it discovered that the apps were generating fraudulent clicks on ads.[24] By the time Google took action, the malicious apps had already spread to an estimated 4.5 to 18.5 million devices.[25] The company behind the malicious apps was projected to make $300,000 per month through the fraudulently generated ad clicks.[26]

---

19 *See* Ahaskar, *supra* note 4.

20 *Countries initially affected in WannaCry ransomware attack*, Wikipedia, https://commons.wikimedia.org/wiki/File:Countries_initially_affected_in_WannaCry_ransomware_attack.png (last visited Oct. 31, 2017).

21 *Ad fraud,* Malwarebytes (Jun. 9, 2016), https://blog.malwarebytes.com/threats/ad-fraud/.

22 *Id.*

23 *Id.*

24 *The Judy Malware: Possibly the largest malware campaign found on Google Play*, Check Point (May 25, 2017), http://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/.

25 *Id.*

26 Thomas Fox-Brewster, *Google Just Killed What Might Be The Biggest Android Ad Fraud Ever*, Forbes (May 26, 2017), https://www.forbes.com/sites/thomasbrewster/2017/05/26/google-shuts-down-massive-ad-fraud-on-play-store/#66eecbb97807.

ADVANCED PERSISTENT THREATS (APTs)

An advanced persistent threat ("APT") is a network attack in which an unauthorized entity gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network. Understanding how APT works can be beneficial for preventing an attack. As described by the security firm FireEye, an APT attack can be described in six stages:

1. The cyber-criminal, or threat actor, gains entry through an email, network, file, or application vulnerability and inserts malware into an organization's network. The network is considered compromised, but not breached.
2. The advanced malware probes for additional network access and vulnerabilities or communicates with command-and-control (CnC) servers to receive additional instructions and/or malicious code.
3. The malware typically establishes additional points of compromise to ensure that the cyber-attack can continue if one point is closed.
4. Once a threat actor determines that they have established reliable network access, they gather target data, such as account names and passwords. Even though passwords are often encrypted, encryption can be cracked. Once that happens, the threat actor can identify and access data.
5. The malware collects data on a staging server, then exfiltrates the data off the network and under the full control of the threat actor. At this point, the network is considered breached.
6. Evidence of the APT attack is removed, but the network remains compromised. The cyber-criminal can return at any time to continue the data breach.

Anatomy of Advanced Persistent Threats, FireEye.[27]

Unlike other cyber threats, an APT attack is usually conducted by nation-state actors, organized criminal actors, corporate espionage actors, or terrorists with high sophistication and advanced resources.[28] The organized attackers often target specific industries where there is valuable information and assets, such as finance, defense and aerospace, entertainment and media, healthcare, manufacturing, technology, and utility industries.[29]

Between March 2014 and April 2015, the United States Office of Personnel Management ("OPM") was under APT attack. Then-FBI Director James Comey estimated 18 million federal employees' records might have been affected.[30]

---

[27] *Anatomy of Advanced Persistent Threats*, FireEye, https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html (last visited Oct. 31, 2017).

[28] *Advanced Persistent Threats: Learn the ABCs of APTs - Part A,* Secure Works, (Sept. 27, 2016), https://www.secureworks.com/blog/advanced-persistent-threats-apt-a.

[29] *Id.*

[30] Evan Perez and Shimon Prokupecz, *First on CNN: U.S. data hack may be 4 times larger than the government originally said,* CNN (Jun. 24, 2015), http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html.

DISTRIBUTED DENIAL OF SERVICE (DDoS)

A Distributed Denial of Service ("DDoS") attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. DDoS attacks target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.[31]

There are three major categories of DDoS attack:

1. Traffic attacks: Traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation.
2. Bandwidth attacks: This DDoS attack overloads the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service.
3. Application attacks: Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

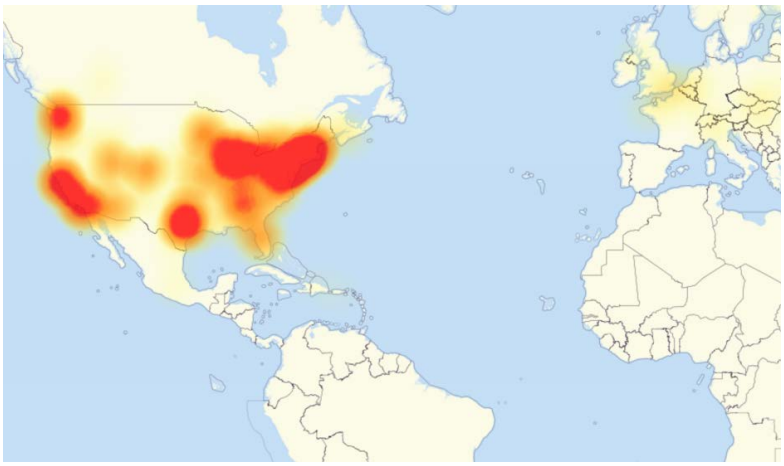
DDoS attacks can be massive in scope. The largest DDoS attack known to date exceeded one terabit per second,[32] and the scale of DDoS attacks is projected to continue to grow as the increase in Internet of Things ("IoT") devices gives attackers a larger number of entry points. In a recent attack, several popular online services were impacted after the groups Anonymous and New Work Hackers attacked Dyn, one of the major Domain Name System ("DNS") providers.[33] This attack caused many high-profile websites like Twitter, Netflix, Airbnb, Amazon, and Reddit to slow their access or go completely offline for hours before Dyn restored service. The figure below shows a map of areas affected by the Dyn attack as of October 21, 2016, 1:45 pm Pacific Time.

---

[31] *What is a DDoS Attack?,* Digital Attack Map, http://www.digitalattackmap.com/understanding-ddos/.

[32] *World's Largest 1 Tbps DDoS Attack Launched from 152,000 Hacked Smart Devices*, The Hacker News (Sept. 27, 2016), https://thehackernews.com/2016/09/ddos-attack-iot.html.

[33] Eric Geller and Tony Romm, *WikiLeaks supporters claim credit for massive U.S. cyberattack, but researchers skeptical*, Politico (Oct. 21, 2016), http://www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145.



A map of internet outages in Europe and North America caused by the Dyn cyber-attack[34]

SQLS INJECTIONS

SQL injection is a code injection technique in which malicious structured query language ("SQL") statements are used to extract data from a database. The technique can provide an attacker with unauthorized access to sensitive data including, customer data, personally identifiable information ("PII"), trade secrets, intellectual property and other sensitive information.

An SQL attack occurs when hackers submit SQL query code into a web form, and the web application that processes this input does not properly check and validate it, thereby allowing the attacker to command the database to access its data.[35] Different commands can achieve different results, and often an attacker will try variations to see what information a database will release. An attacker, for example, can send one type of SQL command to display the entire contents of a database in a web browser, or use other commands to display parts of a database or allow for the ability to add, modify or delete the contents of the database.[36]

Even though the first public discussions of SQL injections appeared around 1998,[37] SQL attacks still occur in a widespread manner and continue to be one of the most common technical vulnerabilities. In April 2017, multiple

---

[34] Lorenzo Franceschi-Bicchierai, *Blame the Internet of Things for Destroying the Internet Today,* Motherboard (Oct. 21 2016), https://motherboard.vice.com/en_us/article/vv7xg9/blame-the-internet-of-things-for-destroying-the-internet-today.

[35] Kim Zetter, *Hacker Lexicon: SQL Injections, an Everyday Hacker's Favorite Attack,* Wired (May 11, 2016), https://www.wired.com/2016/05/hacker-lexicon-sql-injections-everyday-hackers-favorite-attack/.

[36] *Id.*

[37] Sean Michael Kerner, *How Was SQL Injection Discovered?*, eSecurity Planet (Nov. 25, 2013), http://www.esecurityplanet.com/network-security/how-was-sql-injection-discovered.html.

SQL-injection security issues were discovered in the WordPress Facebook Plugin, a tool to integrate one's personal website with Facebook.[38]

KINETIC ATTACKS

Kinetic attacks, also called kinetic bombardment attacks, are intrusions which cause direct or indirect physical damage through the exploitation of vulnerable information and processes.[39] These attacks have been used in the context of espionage and sabotage, and they have been employed criminally in attacks throughout the world.[40]

In one example, StuxNet, a computer worm jointly developed by the U.S. and Israel, attacked Iran's nuclear centrifuge facility in Natanz. The attack reduced centrifuge operational capacity at the Natanz facility by 30% in one year by causing infected centrifuges to increase their normal operating speed by almost 40%.[41] The increase in centrifuge operating speed caused the aluminum centrifugal tubes to expand and come in contact with other tubes, which ultimately destroyed the machines.[42]

In another example, Russian operatives used a kinetic attack to disrupt the electrical network in western Ukraine, causing disruptions to the operation of 27 distribution stations and three power plants. There was evidence that the attackers were able to delay the restoration of power services by wiping information from the computer systems used to control power distribution.[43]

RECENT TRENDS

SMARTPHONES

Smartphones can make an attractive target for online criminals because of the valuable personal information they contain. For example, mobile payment systems allow smartphone users to link their credit cards and bank accounts directly to their mobile devices. Given the amount of valuable personal information contained on smartphones, cyber-criminals are likely to continue targeting these devices in the future.

---

38 *WordPress Facebook Plugin SQL Injection Vulnerability*, Defense Code, http://www.defensecode.com/advisories/DC-2017-04-011_WordPress_Facebook_Plugin_Advisory.pdf (last visited Oct. 31, 2017).

39 Scott D. Applegate, *The Dawn of Kinetic Cyber,* CCDCOE (2013), https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf (last visited Oct. 31, 2017).

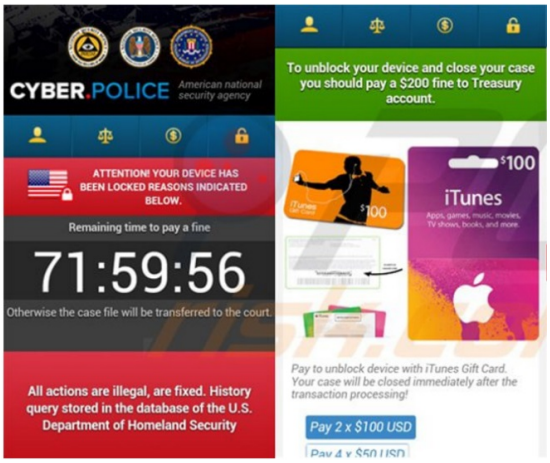
40 *Id.*

41 *Id.*

42 William J. Broadm John Markoff, and David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay,* The New York Times (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all; Holger Stark, *Stuxnet Virus Opens New Era of Cyber War*, Spiegel Online (Aug 8, 2011), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html.

43 Warwick Ashford, *Cyber attacks caused Ukraine power outages, report confirms,* Computer Weekly (Jan. 11, 2016), http://www.computerweekly.com/news/4500270434/Cyber-attacks-caused-Ukraine-power-outages-report-confirms.

Historically, Android devices have been a popular target in this category. In 2015, 3,944 new Android mobile malware variants were detected, which represented a 77% increase over 2014 when 2,227 variants were discovered.[44] However, vulnerabilities on the iOS platform have also been prevalent in recent years. [45] Below is a screenshot of an Android ransomware, Sonorousness, which demanded $200 from victims to unlock the infected device.



Android ransomware Sonorousness

INTERNET OF THINGS (IOT)

Coined by Kevin Ashton of Procter & Gamble and MIT's Auto-ID Center in 1999, the Internet of things ("IoT") is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.[46] The introduction of IoT in consumer devices has had an impact on the ways we live and do business. For example, the Nest Smart Thermostat can learn a family's routines and automatically adjust the temperature based on when people are at home or away, awake or asleep.[47] The August Smart Lock can unlock the door for you automatically when you get home.[48] And Ralph Lauren's Polo Tech

---

44 *See Internet Security Threat Report*, *supra* note 15.

45 *Id.*

46 Arik Gabbai, *Kevin Ashton Describes "the Internet of Things"*, The Smithsonian (Jan. 2015), https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/.

47 *Meet the Nest Learning Thermostat,* Nest, https://nest.com/thermostat/meet-nest-thermostat/ (last visited Oct. 31, 2017).

48 *August Smart Lock,* August, http://august.com/products/august-smart-lock/?utm_source=6916&utm_medium=cpc&utm_campaign=a11-a108-a3961-00&gclid=CLP_x__RqdQCFRmBswodMK0ARA (last visited Oct. 31, 2017).

Shirt tracks the wearer's biometric information and sends that data to the cloud.[49] In the U.S., by some estimates there are 25 online devices per 100 inhabitants.[50] Gartner estimates that 20.8 billion connected things will be in use worldwide by 2020, with the IoT delivering a $2 trillion economic benefit globally.[51]

However, the IoT faces fundamental security challenges, as illustrated by the past three years in which a growing number of attacks have targeted or made use of IoT devices. In July 2015, Chrysler announced a voluntary recall of 1.4 million vehicles after two journalists reported that hackers were able to remotely control a Jeep's brakes and steering wheel.[52] Two months later, a group of Chinese researchers were able to take control of several Tesla Model S vehicles remotely.[53] The Dyn distributed denial-of-service ("DDoS") attack discussed above was a botnet[54] coordinated through a large number of IoT devices, including cameras, residential getaways, and baby monitors, that were infected with a malware.[55] In January 2017, attackers locked the electronic key system and computers of a four-star Austrian hotel and demanded $1,800 in bitcoins to restore functionality.[56] In addition, researchers have found potentially deadly vulnerabilities in numerous medical devices such as insulin pumps, x-ray systems, CT-scanners, and implantable defibrillators.[57]

IoT devices frequently lack stringent security measures, making them a soft and popular target for cybercriminals.[58] IoT devices often contain a system on a chip that executes the actual protocol connection to the internet, and because the chips are generally integrated into the IoT products, users may not be able to change

---

[49] Stu Roberts, *Ralph Lauren Polo Tech shirt reads wearer's biological and physiological info,* New Atlas (Aug. 25, 2014), https://newatlas.com/ralph-lauren-polo-tech/33504/.

[50] *OECD Digital Economy Outlook 2015*, OECD iLibrary (Jul. 15, 2015), http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en.

[51] *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*, Gartner (Nov. 10, 2015), http://www.gartner.com/newsroom/id/3165317.

[52] Chris Welch, *Chrysler recalls 1.4 million cars at risk of being remotely hijacked,* The Verge (Jul. 24, 2015), https://www.theverge.com/2015/7/24/9032179/chrysler-announces-voluntary-recall-hack.

[53] Andrea Peterson, *Researchers remotely hack Tesla Model S,* The Washington Post (Sept. 20, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/?utm_term=.0df1a1bd24ca.

[54] A botnet is a number of Internet-connected devices each of which is running one or more automatic tasks over the Internet.

[55] *See* Franceschi-Bicchierai, *supra* note 34.

[56] Dan Bilefsky, *Hackers Use New Tactic at Austrian Hotel: Locking the Doors,* The New York Times (Jan. 30, 2017), https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html.

[57] Kim Zetter, *Medical Devices That Are Vulnerable to Life-Threatening Hacks,* Wired (Nov. 24, 2015), https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/.

[58] Roger Park, *The Internet of Things (IoT) and Security Risks,* Symantec (Apr. 17, 2015), https://www.symantec.com/connect/blogs/iot-security-risks.

the login information.[59] In addition, according to the security firm Arxan, 80% of IoT applications are not tested for vulnerabilities.[60]

[59] Larry Loeb, *The Internet of Trouble: Securing Vulnerable IoT Devices,* Security Intelligence (Nov. 4, 2016), https://securityintelligence.com/the-internet-of-trouble-securing-vulnerable-iot-devices/.

[60] *Study Confirms Companies are Concerned About Hacking Through Mobile and IoT Applications*, Arxan, https://www.arxan.com/2017-Ponemon-Mobile-Iot-Study/ (last visited Oct. 31, 2017).

Best Practices

As the frequency and severity of cyber-attacks increase, companies face a rapidly evolving security climate. This section provides a guideline for best practices when developing cyber defense strategies.

RISK ASSESSMENTS

A risk-assessment process is often the first step for any risk-prevention program. The goal of a risk assessment is for an organization to understand the cybersecurity threats to organizational operations, organizational assets, and individuals.[61] The requirements for properly assessing risk can vary by industry. In recognition of the importance of addressing cybersecurity risks, the National Institute of Standards and Technology developed a framework, which can be a useful resource when developing a risk assessment plan.[62] Steps that can be included in a thorough risk assessment are discussed below.

IDENTIFY AND DOCUMENT ASSET VULNERABILITIES

Asset inventories are a key component of a risk assessment. To assess risks, organizations should first know what assets they have and what assets are most critical to protect. Cyber-attacks frequently cause harm using manipulation, disablement, theft, or damage of information from electronic systems. Accordingly, assets that are not inherently hazardous can still be used to cause harm. When assessing an asset's vulnerability, the asset's potential for manipulation, the cost to reproduce the asset, and the asset's utility to an assailant can be considered.

IDENTIFY AND DOCUMENT FORESEEABLE INTERNAL AND EXTERNAL THREATS

The scope of a risk assessment should be calculated to identify the reasonably foreseeable threats from within and outside an institution's operations that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, as well as the reasonably foreseeable threats due to the disposal of customer information. Familiarity with the major forms of cyber-attacks, as discussed in the previous section, can help organizations choose the proper risk assessment scope.

IDENTIFY POTENTIAL BUSINESS IMPACTS AND LIKELIHOODS

In addition to identifying reasonably foreseeable internal and external threats, a risk assessment should evaluate the potential damage from these threats. Some impacts are commonly known to managers, such as customer breach notifications, post-breach customer protection measures, regulatory compliance, public relations, crisis

---

61 *Framework for Improving Critical Infrastructure Cybersecurity,* NIST (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

62 *Id.*

communications, legal measures, cybersecurity improvements, and technical investigations.[63] However, some costs are less visible, such as insurance premium increases, increased cost to raise debt, operational disruption, lost value of customer relationships, value of lost contract revenue, devaluation of trade name, and loss of intellectual property.[64]

ASSESS THE SUFFICIENCY OF RISK-MITIGATION MEASURES[65]

Risk mitigation measures can broadly be defined in three categories: physical measures, technical measures, and administrative measures. Physical measures can include methods of restricting physical access to high risk areas, such as data centers. Access can be restricted by using electronic access credentials, dual authentication access readers at entrance doors (e.g., PIN pads or biometric readers), mandatory routine PIN changes, and individualized badging.[66] Additional physical measures can include the use of escorts for all authorized visitors (e.g., maintenance or other vendors), controls logs, and secure automated backup processes.[67]

Technical measures can include software to monitor network traffic and warn the organization's response team of known malware, anomalous activity, or patterns suggestive of malware or attack. Security alerts from an organizations infrastructure tools, for example, can be aggregated and made searchable.[68] Encryption of data is also commonly deployed.[69]

Administrative measures can include written policies and procedures governing user password complexity, employee background checks, and access to areas with sensitive systems or data. Financial institutions are routinely scrutinized on the adequacy of these written policies.[70]

DEFENSE IN DEPTH

The concept of Defense in Depth originated in military strategy to provide barriers to impede the progress of intruders from attaining their goals while monitoring their progress and developing and implementing responses to the incident to repel them. In the cybersecurity paradigm, Defense in Depth involves implementing detective and protective measures to impede the progress of a cyber intruder while enabling an organization to detect and respond to the intrusion with the goal of reducing and mitigating the consequences of a breach.

Defense in Depth has three core concepts: (1) multiple layers of defense, (2) distinguished layers of defense, and (3) threat-specific layers of defense. Multiple-layer defense assures that if one layer is bypassed, another layer can provide sufficient defense. The typical layers used in network defense include patch management, email security and archiving, antivirus software, data encryption, firewalls, anti-spam and spam filters, and digital certificates. To

---

63 *Business impacts of cyber attacks*, Deloitte (July 2016), https://www2.deloitte.com/au/en/pages/media-releases/articles/business-impacts-cyber-attacks.html.

64 *Id.*

65 *Cybersecurity regulation and best practice in the US and UK*, LexisNexis, https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice (last visited Oct. 31, 2017).

66 *Id.* at 5.

67 *Id.*

68 *Id.* at 4.

69 *Id.*

70 *Id.* at 4-5.

provide a more efficient protection system, it is crucial that each layer of defense adopts different techniques or methods, so that even if one layer is bypassed, the intruders would need to spend more effort to penetrate the subsequent layers. Specific layers of defense aim to guard against popular attacks such as computer malware, DDoS, and information theft. The advantage to having threat-specific layers of defense is that it could provide a tailored defense to attacks unique to certain industries.

TRAINING

To better protect against cyber-attacks, employees should understand their roles and responsibilities in protecting sensitive data and company assets. The security lab Kaspersky listed the following tips for employers to educate their employees about cybersecurity:[71]

- Talk to employees regularly about cybersecurity;
- Remember that top management and IT staff are also employees;
- Employees need to cooperate to improve the overall security of the whole system;
- Warn employees to pay attention to social engineering activities;
- Train employees to recognize cyber-attacks;
- Encourage employees to speak up in the event a real cyber-attack happens;
- Conduct cyber-attack drills with employees; and
- Request feedback from employees.

PRE-STAGING BREACH PREVENTION AND RESPONSE EXPERTISE

Because major attacks are often automated and premeditated, changes to the computing environment to which an attacker has access may prematurely alert the attacker that they have been discovered. Before taking investigative or remedial steps, many experienced security advisors recommend that the attack be well identified, and that effective plans to permanently eradicate the unauthorized access should be ready for execution, before the attacker is alerted to discovery.

There are many considerations in the aftermath of a cyber-attack, including notifying those affected, documenting the organization's response, maintaining the privacy and attorney-client privilege of sensitive information, preserving evidence that can identify the source of the attack, and determining the proper level of information to provide to both shareholders and regulators. Additionally, whether to voluntarily notify law enforcement, affected data subjects, affected commercial partners, regulators, and /or data protection authorities is often a complicated, multi-jurisdictional, multi-stakeholder process.

Large financial institutions typically have highly experienced communications experts on their staff. A major cyber-attack is a discreet category of crisis, with diverse causes and PR challenges, that requires targeted preparation. Many financial institutions have found that augmenting the internal team with outside experts with experience on

---

[71] *Top 10 Tips for Educating Employees About Cybersecurity*, Kaspersky Lab (2015), *available at* https://corpcounsel.tradepub.com/free/w_aaaa5769/.

major breaches in the same industry is very valuable. Media training specific to data breach scenarios is also common.

SECURITY AUDITS AND TESTING

In addition to regular system backups and encryption of important data, it is important to perform security audits and testing. Hackers and cyber-attackers are quick to expose online vulnerabilities. It is important to ensure that financial services firms in particular invest in testing the robustness of their security and have the capacity to create patches or rewrite code to fix potential entry points for malicious actors on short notice.

BOARD-LEVEL ATTENTION

As the value of many businesses can be derived from intangible assets such as intellectual property and market data, and such assets are dynamic and mobile, corporate boards should consider making defense of digital assets a top priority. According to a KLAS Research report entitled, *Cybersecurity 2017: Understanding the Healthcare Security Landscape*, only 16% of health service providers reported having "fully functional" security programs. Another 41% reported that they had developed and started to implement a program. However, 43% reported that their organization's security program was either "developing" or "not developed." Smaller hospitals and physician practices lagged in their program development. 18% of survey respondents reported that seven percent or greater of their total IT budget was dedicated to security while 14% of respondents said spending on security made up about 5-6% of their IT budget. The largest segment, 41% of respondents, reported dedicating 3% or less of their IT budget to security, while 27% only allocated 3-4% of their total IT budget on security.

HUMAN RESOURCES POLICIES AND INTEGRATION

The role of human resources ("HR") teams can sometimes be ignored in a cybersecurity defense program. However, human resources teams frequently work with the data that is most vulnerable to attack. According to the Society for Human Resource Management ("SHRM"), HR records contain highly sensitive and private information: social security numbers, dates of birth, bank detail and home addresses.[72] Accordingly, HR professionals should be aware of the importance of protecting data within their own department and the company as a whole.[73]

VENDOR AGREEMENTS

An April 2015 survey of 40 banks by New York's superintendent of financial services found that only about a third required their outside vendors to notify them of any breach to their own networks, which could in turn compromise the confidential information of the bank and its customers.[74] Fewer than half the banks surveyed said they conducted regular on-site inspections to make sure the vendors they hire—like providers of outsourced

---

[72] Drew Robb, *Preventing Hacker Attacks,* SHRM (Jun. 24, 2014), *https://www.shrm.org/hr-today/news/hr-magazine/Pages/0714-technology-security.aspx*.

[73] *The Role of HR In Mitigating Cyber Security Threats,* Global HR (Feb. 24, 2016), http://www.ghrr.com/blog/2016/02/24/the-role-of-hr-in-mitigating-cyber-security-threats/.

[74] *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, New York State Dep't of Fin. Servs. (April 2015), http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf

technology functions, accounting firms, law firms—use adequate security measures.[75] About half require vendors to provide a warranty that their products and data streams are secure and virus-free.[76]

The survey of banks also found that financial firms in the US lag behind their counterparts in Europe when it comes to adding protections to safeguard information shared with third-party firms.[77] For example, the report found that European banks were better at requiring vendors and other outside parties to use multifactor authentication.[78] Because an organization's cybersecurity is often only as good as the cybersecurity of its vendors, it is important to exercise appropriate due diligence in selecting service providers. To better protect themselves, organizations can require service providers to implement appropriate security controls, agree to non-disclosure provisions regarding the institution's systems and data, and monitor and supervise these relationships over the life of an agreement.[79]

INFORMATION SHARING

The financial services sector has established a voluntary organization to share cybersecurity alert and response information in the United States: The Financial Service Information Sharing and Analysis Center ("FS-ISAC"). FS-ISAC collects threat intelligence from across its membership, and from the U.S. Department of Homeland Security and distributes that information to its members in real-time.[80] Industry experts within FS-ISAC verify and analyze threats and identify recommended solutions before alerting FS-ISAC members.[81]

In the UK, the Cyber Security Information Sharing Partnership ("CiSP") works similarly as FS-ISAC. CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time through a secure, confidential, and dynamic environment, with the aim of increasing situational awareness and reducing the impact of cyber-attacks on UK business.[82]

CYBERSECURITY INSURANCE

Like traditional insurance, cybersecurity insurance can mitigate losses from a variety of cyber incidents by transferring some of the financial risk of a security breach to an insurer. Policies frequently cover extortion demands, hacking, DDoS, data breaches, business interruption, and network damage.[83] However, many companies forego available policies, citing the perceived cost of policies, confusion about policy coverage, and uncertainty

---

75 *Id.*

76 *Id.*

77 *Id.*

78 *Id.*

79 Kevin McCoy, *Banks face new cyber security rules for vendors,* USA Today (Apr. 9, 2015), https://www.usatoday.com/story/money/2015/04/09/bank-cybersecurity-threats/25517905/.

80 *About FS-ISAC,* FSISAC, https://www.fsisac.com/about (last visited Oct. 31, 2017).

81 *Id.*

82 *See Cyber Security Information Sharing Partnership*, National Cyber Security Centre (last updated Dec. 19, 2017), https://www.ncsc.gov.uk/cisp.

83 *See, e.g.*, *Cybersecurity Insurance*, U.S. Department of Homeland Security (last visited Mar. 6, 2018), https://www.dhs.gov/cybersecurity-insurance (last updated Aug. 11, 2017).

about the likelihood of a cyber-attack.[84] According to a March 2015 report by the UK Cabinet Office, 10% of UK firms have some form of cyber coverage and only 2% of large UK businesses have standalone cyber-insurance products.[85]

The U.S. cyber insurance market reached an estimated $2 billion in premiums in 2014 and is continuing to grow.[86] While a variety of cyber insurance products are available in the U.S. market, the majority of cyber insurance is directed to data privacy coverage.[87] The focus on data breach coverage is largely due to U.S. regulatory complexity, which includes federal laws regarding health records and state data breach notification laws in almost all states.[88] When purchasing cybersecurity insurance, companies should be mindful of the specific terms of their policy. Many policies do not cover losses stemming from operational mistakes, reputational damage, or industrial espionage.

CRISIS MANAGEMENT

Since cyber-attacks are often complex and multi-faceted, detecting and assessing the scope and impact of an incident may be challenging and time consuming. Therefore, as part of assessing the cybersecurity risks facing an organization, internal processes, protocols, and a crisis management playbook can help organizations better prepare to address risk. The steps below can form part of an effective cybersecurity crisis management plan.

DEFINE THE PARAMETERS OF A CYBERSECURITY CRISIS [89]

The first step can involve simply defining cybersecurity and what that means to the organization. For example, a cybersecurity incident may be defined as a "breach, compromise or disruption of the organization's critical data and/or systems."[90] The definition can be tailored to fit the specific needs of organizations in different industries. Organizations should assess which data and/or systems are considered most critical.

DEVELOP AN INTERNAL ESCALATION PROCESS[91]

Cybersecurity incidents vary in size and degree; depending on the size and nature of an organization, numerous issues and potential threats may be detected on a regular basis. To facilitate appropriate responses to each

---

84 *Id.*

85 *UK Cyber Security Report,* GOV.UK (Mar. 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.

86 Dan Schutzer, *CTO Corner: An Assessment of Cyber Insurance*, Fin. Servs. Roundtable (Feb. 9, 2015), http://www.fsroundtable.org/cto-corner-assessment-cyber-insurance/; Richard S. Betterley, Cyber/Privacy Insurance Market Survey – 2014, The Betterley Report (June 2014).

87 *2016 Cyber Insurance Buying Guide,* American Bankers Association (2016), https://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf.

88 Robert P. Hartwig, Ph.D. & Claire Wilkinson, *Cyber Risks: The Growing Threat*, Insurance Information Institute (June 2014), https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf.

89 Melissa Agnes, *Management Plan,* Melissa Agnes (Jul. 26, 2016), http://melissaagnes.com/5-steps-developping-cyber-security-crisis-management-plan/.

90 *Id*.

91 *Id.*

incident, organizations can develop a set of escalation procedures to ensure upper management is made aware of events determined to be sufficiently serious. Often a filtering process can include a set of questions for first responders, such as the I.T. team, to answer when making the initial assessment of a threat. Effective questions can help first responders assess the potential business impact of each incident. Depending on how the questions are answered, the incident can be escalated to a group dedicated to cybersecurity responses and potentially to senior management.

UNDERSTAND THE LEGAL ASPECTS OF A CYBERSECURITY CRISIS[92]

It is important to understand the legal responsibilities an organization is faced with in the event of a breach. As discussed in greater detail in the following section, various jurisdictions impose different obligations and timelines in the event of a breach depending on the nature of the data involved and additional factors. To help untangle the complexity, an organization's crisis response plan can include a matrix that details the different rules and laws within each jurisdiction in which the organization operates.

DRAFT A CRISIS COMMUNICATIONS HANDBOOK, AND PUT IT TO THE TEST[93]

When drafting playbooks and crisis communication handbooks, it is important to have two main goals in mind: (1) maintaining the trust of your stakeholders; and (2) meeting the legal requirements for notification. To address these goals, it can be helpful to review action items, contact lists, and timelines for each member of the crisis team for the most likely cybersecurity scenarios that pertain to the organization. An outline of the different notifications and parameters for communicating with your stakeholder can also be drafted. Finally, it is important to put the plan and team to test. After a crisis preparedness program is developed, it should be tested to identify gaps and weaknesses.

---

92 *Id.*

93 *Id.*

Legal Issues

REGULATIONS

UNITED STATES

In the US, there are several laws that govern practices for the sharing of information, contacting customers, and maintaining data security.

The Cybersecurity Information Sharing Act of 2015 ("CISA") applies to the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies.[94]

The Gramm-Leach-Bliley Act ("GLBA"), also known as the Financial Services Modernization act of 1999, requires financial institutions to explain their information sharing practices to their customers and to safeguard sensitive data.[95]

The Health Insurance Portability and Accountability Act ("HIPAA") of 1996 includes data privacy and security provisions for safeguarding medical information. HIPAA consists of five Titles, where Title II, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers and health care employers.[96] Furthermore, some courts have found that state law imposes a legal duty to safeguard consumer confidential information entrusted to a commercial entity.[97] Additionally, almost all states have passed laws requiring entities to notify individuals of security breaches involving personally identifiable information.[98]

The Telephone Consumer Protection Act ("TCPA") of 1999, enacted in response to a growing number of telephone marketing calls, limits the use of automatic dialing systems, artificial or prerecorded voice messages, SMS text messages, and fax machines. In 2012, the FCC revised the TCPA rules to require telemarketers to: (1) obtain prior express written consent from consumers before robo-calling them; (2) to restrict telemarketers from using an

---

94 *See* John Evangelakos et al., *A Guide to the Cybersecurity Act of 2015*, Law360 (Jan 12, 2016), https://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015.

95 Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

96 *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub L. No. 104-191, 110 Stat. 1936 (1996); *About HHS*, HHS.gov, https://www.hhs.gov/about/index.html (last visited Oct. 31, 2017).

97 *See, e.g.*, *In re: Sony4 Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014), order corrected, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014)

98 *See* Security Breach Notification Laws, National Conference of State Legislatures (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

"established business relationship" to avoid getting consumer consents; and (3) to require telemarketers to provide an automated and interactive option to "opt-out" of receiving calls from telemarketers.[99]

The Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act establishes requirements when sending unsolicited commercial emails. Specifically, the act (1) bans false or misleading header information, such as deceptive subject lines in emails; (2) requires providing consumers the option to opt out of future emails; and (3) directs the FTC to issue rules and criteria for determining the primary purpose of emails and labeling any sexually commercial emails.[100]

In addition, the U.S. Securities and Exchange Commission ("SEC"), has provided guidance to help public companies determine when they are obligated to report cybersecurity risks to shareholders.[101] The Commission emphasizes that public companies should take steps to inform investors about material cybersecurity risks and incidents in "a timely fashion."[102] While the Securities Act does not specifically address cybersecurity risks, the reporting requirements of the Act, including those pertaining to annual 10-K and quarterly 10-Q filings, require companies to disclose material cybersecurity risks.[103] When considering the materiality of cybersecurity risks, companies should consider the potential for "harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities."[104] When disclosing cybersecurity risks, companies should avoid generic disclosures and try to provide specific information to help investors understand the risks.[105] The SEC further cautions against insider trading related to material non-public cybersecurity information.[106]

EUROPEAN UNION

As discussed in Chapter 3, the EU's General Data Protection Regulation ("GDPR") was passed in 2016 to provide increased protection for personal data across the EU. The GDPR, which takes effect in May of 2018, regulates "the processing of personal data."[107] When the GDPR goes into effect, it will repeal the 1995 data directive and impose

---

[99] *See, e.g.*, Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243 (1991); *Telemarketing and Robocalls*, FCC, https://www.fcc.gov/general/telemarketing-and-robocalls (last visited Oct. 31, 2017).

[100] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 1699 (2003).

[101] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166 (Feb. 26, 2018).

[102] *Id.* at 8167.

[103] *Id.* at 8168.

[104] *Id.* at 8169.

[105] *Id.*

[106] *Id.* at 8167.

[107] The General Data Protection Regulation, Regulation (EU) 2016/679, Art. 4, defines "processing" to mean "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

a number of new obligations on organizations that process personal data. With respect to cybersecurity, the GDPR imposes an obligation on those who control and process personal data to "implement appropriate technical measures and organizational measures to ensure a level of security appropriate to the risk."[108] The GDPR further imposes mandatory data breach reporting, requiring data processors to report a breach to regulators "without undue delay and, where feasible, not later than 72 hours after having become aware of it."[109] The GDPR further authorizes regulators to impose harsh penalties for non-compliance; fines of up to 4% of worldwide annual turnover are possible for some violations.[110]

The Network and Information Security ("NIS") Directive, also taking effect in May 2018, is a directive on the security of network and information systems. It was adopted by the European Parliament to provide legal measures to boost the overall level of cybersecurity in the EU by:

- Requiring Member States to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
- Setting up a cooperation group among all Member States to support and facilitate strategic cooperation and the exchange of information among Member States;
- Setting up a CSIRT Network to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
- Requiring businesses in these sectors that are identified by the Member States as operators of essential services to take appropriate security measures and to notify serious incidents to the relevant national authority; and
- Requiring key digital service providers (search engines, cloud computing services and online marketplaces) to comply with the security and notification requirements.[111]

The Directive on Privacy and Electronic Communications (Directive 2002/58/EC), also known as the E-Privacy Directive, was implemented to work in tandem with the 1995 data directive by addressing specific data privacy concerns. The E-Privacy Directive is perhaps most known for the regulation of webpage cookies. For example, the Directive provides that "[m]ember States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information

---

"personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[108] *Id.* at Art. 32.

[109] *Id.* at Art. 33.

[110] *Id.* at Art. 83.

[111] *The Directive on security of network and information systems (NIS Directive)*, European Commission, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (last update Sept. 19, 2017).

in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller."[112] The Directive also places restrictions on unsolicited marketing communications.[113] Notably, the European Commission has circulated a proposed Regulation on Privacy and Electronic Communications that would supersede the E-Privacy Directive if passed.[114]

PROPOSED LEGISLATION[115]

Until recently, there has been no single law, statute, or regulation requiring businesses to provide security for the data collected from their consumers. In August 2017, U.S. Senators Mark R. Warner (D-VA), Cory Gardner (R-CO), Ron Wyden (D-OR), and Steve Daines (R-MT) introduced bipartisan legislation directed to improving the cybersecurity of devices connected to the Internet.[116] The Internet of Things Cybersecurity Improvement Act of 2017 would mandate standards requiring a base level of security for any IoT devices that are used by the government. The bill would require that devices support patches and password changes and would give security researchers greater legal protection to hack devices to test potential exploits.[117]

Specifically, the proposed Internet of Things Cybersecurity Improvement Act of 2017 would[118]:

- Require that vendors of Internet-connected devices purchased by the federal government ensure: their devices are patchable, they rely on industry standard protocols, they do not use hard-coded passwords, and their systems do not contain any known security vulnerabilities;
- Direct the Office of Management and Budget (OMB) to develop alternative network-level security requirements for devices with limited data processing and software functionality;
- Direct the Department of Homeland Security's National Protection and Programs Directorate to issue guidelines regarding cybersecurity coordinated vulnerability disclosure policies to be required by contractors providing connected devices to the U.S. Government;
- Exempt cybersecurity researchers engaging in good-faith research from liability under the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act when engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines;
- Require each executive agency to inventory all Internet-connected devices in use by the agency.

---

[112] Directive on Privacy and Electronic Communications Art. 5(3) (Directive 2002/58/EC).

[113] *Id*. at Art. 13.

[114] *See* Proposal for an ePrivacy Regulation, European Commission (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[115] Thomas J. Smedinghoff, *An Overview of Data Security Legal Requirements for All Business Sectors*, Locke Lorde http://media.lockelord.com/files/uploads/Insurance/Article%20-%20Data%20Security%20Requirments%20for%20All%20Business%20Sectors.pdf (last visited Oct. 31, 2017).

[116] *Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices,* Mark R. Warner (Aug. 1, 2017), https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices [hereinafter Warner].

[117] Jon Fingas, *Senate bill demands tougher security for the Internet of Things*, Engadget (Aug. 1, 2017), https://www.engadget.com/2017/08/01/senate-iot-security-bill/.

[118] *See* Warner, *supra* note 116.

If this or similar legislation is passed, some commenters expect there to be implications for consumer devices as well as those used in government. For example, manufacturers might find it more cost effective to sell all their devices with security features incorporated, regardless of whether they are intended for government or private consumers. However, since many IoT devices are directed principally to consumers, it is hard to predict to what extent manufacturers would voluntarily adopt the standards into consumer devices should the bill pass.[119]

[119] Rhys Dipshan, *Proposed IoT Cybersecurity Legislation Could Lead to Consumer Device Standards*, Corporate Counsel (Aug. 3, 2017), http://www.corpcounsel.com/id=1202794700025/Proposed-IoT-Cybersecurity-Legislation-Could-Lead-to-Consumer-Device-Standards?mcode=1202617073467&curindex=4&curpage=ALL.