PUBLISHED AUGUST 2021

Cyber Threat Landscape

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

Cyber Threat Landscape

Published August 2021

The cyber threat landscape is continually changing and evolving as attackers develop new tools and discover new attack vectors and defenders find new techniques to counter these attacks. Machine learning and artificial intelligence are being increasingly used by both attackers and defenders, and the importance of these tools is likely to increase in the future.[1] Modern computer networks are complex systems, and a weakness in any component of the system could render the entire system vulnerable.

Most businesses today rely heavily on computer systems, and when these systems do not function as expected or when private data is stolen or lost, the impact to the business can be significant. When critical network infrastructure is compromised (either made unavailable or accessed by unauthorized individuals), the business can be impacted in a number of ways, including:

- Business interruption—Data loss (whether accidental or due to hostile action) could hamper a company's ability to conduct business. For example, if a company's inventory control database goes down, the company may be left unable to handle outgoing orders, leading to significant financial harm. Likewise, if a company's online store website stops working, revenue may plummet.
- Competitive risk—A company may store proprietary business information such as product designs, business strategies, and pricing/cost information on computer systems. If these systems are compromised and the information falls into the hands of a competitor, the company may be placed at a competitive disadvantage.
- Liability risk—Many companies store user and/or employee data. If this information is not handled securely, a company may be held legally liable for any harm caused.
- Direct costs—Victims of cyberattacks may incur significant costs related to the incident. This could include costs for investigation and defense of regulatory actions associated with the incident, payment of ransoms, fines or penalties, costs to restore or replace digital assets, and costs for legal assistance and credit monitoring for victims of the breach.

1 "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks"; Wilson Center blog post; Nov. 28, 2018.

Who conducts cyberattacks, and why?

Attackers use knowledge of computer hardware and software to identify and exploit vulnerabilities in computer systems and networks. These attacks may be conducted by individuals or groups, and the attackers' motives and skill levels vary widely. Some attacks are sophisticated, using previously unknown techniques and vulnerabilities to gain access to the target system. Such attacks typically require advanced knowledge of software design and network services. Other attacks are launched using publicly available hacking software. These attacks do not require any specialized knowledge and can be launched by anyone who can find the software online.[2] While cyberattacks often come from outside an organization, there is also a significant risk of insider attacks from employees who misuse their access to company data and computer resources. A 2018 survey of cybersecurity professionals found that over half had dealt with insider attacks within the previous 12 months.[3]

Cybercrime can be remarkably lucrative. An estimated 76% of 2018 cyber breaches were conducted due to the attacker's financial motivation.[4] A 2018 study found that low-earning cyber-criminals can bring in $3,500+ per month, middle-earners can make $75,000+, and high-earners can make over $166,000 per month.[5] Some make money by holding data "hostage." These attackers gain access to a user's system and install software (ransomware) that encrypts data on the user's system using an encryption key known only to the attacker. To regain access to the data, the user is required to make a payment to the attacker, who then provides the key to unencrypt the data. Paying the ransom does not guarantee that data access will be regained. A 2019 report found that 38.8% of organizations that paid the ransom as directed still lost their data despite paying the ransom.[6] Cybersecurity experts generally recommend against paying such ransoms.[7]

Other attackers attempt to gain access to companies' systems in order to steal the data stored there. Common targets for theft are personally identifiable information (PII), such as names, birthdates, addresses, phone numbers, and Social Security numbers; personal financial information (PFI), such as bank account and credit card numbers; and protected health information (PHI), such as medical history and diagnoses. This information can be used directly for identity theft, sold on the black market, or used as the basis for other types of fraud.[8] Attackers may also target data regarding a company's intellectual property (IP), which can be sold to competitors or on the black market.

2 "Script Kiddie: Unskilled Amateur or Dangerous Hackers?"; *United States Cybersecurity Magazine*.
3 *Insider Threat—2018 Report*; Cybersecurity Insiders and Crowd Research Partners; 2017.
4 *2018 Data Breach Investigations Report*—Executive Summary; Verizon; 2018.
5 *Into the Web of Profit*; Bromium; April 2018.
6 *2019 Cyberthreat Defense Report*; Cyber-Edge; 2019.
7 "Why You Should Never Pay A Ransomware Ransom"; *Forbes*; March 9, 2018.
8 "Hacked Health Records Prized for their Black Market Value"; Fox Rothschild blog post; March 16, 2015.

While most cybercrime is driven by financial motives, some cyber criminals are motivated by other goals such as making a political statement, trying to cause disruption to a specific organization, or simply trying to disrupt society at large. For example, the Anonymous "hacktivist" group made headlines for its attacks on PayPal and Mastercard (2010), Sony (2011), and various U.S. government websites (2012).[9] The group was named one of Time magazine's "World's 100 Most Influential People: 2012".[10] The motivation for these attacks was apparently political, not financial,[11] though the financial impact on the affected organizations was significant. For example, the losses to PayPal were estimated at almost $5 million.[12]

Other cyberattacks occur on behalf of nation-states. Such attacks may intentionally target private companies for strategic reasons.[13] For example, in 2014, attackers broke into the computer networks of Sony Pictures Entertainment, stole a large amount of data, and then erased many of the company's servers,[14] costing the company an estimated $35 million in repair and recovery costs.[15] In 2018 the U.S. Department of Justice officially charged a North Korean programmer (believed to have been operating at the direction of the North Korean government) for his participation in this and several other cyberattacks. The motivation for the Sony attack is believed to have been Sony Pictures' planned release of a comedy film depicting the assassination of the North Korean leader.[16] Private firms may also be unintended targets of government-sponsored attacks. The NotPetya attack, described below, is believed to be an example of one such scenario.

Threat vectors

The complexity of the software and hardware underlying modern computer networks affords attackers a multitude of points upon which to focus their efforts. In practice, external attackers usually rely on legitimate users of the system to gain initial access to a company's network, and then use other techniques to continue the attack. A company targeted in a cyberattack may also be attacked through a third-party vendor or contractor who has access to its systems. In order to properly assess its cyber risk profile, a company may also need to evaluate the systems and protocols of other entities and contractors with whom it has a business relationship.

9 "The Return of Anonymous"; *The Atlantic*; Aug. 11, 2020.
10 "Anonymous"; Time 100: The List; April 18, 2012.
11 "Hacker group Anonymous is a nuisance, not a threat"; *CNN Money*; Jan. 20, 2012.
12 "Anonymous cyberattacks cost PayPal £3.5m, court told"; *The Guardian*; Nov. 22, 2012.
13 "Today's enterprises face increasing risk of state-sponsored cyberattacks"; *Thomson Reuters*; Jan. 14, 2019.
14 "The Sony Hackers Were Causing Mayhem Years Before They Hit the Company"; *Wired*; Feb. 24, 2016.
15 "Hack to cost Sony $35 million in IT repairs"; *Network World*; Feb. 4, 2015.
16 "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions"; U.S. Department of Justice; Sept. 6, 2018.

In the most common form of external attack, known as "phishing," an attacker sends an email message to recipients within the company. The message appears to be legitimate but may contain an infected attachment which, if opened, will grant the attacker access to the recipient's computer. The email may also contain a link to a fake login page, where the attacker can collect the user's login credentials. A 2017 report concluded that 90% to 95% of successful cyberattacks were launched via phishing attacks.[17] If a computer's software is misconfigured or outdated, merely visiting an infected website or opening an infected email could be enough to give an attacker access to the machine.

Attackers may also use software vulnerabilities to gain access to a target system. A software vulnerability may be the result of a misconfiguration (for example, the system administrator may forget to change a default password) or may be due to a problem with the design or coding of the software itself (these are commonly referred to as "bugs"). Many software producers periodically release updates, or "patches," to their software to fix recently discovered bugs. Attackers may use known vulnerabilities to attack unpatched, out-of-date systems, or may use publicly unknown "zero-day" vulnerabilities to attack fully up-to-date software. Additionally, some network-connected devices may not receive security updates from the device manufacturer, or the manufacturer may stop providing patches after some period of time. Companies may also delay applying security patches to production-critical systems, as carrying out the update may require a temporary production slowdown or shutdown. These vulnerable, unpatched devices and systems can become entry points, allowing attackers to gain access to other parts of a company's network.

The majority of cyberattacks are carried out by external attackers, but an estimated 28% of attacks in 2018 involved some level of participation by a company employee.[18] Given that employees typically have a legitimate need to access company systems and data, insider attacks can be especially difficult to defend against.

The use of simple/weak passwords, or the re-use of login credentials across multiple websites, can also contribute to the vulnerability of a company's system. Simple passwords are vulnerable to dictionary-based attacks, where attackers use "dictionaries" of common words/passwords to attempt to gain access to password-protected systems. Even complex passwords, if not of sufficient length, are vulnerable to "brute force" attacks wherein the attacker tries every possible password combination. Many organizations have implemented password complexity and length requirements in order to mitigate against such attacks.

17 "Phishing Remains Top Cyberattack Vector in 2017"; *Infosecurity Magazine*; Sept. 27, 2017.
18 *2018 Data Breach Investigations Report—Executive Summary*; Verizon; 2018.

Once attackers have obtained a legitimate user's login credentials (username and password), they may attempt to use the stolen credentials to access other systems in a process known as "credential stuffing." In a 2018 study, 52% of users were found to reuse identical or slightly modified passwords across multiple online services.[19] In a corporate environment, the practice of password re-use can allow an attacker who has gained initial entry to company systems to easily move into other parts of the network. An attacker who gains access to company systems may also wait for weeks or months before actually launching the attack at a time that will maximize its impact.[20]

Examples of incidents

Recent history offers numerous examples of the impact a cyberattack can have on a company. The following incidents illustrate the variety of forms that such attacks can take and the variety of motivations that may lie behind these attacks.

Target data breach

During a two-week period in late 2013, attackers stole approximately 40 million credit and debit card numbers and 70 million customer records from the Minnesota based retailer Target Corporation. While some recent data breaches have been much larger in terms of the number of records exposed, the incident had a high profile at the time and helped to accelerate movement toward greater security within the payment card industry.[21] The breach is also notable for the relatively complex approach the attackers used to access Target's systems. The attackers used a phishing email to gain access to the network of a refrigeration contractor that provided services to Target. The attackers were then able to collect the credentials used by the contractor to access Target's vendor systems. The attackers were able to use their access to Target's vendor portal to gain access to other portions of the company's systems. Eventually, the attackers reached their goal: Target's in-store point-of-sale terminals that process credit and debit card transactions. The attackers installed software on the terminals that would capture credit and debit card information and periodically send it to a compromised server within Target's network. The attackers could access this server and retrieve the stolen information as needed.[22] As of 2016, Target had incurred a reported $291 million of costs related to the breach, of which roughly $90 million was expected to be covered by the company's cyber insurance policies.[23]

19 "The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services"; Chun Wang et al., 2018.
20 "The Covid-19 Pandemic Reveals Ransomware's Long Game"; *Wired*; April 28, 2020.
21 "Target targeted: Five years on from a breach that shook the cybersecurity industry"; We Live Security; Dec. 18, 2018.
22 "Anatomy of the Target data breach: Missed opportunities and lessons learned"; *ZD Net*; Feb. 2, 2015.
23 "Target's Cyber Insurance: A $100 Million Policy vs. $300 Million (So Far) In Costs"; Patterson Belknap blog post; April 7, 2016.

Dyn distributed denial-of-service (DDoS) attack

The 2016 Dyn attack was short-lived but is an example of a DDoS attack and a possible catastrophic loss scenario for cyber insurers. This attack was directed at a Domain Name Service (DNS) provider, Dyn, which served several prominent websites. The services provided by Dyn translate easily remembered domain names to the more cryptic numeric internet protocol (IP) addresses used to route traffic on the internet. The Dyn attack took place in three waves on October 21, 2016, and caused several well-known websites to become temporarily unavailable including Amazon, the BBC, CNN, GitHub, Netflix, PayPal, Sony PlayStation Network, Squarespace, Twitter, and Visa.[24,25,26] The attacker(s) flooded the Dyn DNS servers with so many fake requests for DNS information that the company's systems were temporarily overloaded and unable to respond to genuine DNS requests. During this period, many users were unable to visit the impacted websites because their web browsers were not able to retrieve website IP addresses from the Dyn servers. The attack was conducted, at least in part, using a "botnet" consisting of tens of thousands of internet-connected devices such as digital video recorders and web cameras. Due to poor security on these devices, attackers were able to cause them to direct a huge amount of bogus traffic toward the Dyn servers.[27] As of this writing, the attacker(s) behind the Dyn attack have not been publicly identified.[28] There was no obvious financial motive for this attack, and some have suggested that a disgruntled gamer launched the attack in an effort to take Sony's PlayStation Network offline.[29] This incident is an example of a catastrophic risk for cyber insurers. In this case, many companies relied on a single entity (Dyn) to provide critical DNS services, and when Dyn was attacked, the effects were widespread. Because the impacted websites were restored quickly, the financial impact of this attack was relatively small. One estimate pegged the total costs of the attack at $110 million, most of which would fall within the insureds' cyber insurance policy deductibles.[30]

NotPetya attack

As of 2020, the costliest cyberattack has been the 2017 NotPetya attack, with total costs estimated as high as $10 billion. The attack began in Ukraine but quickly spread to countries around the world. At its outset, the incident appeared to be a typical ransomware attack. Once the malware gained access to a company's computer systems it would spread

24 "Friday's third cyberattack on Dyn 'has been resolved,' company says"; *CNBC*; Oct. 21, 2016.
25 "Here are the sites you can't access because someone took the internet down"; *Splinter*; Oct. 21, 2016.
26 "U.S. internet disrupted as firm hit by cyberattacks"; *CBS News*; Oct. 21, 2016.
27 "The DDoS Attack Against Dyn One Year Later"; *Forbes*; Oct. 23, 2017.
28 "FBI: How we stopped the Mirai botnet attacks"; TechTarget; March 7, 2019.
29 "Angry Gamer Blamed For Most Devastating DDoS Of 2016"; *Forbes*; Nov. 17, 2016.
30 "Types of cyber incidents and losses"; Enhancing the Role of Insurance in Cyber Risk Management; *OECD Publishing*; Dec. 8, 2017.

automatically from computer to computer, causing the victim's computers to spontaneously shut down. When restarted, the screen would display a message giving the user instructions for paying a ransom and obtaining a key to decrypt their data. Some victims attempted to pay the ransom following the instructions shown on the screens of their locked computers but discovered that the payment did not cause their data to be unlocked.[31] Researchers soon discovered that the data had been encrypted with a random key, so there was no way for the attackers to unlock the data, even if they wanted to do so.[32]

Later investigation revealed that the attack had begun with the servers of a Ukrainian software company that produced a piece of accounting software used widely within that country. Attackers took control of the company's update servers and used them to send the NotPetya malware, disguised as a software update, to computers running the accounting software. The malware took advantage of two vulnerabilities in the Windows operating system to spread automatically within the networks of infected companies. First, the NotPetya worm used a known vulnerability to gain access to unpatched systems. Then a second vulnerability allowed the malware to use the compromised system to find usernames and passwords, which gave it access to other computers with fully up-to-date software. After taking over a target machine, the malware would alter the information stored on the computer's hard drives, effectively destroying any software and data located there. The worm spread with incredible speed, taking down the networks of several large Ukrainian companies in less than 60 seconds from the time the first computers in those networks were infected.[33] The worm quickly spread beyond Ukraine, impacting companies in a wide range of locations and industries. Two of the most heavily impacted companies were the Danish shipping company Maersk and the U.S.-based delivery company FedEx, each of which lost approximately $300 million due to the attack.[34] At the time of the attack, neither company appeared to have had a cyber insurance policy in place to cover such an attack.[35,36] Food and beverage company Mondelez carried a property insurance policy that supposedly provided coverage for "physical loss or damage to electronic data, programs, or software including physical loss or damage caused by the malicious introduction of a machine code or instruction".[37] The company filed a $100 million claim to cover the damages incurred as a result of the attack.[38]

31 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"; *Wired*; Aug. 22, 2018.
32 "ExPetr/Petya/NotPetya is a Wiper, Not Ransomware"; SecureList; June 28, 2017.
33 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"; *Wired*; Aug. 22, 2018.
34 "Is the world ready for the next big ransomware attack?"; CSO Online; March 4, 2019.
35 "Risk management"; Maersk; 2017.
36 "Cyber attack, hurricane weigh on FedEx quarterly profit"; *Reuters*; Sept. 19, 2017.
37 "Cyber Warfare and the Act of War Exclusion"; International Comparative Legal Guides; 2020.
38 "Cyber Insurance Not Valid in Case of Cyber War, Says Major Insurance Company"; *CPO* magazine; Jan. 17, 2019.

Shortly after the attack, Ukrainian officials placed blame on Russia, with which Ukraine was embroiled in an undeclared war.[39] In 2018, the U.S., U.K., and Australian governments officially attributed the attack to the Russian military,[40] though no proof of this allegation has been made public. Government officials believe that the Russian goal was to disrupt Ukrainian energy production and financial and government operations,[41] and that damage to other companies was unintentional. Following this official attribution, Mondelez's insurer denied the company's claim, citing the policy's "act of war" exclusion.[42] This claim denial is reportedly the subject of ongoing litigation between Mondelez and the insurer. [43]

39 "Cyberattack Hits Ukraine Then Spreads Internationally"; *The New York Times*; June 27, 2017.
40 "US, UK, Australia Warn Russia of 'International Consequences'—NotPetya Outbreak Attributed to the Kremlin"; *WCCF Tech*; Feb. 16, 2018.
41 "Russia Accused of Massive $1.2 Billion NotPetya Cyberattack"; *Newsweek*; Feb. 15, 2018.
42 "Cyber Insurance Not Valid in Case of Cyber War, Says Major Insurance Company"; *CPO* magazine; Jan. 17, 2019.
43 "Mondelez's action against Zurich signals potential gap in cyber policies"; *Insurance Business America*; April 4, 2019.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**