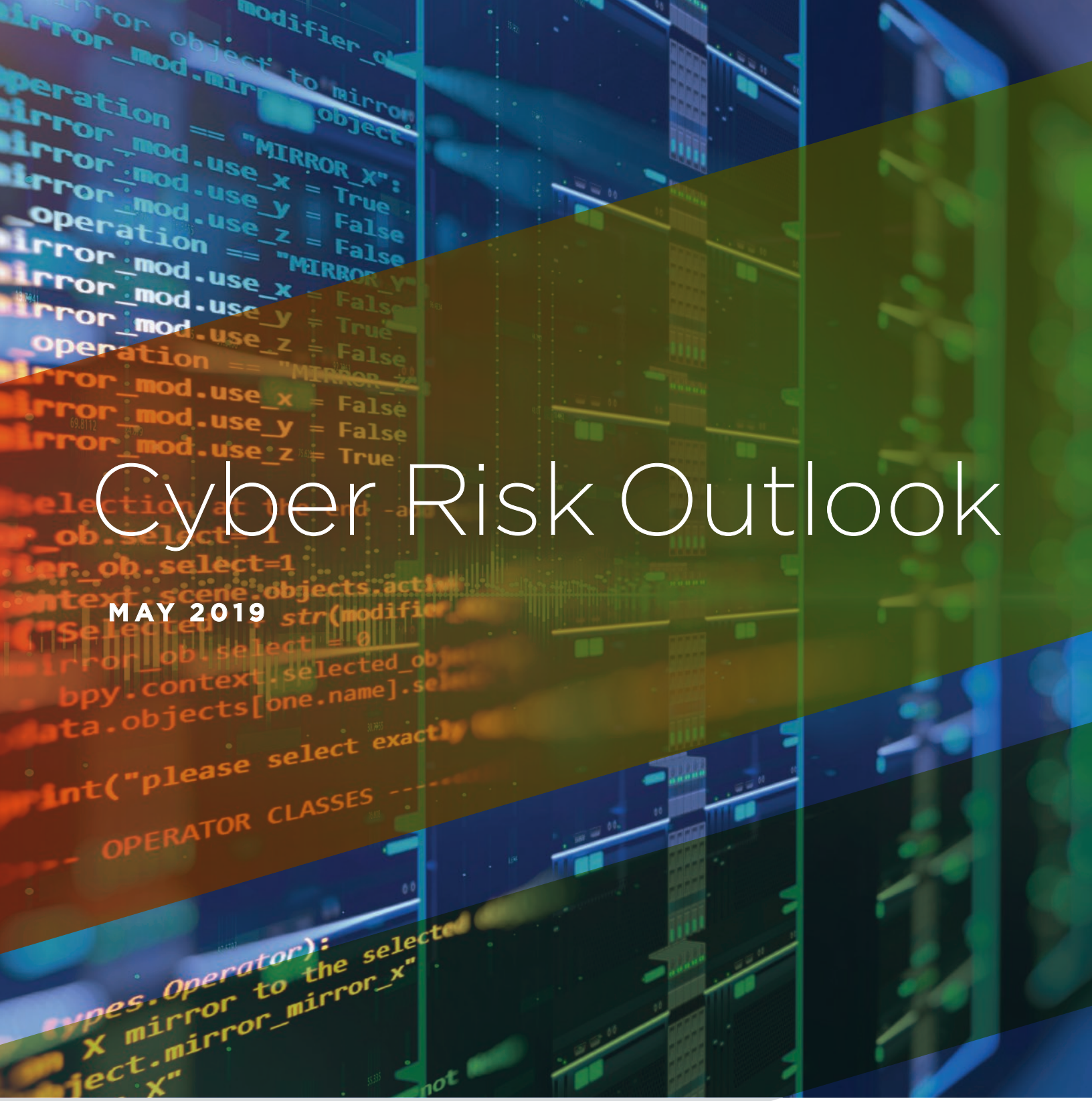


# Cyber Risk Outlook

**MAY 2019**


Centre for
**Risk Studies**

UNIVERSITY OF
CAMBRIDGE
Judge Business School

RMS®

# Cyber Risk Outlook

## TABLE OF CONTENTS




Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE Judge Business School

RMS®


A
B
C
D
3
4
160
140
120
100
80
60
40
20
0
1
2
3
4
5
6
8
9
10
11
12

SECTION 1

# Key Cyber Trends

Cyber risk is changing rapidly. This section identifies 10 key trends that companies should be keeping track of to successfully manage their cyber risk:

1. Increasing Exposure to Digital Attack and Disruption
2. Growth of E-Commerce and Reliance on Internet for Revenue
3. Increasing Propensity for Cyber-Induced Business Interruption
4. Attacks on Digital Supply Chains
5. Growing Potential for Cyber Physical Loss Events
6. Cyber Attacks Becoming Increasingly Political
7. Changing Motivations of Threat Actors
8. Improving Security Standards in Corporates
9. Improvements in Law Enforcement
10. Changes in the Regulatory Environment

### 1. Increasing Exposure to Digital Attack and Disruption

Companies are increasing their interaction with the digital economy at a rapid rate as they move to take advantage of digital efficiencies and information on consumer habits. This increases the overall attack surface being made accessible to external threat actors. The number of devices being operated by businesses, and number of commercial endpoints being connected to the internet, are growing at rates of around 12% annually. New, active websites are increasing at over 26% a year, and the volume of web traffic to commercial websites is typically seeing double-digit annual growth in many sectors. By many accounts this represents a paradigm shift and a transformation of economic business practice that is impacting almost every sector. Some analysts refer to this as the fourth industrial revolution. The digital economy now accounts for almost a third of the GDP of developed economies, up from less than 3% a decade ago.[1]

What is clear is that technologies are becoming polarized, between on-premises software and cloud-based applications, and standardized, around industry-leading products, prompting a homogenization of the digital ecosystem and a loss of diversity in systems. This means that there is increasing potential for systemic failures in IT systems or for systemic exploitation of strategically important technologies that have become standards across the market.

Many businesses are increasingly integrating their data flows and information systems into centralized enterprise resource planning suites and manufacturing information systems. These are generating great efficiencies and improving responsiveness to customer demands, but rendering their business activities more vulnerable to cyber compromise of their IT systems.

[1] National Telecommunications and Information Administration, 2016; Manyika and Roxburgh, 2011

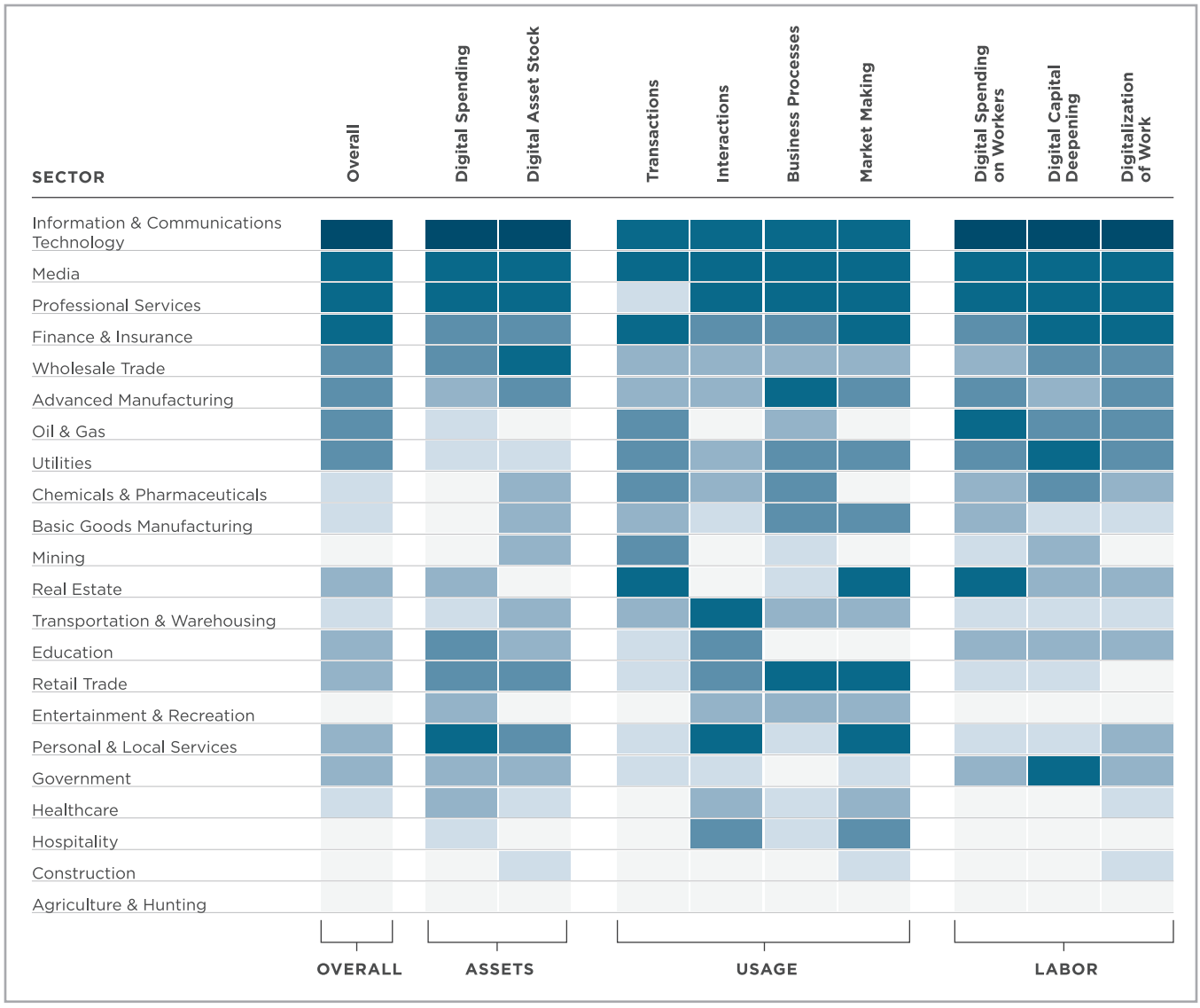



**Figure 1: Relative degree of digitization of business processes by sector. Source: "Which Industries Are the Most Digital and Why?" Harvard Business Review**

The attack surface of a typical business has grown from hardwired desktop operating systems and databases to Wi-Fi-connected mobile devices and even incidental devices, such as internet-enabled coffee machines, that could potentially be overlooked in IT system inventories.[2] The digitization of processes within a company confers great advantages, however the addition of new ports of entry to a company's network increases its exposure to threats and, if left unprotected, its likelihood of exploitation.

Figure 1 shows the variation in digitization of business processes. The variation across sectors is directly related to the dependence of each sector on connected devices for business revenue and management. Relative digitization of industries is measured according to the level of hardware, software, data, and IT service investments, along with the digitization of physical assets such as big data systems in supply chains, connected vehicle fleets, smart buildings, etc.[3] It is no coincidence that the degree of digitization of processes in each sector corresponds to the demand for affirmative cyber insurance and likely concentrations of exposure in a cyber insurance portfolio.

[2] Northcutt, n.d.
[3] Gandhi, Khanna, and Ramaswamy, 2016

## 2. Growth of E-Commerce and Reliance on Internet for Revenue

The exposure to cyber threat is growing most rapidly in the transformation of the retail and commerce space, where disruptive new online business models are challenging traditional business processes. In the U.S., e-commerce sales exceeded half a trillion dollars in 2018, up 13% from 2017.[4] E-commerce now represents 14 cents in every U.S. dollar spent in retail, almost triple its market share a decade ago.[5]

Table 1 gives examples of the casualties that have resulted from this transformation of business model, and Table 2 gives examples of companies founded in the last 10 years that are now valued at over a billion dollars by exploiting trends in digitization of the information economy. The term "unicorn" has been coined to refer to privately held startup companies valued at over US$1 billion. This has been followed by the terms "decacorn" and "hectocorn," for privately held startup companies valued at over US$10 billion and US$100 billion.[6] Ant Financial, a fintech company valued at US$150 billion, is one of the first hectocorns to emerge.[7] It operates Alipay, the world's largest online and mobile payments platform.

The increasing reliance of the economy on the internet increases the vulnerability of business processes to the disruption of the technology, connectivity, and interconnected supply chain of systems that facilitate it. These businesses have specific risk profiles that need detailed analysis for underwriting their cyber risk. Today, these assessments are completed using underwriting questionnaires, although increasingly more automated approaches are being provided by technology companies such as RMS.

| Company | Year Dissolved | Valuation at Peak (US$ Billions) |
|---|---|---|
| **Blockbuster**[8] | 2010[9] | $4.8[10] |
| **Tower Records** | 2006[11] | $1 billion in annual sales[12] |
| **Toys "R" Us** | 2017[13] | $12[14] |

**Table 1: Casualties of the digital revolution: companies dissolved due to their inability to respond to the full impact of digitization on their business**

| Company | Year Founded | Valuation (US$ Billions) |
|---|---|---|
| **Lyft** | 2012 | 30 billion[15] |
| **Snapchat** | 2011 | 8.4 billion market cap as of Nov. 14, 2018[16] |
| **Instagram** | 2010 | 100 billion[17] |
| **Pinterest** | 2009 | 12.3 billion[18] |
| **WhatsApp** | 2009 | 19 billion (bought by Facebook in 2014)[19] |
| **Uber** | 2009 | 90 billion[20] |
| **Slack** | 2009 | 7 billion[21] |
| **Airbnb** | 2008 | 38 billion[22] |

**Table 2: Billion-dollar tech companies founded on the digital economy, less than 10 years old**

[4] Statista, 2019
[5] Ali, 2019
[6] Wikipeda, 2018
[7] Wu and Zhu, 2018
[8] In 2000, Blockbuster passed on the opportunity to buy Netflix for just US$50 million (Chong 2015). Netflix's market cap is now US$125 billion (Yahoo! Finance, 2018a).
[9] Carr, 2010
[10] Carr, 2010
[11] NBC News, 2006
[12] Sisario, 2018
[13] WIkipedia, 2018
[14] Blakemore, 2018
[15] Salinas, 2018
[16] Yahoo! FInance, 2018
[17] McCormick, 2018
[18] Lynley, 2017
[19] Page, 2018
[20] Salinas, 2018b
[21] Lunden and Constine, 2018
[22] Forbes, 2018

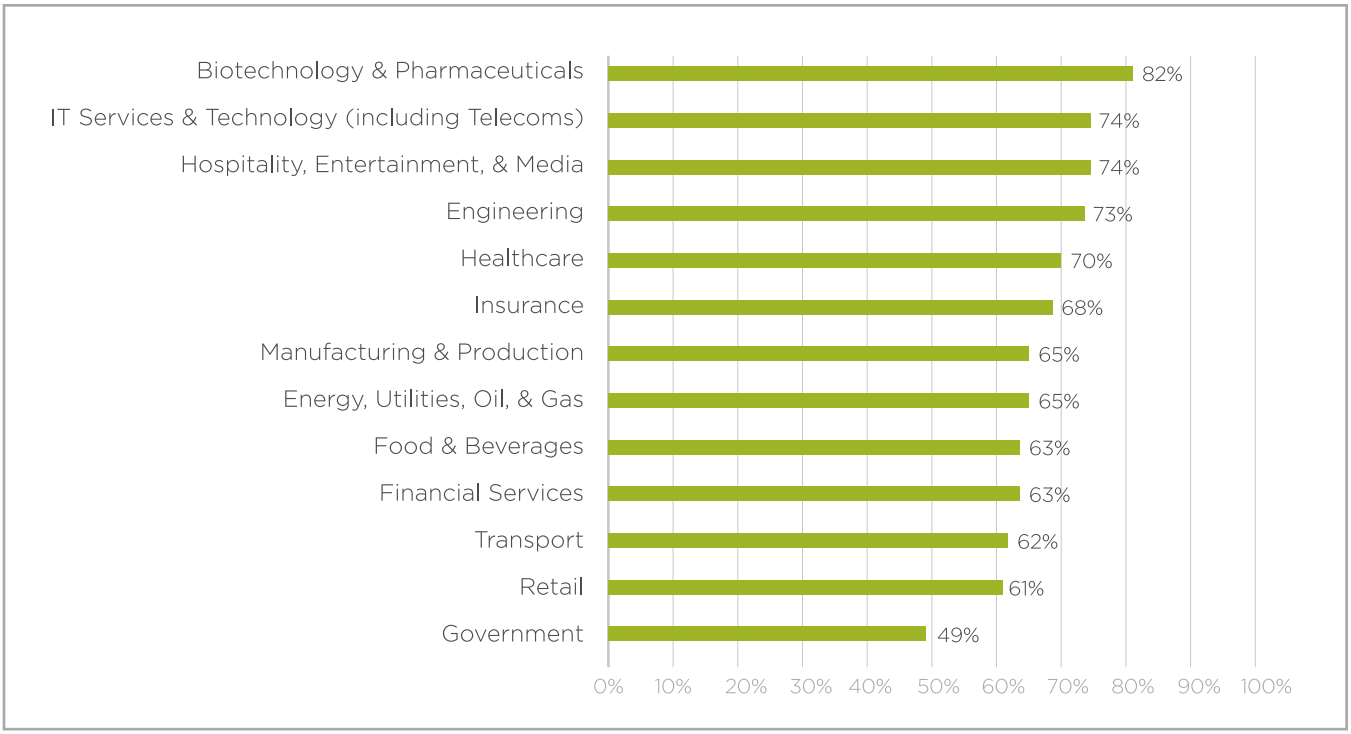



**Figure 2: Propensity for supply chain attacks by sector – percentage of companies in each sector experiencing supply chain attacks. Source: 2018 global CrowdStrike survey.**[23]

### 3. Increasing Propensity for Cyber-Induced Business Interruption

Companies are increasingly digitizing their supply chains, posing a threat to network security of all devices trusted by the network. The digitization of physical assets lengthens the supply chain attack surface, increasing the potential for a single attack to ripple across multiple industries. Services and assets that were once held in-house are transitioning to digitally outsourced vendors. Across all sectors, information and operational technologies are expanding to more integrated online/offline mediums. Even traditional brick-and-mortar sectors are increasingly blurring the lines between their physical and digital assets, as seen with the use of connected vehicles in fleet management.

Most private individuals and companies operate within the context of multiple connections to third-party suppliers, technical support systems, and data flow controls that they do not necessarily have control over or even sight of.[24] Attacking through security weaknesses in smaller suppliers is an easier way to compromise a large company than breaching it directly.[25] Attackers are increasingly utilizing these third- and fourth-party supply chain partners to access target networks. The number of weaponized software updates and pre-packaged devices used by attackers is growing, allowing them to take advantage of the fact that supplier ecosystems are often out of the target companies' control.[26] Even the most secure organization is now vulnerable to attack through its digital supply chain, so it is critical for insurers to assess not just the IT security, but also the reliance and resiliency of an insured's digital supply chain.

In a 2018 survey of 1,300 companies across the U.S., Canada, the U.K., Mexico, Australia, Germany, Japan, and Singapore, two-thirds of companies said they have been targeted with a supply chain attack costing an average of US$1.1 million per attack, with 34% of companies reporting that their operations had been disrupted. For U.S. companies, this cost is US$1.27 million per attack. Though U.S. organizations averaged a 12-hour response time, attacks can take up to 63 hours to detect and remediate. For many companies, downtimes of this duration can lead to heavy losses and reputational damage.

[23] Ray et al., 2018
[24] Budd, 2018
[25] ESET, 2018
[26] Larson, 2018

| Name of Attack | Date | Type of Breach | Vector | Company Affected | Cost |
|---|---|---|---|---|---|
| **WannaCry Variant** | 2018 | Ransomware | Third-party software[27] | Taiwan Semiconductor Manufacturing Company (TSMC) | US$170 million[28] |
| **Microsoft Cryptomining** | 2018 | Cryptomining | A compromised PDF editor vendor and six software vendors working with the font packages[29] | Microsoft's third-party suppliers and their customers | Not yet declared |
| **Tesla Malicious Insider** | 2018 | Malicious insider | Disgruntled employee hacked Tesla's manufacturing operating system and sold videos of how system works[30] | Tesla | None yet disclosed |
| **NotPetya** | 2017 | Destructive wiper | M.E.Doc software update[31] | Multiple companies, including:<br>Cadbury factory in Tasmania | <br>US$147 million[32] |
| | | | | Maersk shipping | US$300 million |
| | | | | FedEx's TNT Express Division | US$300 million |
| **XcodeGhost** | 2015 | Trojan | A malicious copy of Xcode, Apple's developer environment, was hosted in China | Apple customers were the targets | 500 million users affected. 50 iOS apps infected, including WeChat[33] |
| **Supermicro & Elemental supply chain compromise**[34] | 2015 | Nation-state cyber espionage with hardware | Chinese-designed microchip for cyber espionage added to motherboards used by U.S. companies | Apple, the CIA, the Navy, and the Department of Defense | Unknown |
| **Target Data Breach**[35] | 2013 | Data breach | Phishing email stole passwords from Target's HVAC vendor. Malware inserted into POS system in 1,800 stores. | Target retail | US$200 million. Profits fell 46% in the fourth quarter of 2013. |
| **RSA-Lockheed Martin Attack**[36] | 2011 | Data breach | Phishing email with zero-day vulnerability in Adobe's Flash software installed a backdoor. SecurID database used for two-factor authentication exposed. | Intruder used stolen SecurID token as a valid credential to access Lockheed Martin systems. | The original breach cost RSA's parent company EMC US$66 million.[37] Lockheed's advanced Cyber Kill Chain, a system that cost millions to develop, stopped an attack.[38] |

**Table 3: Notable supply chain attacks**

[27] Wu, 2018
[28] White, 2018
[29] Arghire, 2018
[30] Mills, 2018
[31] O'Conner, 2017
[32] The Guardian, 2017
[33] Rossignol, 2015
[34] Robertson and Riley, 2018; Bloomberg's investigation has received robust denials from all companies named.
[35] Shu et al., 2017
[36] Davey, 2016
[37] Hoffman, 2011
[38] Higgins, 2013

## 4. Attacks on Digital Supply Chains

### *Manufacturing*

Manufacturing typically experiences an unusually high volume of reconnaissance behavior, accounting for 46% of all U.K. cyber attacks in 2017. This suggests that attackers are mapping out manufacturing networks to locate critical assets.

### *Energy*

Energy systems are particularly at risk because of their social and economic importance. The supply, processing, and distribution of energy occurs at a transnational level. This complexity increases the vulnerability of the energy supply chain to accidental and deliberate intervention, in turn increasing the vulnerability of all individuals and businesses relying on that supply of energy. This includes links to other industries such as agriculture, food production, and transport. This risk was demonstrated in April 2018 when four U.S. pipeline companies experienced a shutdown of their electronic systems used for communicating with customers. The shutdown lasted for several days. Three companies later confirmed it was the result of a cyber attack.

### *IT*

Software supply chain attacks are commonly seen with trojan apps and malicious code hidden in software updates. When a user downloads an application or update, they unknowingly download the malicious executable as well. This usually requires the application creator or vendor to have been compromised. Most commercial antivirus applications will detect more common, generic intrusions.

### *Industrial Robotics*

Looking forward, the industrial robotics sector unlocks a broader attack surface. An industrial robot is an automated, programmable machine used in manufacturing. It is generally capable of movement on two or more axes, which means the function an individual robot performs is often quite simple, such as linear welding. The International Federation of Robotics reports that global robot installations are expected to increase by 15% on average per year from 2018 to 2020, representing over 1.7 million new industrial robots installed in factories around the world.[39] However, these are highly vulnerable systems.

The software running on these devices is often outdated, based on vulnerable operating systems and libraries, and sometimes relies on legacy systems. Their authentication systems may be weak with default, interchangeable credentials in use. Attackers may be able to access the tens of thousands of industrial devices that reside on public IP addresses, which can include exposed industrial robots.[40] The vulnerability and accessibility of these systems make them attractive, impactful targets. Because industrial robotics are common in manufacturing, the potential downstream impacts on consumers are significant.

These types of attacks have increased the demand for businesses to obtain non-damage business interruption insurance. Traditional insurance policies have tended to cover business interruption as an adjunct to physical damage, such as when a fire causes a factory to cease production. Cyber attacks can cause business interruption without triggering the physical damage terms. Non-damage business interruption coverages are being offered as extensions of cover in property insurance policies as well as in affirmative cyber insurance products.

## 5. Growing Potential for Cyber Physical Loss Events

Physical cyber attacks have long been expected, but are now becoming more common.[41] Of most concern are those targeted on public and private critical national infrastructure.[42] Targeting has included public and private organizations such as energy utilities, water treatment facilities, and transportation networks, along with manufacturing and aviation industries.[43]

In the first two quarters of 2018, 40% of all monitored industrial control systems reportedly came under attack.[44] The complex nature of industrial control environments leaves few industries prepared to cope with well-resourced cyber attackers. Threat actors commonly take advantage of poor cyber hygiene, the rise of IoT, and constrained security budgets in industrial sectors.[45] Locations that were previously thought to be secure can now be threatened with physical disruption. The scope and scale of physical cyber attacks have escalated from being able to cause disruption in business processes to a capability to cause physical destruction. Future attacks that trigger fires, damage to machinery, and physical loss to major assets may trigger unanticipated claims to insurers through traditional non-cyber insurance lines.

### *Escalating Threat*

Attacks on critical infrastructure require specialized knowledge, research, and significant resources in order to become operational.[46] To date, most physical cyber attacks can be attributed to nation-state and state-sponsored

[39] Heer, 2018
[40] Quarta et al., 2017
[41] Erez, 2018
[42] CPNI, 2018
[43] US-CERT, 2018
[44] Kapersky, 2018
[45] NAIC, 2017
[46] Patterson, 2018

cyber threat actors. However, it is possible that new varieties of cyber threat actors will begin to target critical national infrastructure as tools and capabilities improve to enable them to carry out cyber physical attacks. At least five distinct strands of malware and at least seven threat actor groups have been identified that specifically target industrial control systems.[47]

Especially threatening are evolving trends in destructive malware, such as TRITON, which was designed to undermine safety systems in industrial control environments.[48] If successful in causing physical destruction and death, malware like TRITON can trigger war-like responses that lead to further disruption, losses, and even death.

The Centre for the Protection of National Infrastructure in the U.K. defines critical national infrastructure as "facilities, sites, information, people, networks and processes necessary for a country to function and upon which daily life depends."[49]

### *The Threat to Localities*

Contagious malware events such as ransomware are increasingly targeting critical national infrastructure, demanding payments to restore encrypted files or capability. These attacks are often targeted on local communities' IT infrastructure.[50] One of the more successful extortion gangs is known as the SamSam Group. SamSam targets specific localities and is estimated to have made US$6 million in ransom payments since 2015. More than half of SamSam's targets can be considered critical national infrastructure.[51] Attacks attributed to SamSam include a May 2018 ransomware attack that crippled Atlanta's government for weeks[52] and a reported attack on an unnamed hospital in January that extorted US$55,000 from the operators.[53] Other notable recent events include a possible WannaCry-type ransomware attack affecting a

[47] Caltagirone, 2018
[48] Johnson et al., 2017
[49] CPNI, 2018
[50] Kamp and Calvert, 2018
[51] Sophos, 2018
[52] Blinder and Perlroth, 2018
[53] Trend Micro, 2018
[54] NCSC US, 2018
[55] USTR, 2018
[56] Johnson et al., 2017
[57] Dragos, 2017
[58] Newman, 2018b
[59] JLT, 2018

## TRITON: A New Breed of Destructive Malware

One of the most serious recent cases of physically destructive malware has been TRITON. Emerging in the last two weeks of 2017, TRITON is a malware specifically designed to attack industrial control systems (ICS).[54] Significantly, TRITON is the first malware constructed to disable the safety systems within an industrial environment. Disabling safety systems is obviously dangerous, if an emergency does occur, but the insertion of malware can itself cause harm.[55]

So far, TRITON has only surfaced in one target. In that deployment, a failure in TRITON's code caused industrial operations to halt. The halt in operations alerted authorities, sparking an intense period of study.[56] It has since been alleged that TRITON targeted a petrochemical facility located in Saudi Arabia.[57] FireEye Intelligence has attributed TRITON to security researchers from the Central Scientific Research Institute of Chemistry and Mechanics in Russia. The research institute has the capabilities and mandate to research ICS and is state owned.[58]

Several researchers have commented that construction of TRITON requires an advanced skillset and intimate knowledge of industrial control and safety systems, which was confirmed with the realization the malware was likely reverse engineered.[59] As TRITON illustrates, malware designed to cause disruption and possible destruction is evolving to higher levels of sophistication and effectiveness.

Once a self-replicating malware is released, its spread is generally uncontrollable, creating loss for both intended and unintended targets.

national security contractor's manufacturing operation[60] and a ransomware attack against Puerto Rico's only energy utility.[61]

### 6. Cyber Attacks Becoming Increasingly Political

The past year has seen a rise in publicly attributed state-backed cyber activity designed to achieve political aims, with the political and cyber world becoming increasingly intertwined. In the twenty-first century, states are seeking to utilize digital technologies to align cyber politics with physical politics through digital election interference and social media manipulation.[62]

#### *Cyber Politics Influencing Real-World Politics*

States have the potential to act nefariously on the internet through their own cyber capabilities or the capabilities of other cyber threat actors whose interests align with the state.[63] Common state activity on the internet consists of traditional and corporate espionage, intellectual property theft, and disruptive attacks.[64] This type of behavior by nation-states is leading to real-world political and corporate impacts. Accusations of intellectual property theft have underpinned the recent trade dispute between the U.S. and China.[65] Both WannaCry and NotPetya, as two truly systemic cyber attacks, caused global disruption to corporations in a wide variety of sectors[66] and threatened critical national infrastructure like the U.K. NHS.[67] Further, nation-state cyber election interference, such as that experienced during the 2016 U.S. presidential election, remains a source of domestic and international tension.[68]

Nation-states have been careful to keep their cyber incursions into each other's territories well below the threshold of an act of war.[69] If the scope and scale of these attacks persist, then deterrence could potentially break down. Some suggested solutions include international agreements to limit aggressive cyber incursions between countries, framed as a cyber "Geneva Convention" to prevent cyber politics from escalating above the threshold of war.[70]

#### *State-Backed Actors*

State-backed cyber activities also threaten the corporate realm. Corporations are sometimes targeted by adversarial states so that a state can gain advanced knowledge or economic advantage. Commonly targeted areas include intellectual property theft, corruption of supply chains, and disruptive attacks.[71] Often these types of attacks can lead to reputational ruin,[72] economic loss through an inability to continue normal operations,[73] regulatory fines,[74] and clean-up and mitigation costs.[75] The former director of the National Security Agency, Keith Alexander, deemed cyber industrial espionage as the "greatest transfer of wealth in history."[76]

Nation-states have also been responsible for systemic events that drive global disruption and loss, including the notorious WannaCry[77] and NotPetya[78] attacks in 2017. Sometimes cyber incidents affect corporations in unexpected ways. NotPetya triggered losses in the insurance industry under silent cyber, as several traditional insurance policies did not have clauses excluding cyber loss.[79] Accumulating corporate losses due to systemic cyber events can be especially trying. It is believed that most of the victims of NotPetya, such as Maersk, were unintentionally harmed. Once a self-replicating malware is released, its spread is generally uncontrollable, creating loss for both intended and unintended targets.[80]

[60] Perlroth, 2018
[61] Brown, 2018
[62] FireEye Intelligence, 2018
[63] Miller and Reese, 2018
[64] Maurer, 2018
[65] National Audit Office, 2018
[66] C.N.N. Library, 2018
[67] Rid, 2012
[68] Wheeler, 2018
[69] NCSC US, 2018
[70] Aon, 2018
[71] Bouveret, 2018
[72] UK Government, 2018
[73] Anderson et al. 2013
[74] Rogin, 2012
[75] Department of Justice, 2018
[76] NCSC, 2018a
[77] Gallin, 2018
[78] NCSC CSAN, 2018
[79] Department of Defense, 2018
[80] NCSC US, 2018

### *Fighting Back*

Western nation states such as the U.S. have begun to articulate increasingly offensive cyber strategies to combat the growing threat posed by nation-state actors. The U.S. Department of Defense's (DOD) 2018 cyber strategy dramatically expands the scope and scale of U.S. offensive cyber capabilities. It pointedly identifies long-term and daily strategic cyber competition between the U.S., China, and Russia. Strategic goals include enhancing public and private partnerships and international cooperation. The protection of critical national infrastructure despite military utility and ownership is especially important, as the U.S. military is acknowledging the actualized threat that disruptive cyber attacks represent. Finally, the DOD cyber strategy allows for the U.S. to "defend forward" by actively identifying, pursuing, and destroying cyber threats before an attack.[81]

The DOD cyber strategy will likely lead to intensified nation-state cyber competition. The characteristics of nation-state cyber competition are likely to become increasingly disruptive. If deterrence breaks down and nation-states choose to escalate offensive cyber campaigns, then the digitized business environment of the 21st century could become severely compromised.

### *Espionage, Supply Chains, and Reputational Risk*

The U.S. government has consistently highlighted the dangers corporations face in an intense geopolitical climate, including economic, industrial, and technology-related intellectual property theft.[82] Some analysts have estimated that intellectual property theft from U.S. private corporations by a single geopolitical adversary could be causing annual losses of US$20 billion to US$30 billion.[83]

Governments have started to ban companies originating from rival geopolitical states in order to mitigate espionage. The most prominent example is the late 2017 U.S. government banning of Kaspersky products on U.S. government networks.[84] Prior to the official ban, Best Buy, a U.S.-based retailer, pulled all Kaspersky products in anticipation of American government action.[85] There have been several high-profile instances in which governments have continued to ban products originating from their geopolitical rival's territories.

In November 2018, America placed export restrictions on the Chinese-based chip manufacturer Fujian Jinhua because it is thought that U.S. military supply chains could become compromised and reliant on a peer competitor's manufacturing base.[86] Similarly, the U.K. has found that certain Huawei products used in the telecommunications sector could pose a threat to national security. Some of the U.K.'s main concerns are deficiencies in the engineering processes and within Huawei's supply chains.[87] Finally, commentators have publicly acknowledged that they have seen increased foreign intelligence activity in non-traditional intelligence collection areas such as in Silicon Valley. Silicon Valley represents a high-value intelligence target as intellectual property theft, economic espionage, and military advantage could all be gained by targeting high-technology companies.[88] Corporates run the risk of lost profits, regulatory fines, increased compliance costs, and reputational ruin by ignoring the actions of malicious geopolitical actors.

## 7. Changing Motivations of Threat Actors

The past year has seen an upsurge in cyber threat actor activity in the informal economy, particularly from nation-state and state-sponsored actors.[89] Threat actors continue to utilize black markets, mercenary skills, and hacker networks to achieve their aims. Commoditization of malware continues to lower the barriers of entry into the black economy for less-skilled actors.

### *State-Sponsored Activity Increased, Becoming Financially Motivated*

For companies in the private sector, the increased activity of state-sponsored groups is a concern, particularly aligned to trends where they demonstrate increasing involvement in cyber crime activity that generates a financial reward. State-sponsored groups typically constitute an "advanced persistent threat" (APT) with superior skills and large budgets, giving them significant capability to cause losses to private-sector businesses.

State-sponsored groups often engineer and use zero-day exploits, design malware for specific targets, and use misdirection techniques as a layer of subterfuge in their attacks.[90] Evidence that these groups are now targeting commercial organizations for financial gain raises the overall risk level for financial and retail service sectors. The resources of these attack groups may potentially be constrained by budgets and approval chains of command set by their sponsor state, but they also have access to the top pools of talent. Sometimes these groups operate as a legal entity in their host country.[91] Companies targeted by sophisticated and well-resourced state-sponsored groups are more likely to be subjected to large-scale cyber attacks, which could potentially result in significant losses.

[81] Lewis, 2018
[82] NCSC US, 2018
[83] Lewis, 2018
[84] Volz, 2017
[85] HCSEC, 2018
[86] The Economist, 2018
[87] HCSC, 2018
[88] Dorfman, 2018
[89] Accenture Security, 2018
[90] Cyberreason Intel Team, 2017
[91] Europol Cybercrime Centre, 2018

## Gallmaker Hacking Group Embraces "Living Off the Land"

In October 2018, researchers identified a threat actor group called Gallmaker that has been attributed to several cyber espionage campaigns targeting military, government, and defense sectors in Eastern Europe and the Middle East, utilizing living off the land (LotL) techniques and publicly available hacking tools.[92] These threat actors exploited the Microsoft Office Dynamic Data Exchange tool to gain access to victim's machines.[93] Once in the system, Gallmaker used the tool to remotely execute commands in the victim's memory (RAM), resulting in an exfiltration of sensitive data.

The threat actor often remained undetected for months after initial infection. In fact, Gallmaker's operations were first detected in 2014, suggesting that the attribution period took upwards of four years. This is a testament to the covertness of LotL attack vectors and how this tactic could cause significant harm to corporations in the future.

[92] Symantec, 2018b
[93] Shaun Nichols, 2018b
[94] Note: As a proportion of the total number of cyber attacks in the black economy.
[95] Symantec Security Response, 2017
[96] Kelly Sheridan, 2018
[97] Vasilios Hioureas, 2018
[98] Stan Gibson, 2018
[99] Candid Wueest, 2017
[100] Gartner, 2018

Figure 3 shows the estimated breakdown of losses triggered to the private sector economic activities by the types of threat actor.

As outlined in Figure 4, the most actively known threat actor groups from 2016 to the end of 2017 are Russian-backed actors (Sofacy and Cozy Bear), with the financially motivated North Korean state-sponsored group Lazarus as the third most active.[94] However, as shown in Figure 3, the estimated global economic loss from cyber attacks is still derived predominately from the activity of organized cyber criminal groups. As state-sponsored groups increasingly engage in financially motivated attacks, they will become responsible for an ever-greater share of the global economic loss from cyber crime.

***Threat Actors "Living Off the Land"***

There is a growing trend of cyber threat actors using "living off the land (LotL)" tactics, also known as "fileless attacks," which came to light in 2018. For these tactics, threat actors exploit legitimate and trusted tools or applications in a computer to gain entry into a system, cutting out the need to execute malicious files to launch an attack.[95] Between January and July of 2018, LotL attacks were estimated to have increased by 94%.[96]

By exploiting trusted applications and tools, cyber threat actors can hide their activity in legitimate computer processes, reducing the likelihood of detection during an operation.[97] LotL tactics elude traditional detection techniques such as antivirus software, as there is no payload to trigger the malware signature.[98] Fileless malware increases the rate of successful infection and anonymity of the group, reducing the risk of legal action against the actors and raising threats to corporations across sector and size.[99]

***For-Sale Malware Lowers Barriers to Entry***

The evolution of for-sale malware sold on online black markets has changed the threat landscape companies face and has resulted in new trends in attack vectors. Threat actors can purchase ready-made exploit kits, ransomware, and even zero-day exploits on the black market. The ease of use of these products allows less-skilled criminal hackers to launch more powerful attacks than they could otherwise achieve with their own skills, increasing the impact of their attacks. Commoditized malware, such as exploit kits and zero-day vulnerabilities, can be acquired for sums as low as US$20,000, as shown in Table 4.

### 8. Improving Security Standards in Corporates

Worldwide expenditure on information security exceeded US$114 billion in 2018, an increase of over 12% on 2017.[100] Costs include growing investment in pre-emptive cyber security measures utilizing artificial intelligence

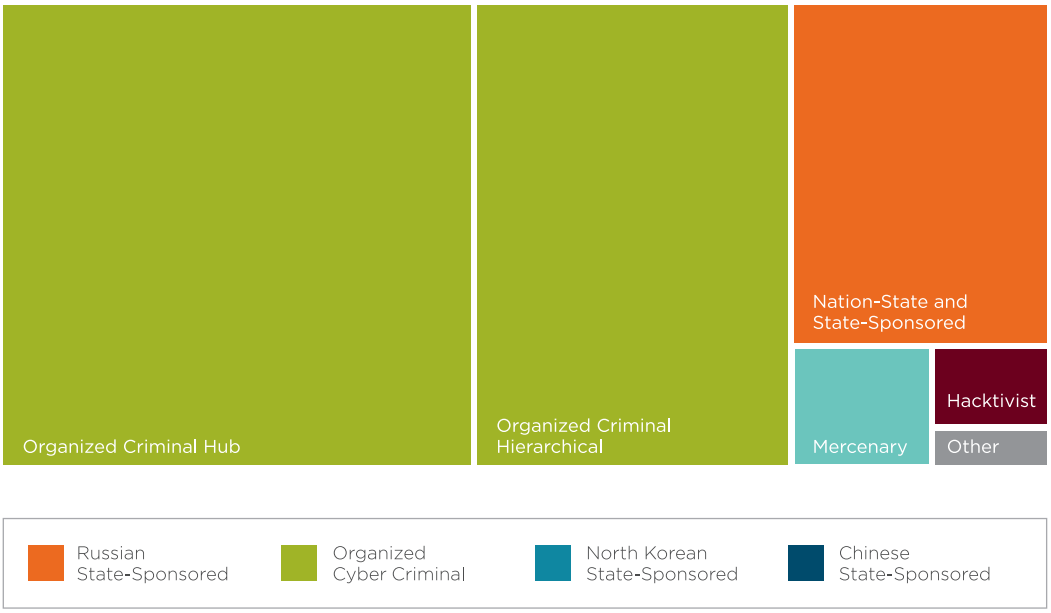



**Figure 3: Proportion of cyber loss estimated to be caused by threat actor category. Source: CCRS.**

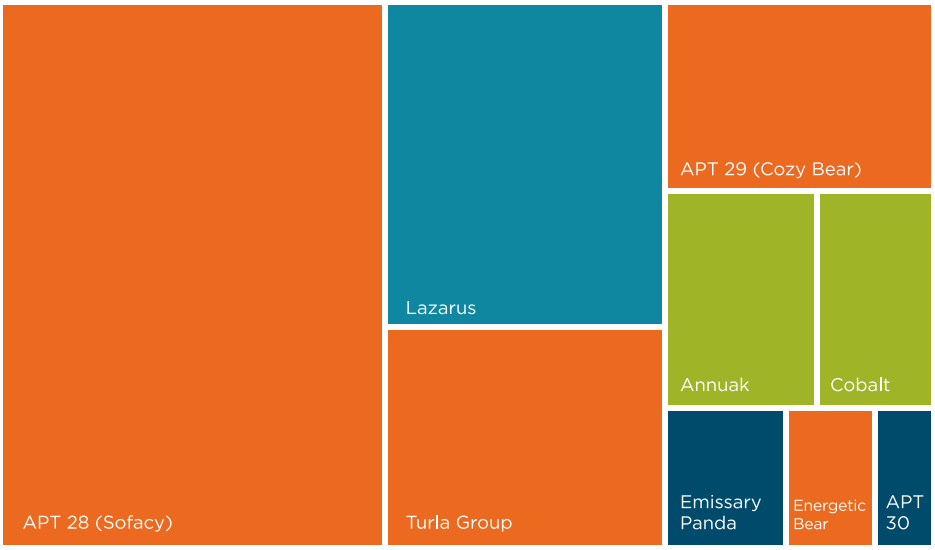



**Figure 4: Activity by individual named threat actor group from 10/2016 to 12/2017. Source: MISP.**

and machine learning: almost 50% of businesses now incorporate some type of AI-driven cyber security.[101] AI will dramatically increase the overall costs of cyber security and likely start a cyber arms race between organizations and malicious actors.[102] Patching procedures and technologies remain an important component of corporate security, ensuring that the known vulnerabilities in commercial software are patched as soon as solutions are available.

In 2018, SCADA, digital technology used in an industrial environment, saw an increase of 30% in discovered vulnerabilities.[103] Companies that have streamlined their incident response procedures to detect compromises earlier have improved their cyber security postures and reportedly have reduced their average business interruption costs. However, median dwell times, the time it takes a corporation to notice it has been compromised, has steadily increased, and in 2018 averaged 101 days globally.[104]

[101] Bird, 2018
[102] Giles, 2017
[103] Trend Micro, 2018
[104] Mandiant, 2018

# The Potential for Corporations to Hack Back

Corporations who have suffered devastating cyber attacks are no longer willing to passively accept their fate. In the past few years, an intense debate on corporate ability to hack back has taken place. Hacking back is when the victim of a cyber attack detects an attack and aggressively follows the attacker outside of corporate networks.

Methods of hacking back reside in a grey area of legality.[105] Almost all forms of hacking back currently violate the U.S. Computer Fraud and Abuse Act (CFAA). The U.S. has sought to address this problem by introducing legislation that is yet to pass called the Active Cyber Defense Certainty Act (ACDC), which would allow hacking back under certain circumstances.[106] In the spring of 2018, the Georgia State Legislature proposed legislation that would allow corporations to hack back in the event of a cyber attack.

The legislation was ultimately vetoed.[107] Several issues other than illegality arise when considering hacking back. For instance, if corporations hack back a nation-state or state-backed actor, then the ramifications could lead to an escalation of state-on-state cyber attacks, or even war in extreme cases.[108] Other negative potentials include causing collateral damage to innocent parties, which would legally, financially, and reputationally harm the party hacking back.[109]

Some security researchers think that weaknesses in current corporate cyber security postures are overstated. Rather than hacking back, better allocated resources toward current defensive cyber security solutions would lead to greater protection.[110]

[105] Schmidle, 2018
[106] Giles, 2017
[107] Chalfant, 2018
[108] Knake, 2018
[109] Hayes and Briggs, 2018
[110] Eenheid, 2018

| Type of Malware | Kit Name | Price (US$) |
|---|---|---|
| **Exploit kits** | Whitehole | $600/month |
| | Sweet Orange | $1,800/month |
| | Elenore | $1,000 |
| | Gpack | $1,000 |
| | Cool (+ cryptor + payload) | $10,000/month |
| **Zero-day** | Windows | $60,000 |
| | Microsoft Office | $50,000 |
| | Mac OSX | $20,000 |
| | iOS | $100,000 |
| | Chrome/Internet Explorer | $80,000 |
| | Adobe Reader | $50,000 |

**Table 4: Prices of commoditized malware**[111]

**Operation Power Off Members**[113]

- U.K. (National Crime Agency)
- The Netherlands
- Germany
- Scotland
- Australia
- Canada
- Italy
- Spain
- Serbia
- United States
- Croatia
- Hong Kong
- Europol
- Joint Cyber Action Taskforce

**Participants of "Operation Power Off," which seizes infrastructure of cyber hackers and disrupts illegal cyber attacks.**

## 9. Improvements in Law Enforcement

Governments and private industry are continuing to fight back against malicious cyber threat activity. Increased levels of coordination between nation-states, law enforcement agencies, and private-industry partners have coalesced into a coherent cyber deterrent. Through international cooperation, the costs and penalties to a threat actor of committing malicious cyber activity will likely rise. Actions, such as the FBI take down of criminal "booter" and "stresser" sites in 2018, provide strong deterrence for other cyber criminals.[112]

### *Law Enforcement and Internationalization*

International cooperation between nation-states and their national cyber security communities steadily increased in 2018. Several national and transnational law enforcement agencies have taken the fight to malicious cyber threat actors. This past year, Operation Power Off, with collaboration from at least a dozen nation-states, culminated in the seizure of infrastructure and the arrest of members of the world's largest DDoS-as-a-service website, Webstressor.org. This website was thought to charge fees of fifteen euros a month and is alleged to be responsible for over 4 million worldwide DDoS attacks.[114]

Last year, Tesco Bank and six other U.K. financial institutions are alleged to have suffered severe disruption emanating from the Webstressor.org service.[115] Greater international participation and cooperation in the pursuance of cyber criminal activity will increase costs and in time should deter criminal behavior.

## 10. Changes in the Regulatory Environment

The General Data Protection Regulation (GDPR) came into effect on May 25, 2018. Since then, headlines have reported the potential of dramatic costs to breached companies. However, it is unclear whether these speculative figures will equate to real fines issued along GDPR lines and within expected timelines for regulatory procedures.

Each country in the European Union is implementing GDPR at its own pace. As of the end of 2018, the Information Commissioner's Office (ICO) in the U.K. had not yet issued any GDPR-related fines. Fines issued in 2018 continued to fall under the Data Protection Act 1998 rather than the Data Protection Act 2018 and the EU's GDPR. Some notable fines issued by the ICO in 2018 are shown in Table 5.[116]

Several smaller fines and warnings have been issued to companies that remain underprepared for GDPR. In the U.K., the ICO has sent out warning letters to 34 organizations, including the NHS, which have failed to pay data protection fees. These companies face fines if requirements are not met.[117] Complaints have been made against large companies such as Facebook and Google, with estimates of potential fines of billions of dollars for breached member data.[118]

[111] Ablon, Libicki, and Golay 2014
[112] Krebs, 2018
[113] Eenheid, 2018
[114] Europol, 2018
[115] Bond, 2018
[116] Information Commissioner's Office, 2018
[117] Affi-Sabet, 2018
[118] Brandom, 2018

| Company | Sector | Date | Reason | Fine |
|---|---|---|---|---|
| **Heathrow Airport** | Transportation/ aviation/aerospace | October 8, 2018 | Failing to ensure that the personal data held on its network was properly secured | £120,000 |
| **Equifax** | Finance/insurance | September 20, 2018 | Failing to protect the personal information of up to 15 million U.K. citizens during a cyber attack in 2017 | £500,000 |
| **Independent inquiry into child sexual abuse** | Government | July 18, 2018 | Revealing identities of abuse victims in mass email | £200,000 |
| **Crown Prosecution Service** | Government | May 16, 2018 | Lost unencrypted DVDs containing records of police interviews | £325,000 |
| **Holmes Financial Solutions Ltd.** | Finance/insurance | January 31, 2018 | Instigated the transmission of automated marketing calls to individuals without their prior consent | £300,000 |
| **Carphone Warehouse** | Entertainment and media | January 10, 2018 | Failure to secure the system allowed unauthorized access to the personal data of over three million customers and 1,000 employees | £400,000 |

**Table 5: Regulatory fines in 2018**

While GDPR was predicted to greatly influence the financial impact of breaches in 2018, the fact that the posed fines have yet to materialize into company losses does reduce this expectation. The first significant fines for 2018 are likely to be seen in 2019 to allow for the due diligence of various regulatory bodies to assess complaints.

### *GDPR Limits*

The U.K. Data Protection Act of 1998 limited penalty fines to £500,000. The new Data Protection Act 2018, which came into effect alongside GDPR, provides a range of new penalties issuable by the ICO, including 4% of global turnover or a fine of £17 million, whichever is higher. For a company like Facebook, which previously received the maximum £500,000 fine under the old regulations, this could still result in a US$1.63 billion (£1.27 billion) fine under GDPR as investigations are ongoing.[119]

### *Insurance and GDPR*

Insurance coverages typically do not indemnify companies against criminal penalties, but in some circumstances may cover civil fines, so the impact that GDPR will have on insurance payouts will vary from one jurisdiction to another. Individual cases may come down to specific details to do with whether the fine is classed as criminal or civil as well as the conduct of the insured.[120] Finland and Norway could permit coverages for GDPR fines because insurance in these countries is permitted to cover civil fines. However, insurers in the U.K., France, Italy, and Spain, among other regions, face the cost of defending against the response to GDPR fines.[121]

### *Global Data Privacy Laws*

Data privacy regulations are lagging globally but some clear leaders have started to emerge. The United States, Canada, Europe, and India, in particular, have strong regulations.

In August 2017, the Supreme Court of India ruled that privacy is a fundamental right essential to life and liberty. This paved the way for a draft bill entitled the Personal Data Protection Bill 2018, which, if passed by the Parliament, will establish safeguards for accountability and transparency.[122] Structured similarly to GDPR, the penalties for violations are 2% of global turnover or approximately $700,000, whichever is higher.[123] This follows Pakistan's Personal

[119] Solon, 2018
[120] Insurance Journal, 2018
[121] Daley, 2018
[122] Wadhwa, 2018
[123] Ministry of Electronics & Information Technology – Government of India, 2018

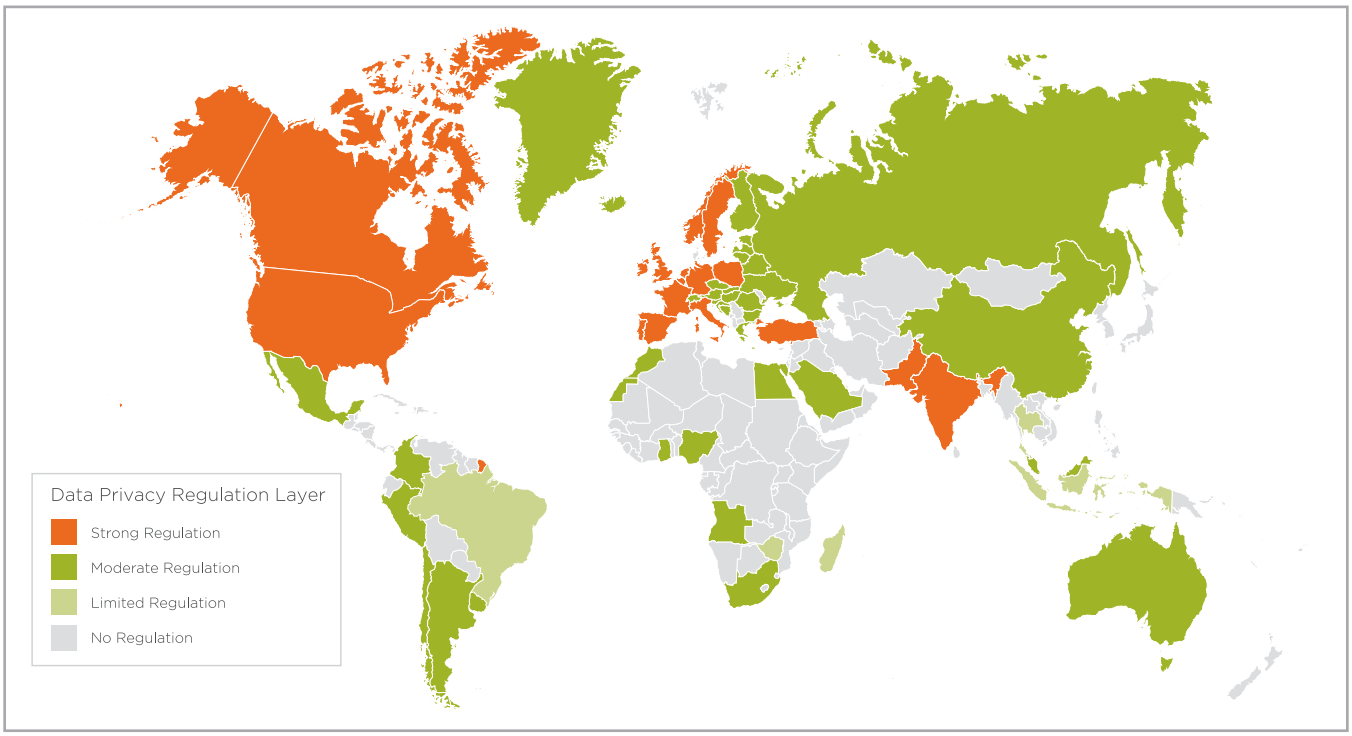



**Figure 5: Global data privacy regulations. Source: DLA Piper and CCRS.**[124]

Data Protection Bill 2018, which was influenced by the implementation of GDPR in the EU. Violations will be subject to up to two years imprisonment and up to $37,000.[125]

In the United States, California signed into law the most stringent data protection regulations in the United States in June 2018. The Consumer Privacy Act of 2018 will become enforceable in 2020 and gives Californian residents control over what information is gathered about them.[126]

California became the first state with an IoT cyber security law in August 2018. Coming into effect in 2020, all manufacturers of connected devices must equip their devices with reasonable security features including a unique password for each device.[127] Changes in California often forecast national trends, so these laws could signal the likely spread of more stringent cyber regulations across many other states in the U.S.

[124] Data compiled and reviewed from the following sources to create this map: (DLA Piper, n.d.; CNIL, 2018; Privacy International, 2018; Hedrich, Wong, and Yeo, 2017).
[125] Wikipedia, 2018
[126] Mazzoni, 2018
[127] Robertson, 2018


Index

SECTION 2

# Data Exfiltration

Data exfiltration remained a prominent cause of insured losses in 2018. Breaches have become costlier across most jurisdictions, and there is little indication that this trend will change in 2019, as regulatory fines are likely to come into full effect. While there has been a decrease in reported breaches, the average size of data breaches continued to increase in 2018.

### *Rising Cost of Data Breaches*

The cost of data breaches continues to increase year-by-year, with reputational and regulatory costs identified as main drivers of the increase for 2018.[128] In 2018, the average cost of a data breach globally was US$3.86 million – a 6.4% increase from 2017. This was due to so-called "mega-breaches" where 1–50 million records are compromised, resulting in losses between US$40 to US$350 million.[129]

Indirect losses including customer churn, business interruption, and management strategies to handle the breach were significant contributors to these large losses. Large-scale breaches (over 1 million records) typically cause reputational damage to the affected company, which results in share price reduction and loss of customers for some period.[130] Reputational costs are often suffered even after the remediation period of the data breach and, in extreme cases, continue to impact a company's financial results for years.

[128] Larry Ponemon, 2018
[129] Ponemon, 2018
[130] Larry Ponemon, 2018
[131] John McCrank and Jim Finkle, 2018
[132] Higgins, 2018
[133] Schick, 2017
[134] Malhotra, 2018
[135] Bisson, 2018
[136] Bisson, 2018

Incident response costs are also driving the increase in the cost of data breaches. As the cyber threat landscape becomes more complex and demand for cyber security resources increases, the costs in remediating data breaches, particularly for large-scale events, has increased. In 2018, Equifax reported that the total cost of their breach could be upwards of US$439 million, with some experts calling the event "the most expensive breach in history."[131] This event resulted in significant losses for insurers, with over US$125 million of the losses covered by insurance. Some estimate the cost of the breach could increase to US$600 million as there are civil lawsuits and regulatory fines still pending.

### *Cause of Breaches*

Companies' exposure to large-volume data loss events is often dependent on the vigilance of their security. New studies indicate that nearly 60% of data breaches that occurred in the last two years were attributed to a known vulnerability the organization had not yet patched.[132]

Even with vigilant security systems, the breach threat posed by insiders, be it malicious or accidental, remains one of the highest concentrations of risk within a company, accounting for nearly 75% of security breaches.[133] The year 2018 began with such an incident in the Aadhaar data breach of 1.1 billion records.[134] As outlined in Table 6, this was one of the first and largest reported data breaches of 2018. The breach was attributed to purchased login credentials, which gave users access to personal information including name, address, photo, phone number, and the email address of all registered citizens in India.[135]

Accidental disclosures continued to be a realized threat throughout 2018 with companies such as MyHeritage, Panera Bread, and the fitness app PumpUp unintentionally exposing a combined 135 million personal records in 2018.[136] Fortunately, in some of these cases the cyber security community identified the exposed data before it could be exploited by criminal entities.

***Data Loss Increasingly Caused by Third-Party Breaches***

An emerging trend in 2018 is data loss through supply chain attacks. The retail industry is particularly susceptible to supply chain compromises as physical and online financial payment systems are often provided by third-party vendors. In 2018, the retail giant Saks Fifth Avenue and Lord & Taylor had a record-breaking 5 million credit and debit card details stolen by a threat actor group referring to themselves as the "JokerStash Hacking Syndicate."[137] Ticketmaster U.K., the online events ticket vendor, reported a compromise in their third-party chatbot software on their site in June 2018, resulting in the theft of 40,000 customer credit cards.[138] The compromised chatbot software affected an estimated 800 other e-commerce firms.[139]

Continued growth in IoT and reliance on third-party vendors means supply chain attacks are a source of systemic risk, which will continue to grow over time with the potential for significant accumulation losses for the insurance industry.

> The retail industry is particularly susceptible to supply chain compromises as physical and online financial payment systems are often provided by third-party vendors.

[137] Cyber GRX, 2018
[138] BBC, 2018
[139] Yonathan Klijnsma and Jordan Herman, 2018
[140] Isaac and Frenkel, 2018
[141] Kevin Kelleher, 2018
[142] Schechner, 2018

## Facebook Data Breach

In September 2018, the social media giant Facebook was subjected to a significant data breach that resulted in an estimated 50 million accounts being compromised by hackers.[140] The attackers exploited three bugs in the "view as" feature on the platform that allowed malicious actors to steal access tokens for the accounts. These tokens allowed the actors to take full control of victims' profiles and gain access to third-party applications such as Spotify.

On the day the breach was disclosed, Facebook's share price fell by 3%, wiping US$13 billion off the company's market capitalization.[141] Facebook may also face a substantial penalty if the company is found to be in violation of GDPR regulations, with some estimates suggesting that the fine could reach as much as US$1.63 billion.[142]

Corporations should be aware that significant indirect losses can stem from reputational risk caused by data loss events. Stock price decreases and increased customer turnover following a data loss incident can cause significant revenue loss.

| Company[143] | Country | Number of Records | Date | Severity |
|---|---|---|---|---|
| **Aadhaar** | India | 1,190,000,000 | January 2018 | P8 |
| **Exactis** | United States | 340,000,000 | June 2018 | P8 |
| **Twitter** | United States | 336,000,000 | 2018 | P8 |
| **Under Armour** | United States | 150,000,000 | March 2018 | P8 |
| **Huazhu Hotels Group** | China | 130,000,000 | August 2018 | P8 |
| **MindBody** | United States | 114,000,000 | 2018 | P8 |
| **MyHeritage** | Israel | 92,300,000 | October 2018 | P7 |
| **T-Mobile** | United States | 74,000,000 | August 2018 | P7 |
| **Sungy Mobile Limited** | China | 50,600,000 | May 2018 | P7 |
| **Facebook** | United States | 50,000,000 | September 2018 | P7 |
| **MyEtherWallet** | United States | 50,000,000 | April 2018 | P7 |
| **Localbox** | United States | 48,000,000 | April 2018 | P7 |
| **Andhra Pradesh Government** | India | 45,000,000 | 2018 | P7 |
| **Panera Bread** | United States | 37,000,000 | April 2018 | P7 |
| **Ticketfly** | United States | 27,000,000 | May 2018 | P7 |
| **Comcast Xfinity** | United States | 26,500,000 | May 2018 | P7 |
| **Animoto** | United States | 22,000,000 | July 2018 | P7 |
| **Timehop** | United States | 21,000,000 | July 2018 | P7 |

**Table 6: Selected recent large-scale data breaches**

### *Decline in Incidents of Data Breaches in the U.S. but Increased Reporting in the EU*

Figure 6 shows that incidents of data breaches have significantly declined in 2018, with incidents of breaches falling by 40% compared with 2017. The major decline is in smaller-scale data breach incidents. For large data breaches, involving more than 1 million records, the decline is less marked: There were 10% fewer incidents in 2018 than 2017. This suggests that the threat of large-volume data breaches to companies has remained relatively consistent. In fact, the number of incidents involving over 100 million records has remained at the 2017 record high of 6 events annually.

The change in the regulatory landscape has resulted in the growth in reported incidents of data breaches in Europe. General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, requires all companies to notify their country's regulatory body within 72 hours of detection or face significant fines. To avoid these fines, companies have been diligent in reporting breaches, with the Information Commission Office (ICO) in the U.K. stating that the number of self-reported incidents quadrupled in June 2018.[144]

The decline in the incidents of data breaches in the U.S. in 2018 could be attributed to the fall in the value of stolen records on the black market. Cyber threat actors often monetize the proceeds of a data breach by selling their stolen records on black markets to other criminal gangs. The high incident rate of data breaches over the last decade has resulted in an abundant supply of records on

[143] Note: Two Facebook data breaches have been excluded from this list as exfiltration of data did not occur.
[144] Matthew Schwartz, 2018

The decline in the incidents of data breaches in the U.S. in 2018 could be attributed to the fall in the value of stolen records on the black market.

black markets, which outstrips demand. The black-market price of U.S. Visa credit cards has dropped from US$80 dollars in 2012 to US$7 in 2018.[145] This has resulted in a decline in profitability of data exfiltration campaigns by cyber criminals.

Advances in anti-fraud measures have increased the difficulty for cyber criminals to monetize stolen data, particularly financial records such as credit card numbers, making credit card data theft less attractive to criminals.[146] As data exfiltration attacks have diminished, other forms of cyber attacks have increased, notably ransomware and extortion, presumably as criminals have found these activities more rewarding. However, this could potentially reverse in the future, as cyber black markets increase their stability, maturity, and anonymity and if demand for stolen credit cards returned to previous levels.[147]

***Increasing Average Size of Data Breaches in the U.S.***

The average size of data breaches in the U.S. increased substantially between 2015 and 2017. In 2018 this trend continued, with the average severity of data breaches increased by 32% compared with 2017. Globally, the average size of data breaches has declined. The increasing trend in severity of data exfiltration attacks in the U.S. may be related to the increasing amount of data that companies hold. Companies continue to harvest their customers' data at an ever-increasing volume, particularly in the tech and social media industries. As the global number of internet and social media users continues to increase, for example, at rates of 7% and 13% respectively in 2018, the volume of data being held by companies about their customers and contacts will continue to grow. The potential for ever-larger-scale data breaches will grow with this trend and increase volatility for cyber insurers.[148]

[145] Armor, 2018
[146] Nicolas Christin, 2018
[147] Armor, 2018
[148] We Are Social, 2018

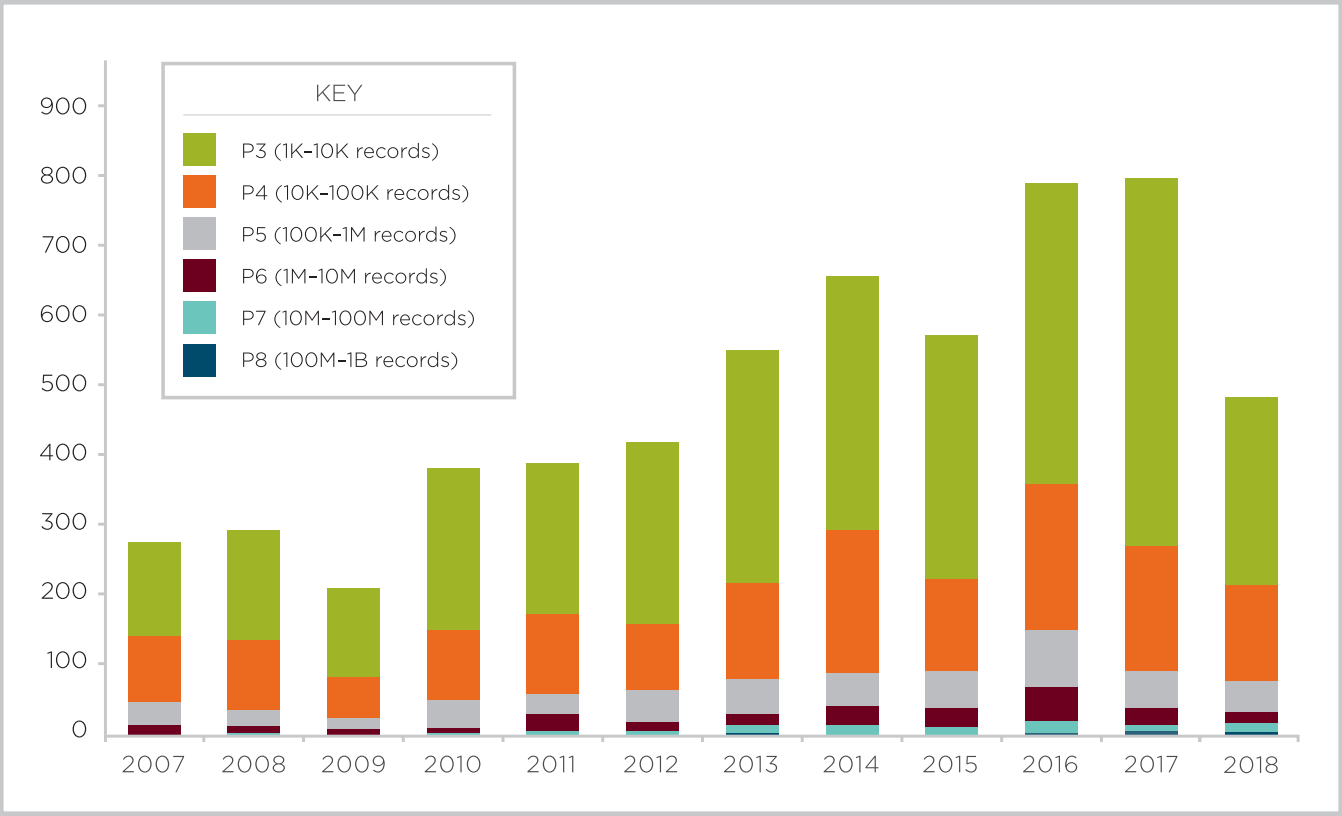



**Figure 6: Number of U.S. data exfiltration events (greater than 1,000 records) over time. Source: RMS Cyber Loss Experience Database.**

SECTION 3

# Contagious Malware


Malicious software continues to pose a significant threat to corporations. The interconnected nature of corporate networks has allowed contagious malware to scale rapidly, globalizing once-isolated incidents.[149] To date, ransomware has represented one of the most formidable versions of contagious malware. Europol has estimated that various cyber criminals have made over US$25 million from their ransomware in the past two years.[150] However, the cost of ransom payments is relatively minor compared with the potential losses that these malware attacks can inflict from business interruption by encrypting servers, wiping critical data, and disabling vital systems.

## Self-Propagating Malware Causes Significant Disruption

In the last two years, there has been a significant increase in ransomware events penetrating deeper into business IT networks with self-propagating malware.[151] Usually, ransomware takes advantage of human error such as through phishing or the clicking of malicious links. Other points of entry include the use of exploits designed to take advantage of software vulnerabilities or poor cyber hygiene practices.[152]

Once a company is infected with a piece of self-propagating ransomware, often referred to as a "cryptoworm," it can spread through a system without human interaction. Once in a network, cryptoworms target vulnerable devices within that network and copy themselves onto vulnerable hosts. This is different from typical viruses where the malware requires the user of a device to activate a program or email or download a file to infect other devices within a network.

The increased contagiousness of cryptoworms was illustrated by the WannaCry and NotPetya attacks in 2017. The WannaCry ransomware cryptoworm resulted in an estimated US$4 billion of loss globally.[153] NotPetya's wiper cryptoworm caused an estimated US$10 billion in losses.[154] Self-propagating ransomware capable of spreading through corporate networks represents a next generation of cyber threat and will likely be used again. The capability of such malware to impact large numbers of companies simultaneously makes it a source of systemic tail-risk losses in the cyber risk landscape.

It is essential to understand the threat posed from self-propagating malware because the losses derived from cyber attacks are largely dependent on the rate in which the malware can spread within a system. Malware, which moves quickly and without restraint through a system, has the potential to infect more devices before company remediation, resulting in higher clean-up and business interruption costs.

## Ransomware Has Replaced Banking Trojans as the Malware of Choice for Financial Gain

Ransomware replaced banking trojans for financially motivated cyber criminals in 2018, likely due to the profitability of self-propagating ransomware, combined with increasing security levels preventing trojan incursion in banking systems. Europol reported that the number of cyber attacks involving banking trojans halved in Europe in 2018.[155]

[149] Greenberg, 2018
[150] Europol, 2018a
[151] Cisco, 2018a
[152] Palmer, 2018
[153] Gallin Luke, 2017
[154] Reinsurance, 2018
[155] Europol Cybercrime Centre, 2018

The substitution of banking trojans by ransomware is attributed to the relative ease in which to monetize the proceeds of their attacks. Monetizing the proceeds of a financial heist involving banking trojans often involves a complex money-laundering process. The increasing security measures implemented by financial institutions and the closure of black markets increases the costs and reduces the benefits of these types of attacks. Ransomware often circumvents these monetization burdens by demanding a ransom in cryptocurrency such as Monero, which is less traceable, especially when laundered through multiple crypto-wallets.

### Malware Goes Mobile

The vulnerability of mobile phones has led to a significant increase in mobile malware variants including ransomware, banking trojans, adware, and even spyware. Recent reports suggest that 87% of all Android smartphones are exposed to at least one critical vulnerability, and 95% of Android devices can be hacked by a simple text, and malware – including mobile trojans, ransomware, and botnets – can be dropped into the device.[156]

Although affirmative cyber insurance products may not always include coverage for mobile phone loss, this growing trend may represent opportunities for cyber insurers or potential loss accumulations for the future.

Mobile malware incidents are most prominent in emerging and developing economies. Kaspersky reported that in Q2 of 2018, Bangladesh, China, and Iran had the highest share of mobile users attacked by mobile malware.[157] This has been attributed to a high penetration of mobile devices that have not been updated to the most recent patches. Even in the U.S., 71% of all Android users on five major U.S. carriers were running security patches that were at least two months old in 2017.[158]

### Contagious Malware: Not Just Bad for Business

The potential for contagious malware to negatively impact society is both broad and dangerous. Over 25% of one cyber insurer's total cyber claims in 2017 were a consequence of ransomware attacks.[159] The indiscriminate nature of contagious malware means that public services and business activities are equally vulnerable. The year 2017 saw global cyber contagions WannaCry and NotPetya wreak havoc across the globe. In the U.K., WannaCry disrupted over 34% of all NHS Trusts in England, causing widespread disruption to appointments, care, and treatment.[160] During NotPetya, Merck, a U.S.-based pharmaceutical company, encountered unanticipated interruption to its manufacturing processes.[161] Contagious malware is also starting to affect localities. In March 2018, the city of Atlanta experienced weeks of citywide disruption due to a ransomware attack that demanded over US$50,000. Atlanta has spent over US$2.6 million in incident response and other measures designed to return normal services and mitigate against future attacks.[162]

> Malware, which moves quickly and without restraint through a system, has the potential to infect more devices before company remediation, resulting in higher clean-up and business interruption costs.

Contagious malware has also become one of the preferred tools of geopolitical rivals. The global cyber contagions NotPetya[163] and BadRabbit have been publicly attributed to the Russian military intelligence agency the GRU and their state-backed actors.[164] Likewise, the U.S. has indicted a North Korean citizen thought to have perpetrated the WannaCry ransomware attack in coordination with the North Korean APT Lazarus Group.[165] Nation-states and their proxies are using their cyber capabilities for increasingly disruptive, damaging, and costly cyber attacks. Unfortunately, the indiscriminate nature of contagious malware means that nation-states can rarely exert control once contagious malware is used, causing unintended widespread disruption and loss.[166]

[156] Thomas, Beresford, and Rice, 2015
[157] Kapersky Lab, 2018a
[158] Brian Duckering, 2017
[159] Insurance Times, 2018
[160] National Audit Office, 2018
[161] Merck, 2018
[162] Newman, 2018a
[163] NCSC, 2018b
[164] NCSC, 2018c
[165] DOJ, 2018
[166] NCSC CSAN, 2018

# NotPetya Losses: A Retrospective

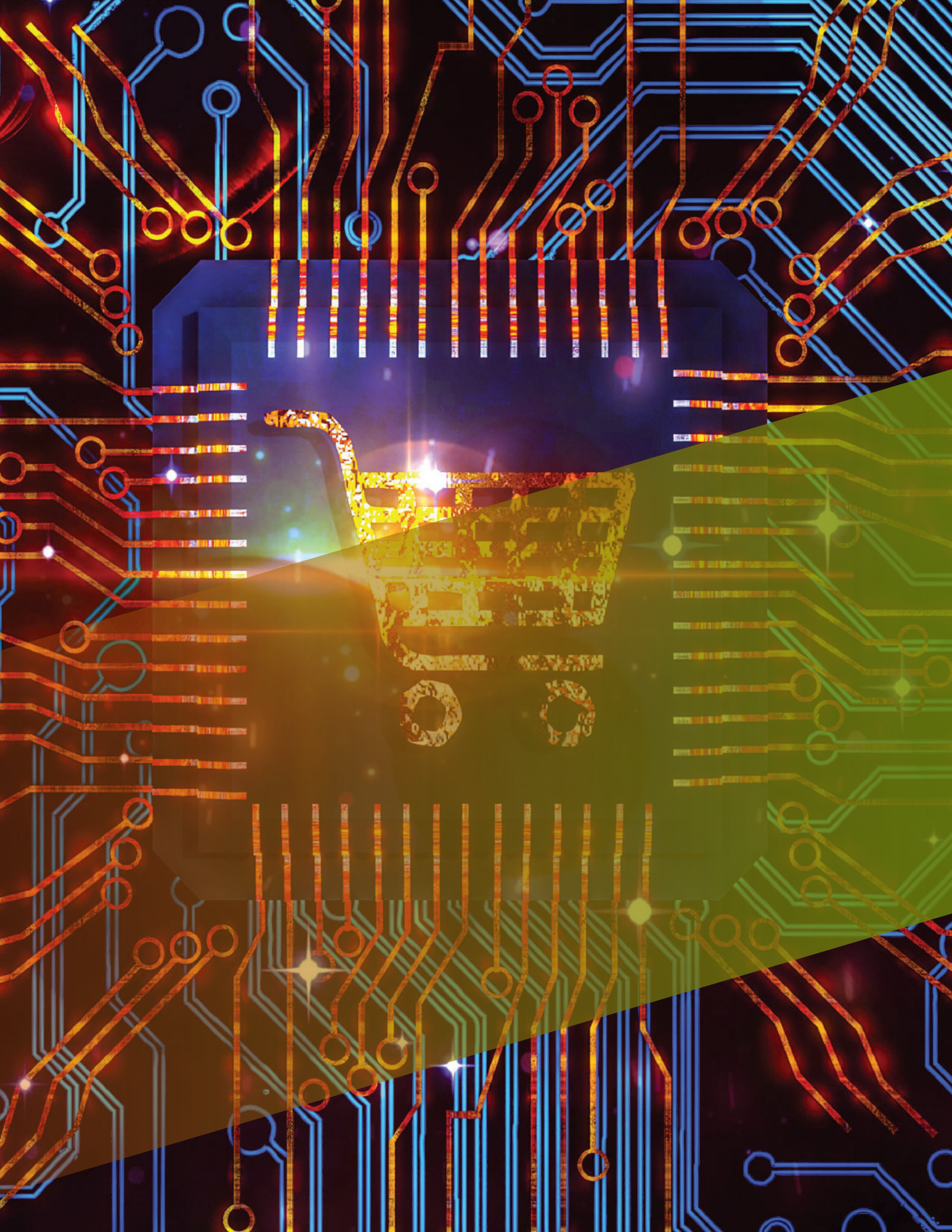
After it impacted hundreds of major companies around the world in June 2017, NotPetya remains the highest loss-making incident of contagious malware history. It is reported that total economic loss attributed to NotPetya exceeds US$10 billion.[167] It has been estimated that total insured losses, including silent cyber, will exceed US$3 billion.[168]

Several global companies experienced severe disruption and loss. Merck, a U.S.-based pharmaceutical company, reported direct losses of just under US$1 billion.[169] By the first quarter of 2018, FedEx claimed more than a US$300 million loss due to lost revenue and IT recovery.[170] At the end of 2017 Mondelez International reported a 0.4% decline in revenue and growth and over US$84 million in recovery costs.[171] And Maersk, a company vital to the globalized economy and supply chains, estimates total costs between US$250 million and US$300 million. In response to the attack, Maersk has dedicated significant resources to enhancing cyber resilience to reduce the likelihood and impact of future attacks of this type.[172]

Could these costs be prevented in the future? Some suggest that an up-to-date cyber security posture can help mitigate the effects of contagious malware. However, NotPetya was designed to recognize patches and propagate around patched systems within corporate networks.[173] Other cyber security specialists have commented that NotPetya had the capability to spread and infect over 1,000 computers within a corporate network in under two minutes.[174]

Clearly today's globalized and interconnected business environment, dependent on information technology, is amplifying the effects of contagious malware.[175] In the future, the increasing integration of connected infrastructure, especially the rise in the use of IoT and other smart innovations, will likely lead to an increase in the scope, scale, and severity of contagious malware events.

[167] Greenberg, 2018
[168] PCS, 2018, and RMS Cyber Loss Experience Database
[169] Merck, 2018
[170] FedEx, 2018
[171] Mondelez International, 2017
[172] A.P. Moller – Maersk, 2017
[173] Symantec, 2017
[174] Nash, Castellanos, and Janofsky, 2018
[175] Greenberg, 2018



SECTION 4

# Financial Theft


Financial theft remained a major source of cyber attacks and cyber-enabled fraud in 2018. Networks of trust involving financial transactions continue to be exploited and back-end systems remain a target for financially motivated cyber criminals. The implementation of Europay, Mastercard, and Visa (EMV) technology that authenticates chip-card transactions has reduced physical point-of-sale fraud, but new vectors of attack have emerged. Digital currency theft reached record-breaking levels in 2018.

## EMV Rollout

Physical cyber fraud on point-of-sale transaction systems involving counterfeit debit and credit cards declined in 2018. This trend was attributed to the marked growth in chip-enabled credit and debit cards in the Asia-Pacific region and the U.S. An estimated 90% of all terminals in the U.S. will be EMV compatible by 2020.[176] Globally, 54% of all card-present payments in 2017 were estimated to have used EMV standard and approximately 81% of credit cards are now EMV-enabled.[177] The main driver in the growth of EMV implementation has been the policy introduced by EMV credit card companies in 2016 requiring U.S. retailers to upgrade their point-of-sale transaction systems to accept EMV-chip-enabled cards or face liability for card-present fraud.

Card-present fraud is still a cause of significant global losses. Card skimming from corrupted ATM machines and other point-of-sale terminals remains widespread in Europe and the U.S., and cyber criminals have been known to create fake companies using legitimate business information to set up point-of-sale transaction systems and ATMs to skim credit card details.[178]

## The Evolution of Fraud in Technology

To circumvent the implementation of EMV technology, criminal groups have altered their methods of customer-side financial theft. Online fraud now dominates the financial theft landscape and plagues the global e-commerce industry. In the first quarter of 2018, the growth of attacks on the e-commerce industry outpaced online transaction growth by 83% in comparison to Q1 of 2016.[179] The attack rate on the U.S. e-commerce industry also grew by 93% in Q1 compared to the previous year. Estimates suggest that by 2020, the cost of "chargebacks," which is the demand by credit card companies to reimburse fraudulent transactions, could reach US$31 billion in the e-commerce industry.[180]

As technology evolves, fraudsters have adapted increasingly successful measures to extract profits. The mobile commerce (m-commerce) sector experienced widespread adoption in 2018, with an increase from 57% to 70% of medium-to-large digital goods retailers now using mobile transactions to drive sales.[181] However, m-commerce retailers are highly susceptible to fraud and every $1 of fraud costs a retailer an average of $3.29. Threat actors often target m-commerce for identity theft, which represents 39% of all fraud in m-commerce. As the influence of mobile technologies in society grows, m-commerce will remain a target for fraud.

Implementation of security measures to combat online fraud continued into 2018, with banks implementing

[176] Allen Friedman, 2017
[177] Jim Daly, 2018
[178] Europol Cybercrime Centre, 2018
[179] ThreatMatrix, 2018
[180] Emily Vuitton, 2017
[181] LexisNexis, 2018

two-factor authentication for online transactions and GeoBlocking to halt the cashing-out of debit and credit cards in non-EMV countries.[182] However, threat actors have been resilient and quick to adapt to new security measures, historically; it is likely that cyber criminals will find new ways to exploit the changing e-commerce security landscape.

Cyber criminals have also embraced social engineering as a method of financial theft, with "whaling" (also known as "president's fraud") attacks increasing by 136% between December 2016 and May 2018 in the U.S.[183] Whaling attacks involve malicious actors masquerading as a trusted colleague or supplier to trick senior and C-suite level executives into actioning cash transfers to fraudulent attacks. Financial theft through whaling has cost companies US$12.5 billion globally between October 2013 and May 2018.[184]

### Record-Breaking Incidents of Digital Currency Theft

An emerging cyber trend in 2018 was direct attacks on cryptocurrency exchanges. High-profile theft on crypto-currency exchanges in Japan increased by an estimated 300% from 2017 to 2018, with the exchange Coincheck suffering a record-breaking loss of US$516 million worth of NEM cryptocurrency.[185] The Tokyo-based exchange declared that it would repay US$425 million of the virtual money to the 260,000 victims.[186] Attacks directly on cryptocurrency exchanges rather than on individual crypto-wallets has resulted in a significant increase in the volume of digital currency stolen, resulting in an estimated US$1.1 billion loss in the first half of 2018.[187]

The volume of digital currency traded in Japan greatly increased following the recognition of crypto-exchanges by the government in 2017.[188] In fact, the traded volume of Bitcoin in Japan increased from US$22 million in 2014 to US$97 billion in 2017, a 444,000% increase.[189]

A major development in the crypto market this year is the introduction of cryptocurrency theft coverage by global insurers. Some insurers now offer cryptocurrency theft coverage in cyber affirmative policies, which includes cover of theft of cryptocurrencies in digital wallets caused by malicious outsiders.[190] Other types of crypto-insurance include general company policies, which cover blockchain start-ups, and some insurers are offering crypto-theft protection under specie policies.[191] Insurers have limited the rollout of this coverage due to uncertainties in the potential exposure they could face. The significant increase in crypto-theft in 2018 will likely be a concern for insurers offering the product and may limit the number of insurance companies entering the crypto-insurance market.

### Financial Transaction Theft

Attacks on back-end systems in the financial services sector, including inter-bank transaction networks, continues to be a potential source of systemic tail risk. There have been a number of high-profile incidents on the SWIFT network, including the Lazarus Group SWIFT financial theft of 2016, considered one of the most audacious cyber bank heists of its kind, which could have resulted in almost US$1 billion of loss.[192] The 2016 campaign successfully stole US$81 million from financial institutions including the U.S. Federal Reserve and several commercial banks.[193] Other SWIFT cyber attacks include the Far Eastern International Bank cyber heist, which could have resulted in a potential US$60 million stolen, but banking officials managed to recover most of the stolen funds, resulting in only US$500,000 loss.[194]

In response to these attacks, SWIFT announced an updated security protocol in 2017. Since the weakness was in the security of a member bank rather than a vulnerability in the SWIFT technology itself, SWIFT introduced a mandatory "Customer Security Control Framework."[195] The framework requires that users of the SWIFT network comply with 16 mandatory security controls, which focus on segregating the SWIFT critical systems by the end of 2018. By January 2018, 89% of SWIFT members were adhering to this security measure.[196] Increased security protocol measures are planned for 2019, which will involve 19 additional controls.[197]

[182] Europol Cybercrime Centre, 2018
[183] Shaun Nichols, 2018a
[184] Shaun Nichols, 2018b
[185] Spilotro, 2018
[186] Takahiko Wada and Chang-Ran Kim, 2018
[187] Rooney, 2018
[188] Jonnie Emsley, 2018
[189] Jonnie Emsley, 2018
[190] Suzanne Barlyn, 2018
[191] Kevin Helms, 2018
[192] Joshua Hammer, 2018
[193] Kaspersky Lab, 2018b
[194] Ian Thompson, 2017
[195] SWIFT, n.d.
[196] Finextra, 2018
[197] Paul Koetsier and Ton Diemontt, 2018

A major development in the crypto market this year is the introduction of cryptocurrency theft coverage by global insurers.

***Continued Vulnerabilities in the SWIFT Network***

In 2018, sophisticated attacks on third-party back-end systems continued. Banco de Chile (Central Bank of Chile) was subjected to an attack on their SWIFT network resulting in a US$10 million loss.[198] The cyber criminals used a destructive wiper and ransomware as misdirection to allow for transactions to be made on the SWIFT network.[199] In May 2018, the Banco de Mexico (Bank of Mexico) reported an attack that targeted their domestic inter-banking payment system, SPEI, resulting in a US$15 million loss.[200]

The new safety protocols introduced by SWIFT may reduce the likelihood of further attacks. However, threat actors are likely to continue to exploit banks with the weakest security to gain access to financial transaction networks. The scale of these networks creates significant challenges to their operators in terms of oversight of participating banks security and mitigation of attacks.

[198] Jeremy Kirk, 2018
[199] Pierluigi Paganini, 2018
[200] Michael O'Boyle, 2018

SECTION 5

# Cloud Outage

Cloud computing continues to be rapidly adopted by companies of every size and sector. The shared pool of resources hosted on the cloud gives companies access to services that can be rapidly provisioned with minimal effort. However, the use of these shared resources comes with shared vulnerability in the event of an outage or breach.

## Cloud Security: A Shared Responsibility

Security remains one of the highest concerns with cloud computing, particularly in storage services, with reports that just over half of organizations using the cloud had at least one public data exposure of their hosted data in the last year.[201] A key aspect of hosted services is the large dedicated teams of security professionals that maintain the services. However, safety of services and data hosted on the cloud is the responsibility of both the provider and the consumer. Malicious attacks are often attempted against cloud systems but the highly secure environments that are maintained by the cloud providers ensures that very few succeed. The most likely cause of cloud outages are operational errors by the providers and poor configuration by users.

Of those companies reporting potential account compromises, less than a third could be attributed to the cloud provider.[202] Instead, the blame and costs fell to cloud clients who implemented poor configurations, incorrect settings, and simple passwords, failing to secure their data. Rather than being a misstep by Amazon Web Services (AWS), the critical data exposures from Tesla and FedEx in 2018, hosted on the AWS S3 services, were not password-protected by the client companies.[203]

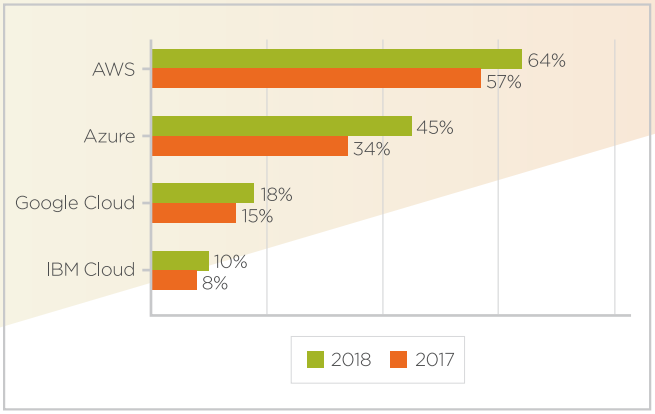



**Figure 7: Annual growth rates of the big four cloud service providers. Source: Rightscale's 2018 State of the Cloud Report.**

Cloud adoption is predicted to climb quickly to service the growth of IoT devices. It is projected that IoT growth will total 20 billion connected devices by 2020,[204] translating to roughly 400 million servers to support them, many of which will be in cloud data centers.[205] Globally, cloud spending is predicted to surpass US$500 billion by the year 2020 with 26% of enterprises spending more than US$6 million a year on the pubic cloud annually.[206]

The areas of highest new uptake over the next five years are forecast to be in the Asia-Pacific region, as they start to match the U.S. and Europe adoption rates.[207]

[201] DeNisco Rayome, 2018
[202] DeNisco Rayome, 2018
[203] Forest, 2018
[204] Gartner, 2017
[205] Business Sweden, n.d.
[206] Rightscale, 2018
[207] Jyotsana, 2018

### Concentration Risks in Big Four Service Providers

The public cloud market continues to be dominated by Amazon Web Services (AWS), closely followed by Microsoft, Google, and IBM.[208] There is little indication that this will change in the foreseeable future due to the established trust and reliability of these providers paired with the heavy investment required to enter the market in terms of talent and infrastructure.[209]

Perhaps due to the high adoption rates in previous years, AWS had the lowest growth of the top four providers from 2017 to 2018 at 15%. Microsoft led the way at 25%, followed by Google at 26%, and IBM at 50%.[210] The high adoption rates seen in AWS and Microsoft are largely due to beginners entering cloud computing rather than companies with established cloud strategies switching providers. Overall, early cloud adopters seem to find AWS (47%) and Microsoft (48%) the clear front-runners for entering the cloud space. The low early-stage adoption rates for Google (18%) and IBM (14%) indicate a marked difference in clientele, with these cloud providers appealing to those with an established cloud strategy.[211]

As reliance on cloud services continues to grow, so does the price of downtime for clients and providers.

Cloud reliability remains one of its stronger attributes. The probability of a top cloud service provider (CSP) suffering from a complete outage is low, but it would have a catastrophic impact on the global economy. A more likely occurrence is downtime for particular services within the cloud. Although service-level agreements still contractually deliver services with a reliability of 99.9%, downtime remains a costly threat.[212] Each of the services provided by a CSP rely on other services so they are interdependent and depend on the reliability of each other. Often, the system provided to companies via the cloud is the same as the one that runs several of the services delivered by the CSP. Some key services can be identified as "core" services, where their failure would trigger cascading failure of other services. Others are "peripheral," where their failure would be limited to their branch of the network.

The impact of losses is often determined by their timing and root causes. Losses that occur on days of heavy e-commerce traffic have greater impacts, such as the Amazon "Prime Day" disruptions.[213] Disruptions from external sources such as malware are often difficult to trace in a cloud environment. Disruptions remain feasible from physical external perils to the data center facilities, ranging from fires and natural catastrophes through to extreme weather events. Disruption from destructive perils could give rise to lengthy durations of outages.

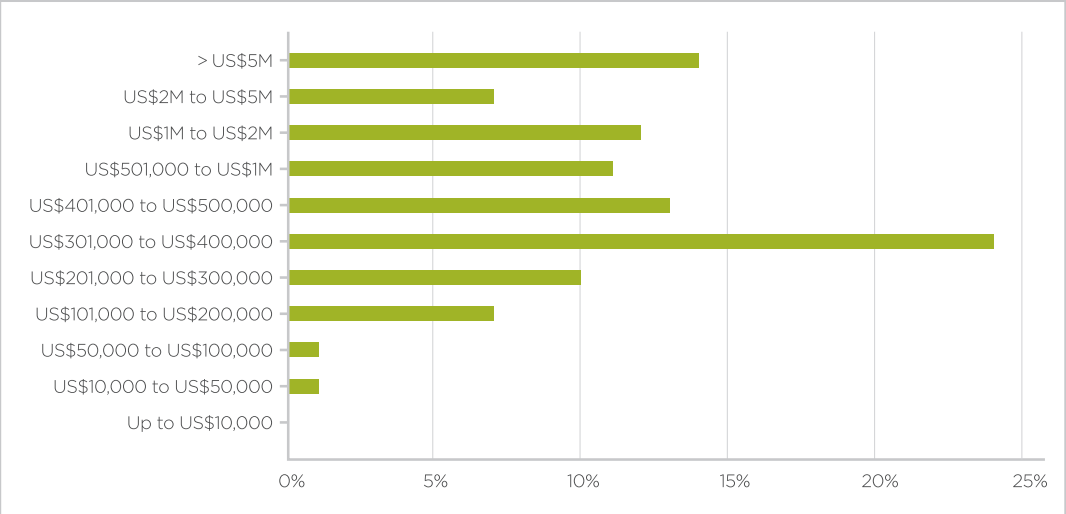



**Figure 8: Average cost of server downtime (2017 and 2019)**

[208] Jyotsana, 2018
[209] Jyotsana, 2018
[210] Rightscale, 2018
[211] Rightscale, 2018
[212] Lavrentieva, 2017
[213] Kaplan, 2018

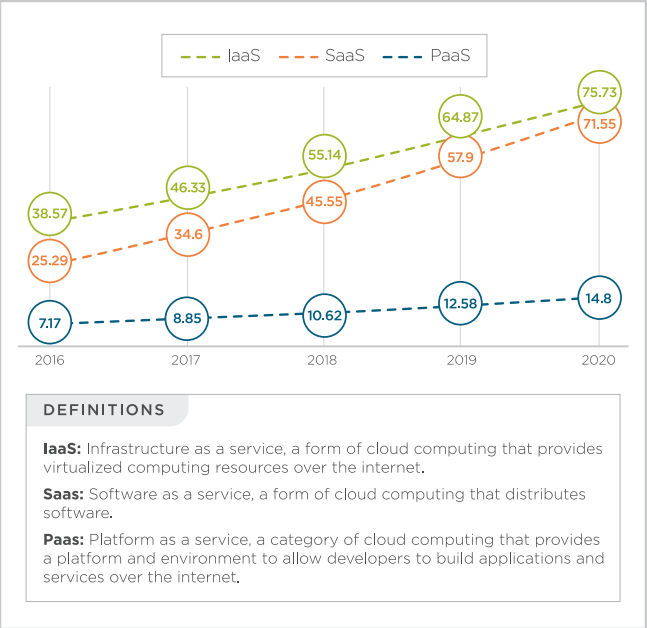



**Figure 9: Projections for cloud market growth. Market revenue in billions of dollars. Source: n'cloud.**[214]

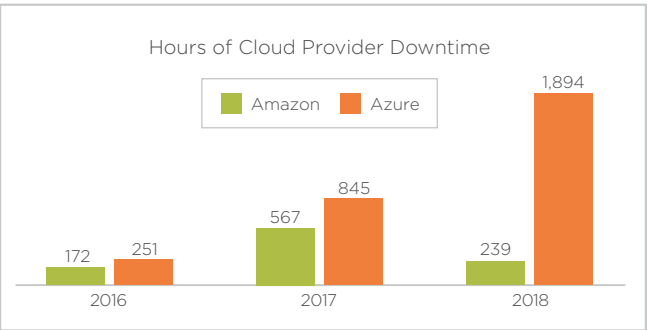



**Figure 10: Number of hours of enterprise server downtime in 2017 and 2018**

[214] n'cloud, 2017

## Amazon Prime Day Disruption

Amazons Prime Day, reported as the online retailer's second biggest shopping day of the year, was beset with issues shortly after its 3 p.m. U.S. launch. Affecting mainly the U.S., the day was hit with server issues including the AWS management console and Alexa services, with disruptions also hitting parts of Europe. Shoppers reported issues getting onto the website, logging into their accounts, and during the checkout process. Analytics provider One Click Retail estimates that Amazon lost US$1.2 million in sales per minute of downtime. Nevertheless, sales set a record for Prime Day, which, undoubtedly due to server errors, did not reach its full potential.

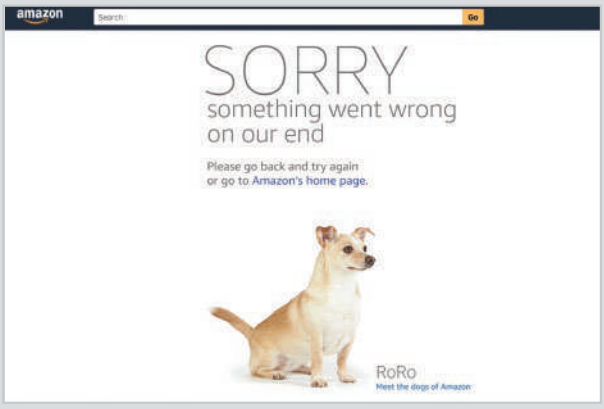



**Figure 11: Screen shown to customers on Amazon Prime Day who failed to complete their purchases. Source: TheVerge.com.**

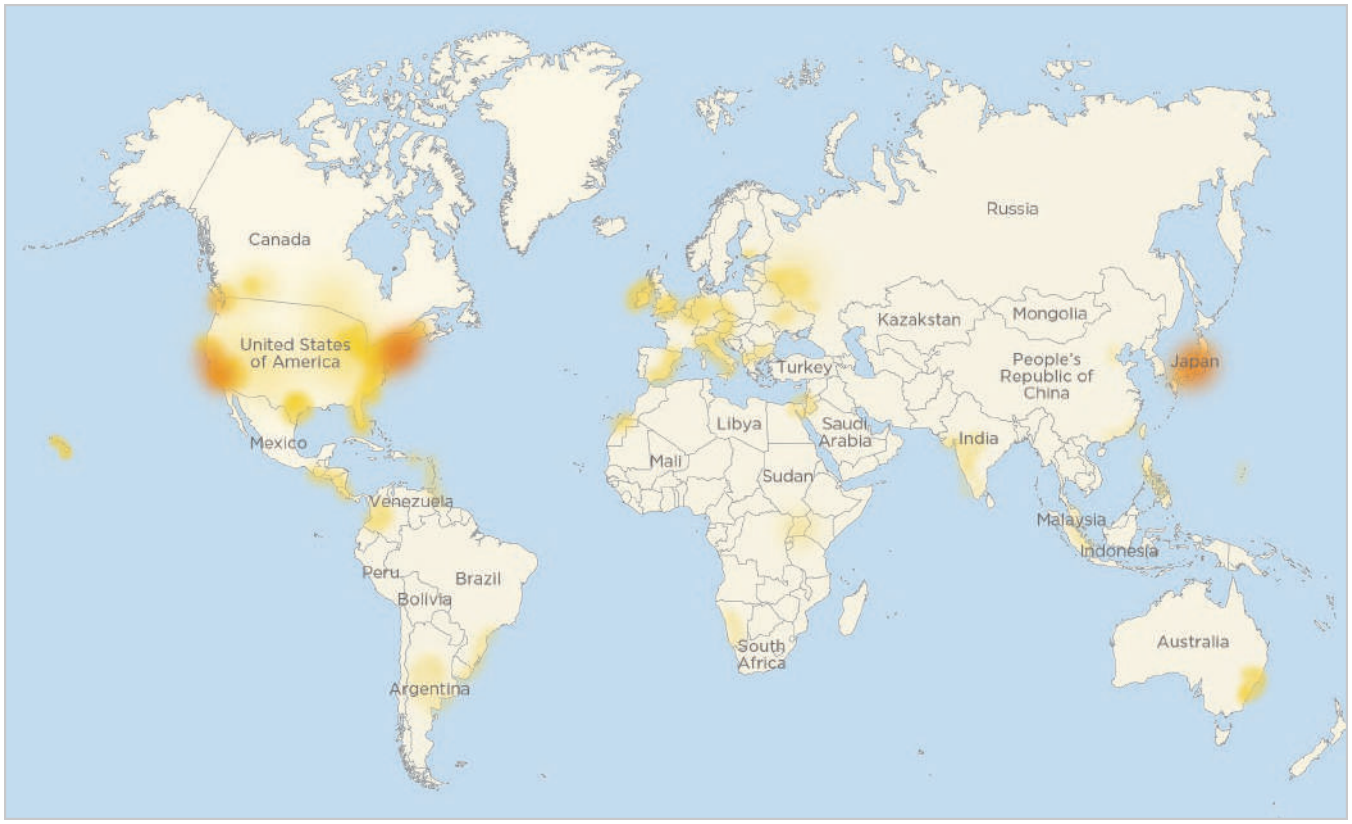



**Figure 12: Heat map of global services disruptions of AWS on Amazon Prime Day**

### Weathering the Clouds

Weather conditions worldwide significantly contributed to downtime in 2018. These inclement conditions included prolonged periods of high temperatures in the U.S. and Europe (Microsoft), which affected service delivery across the globe,[215] as well as nor'easter winds and rain (AWS, Equinix)[216] and lightning strikes (Microsoft).[217]

While its name suggests otherwise, it is essential to remember cloud computing is a grounded, physical technology that needs to weather metaphorical and physical storms. In 2016, it was estimated that about 12% of data center outages could be attributed to weather. While cloud strategies for technical protection continue to progress, the threat of weather remains.[218]

While its name suggests otherwise, it is essential to remember cloud computing is a grounded, physical technology that needs to weather metaphorical and physical storms.

[215] Mackie, 2018
[216] Tsidulko, 2018
[217] Mackie, 2018
[218] Ponemon, 2016


http://www.
View
Favorites
New Tab

SECTION 6

# Denial of Service Attacks

A distributed denial of service (DDoS) attack is a form of cyber attack that increases the traffic on a network, overwhelming it and making it inaccessible to legitimate users.[219] DDoS attacks often exploit connected devices with low security to increase the severity of their attacks. As the IoT landscape expands and evolves at a pace that IoT security has yet to match, the intensity of DDoS attacks continues to grow, with the largest attack to date seen in 2018.[220]

### Number of Attacks and Duration

The number of DDoS attacks continues to increase year-on-year, with millions of attacks reported annually. In 2018, DDoS attacks increased by 40% as large organizations faced an average of eight attacks per day.

While the number of attacks has increased, the duration of them has decreased: over three-quarters of attacks now last less than 10 minutes.[221] Attacks over 10 gigabits per second (Gbps) have doubled, but the majority (94%) of DDoS attacks recorded are still low intensity (less than 5 Gbps), often resulting in the slowing of service delivery rather than complete shutdown. These low-and-slow attacks may be difficult to distinguish from regular traffic and require very little bandwidth, making them hard to mitigate. However, they still have the effect of preventing genuine users from accessing the service, resulting in similar detrimental outcomes on customer retention compared to larger, brute-force attacks.[222]

### The Real Cost of DDoS

The effects of a DDoS attack vary depending on the target. In the case of a news organization, such as the BBC, which experienced a DDoS attack in 2015, customers may be unable to access news content.[223] In more severe cases, such as the 2016 DDoS attack on HSBC, customers may be prevented from accessing their online banking and completing transactions.[224]

After suffering from a DDoS attack, 57% of targeted organizations report reputation and brand damage as the primary business impact, with operational expenses a secondary concern. In 2018, 56% of victims reported a financial impact ranging from US$10,000 to US$100,000,[225] with some even reporting losses as high as US$2.5 million for a single attack.[226] High direct costs are from business interruption resulting from server downtime, cloud disruption, and brand and reputation damage that leads to a dip in company profits as customers move to competitors.

Operational efforts to prevent and recover from the attack are especially costly. In some instances, sensitive data is permanently lost. Indirect losses may be caused by insidious activities that accompany the attack such as malware injection or data exfiltration.[227] In fact, DDoS attacks mask network intrusion a third of the time,[228] and 9 out of 10 companies that experience a DDoS attack also have a significant data breach.[229]

[219] Kohout, 2015
[220] ESET, 2018
[221] Corero Network Security, Inc., 2018
[222] CloudFlare, n.d.
[223] BBC, 2015
[224] Schwartz, 2016
[225] Whalen, 2018
[226] Patton, 2018
[227] Patton, 2018; Kaspersky, 2015
[228] Kaspersky, 2015
[229] Reo, 2017

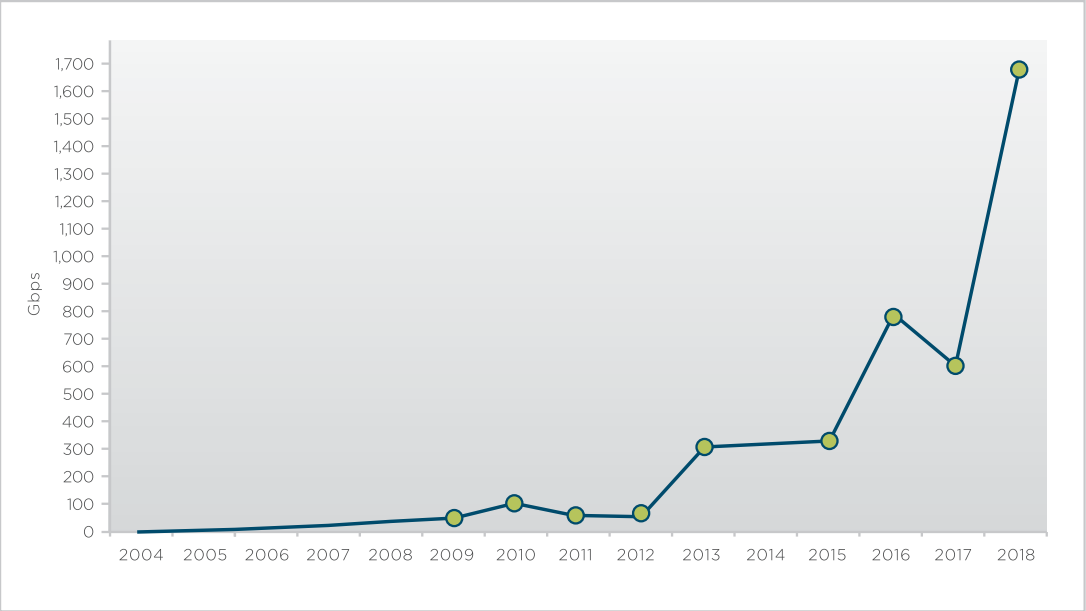



**Figure 13: Peak DDoS attack intensity from 2004 through 2018**[230]

## Application Techniques

### *Application Layer Attacks*

Many threat actors launching DDoS attacks have changed their approach from primarily targeting the network layer, which provides paths for data to move along, to targeting the application layer, which provides the interface between applications and the network. The application layer is appealing to attackers because of its diversity. New amplification techniques using the application layer are increasing attack capabilities, enabling them to be more impactful and damaging despite their decreased duration.

### *rDDoS*

Two in five businesses report experiencing a reflection amplification DDoS (rDDoS), with one-third of affected organizations reporting an inability to mitigate such attacks.[231] rDDoS attacks exploit the difference in bandwidth use between the attacker and the target, often utilizing memcached systems or NTP, and DNS protocols. Though the Memcached vulnerability has been around for over a decade,[232] in early 2018, memcached amplification attacks made headlines, giving businesses a new type of rDDoS attack to look out for.[233]

[230] Anstee et al., 2016
[231] Cisco, 2018b
[232] Corero Network Security, Inc., 2018
[233] Vaughn Nichols, 2018

### *DDoS Attacks Increased by the Cloud*

As cloud computing, the IoT, network security, and the application layer expand, so too will the intensity of DDoS attacks companies have experienced. It is likely that the size of DDoS attacks will continue to increase year-on-year, increasing in line with bandwidth capabilities.

DDoS attacks have changed from primarily targeting the network layer used for delivering data to targeting the application layer, which provides the functionality of the business.

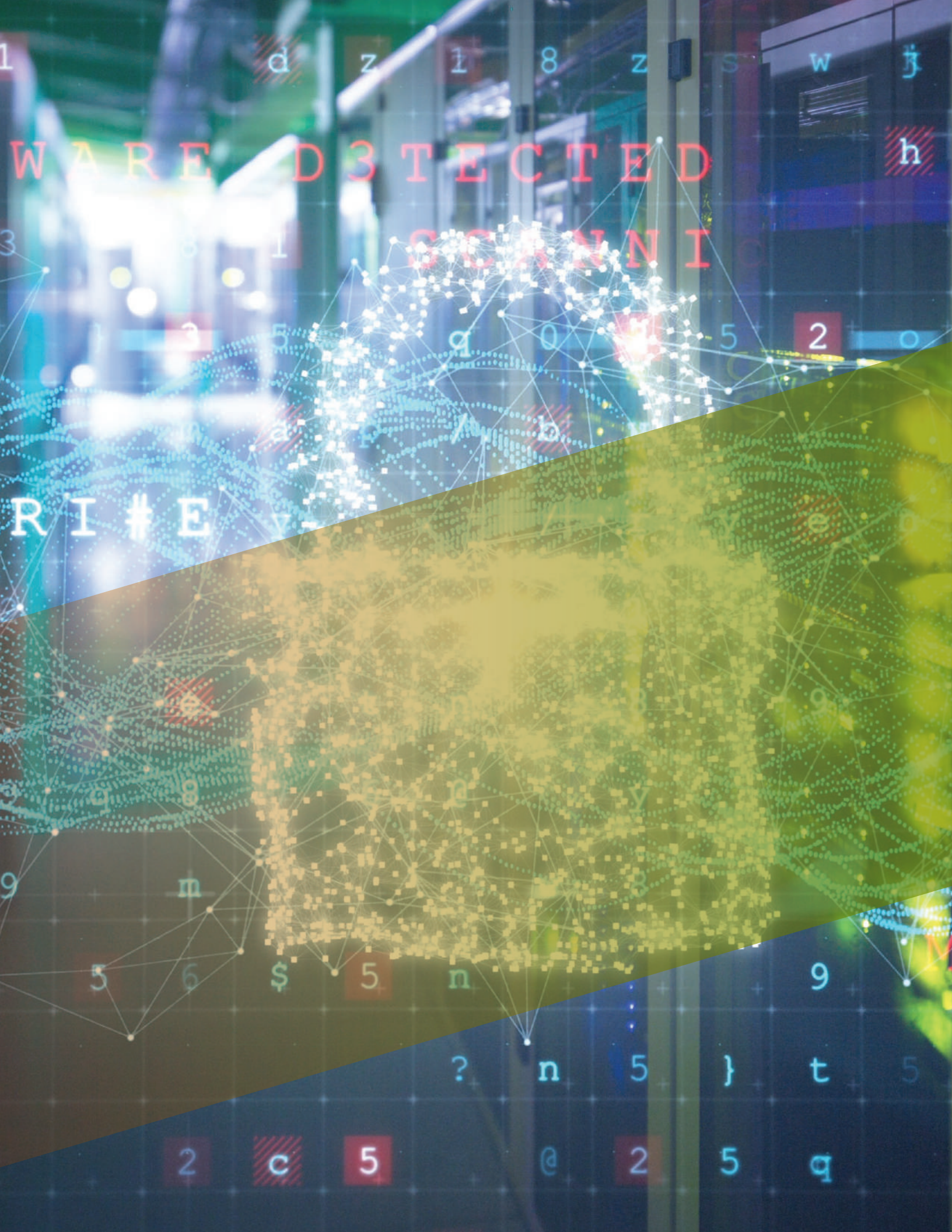
# Record-Breaking DDoS Attacks

Two of the highest intensity DDoS attacks identified to date occurred early in 2018.

The first hit GitHub on February 28, peaking at 1.35 terabytes per second (Tbps) via 126.9 million packets per second. This brought GitHub down for 5 minutes of full downtime and an additional 4 minutes of intermittent downtime.[234] With annual revenue estimated at US$300 million,[235] the direct economic loss is approximately US$5,000 in just a handful of minutes before accounting for losses from productivity loss and reputational damage. Before this attack, the largest DDoS attack recorded was 800 Gbps in 2016.

Just 5 days after GitHub experienced the world's largest DDoS, an even larger DDoS attack hit NETSCOUT Arbor on March 5, peaking at 1.7 Tbps.[236] This marked an increase of 113% since 2016. Both the GitHub and NETSCOUT Arbor volumetric DDoS attacks were amplified with memcached servers to maximize the scale of the attack.

[234] Skottler, 2018
[235] Sherman, 2018
[236] Bienkowski, 2018


WARE D3TECTED
SCANNI
RI#E

SECTION 7

# Managing Cyber Risk

Cyber risk continues to evolve. This report describes how the risk landscape is changing in many different dimensions, all of which have implications for how businesses can manage their own cyber risk. The imperative is to adapt to the changing risk landscape.

The sections of this report explain how cyber risk is changing and the evidence for trends that are emerging and that are likely to affect our cyber risk management strategies in the coming months and years. The first section of this report discusses 10 general trends that we believe will influence the cyber risk outlook for the next year and beyond. The subsequent sections describe how the main loss processes for cyber, from data exfiltration to denial of service attacks, are each evolving, and the patterns of risk that they now represent.

### Managing Through a Changing Risk Landscape

There are changes in the amount and types of systems that are exposed, changes in the strategies that hackers are using to find more rewards, and changes in the responses and security technologies being deployed to thwart them.

Cambridge Centre for Risk Studies, in collaboration with Risk Management Solutions, has monitored and published reports on the changing nature of cyber risk since 2014. The rate of change of cyber risk is now faster than at any time over the past six years. Risk managers cannot assume that the status quo and patterns of attacks that they are currently dealing with will continue. They should expect these patterns to change. This report suggests trends that will shape the future risk landscape to help managers anticipate these changes and stay ahead of the game.

### Cyber Insurance Portfolio Management

Cyber insurers are faced with challenges as they face a growing, competitive, and softening market. Changing patterns of risk make it more challenging to apply actuarial analysis of past years of claims experience to next year's likely cost structure. Most crucially, the potential for accumulation risk from a major cyber catastrophe is continually shifting. RMS tracks and calibrates its market-leading RMS Cyber Solutions risk models with regular updates and improvements to help clients keep track of these changing trends and apply them to safely manage portfolios of cyber policies.

### Protecting Society

The recent book, *Solving Cyber Risk*,[237] captures many observations on the nature of cyber risk and how the trends of cyber risk have been changing over time. It is noted that cyber risk involves many different stakeholders, and that it will take a concerted effort by many different organizations and agencies, investment in law enforcement, legal reforms, and changes in the economics of software production to make a radical reduction in the loss rates to society from cyber attacks. It should not be necessary to wait until a major catastrophe occurs before these reforms and investments are made.

[237] Coburn, Leverett, Woo, 2019

One of the greatest challenges for cyber risk analysts is to help organizations plan their multi-year business cycles to combat loss and justify investment in cyber risk reduction.

**The Future of Cyber Risk**

This report has summarized the current trends that are likely to persist for the next year or two. Businesses, however, need to plan over time cycles of multiple years. One of the greatest challenges for cyber risk analysts is to help organizations plan their multi-year business cycles to combat loss and justify investment in cyber risk reduction. The next priorities of risk researchers such as ourselves is to provide longer-term guidance for the potential shape of the cyber risk landscape over the next decade and beyond. We accept the challenge and look forward to helping define the future of cyber risk.

# References


Ablon, Lillian, Martin C Libicki, and Andrea A Golay. 2014. "Markets for Cybercrime: Tools and Stolen Data. Hackers' Bazaar." RAND Corporation - National Security Research Division.

Accenture Security. 2018. "Gaining Ground on the Cyber Attacker." https://www.accenture.com/t00010101T000000Z__w__/fr-fr/_acnmedia/PDF-84/Accenture-Security-State-of-Cyber-Resilience-2018.pdf.

Afifi-Sabet, Keumars. 2018. "NHS Faces Regulatory Action over Unpaid Data Protection Fees." ITPro. September 26, 2018. http://www.itpro.co.uk/information-commissioner/31994/nhs-faces-regulatory-action-over-unpaid-data-protection-fees.

Allen Friedman. 2017. "EMV's Working, and Stragglers Need to Get on Board." PaymentsSource. September 29, 2017. https://www.paymentssource.com/opinion/emv-holdouts-face-security-risk.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. "Measuring the Cost of Cybercrime." In The Economics of Information Security and Privacy, edited by Rainer Böhme, 265–300. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12.

Anstee, Darren, C.F Chui, Paul Bowen, and Gary Sockrider. 2016. "Worldwide Infrastructure Security Report | Arbor Networks Special Report." 11. NETSCOUT Arbor. http://www.icir.org/vern/cs261n/papers/Arbor-WISR2016.pdf.

Aon. 2018. "Aon-Pentland-Analytics-Reputation-Report-2018-07-18.Pdf." 2018. https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf?utm_source=aoncom&utm_medium=storypage&utm_campaign=reprisk2018.

A.P. Moller – Maersk. 2017. "A.P._Moller_-_Maersk_Annual_Report_2017.Pdf." 2017. http://files.shareholder.com/downloads/ABEA-3GG91Y/6115885668x0x971046/54DA7595-1904-4118-9174-E741CB7621D4/A.P._Moller_-_Maersk_Annual_Report_2017.pdf.

Arghire, Ionut. 2018. "Microsoft Uncovers Multi-Tier Supply Chain Attack." Security Week. July 27, 2018. https://www.securityweek.com/microsoft-uncovers-multi-tier-supply-chain-attack.

Armor. 2018. "The Black Market Report: A Look Inside the Dark Web." https://cdn.armor.com/app/uploads/2018/03/27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf.

August 15, Dan Patterson |, Dan Patterson, and 7:48 Am Pst. 2018. "Why Hacking Industrial Control Systems Is an Extension of Statecraft." TechRepublic. August 15, 2018. https://www.techrepublic.com/article/why-hacking-industrial-control-systems-is-an-extension-of-statecraft/.

BBC. 2015. "Web Attack Knocks BBC Websites Offline." BBC. December 31, 2015. https://www.bbc.co.uk/news/technology-35204915.

———. 2018. "Ticketmaster Admits Hack Attack." BBC News, June 27, 2018, sec. Technology. https://www.bbc.com/news/technology-44628874.

Bienkowski, Tom. 2018. "No Sooner Did the Ink Dry: 1.7Tbps DDoS Attack Makes History." NETSCOUT Arbor. https://www.netscout.com/news/blog/security-17tbps-ddos-attack-makes-history.

Bird, jane. 2018. "AI Is Not a 'Silver Bullet' against Cyber Attacks | Financial Times." September 26, 2018. https://www.ft.com/content/14cd2608-869d-11e8-9199-c2a4754b5a0e.

Bisson, David. 2018. "The 10 Biggest Data Breaches of 2018… So Far." Barkly. July 2018. https://blog.barkly.com/biggest-data-breaches-2018-so-far.

Blakemore, Erin. 2018. "Inside the Rise and Fall of Toys 'R' Us." HISTORY. March 19, 2018. https://www.history.com/news/toys-r-us-closing-legacy.

Blinder, Alan, and Nicole Perlroth. 2018. "A Cyberattack Hobbles Atlanta, and Security Experts Shudder." The New York Times, September 26, 2018, sec. U.S. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

Bond, David. 2018. "Seven UK Banks Targeted by Coordinated Cyber Attack," April 25, 2018.

Bouveret, Antoine. 2018. "IMF.Pdf." IMF.

Brandom, Russell. 2018. "Facebook and Google Hit with $8.8 Billion in Lawsuits on Day One of GDPR." The Verge. May 25, 2018. https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe.

Brian Duckering. 2017. "Mobile Threat Intelligence Report – 2016 in Review." Symantec Offical Blog. March 23, 2017. http://www.symantec.com/connect/blogs/mobile-threat-intelligence-report-2016-review.

Brown, Nick. 2018. "Puerto Rico Power Utility Hacked but Customer Data Not at Risk." Reuters, March 19, 2018. https://uk.reuters.com/article/us-usa-puertorico-cyberattack/puerto-rico-power-utility-hacked-but-customer-data-not-at-risk-idUKKBN1GV30A.

Budd, Christopher. 2018. "Don't Panic About Software Supply Chain Attacks." Research Center, Palo Alto Networks. July 21, 2018. https://researchcenter.paloaltonetworks.com/2018/06/unit42-dont-panic-software-supply-chain-attacks/.

Business Sweden. n.d. "Understanding the Cloud: It's Child's Play." Data Centers by Sweden. Accessed October 12, 2018. https://www.business-sweden.se/en/Invest/industries/Data-Centers-By-Sweden/news-and-downloads/investment-news/understanding-the-cloud-its-childs-play/.

Butler, Nick. 2018. "Why Cyber Attack Is the Biggest Risk for Energy Companies." Financial Times. October 8, 2018. https://www.ft.com/content/109350ea-c6f2-11e8-ba8f-ee390057b8c9.

Caltagirone, Sergio. 2018. "The Current Industrial Threat Landscape: Reality Above Theory." February 5, 2018. https://dragos.com/blog/20180502ThreatLandscape.html.

Candid Wueest. 2017. "Attackers Are Increasingly Living off the Land." Symantec Security Response. July 12, 2017. http://www.symantec.com/connect/blogs/attackers-are-increasingly-living-land.

Carr, Austin. 2010. "Blockbuster Bankruptcy: A Decade of Decline." Fast Company. September 2, 2010. https://www.fastcompany.com/1690654/blockbuster-bankruptcy-decade-decline.

Chalfant, Morgan. 2018. "Georgia Governor Vetoes Controversial Hacking Legislation." Text. TheHill. May 8, 2018. https://thehill.com/policy/cybersecurity/386770-georgia-governor-vetoes-controversial-hacking-legislation.

Chapman, Sophie. 2018. "Manufacturing Accounted for 46% of All UK Cyber-Attacks in 2017." Manufacturing Global. May 4, 2018. https://www.manufacturingglobal.com/technology/manufacturing-accounted-46-all-uk-cyber-attacks-2017.

Chong, Celena. 2015. "Blockbuster's CEO Once Passed up a Chance to Buy Netflix for Only $50 Million." Business Insider UK. July 17, 2015. http://uk.businessinsider.com/blockbuster-ceo-passed-up-chance-to-buy-netflix-for-50-million-2015-7.

Cisco. 2017. "The Zettabyte Era: Trends and Analysis." Cisco. June 7, 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

———. 2018a. "Annual Cyber Security Report." Cisco.

———. 2018b. "Annual Cybersecurity Report." Cisco. https://www.cisco.com/c/en_uk/products/security/security-reports.html.

CloudFlare. n.d. "Low and Slow Attack." CloudFlare. Accessed October 30, 2018. https://www.cloudflare.com/learning/ddos/ddos-low-and-slow-attack/.

CNIL. 2018. "Data Protection around the World." CNIL. 2018. https://www.cnil.fr/en/data-protection-around-theworld.

C.N.N. Library. 2018. "2016 Presidential Campaign Hacking Fast Facts." CNN. November 24, 2018. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Coburn, A., Leverett, E., Woo, G. 2019. Solving Cyber Risk: Protecting Your Company and Society. Wiley.

Connor, Fred o'. 2017. "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue." Cybereason. https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue.

Corero Network Security, Inc. 2018. "CORERO | Half Year 2018 DDoS Trends Report." Corero Network Security, Inc. http://info.corero.com/rs/258-JCF-941/images/H1-2018-Corero-Trends-Report-Final.pdf.

CPNI. 2018. "Critical National Infrastructure | CPNI | Public Website." 2018. https://www.cpni.gov.uk/critical-national-infrastructure-0.

CyberGRX. 2018. "Top 11 Third-Party Breaches of 2018 (So Far) - Data Breach Report." CyberGRX. June 7, 2018. https://www.cybergrx.com/resources/blog/top-11-third-party-breaches-of-2018-so-far-data-breach-report/.

Cyberreason Intel Team. 2017. "Russia and Nation-State Hacking Tactics: A Report from Cybereason Intelligence Group." Cybereason. June 5, 2017. https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity.

"CYBER_STRATEGY_SUMMARY_FINAL.Pdf." n.d. Accessed October 4, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Daley, William. 2018. "Will Insurance Provide Coverage for GDPR Fines?" JDSupra. October 1, 2018. https://www.jdsupra.com/legalnews/will-insurance-provide-coverage-for-84803/.

Davey, Gavin. 2016. "Analysis of RSA Lockheed Martin Attack." Slideshare. January 21, 2016. https://www.slideshare.net/GavinDavey2/analysis-of-rsa-lockheed-martin-attack.

DeNisco Rayome, Alison, 2018, and 6:27 Am Pst. 2018. "51% of Companies Publicly Exposed Cloud Storage Services in the Past Year." TechRepublic. May 15, 2018. https://www.techrepublic.com/article/51-of-companies-publicly-exposed-cloud-storage-services-in-the-past-year/.

Department of Justice. 2018. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Deshmukh, Rashmi V, and Kailas K Devadkar. 2015. "Understanding DDoS Attack & Its Effect in Cloud Environment." Procedia Computer Science 49: 202–10. https://doi.org/10.1016/j.procs.2015.04.245.

DLA Piper. n.d. "Global Data Protection Laws in the World." DLA Piper. Accessed August 22, 2018. https://www.dlapiperdataprotection.com/.

DOJ. 2018. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Dorfman, Zach. 2018. "How Silicon Valley Became a Den of Spies." POLITICO Magazine. July 27, 2018. https://politi.co/2vakzPL.

Dragos. 2017. "TRISIS-01.Pdf." 2017. https://dragos.com/blog/trisis/TRISIS-01.pdf.

Eenheid, Landelijke. 2018. "Operation Power Off – Police close down largest DDoS website." April 25, 2018. https://www.politie.nl/nieuws/2018/april/25/operation-power-off-%E2%80%93-police-close-down-largest-ddos-website.html.

Emily Vuitton. 2017. "Ecommerce Payment Fraud Outlook 2017-2020." Chargeback. March 21, 2017. https://chargeback.com/ecommerce-payment-fraud-outlook-2020/.

Erez, Noam. 2018. "Cyber Attacks Are Shutting down Countries, Cities and Companies. Here's How to Stop Them." World Economic Forum. June 22, 2018. https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/.

ESET. 2018. "Cyber Security Trends 2018: The Cost of Our Connected World." ESET. https://www.welivesecurity.com/wp-content/uploads/2017/12/ESET_Trends_Report_2018.pdf.

Europol. 2018a. "Internet Organised Crime Threat Assessment (IOCTA) 2018." Europol. 2018. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

———. 2018b. "World's Biggest Marketplace Selling Internet Paralysing DDoS Attacks Taken down." Europol. April 25, 2018. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down.

Europol Cybercrime Centre. 2018. "Internet Organised Crime Threat Assessment." Europol.

FedEX. 2018. "060402fa-5206-4f28-9bcc-F815ba4e0fd0.Pdf." August 31, 2018. http://d18rn0p25nwr6d.cloudfront.net/CIK-0001048911/060402fa-5206-4f28-9bcc-f815ba4e0fd0.pdf.

Finextra. 2018. "89% of Swift Member Banks Meet Security Deadline." Finextra Research. January 26, 2018. https://www.finextra.com/pressarticle/72346/89-of-swift-member-banks-meet-security-deadline.

FireEye Intelligence. 2018. "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers « TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers." FireEye. October 23, 2018. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html.

Forest, Conner. 2018. "Leaked FedEx Customer Data Was Stored on Amazon S3 Server with No Password." TechRepublic. February 15, 2018. https://www.techrepublic.com/article/leaked-fedex-customer-data-was-stored-on-amazon-s3-server-with-no-password/.

Gallin Luke. 2017. "Total WannaCry Losses Pegged at $4 Billion - Reinsurance News." ReinsuranceNews (blog). September 25, 2017. https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/.

Gallin, Luke. 2018. "Silent Cyber Drives Petya Loss to $2.7 Billion, Says PCS - Reinsurance News." ReinsuranceNe.Ws (blog). May 23, 2018. https://www.reinsurancene.ws/silent-cyber-drives-petya-loss-to-2-7-billion-says-pcs/.

Gandhi, Prashant, Somesh Khanna, and Sree Ramaswamy. 2016. "Which Industries Are the Most Digital (and Why)?" Harvard Business Review. https://hbr.org/2016/04/a-chart-that-shows-which-industries-are-the-most-digital-and-why#comment-section.

Gartner. 2017. "Leading the IoT: Gartner Insights on How to Lead in a Connected World." Gartner, Inc.

———. 2018. "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019." August 15, 2018. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

Giles, Martin. 2017. "The Worst Idea in Cybersecurity Refuses to Die." MIT Technology Review. January 12, 2017. https://www.technologyreview.com/s/609555/hacking-back-makes-a-comeback-but-its-still-a-really-bad-idea/.

———. 2018. "AI for Cybersecurity Is a Hot New Thing—and a Dangerous Gamble." MIT Technology Review. November 8, 2018. https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hayes, Julian, and Harvey Briggs. 2018. "Doing unto Others…the Law and Efficacy of Hacking Back." BCL Solicitors LLP (blog). May 15, 2018. http://www.bcl.com/doing-unto-othersthe-law-and-efficacy-of-hacking-back/.

HCSEC. 2018. "20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.Pdf." 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

Hedrich, Wolfram, Gerald Wong, and Jaclyn Yeo. 2017. "Cyber Risk in Asia-Pacific: The Case for Greater Transparency." Marsh & McLennan. http://www.mmc.com/content/dam/mmc-web/Files/APRC/aprc-cyber-risk-in-asia-pacific.pdf.

Heer, Carsten. 2018. "Industrial Robot Sales Increase Worldwide by 31 Percent." International Federation of Robotics. June 20, 2018. https://ifr.org/ifr-press-releases/news/industrial-robot-sales-increase-worldwide-by-29-percent.

Higgins, Kelly. 2018. "Unpatched Vulnerabilities the Source of Most Data Breaches." Dark Reading. April 5, 2018. https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465.

Higgins, Kelly Jackson. 2013. "How Lockheed Martin's 'Kill Chain' Stopped SecurID Attack." Dark Reading. December 2, 2013. https://www.darkreading.com/attacks-breaches/how-lockheed-martins-kill-chain-stopped-securid-attack/d/d-id/1139125.

Hoffman, Stefanie. 2011. "RSA SecureID Breach Costs EMC $66 Million." CRN. July 28, 2011. https://www.crn.com/news/security/231002862/rsa-secureid-breach-costs-emc-66-million.htm.

Hudson, Andrew. 2012. "The Rise and Fall of Kodak." PhotoSecrets (blog). August 29, 2012. https://www.photosecrets.com/the-rise-and-fall-of-kodak.

Ian Thomson. 2017. "Hackers Nick $60m from Taiwanese Bank in Tailored SWIFT Attack." October 11, 2017. https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/.

Information Commissioner's Office. 2018. "Heathrow Airport." Information Commissioner's Office. https://ico.org.uk/action-weve-taken/enforcement/heathrow-airport/.

Insurance Journal. 2018. "GDPR Insurance: Coverage for Fines Hard to Find But Other Non-Compliance Costs Insurable." Insurance Journal. May 16, 2018. https://www.insurancejournal.com/news/international/2018/05/16/489339.htm.

Insurance Times. 2018. "Ransomware Attacks Make up Quarter of AIG Cyber Claims." Insurance Times. May 30, 2018. https://www.insurancetimes.co.uk/ransomware-attacks-make-up-quarter-of-aig-cyber-claims/1427272.article.

Isaac, Mike, and Sheera Frenkel. 2018. "Facebook Security Breach Exposes Accounts of 50 Million Users." The New York Times, September 28, 2018, sec. Technology. https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

Jeremy Kirk. 2018. "Banco de Chile Loses $10 Million in SWIFT-Related Attack." Bank Info Security. June 13, 2018. https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075.

Jim Daly. 2019. "Nearly Two-Thirds of Global POS Card Transactions Now Involve EMV Chip Cards and Terminals." Digital Transactions (blog). April 19, 2019. https://www.digitaltransactions.net/nearly-two-thirds-of-global-pos-card-transactions-now-involve-emv-chip-cards-and-terminals/.

JLT. 2018. "Global Malware Attacks One Year on | Cyber Decoder | JLT Specialty." June 17, 2018. http://www.jltspecialty.com/our-insights/publications/cyber-decoder/global-malware-attacks-one-year-on.

John McCrank, and Jim Finkle. 2018. "Equifax Breach Could Be Most Costly in Corporate History." Reuters, March 2, 2018. https://uk.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUKKCN1GE257.

Johnson, Blake, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Glyer. 2017. "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure « Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure." FireEye. December 14, 2017. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

Jonnie Emsley. 2018. "Blockchain and Cryptocurrency: Japan's Economic Elixir?" CryptoSlate (blog). July 2, 2018. https://cryptoslate.com/blockchain-cryptocurrency-japans-economic-elixir/.

Joshua Hammer. 2018. "The Billion-Dollar Bank Job." The New York Times, May 3, 2018, sec. Magazine. https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html, https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.

Jyotsana. 2018. "2018 CSP Comparison - MS Azure vs AWS vs IBM vs Google." ZNetLive Blog - A Guide to Domains, Web Hosting

& Cloud Computing. February 20, 2018. https://www.znetlive.com/blog/comparing-top-4-public-cloud-providers-in-2018-microsoft-azure-vs-aws-vs-ibm-vs-google/.

Kamp, Jon, and Scott Calvert. 2018. "Ransom Demands and Frozen Computers: Hackers Hit Towns Across the U.S." Wall Street Journal, June 24, 2018, sec. US. https://www.wsj.com/articles/ransom-demands-and-frozen-computers-hackers-hit-towns-across-the-u-s-1529838001.

Kaplan, Macia. 2018. "Amazon's 2018 Prime Day Sets Record Despite Glitches." Practical Ecommerce (blog). July 19, 2018. https://www.practicalecommerce.com/amazons-2018-prime-day-sets-record-despite-glitches.

Kaspersky. 2015. "Collateral Damage: 26% of DDoS Attacks Lead to Data Loss." Kaspersky. September 17, 2015. https://www.kaspersky.com/about/press-releases/2015_collateral-damage-26-of-ddos-attacks-lead-to-data-loss.

———. 2018. "More than 40% of ICS Computers Were Attacked in H1 2018 | Kaspersky Lab." June 9, 2018. https://www.kaspersky.com/about/press-releases/2018_ics-computers-attacked-in-h1.

Kaspersky Lab. 2018a. "IT Threat Evolution Q2 2018. Statistics." Securelist - Kaspersky Lab's Cyberthreat Research and Reports (blog). 2018. https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/.

———. 2018b. "Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies." June 7, 2018. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html.

Kelly Sheridan. 2018. "Fileless Attacks Jump 94% in First Half of 2018." Dark Reading. August 28, 2018. https://www.darkreading.com/endpoint/fileless-attacks-jump-94--in-first-half-of-2018/d/d-id/1332686.

Kevin Helms. 2018. "Big-Name Insurers Stepping Up Their Crypto Game." Bitcoin News. July 21, 2018. https://news.bitcoin.com/insurers-crypto/.

Kevin Kelleher. 2018. "Facebook Loses Around $13 Billion in Value After Data Breach Affects 50 Million of Its Users." Fortune. September 28, 2018. http://fortune.com/2018/09/28/facebook-stock-falls-after-security-breach/.

Knake, Robert K. 2018. "Instead of Hacking Back, U.S. Companies Should Let Cyber Command Do It for Them." Council on Foreign Relations. May 30, 2018. https://www.cfr.org/blog/instead-hacking-back-us-companies-should-let-cyber-command-do-it-them.

Kohout, Jiri. n.d. "How DDoS Attacks Can Sink Your Business." TeskaLabs. Accessed October 30, 2018. https://www.teskalabs.com/blog/how-ddos-can-sink-your-business.

Kuchler, Hannah. 2018. "Microsoft Alleges New Russia Hack Targeting US Political Groups." Financial Times. August 21, 2018. https://www.ft.com/content/0ef4d264-a4c8-11e8-8ecf-a7ae1beff35b.

Larry Ponemon. 2018. "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT." Security Intelligence (blog). July 11, 2018. https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/.

Larson, Dan. 2018. "Global Survey Reveals Supply Chain as a Rising and Critical New Threat Vector." Crowd Strike. July 23, 2018. https://www.crowdstrike.com/blog/global-survey-reveals-supply-chain-as-a-rising-and-critical-new-threat-vector/.

Lavrentieva, Tatiana. 2017. "How to Slay the Dragon of Cloud SLA's." Cloud Technology Partners (blog). July 26, 2017. https://www.cloudtp.com/doppler/slaying-the-dragon-of-cloud-slas/.

Lewis, James Andrew. 2018. "How Much Have the Chinese Actually Taken?" March 22, 2018. https://www.csis.org/analysis/how-much-have-chinese-actually-taken.

LexisNexis. 2018. "LexisNexis Risk Solutions 2018 True Cost of Fraud Study -- Retail Edition Pdf.Pdf."

Lloyd's, and AIR. 2018. "Cloud Down: Impacts on the US Economy."

Lunden, Ingrid, and Josh Constine. 2018. "Slack Is Raising $400M+ with a Post-Money Valuation of $7B or More." TechCrunch (blog). August 2018. http://social.techcrunch.com/2018/08/07/slack-raising/.

Lynley, Matthew. 2017. "Pinterest Raises $150M at a $12.3B Valuation as It Makes a Full Press into Visual Search." TechCrunch (blog). November 2017. http://social.techcrunch.com/2017/06/06/pinterest-raises-150m-at-a-12-3b-valuation-as-it-makes-a-full-press-into-visual-search/.

Mackie, Kurt. 2018. "Microsoft Cloud Services Stumble After Outage Hits Texas Datacenter -." Redmond Channel Partner. September 4, 2018. https://rcpmag.com/articles/2018/09/04/microsoft-cloud-outage-datacenter.aspx.

Mackie, Kurt, and 2018. 2018. "Microsoft's Cloud Outage Postmortem: What Went Wrong in Texas -." Redmond Channel Partner. September 11, 2018. https://rcpmag.com/articles/2018/09/11/microsoft-cloud-outage-postmortem.aspx.

Malhotra, Ashish. 2018. "The World's Largest Biometric ID System Keeps Getting Hacked." Motherboard (blog). January 8, 2018. https://motherboard.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system.

Malik, Naureen S, and Meenal Vamburkar. 2018. "Cyberattack Pings Data Systems of At Least Four Gas Networks." Bloomberg. April 3, 2018. https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts.

Mandiant. 2018. "Mtrends-2018.Pdf."

Manyika, James, and Charles Roxburgh. 2011. "The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity | McKinsey." 2011. https://www.mckinsey.com/industries/high-tech/our-insights/the-great-transformer.

Matthew Schwartz. 2018. "Under GDPR, Data Breach Reports in UK Have Quadrupled." Bank Info Security. July 25, 2018. https://www.bankinfosecurity.com/under-gdpr-data-breach-reports-in-uk-have-quadrupled-a-11249.

Maurer, Tim. 2018. Cyber Mercenaries: The State, Hackers, and Power. 1st ed. Cambridge University Press. https://doi.org/10.1017/9781316422724.

Mazzoni, Mary. 2018. "What New U.S. Data Privacy Laws Mean for Business." Triple Pundit. October 18, 2018. https://www.triplepundit.com/special/data-privacy-symantec-series-2018/what-new-u-s-data-privacy-laws-mean-for-business/.

McCormick, Emily. 2018. "Instagram Is Estimated to Be Worth More than $100 Billion." Bloomberg. June 25, 2018. https://www.bloomberg.com/news/articles/2018-06-25/value-of-facebook-s-instagram-estimated-to-top-100-billion.

Merck. 2018. "Merck & Co SEC 10-K." February 27, 2018. https://www.sec.gov/Archives/edgar/data/310158/000031015818000005/mrk1231201710k.htm.

Michael O'Boyle. 2018. "Mexico Central Bank Says Hackers Siphoned $15 Million from Five..." Reuters, May 17, 2018. https://www.reuters.com/article/us-mexico-cyber/mexico-central-bank-says-hackers-siphoned-15-million-from-five-companies-idUSKCN1IH38Q.

Miller, Steve, and Evan Reese. 2018. "A Totally Tubular Treatise on TRITON and TriStation « A Totally Tubular Treatise on TRITON and TriStation." FireEye. July 6, 2018. https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html.

Mills, Chris. 2018. "Tesla Sues Former Employee for Hacking Production Lines, Stealing Data, and Lying to the Press." BGR Media. June 20, 2018. https://bgr.com/2018/06/20/tesla-factory-production-sabotaged-lawsuit/.

Ministry of Electronics & Information Technology – Government of India. 2018. "The Personal Data Protection Bill, 2018." Ministry of Electronics & Information Technology – Government of India. http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

Mondelez International. 2017. "Files-Api.Pdf." December 31, 2017. https://ir.mondelezinternational.com/system/files-api?file=migration/secfilings/0001193125-18-037332/pdf.pdf&file_alias=36196&CIK=1103982&filingID=1193125-18-37332.

NAIC. 2017. "Niac-Cyber-Study-Draft-Report-08-15-17-508.Pdf." August 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

Nash, Kim S., Sara Castellanos, and Adam Janofsky. 2018. "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs." Wall Street Journal, June 27, 2018, sec. Pro Cyber. https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

National Audit Office. 2018. "Investigation-WannaCry-Cyber-Attack-and-the-NHS.Pdf." 2018. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

National Telecommunications and Information Administration. 2016. "Initial Estimates Show Digital Economy Accounted for 6.5 Percent of GDP in 2016." 2016. https://www.ntia.doc.gov/blog/2018/initial-estimates-show-digital-economy-accounted-65-percent-gdp-2016.

NBC News. 2006. "The Day Music Died? No, but Tower Records Is." NBC NEws. October 16, 2006. http://www.nbcnews.com/id/15251144/ns/business-us_business/t/day-music-died-no-tower-records/.

n'cloud. 2017. "The Cloud Market Revenue Doubles in the next 3 Years up to 162 Billion in USD." 2017. https://www.ncloud.swiss/en/ico/market/.

NCSC. 2018a. "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack - NCSC Site." February 15, 2018. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

———. 2018b. "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack - NCSC Site." February 15, 2018. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

———. 2018c. "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed - NCSC Site." April 10, 2018. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

NCSC CSAN. 2018. "Cyber_security_assessment_netherlands_2018.Pdf."

NCSC US. 2018. "20180724-Economic-Espionage-Pub.Pdf." 2018. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

NCSC (US). 2018. "20180724-Economic-Espionage-Pub.Pdf." 2018. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

Netcraft. 2018. "Web Server Survey | Netcraft." Netcraft. 2018. https://news.netcraft.com/archives/category/web-server-survey/.

Newman, Lily Hay. 2018a. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare." Wired, April 24, 2018. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

———. 2018b. "Russia Has Been Linked to Malware That Targets Industrial Equipment." Wired, October 23, 2018. https://www.wired.com/story/triton-malware-russia-industrial-controls/.

Nicolas Christin. 2018. "After the Breach: The Monetization and Illicit Use of Stolen Data." Subcommittee on Terrorism & Illicit Finance. https://www.andrew.cmu.edu/user/nicolasc/publications/20180315-testimony-christin.pdf.

Northcutt, Stephen. n.d. "The Attack Surface Problem." SANS Technology Institute. Accessed October 9, 2018. https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface.

Osborn, Joshua. 2018. "Seven Effects of DDoS Attacks on Cloud Environments." Compare the Cloud. May 2, 2018. https://www.comparethecloud.net/articles/seven-effects-ddos-attacks-cloud/?cn-reloaded=1.

Page, Vanessa. 2018. "How WhatsApp Makes Money." Investopedia. May 1, 2018. https://www.investopedia.com/articles/personal-finance/040915/how-whatsapp-makes-money.asp.

Palmer, Danny. 2018. "What Is Ransomware? Everything You Need to Know about One of the Biggest Menaces on the Web." ZDNet. August 22, 2018. https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/.

Patton, Steve. 2018. "Counting the Cost of DDoS Attacks." Telesoft. August 29, 2018. https://www.telesoft-technologies.com/blog/item/counting-the-cost-of-ddos-attacks.

Paul Koetsier, and Ton Diemontt. 2018. "The Impact of SWIFT Security Requirements." KPMG. September 28, 2018. https://home.kpmg.com/nl/nl/home/insights/2018/09/the-impact-of-swift-security-requirements-on-the-banking-community.html.

PCS, 4. 2018. "PCS: NotPetya Insured Losses Now $3bn+." Re-Insurance. September 2018. https://www.re-insurance.com/news/pcs-notpetya-insured-losses-now-3bn/1627.article.

Perlroth, Nicole. 2018. "Boeing Possibly Hit by 'WannaCry' Malware Attack - The New York Times." March 28, 2018. https://www.nytimes.com/2018/03/28/technology/boeing-wannacry-malware.html.

Pierluigi Paganini. 2018. "Crooks Used a KilllDisk Wiper in an Attack against Banco de Chile as Diversion for a SWIFT Hack." Security Affairs. June 10, 2018. https://securityaffairs.co/wordpress/73372/cyber-crime/banco-de-chile-killdisk.html.

Ponemon. 2016. "Cost of Data Center Outages." Data Center Perfomance Benchmark Series. Ponemon.

———. 2018. "IBM Security Services – The 2018 Cost of a Data Breach Study by the Ponemon Institute." July 11, 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&.

Privacy International. 2018. "State of Privacy." January 2018. 2018. https://privacyinternational.org/type-resource/ state-privacy.

Quarta, Davide, Marcello Pogliani, Mario Polino, Andrea. M Zanchettin, Stefano Zanero, and Federico Maggi. 2017. "Rogue Robots: Testing the Limits of an Industrial Robot's Security." Trend Micro and Politecnico di Milano. https://c-5uwzmx78pmca09x24lwkcumvbax2ebzmvluqkzwx2ekwu.g00.cnet.com/g00/3_c-5eee.kvmb.kwu_/c-5UWZMXPMCA09x24pbbx78ax3ax2fx2flwkcumvba.bzmvluqkzw.kwux2fiaambax2fex78x2fex78-qvlcabzqit-zwjwb-amkczqbg.x78ln_$/$/$/$?i10c.ua=1&i10c.dv=14.

Ray, Joshua, Howard Marshall, Rob Coderre, Emily Cody, and Jayson Jean. 2018. "Cyber Threatscape Report 2018 | Midyear Cybersecurity Risk Review." Accenture. https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report-2018.

Reinsurance. 2018. "PCS: NotPetya Insured Losses Now $3bn+." Re-Insurance. September 4, 2018. https://www.re-insurance.com/news/pcs-notpetya-insured-losses-now-3bn/1627.article.

Reo, Joy. 2017. "Theft and DDoS Attacks Go Hand in Hand." Corero. October 17, 2017. https://www.corero.com/blog/846-theft-and-ddos-attacks-go-hand-in-hand.html.

Reuters. 2017. "Best Buy Stops Sale of Russia-Based Kaspersky Products." Reuters, September 8, 2017. https://uk.reuters.com/article/us-usa-kasperskylab-best-buy-idUKKCN1BJ2M4.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." Journal of Strategic Studies 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Rightscale. 2018. "Rightscale 2018 State of the Cloud Report." Rightscale. https://assets.rightscale.com/uploads/pdfs/RightScale-2018-State-of-the-Cloud-Report.pdf.

Roberston, Jordan, and Michael Riley. 2018. "The Big Hack: How China Used a Tiny Chip to Infiltrate Amazon and Apple." Bloomberg Businessweek. October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Robertson, Adi. 2018. "California Just Became the First State with an Internet of Things Cybersecurity Law." The Verge. September 28, 2018. https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

Rogin, Josh. 2012. "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History' – Foreign Policy." September 7, 2012. https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

Rooney, Kate. 2018. "$1.1B in Cryptocurrency Was Stolen This Year, and It Was Easy to Do." June 7, 2018. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html.

Rossignol, Joe. 2015. "What You Need to Know About IOS Malware XcodeGhost." MacRumors. September 20, 2015. https://www.macrumors.com/2015/09/20/xcodeghost-chinese-malware-faq/.

Salinas, Sara. 2018a. "Lyft Valuation Now $15.1 Billion." CNBC. June 27, 2018. https://www.cnbc.com/2018/06/27/lyft-valuation-now-reported-15-billion.html.

———. 2018b. "Toyota to Invest $500 Million in Uber at Reported Valuation of $72B." CNBC. August 27, 2018. https://www.cnbc.com/2018/08/27/toyota-to-invest-500-million-in-uber-at-a-valuation-of-72b-wsj.html.

Schechner, Sam. 2018. "Facebook Faces Potential $1.63 Billion Fine in Europe Over Data Breach." Wall Street Journal, September 30, 2018, sec. Tech. https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906.

Schick, Shane. 2017. "Insider Threats Account for Nearly 75 Percent of Security Breach Incidents." Security Intelligence (blog). August 28, 2017. https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/.

Schmidle, Nicholas. 2018. "The Digital Vigilantes Who Hack Back," April 30, 2018. https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

Schwartz, Mathew J. 2016. "DDoS Attack Slams HSBC." Bank Info Security. January 29, 2016. https://www.bankinfosecurity.com/ddos-attack-slams-hsbc-a-8835.

Shaun Nichols. 2018a. "Yar, Thar She Blows: Corp-Cash-Stealing Email Whaling Attacks Now a $12.5bn Industry." The Register. July 17, 2018. https://www.theregister.co.uk/2018/07/17/email_whaling_attacks/.

———. 2018b. "Who Needs Custom Malware? 'Govt-Backed' Gallmaker Spy Crew Uses off-the-Shelf Wares." October 10, 2018. https://www.theregister.co.uk/2018/10/10/gallmaker_hacking_group/.

Sherman, Alex. 2018. "GitHub Was Also Talking to Google about a Deal, but Went with Microsoft Instead." CNBC. June 5, 2018. https://www.cnbc.com/2018/06/05/github-interest-from-google-and-others-revenue-about-300-million.html.

Shu, Xiaokui, Ke Tian, Andrew Ciambrone, and Danfeng Yao. 2017. "Breaking the Target: An Analysis of Target Data Breach and Lessons Learned." ArXiv E-Prints, January. https://arxiv.org/pdf/1701.04940.pdf.

Sisario, Ben. 2018. "The Power of Tower Records." The New York Times. June 8, 2018. https://www.nytimes.com/2018/03/06/business/media/tower-records-music.html.

Skottler. 2018. "February 28th DDoS Incident Report." GitHub Engineering. https://githubengineering.com/ddos-incident-report/.

Solon, Olivia. 2018. "Facebook Faces $1.6bn Fine and Formal Investigation over Massive Data Breach." The Guardian, October 3, 2018, sec. Technology. https://www.theguardian.com/technology/2018/oct/03/facebook-data-breach-latest-fine-investigation.

Sophos. 2018. "SamSam-The-Almost-Six-Million-Dollar-Ransomware.Pdf." 2018. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf.

Spilotro, Tony. 2018. "Japan Sees Rising Crypto Theft, $540 Million Stolen in First Six Months of 2018." NewsBTC (blog). September 20, 2018. https://www.newsbtc.com/2018/09/20/japan-sees-rising-crypto-theft-540-million-stolen-in-first-six-months-of-2018/.

Stan Gibson. 2018. "It's Time to Evict Bad Actors 'Living off the Land.'" Symantec. August 22, 2018. https://www.symantec.com/blogs/feature-stories/its-time-evict-bad-actors-living-land.

Statista. 2017. "Number of Internet Users Worldwide 2005-2017." Statista. 2017. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

Suzanne Barlyn. 2018. "Insurers Begin to Offer Cryptocurrency Theft Cover, Tackling Risks of Growing Sector." Insurance Journal. February 1, 2018. https://www.insurancejournal.com/news/international/2018/02/01/479202.htm.

SWIFT. N.D. "Customer Security Programme (CSP)." SWIFT. N.D. https://www.swift.com/myswift/customer-security-programme-csp/security-controls.

Symantec. 2017. "Petya Ransomware Outbreak: Here's What You Need to Know." October 24, 2017. https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper.

———. 2018. "Gallmaker: New Attack Group Eschews Malware to Live off the Land." October 10, 2018. https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group.

Symantec Security Response. 2017. "What Is Living off the Land?" Symantec Blog (blog). October 3, 2017. https://medium.com/threat-intel/what-is-living-off-the-land-ca0c2e932931.

Takahiko Wada, and Chang-Ran Kim. n.d. "Hacked Tokyo Cryptocurrency Exchange to Repay Owners $425 Million." Reuters. Accessed October 22, 2018. 28 January 2018.

The Economist. 2018. "An American Ban Defangs a Nascent Chinese Chip Champion." The Economist, November 3, 2018. https://www.economist.com/business/2018/11/03/an-american-ban-defangs-a-nascent-chinese-chip-champion.

The Guardian. 2017. "Petya Cyber-Attack: Cadbury Factory Hit as Ransomware Spreads to Australian Businesses." The Guardian. June 28, 2017. https://www.theguardian.com/technology/2017/jun/28/petya-cyber-attack-cadbury-chocolate-factory-in-hobart-hit-by-ransomware.

Thomas, Daniel R., Alastair R. Beresford, and Andrew Rice. 2015. "Security Metrics for the Android Ecosystem." In Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '15, 87–98. Denver, Colorado, USA: ACM Press. https://doi.org/10.1145/2808117.2808118.

ThreatMetrix. 2018. "Q1 2018 Cybercrime Report." Global Insights from the ThreatMetrix. https://www.threatmetrix.com/info/q1-2018-cybercrime-report/.

Trend Micro. 2018a. "2018 Midyear Security Roundup: Unseen Threats, Imminent Losses," 40.

———. 2018b. "SAMSAM Ransomware Hits US Hospital, Management Pays $55K Ransom - Security News - Trend Micro USA." January 17, 2018. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/samsam-ransomware-hits-us-hospital-management-pays-55k-ransom.

Tsidulko, Joseph. 2018. "The 10 Biggest Cloud Outages Of 2018 (So Far)." CRN. August 1, 2018. https://www.crn.com/slide-shows/security/300107391/the-10-biggest-cloud-outages-of-2018-so-far.htm/11.

UK Government. 2018. "New Fines for Essential Service Operators with Poor Cyber Security." GOV.UK. August 9, 2018. https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security.

US-CERT. 2018. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors | US-CERT." March 15, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A.

USTR. 2018. "Section 301 FINAL.Pdf." March 22, 2018. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

Vasilios Hioureas. 2018. "Fileless Malware: Getting the Lowdown on This Insidious Threat." Malwarebytes Labs. August 29, 2018. https://blog.malwarebytes.com/threat-analysis/2018/08/fileless-malware-getting-the-lowdown-on-this-insidious-threat/.

Vaughan-Nichols, Steven J. 2018. "Memcached DDoS: The Biggest, Baddest Denial of Service Attacker Yet." ZDNet. March 1, 2018. https://www.zdnet.com/article/memcached-ddos-the-biggest-baddest-denial-of-service-attacker-yet/.

Volz, Dustin. 2017. "Trump Signs into Law U.S. Government Ban on Kaspersky Lab Software." Reuters, December 12, 2017. https://uk.reuters.com/article/us-usa-cyber-kaspersky-idUKKBN1E62V4.

Wadhwa, Anjani Soni. 2018. "The Personal Data Protection Bill, 2018 - Data Protection - India." Mondaq. November 1, 2018. http://www.mondaq.com/india/x/750792/Data+Protection+Privacy/The+Personal+Data+Protection+Bill+2018.

We Are Social. 2018. "Digital in 2018: World's Internet Users Pass the 4 Billion Mark." We Are Social. January 30, 2018. https://wearesocial.com/blog/2018/01/global-digital-report-2018.

Whalen, Kevin. 2018. "Frequency and Complexity of DDoS Attacks Is Rising." NETSCOUT Arbor. https://www.netscout.com/news/press-release/complexity-ddos-attacks.

Wheeler, Tarah. 2018. "In Cyberwar, There Are No Rules." Foreign Policy (blog). 09 2018. https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/.

White, Edward. 2018. "Apple Chip Supplier TSMC Warns of $170m Hit from Virus." Financial Times. August 6, 2018. https://www.ft.com/content/2fe5e096-9909-11e8-9702-5946bae86e6d.

Wikipeda. 2018. "Unicorn (Finance)." Wikipedia. https://en.wikipedia.org/w/index.php?title=Unicorn_(finance)&oldid=864369499.

Wikipedia. 2018a. "Personal Data Protection Bill 2018." Wikipedia. https://en.wikipedia.org/w/index.php?title=Personal_Data_Protection_Bill_2018&oldid=868543522.

———. 2018b. "Toys 'R' Us." Wikipedia. https://en.wikipedia.org/w/index.php?title=Toys_%22R%22_Us&oldid=868522838.

Wright, Rob. 2018. "Dragos' Robert Lee Discusses Latest ICS Threats, Hacking Back." SearchSecurity. May 31, 2018. https://searchsecurity.techtarget.com/news/252442219/Dragos-Robert-Lee-discusses-latest-ICS-threats-hacking-back.

Wu, Debby. 2018. "IPhone Chipmaker Blames WannaCry Variant for Plant Closures." Bloomberg. August 6, 2018. https://www.bloomberg.com/news/articles/2018-08-06/iphone-chipmaker-blames-wannacry-variant-for-plant-closures.

Wu, Kane, and Julie Zhu. 2018. "Explainer: Ant Financial's $150 Billion Valuation, and the Big Recent Bump-Up." Reuters, April 18, 2018. https://www.reuters.com/article/us-antfinancial-valuation-idUSKBN1HP1AA.

Yahoo! Finance. 2018a. "NFLX : Summary for Netflix, Inc. - Yahoo Finance." Yahoo! Finance. November 14, 2018. https://finance.yahoo.com/quote/NFLX/.

———. 2018b. "SNAP : Summary for Snap Inc. - Yahoo Finance." Yahoo! Finance. November 14, 2018. https://finance.yahoo.com/quote/SNAP/.

Yonathan Klijnsma, and Jordan Herman. 2018. "Inside and Beyond Ticketmaster: The Many Breaches of Magecart." RiskIQ. July 9, 2018. https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/.

# Acknowledgements

Report prepared by Cambridge Centre for Risk Studies, in collaboration with Risk Management Solutions, Inc.

### Report Citation

Coburn, A.W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., Harvey, T. (2019). *Cyber risk outlook*. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc.

**Risk Management Solutions, Inc.**

Dr. Andrew Coburn, *SVP, Cyber Risk Research*
Dr. Christos Mitas, *VP, Head of Cyber Risk Modeling*
Tom Harvey, *Senior Manager, Cyber Product Management*
Dave Gatey, *Senior Director, Modeling*
Russell Thomas, *Principal Modeler, Cyber Risk Modeling*
Hichem Boudali, *Senior Modeler, Cyber Risk*
Christopher Vos, *Lead Modeler, Cyber Risk*
Damini Mago, *Cyber Risk Analyst*
Gordon Woo, *Catastrophist*
Simon Arnold, *Senior Manager, Cyber Risk*
John Agorgianitis, *Senior Modeler, Cyber Risk*
EunJin Kim, *Modeler, Cyber Risk*
Ieuan George, *Modeler, Cyber Risk*
Danielle Smith, *Risk Analyst, Cyber Product Management*
Edida Rajesh, *Senior Director, Risk Modeling*
Parveen Singh, *Cyber Risk Modeler*
Vicky Suman, *Cyber Risk Modeler*

**Cambridge Centre for Risk Studies**

Dr. Jennifer Daffron, *Cyber Risk Research Lead*
Éireann Leverett, *Senior Cyber Risk Researcher*
Kelly Quantrill, *Research Assistant, Data Science*
James Bordeau, *Research Assistant, Geopolitical Risk*
Andrew Smith, *Research Assistant, Economics*
Philip Cameron, *Research Assistant, Analytics*
Jennifer Copic, *Research Associate, Insurance*
Tamara Evan, *Research Assistant, Business Intelligence*
Kayla Strong, *Risk Lead: Scenario Analytics*
Olivia Majumdar, *Editorial Assistant*
Ken Deng, *Risk Lead: Research Assistant*
Oliver Carpenter, *Risk Lead: Scenario Analytics*
Timothy Douglas, *Research Assistant*
Simon Ruffle, *Director of Research and Innovation*
Professor Daniel Ralph, *Academic Director*
Dr. Michelle Tuveson, *Executive Director*

RMS solutions help insurers, financial markets, corporations, and public agencies evaluate and manage risks throughout the world, promoting resilient societies and a sustainable global economy.

---

Risk Management Solutions, Inc.
7575 Gateway Blvd., Suite 300
Newark, CA 94560 USA
www.rms.com



Centre for
**Risk Studies**

UNIVERSITY OF
CAMBRIDGE
Judge Business School

RMS®