REPORT

McAfee

The Hidden Costs of Cybercrime

By Zhanna Malekos Smith and Eugenia Lostri
James A. Lewis, Project Director

Table of Contents

Executive Summary

Since 2018, we estimated that the cost of global cybercrime reached over $1 trillion.

We estimated the monetary loss from cybercrime at approximately $945 billion. Added to this was global spending on cybersecurity, which was expected to exceed $145 billion in 2020. Today, this is $1 trillion dollar drag on the global economy.

This is our fourth report on the cost of cybercrime. Our reports surveyed publicly available information on national losses, and, in a few cases, we used data from not-for-attribution interviews with cybersecurity officials. Our 2018 report found that cybercrime cost the global economy more than $600 billion. Our new estimate suggests a more than 50% increase in two years.

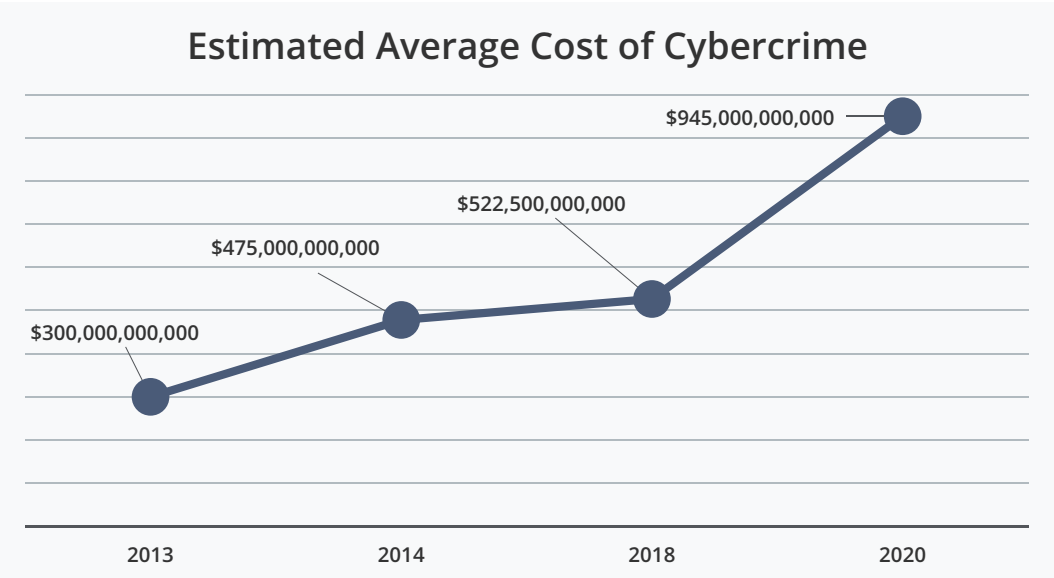

Figure 1. The average cost of cybercrime.

Acknowledgements

CSIS would like to thank Jeffrey Berwokitz, William Crumpler, Akinori Kahata, Sean Kucer, Cormac O'Harrow, Benjamin Shaver, and Duke University's Office of Information Technology STINGAR Project for their valuable research assistance.

But what accounts for this increase? This can be explained by better reporting and that, unfortunately, cybercriminals are using more effective techniques. More countries and organizations are reporting cybercrimes. In addition, ransomware and phishing-related schemes have increased dramatically, with cybercriminals "actively target[ing] organizations that include healthcare bodies, pharmaceutical companies, academia, medical research organizations, and local governments."[1]

It is no secret that cybercrime can harm public safety, undermine national security, and damage economies. What is less well known are the hidden costs that organizations may not be aware of, such as lost opportunities, wasted resources, and damaged staff morale. This report provides insights on the hidden costs of cybercrime. It aims to help decision makers in companies and governments improve their understanding of the hidden costs of cybercrime.

In researching this report, we surveyed 1,500 companies. Only 4% claimed that they did not experience any sort of cyber incident in 2019. The damage from malware and spyware represented the highest cost to organizations, closely followed by data breaches. However, 92% of respondents identified other damage besides financial costs. Affected companies said the biggest non-monetary loss was in productivity and lost work hours. The longest average interruption to operations was 18 hours, averaging more than half a million dollars.

Despite this, we found that most organizations do not have plans in place to reduce the effect of security incidents on their operations. In fact, IT decision makers think some departments are not made aware of IT security incidents. Amazingly, slightly more than half of the surveyed organization said they do not have plans to both prevent and respond to a cyber incident. Out of the 951 organizations that had a response plan, only 32% said the plan was actually effective. Usually, the board or the C-suite was not involved in developing the plans.

Only a small proportion of organizations have a plan to both prevent and respond to IT security incidents

In order to minimize the impact of such incidents, organizations must ensure they have plans in place to both prevent and respond to security incidents. Although it's comforting to see that there are very few organizations who don't have any plans in place, there is still room for improvement. Organizations in Japan are the most likely to not have plans in place for prevention, nor response, which may explain why they're also the most likely to experience the highest impact of cost (slide 15)

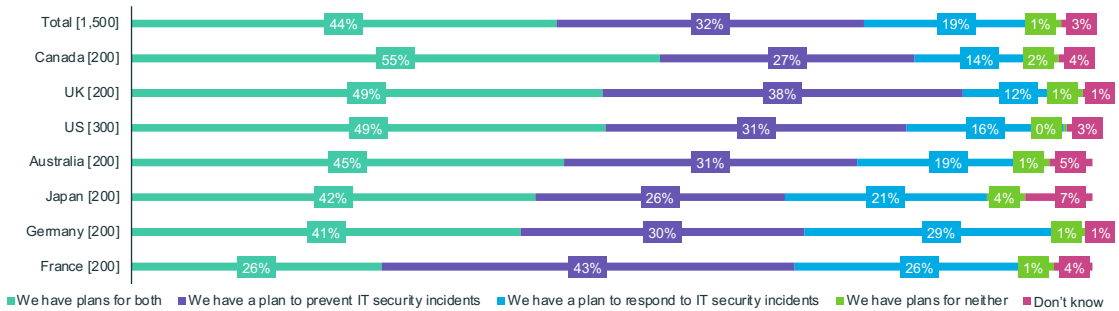

Figure 2. Proportion of organizations that have a plan to prevent and respond to IT security incidents.

One of the biggest challenges is the lack of an organization-wide understanding of cyber risk. This makes companies and agencies vulnerable to sophisticated social engineering tactics, and, once a hack has succeeded, they fail to recognize the problem in time to stop the spread of malware. The increased (and unavoidable) use of personal devices, such as smartphones or tablets, expands the attack surface and complicates the management of cybersecurity. The time and cost of recovery can be considerable and can often involve outside organizations specializing in cybersecurity, public relations, and legal teams. More improvement is needed to prevent incidents from occurring, in addition to helping restore service, operations, and morale, and any damage to the brand.

The reality of cybersecurity is that we cannot eliminate risk. At best, we can manage it. Publicly available information suggests that a few firms have lost hundreds of millions of dollars and many more firms have lost tens of millions of dollars, but these losses have so far proven to be manageable. Relatively basic measures could improve performance—better cyber hygiene and, as our survey found, better planning and greater awareness among employees of the cost of cybercrime.

The Hidden Costs of Cybercrime

The Hidden Costs of Cybercrime: The Global Cost

Cybercrime appears unstoppable. There are thousands of cybercrimes every year, ranging in cost from a few hundred dollars to the millions. The risk of cybercrime to operations and profits continues to grow for many organizations. The time it takes to remedy a cyber incident can be considerable. Companies and agencies need to do more to prevent cyber incidents from occurring. And they also need to do more to speed up service restoration, address business disruptions, and repair damage to employee morale and customer trust.

Using the model developed for earlier reports, we estimate the monetary cost of cybercrime at around $945 billion, or just over 1% of global gross domestic product (GDP). This is a significant increase from our 2018 estimate of approximately $600 billion. Better reporting explains some of the increase. However, even with these qualifications, it is clear that cybercrime continues to grow rapidly. With global spending on cybersecurity expected to exceed $145 billion in 2020, cybercrime is now a $1 trillion dollar drag on the global economy.

Cybercrime is increasing because it pays, it can be easy, and the risk to cybercriminals can be low. Although cyber law enforcement has also improved, the most sophisticated cybercriminals usually escape arrest prosecution and jail time. Cybercrime is also increasing because we rely on cyberspace to conduct our daily lives and business. Faster adoption of new technologies by cybercriminals—artificial intelligence (AI), synthetically generated images like deep fakes, and more—gives them an edge and explains some of this increase. The bottom line is that cybercrime is safe and profitable, occurs in an environment that is constantly expanding, and thrives in vulnerable systems.

The most expensive forms of cybercrime are economic espionage, the theft of intellectual property, financial crime and, increasingly, ransomware. These account for the greatest losses. We estimate that intellectual property (IP) theft and financial crime account for two thirds of monetary losses and pose the greatest threat to companies. These are accompanied by a range of crimes against consumers and smaller enterprises

that usually do not involve major losses but can affect thousands of individuals. However, hidden behind the headline figure are other, less obvious costs that are paid by companies and consumers in a variety of different ways. These other hidden costs, beyond the direct losses, are the focus of this report.

The theft of personally identifiable information (PII) and monetary assets is dramatic and damaging, but the most important cost of cybercrime may come from the damage to company performance and the aggregate damage to national economies. Our sources include the results of a survey of 1,500 executives from around the world, published data, interviews, and estimates by government agencies and companies in other countries.

Two thirds of the companies surveyed experienced some kind of cyber incident in 2019. The average interruption to operations was 18 hours. The average cost for their most expensive incident was more than half a million dollars. Almost all affected companies said the costs went beyond the monetary loss—the biggest non-monetary loss was in productivity and lost work hours. Amazingly, slightly more than half of the surveyed organization said they do not have a plan to prevent and respond to a cyber incident.

We found a lack of organization-wide understanding of cyber risk. This makes companies and agencies vulnerable to sophisticated social engineering tactics and, once a user is hacked, not organizations are unable to recognize the problem in time to stop the spread of malware. The increased (and unavoidable) use of personal devices such as smartphones or tablets expands the attack surface and endpoints for attack and complicate management of cyberdefense.

Costs Other Than Cash

Cybercrime has many hidden costs—from opportunity costs, time and money spent on cybersecurity decision-making, the effect of downtime, loss of productivity, and damage to brand and image. Most of these costs do not have an easily assigned dollar value, but we must consider them in assessing the effect of cybercrime.

Opportunity costs

Opportunity cost is the income (or production) lost when a resource cannot be used, or a service not provided, because of a cyber incident. We found that opportunity costs, such as lost sales, reduced efficiency, and the overall disruption of usual business, make up a large proportion of the indirect effects. A calculation of the cost of cybercrime needs to consider opportunity costs, such as forgone opportunities or lost benefits that would otherwise have been obtainable for activities in cyberspace. Additional spending on cybersecurity that would not be required in a more secure environment is one example. Others include lost sales, lower productivity, or a decision to avoid or limit internet use for some activities because of the risk.

We have identified four kinds of opportunity costs: lower productivity, reduced research and development (R&D) spending, risk-averse behavior, and increased spending on cyberdefenses.[2] The latter is still a common reaction

to suffering an IT security incident. Of the 1,332 survey respondents who experienced such an incident in 2019, 45% invested in new security software. Thirty-nine percent increased the budget for security incidents. And 30% hired new IT security staff. Companies pay a "risk premium" because of increased cybercrime. We can estimate the cost of this risk premium by looking at the rate of growth in the cybersecurity market. In 2019, the global cybersecurity market was worth around $145 billion, up from $113 billion in 2015.[3]

Organizations need to consider not only direct losses, but also need to add up the costs from business disruption, downtime, and lost opportunities. Cybercrime can lead to risk-averse behavior by both organizations and individuals. Being the victim of cybercrime is a traumatic experience, given the concerns over the exposure of personal information or the financial impact.[4] Aside from leaving victims annoyed, angry, or even ashamed, cybercrime may also lead to a decrease in online engagement.[5]

Moving online is increasingly unavoidable, particularly during the COVID-19 lockdowns. In the past, survey data showed that privacy and security concerns kept some households from engaging in online activity. While the reluctance to engage online has decreased, there has been a corresponding increase in public concern over privacy in many countries. The risk to privacy does not always stem directly from cybercrime, but high-profile breaches create a pervasive sense of risk when it comes to being online.[6] Nowadays, there seems to be a widespread reassessment of the costs to privacy that online activity can create and greater awareness of the need for organizations to protect their users' data, accompanied by a growing demand for regulation. It is worth highlighting that, despite usual claims from organizations that they have suffered "highly sophisticated" attacks that were impossible to preempt, most struggle with some of the most common vulnerabilities and fail to follow the known best practices.

System downtime

Downtime is the normal result of an IT security incident—the time during which technology and systems cannot be used at their normal level of functionality. Be it ransomware preventing access to the organization's systems and data or having to be reset to counter an intrusion, removing access to technology systems greatly affects organizations. It can prevent the regular development of operations, affecting both staff and consumers. We found that downtime is a common experience for around two thirds of respondents' organizations.

The financial impact of downtime to any given department in an organization averaged $590,000. For 33% of the respondents, the cost was between $100,000 and $500,000. Not surprisingly, engineering departments experience greater losses averaging $965,000, contrasting sharply with the human resources departments, which suffered losses around $89,000. Engineering departments may experience higher costs

because of their requirements to have access to certain files and software that are integral to the day-to-day operations of the business. The cost of a hack was, on average, 10 times more for engineering departments than for human resources (HR).

Engineering departments were also offline almost twice as long as other departments. While the engineering department's longest downtime was an average of 26 hours, it was only 15 hours for HR, closer to the average of 18 hours across all departments. The cost of downtime varies depending on the department. This is true for departments such as engineering and business direction and strategy.

Longer downtime incidents were more damaging. The average cost to organizations from their longest amount of downtime in 2019 was $762,231. Unsurprisingly, the larger the organization, the higher the cost, with organizations with more than 5,000 employees reporting almost double the cost from the longest amount of downtime than those organizations with 1,000 to 2,999 employees.

Our survey showed that out of 1,500 respondents, 68% reported they had experienced downtime because of IT security incidents, usually lasting less than a day. On average, the longest downtime because of an IT security incident lasted 18 hours. Downtime exceeding more than a couple of days is unusual, with less than 1% having suffered more than seven days of downtime.

A recent IT security incident against Avon, for instance, rendered access to the company systems unusable for almost a month. Initially disclosed to the U.S. Securities and Exchange Commission on June 9,[7] the incident (its nature has not been confirmed at the time of writing) affected operations in the United Kingdom, Argentina, Brazil, Poland, and Romania.[8] The cyberattack reportedly affected Avon's backend systems—thus preventing users from placing orders[9]—forcing the website to go offline, curtailing online sales,[10] and preventing access to the systems and documents by its workers.

The latest report to the Securities and Exchange Commission (on June 26) reported that Avon had "reestablished most of its operating systems and resumed operations in most of its markets."[11] The financial impact of this event will be harder to determine, especially as it happened in the midst of the COVID-19 pandemic. For instance, Avon's quarterly report from May clarified that at the time they were "unable to estimate the long-term impact of the economic paralysis arising from efforts to curb the spread of the COVID-19 virus and the expected reduction in activity on our business, results of operations and financial condition."[12]

But even if downtime per incident does not exceed one day, repeated incidents that cause downtime amount to significant periods that organizations are not able to use their systems as expected. Freedom of information requests sent to British universities revealed that they experience almost a week of downtime per year. On average, they "suffered 18 unplanned outages a year."[13]

In March 2019, a ransomware attack hit Norsk Hydro, a Norwegian aluminum manufacturing company with operations in 40 countries. Media reports estimate the ransomware attack to have cost around $71 million.[14] Impacting the entire organization, it affected operations in several countries and limited production capacity for a significant amount of time. For instance, the Alunorte refinery in Brazil only lifted restrictions in its plant by May, running at 80% of its capacity by June.[15] Norsk Hydro announced that they had resumed normal operations only by November 2019.[16]

Reduced efficiency

Organizations lost, on average, nine work hours when experiencing downtime. For instance, the NotPetya ransomware attack temporarily shut down the Danish shipping company Maersk, which supports approximately 20% of the world's shipping needs.[17] Michael McConnell, former NSA Director and the second Director of National Intelligence, said "the damage to Maersk for recovery was on the order of three billion dollars."[18] Other major international businesses were affected, like the global delivery company FedEx, which lost approximately "$300 million after the operations of the firm's TNT Express unit in Europe were disrupted,"[19] as well as the American pharmaceutical company Merck and Russian oil company Rosneft.[20]

Unraveling the exact cost of industry disruption such as missed deliveries and re-installation of essential equipment is part of the story. The Chairman of Møller-Maersk painted a bleak picture when describing the immense scale of disruption from the ransomware attack and the difficulty in quantifying the amount of harm caused: "Imagine a company where a ship with 10 to 20 thousand containers is entering a port every 15 minutes, and for 10 days, you have no IT... It's almost impossible to even imagine."[21] Prior to NotPetya, he described Maersk's cybersecurity posture as being about average "like many companies." Now, the company seeks to "have cybersecurity as a competitive advantage."[22]

Brand damage and loss of trust

Damage to brand and reputation is a long-term consequence of IT security incidents. This is something businesses should be more concerned about preventing. Twenty-six percent of respondents identified damage to brand from the downtime experienced because of a cyberattack. The cost of rehabilitating the brand, working with media relations, or hiring new employees is part of the cost of cybercrime.

Reputation is, in large part, a matter of perception—a perception of negligence and lack of protection for data privacy that can lead customers away from a business. A 2017 study found that 87% of consumers indicated they would change suppliers if they did not trust how their data was being handled by a company.[23]

This is not exclusively a matter of preventing an incident. How an organization responds and how open and forthcoming about the situation they are can go a long way in maintaining consumer trust.[24] There has been increasing awareness by consumers of the use and

misuse of their data, and expectations regarding data protection are increasing. Transparency and informing customers when their financial or personal data may have been compromised are essential to maintain trust and manage a crisis. Only 26% of organizations that had security incidents in 2019 shared information about the most severe incident with clients or customers.

IP theft

IP theft is part of the opportunity cost to companies. IP theft can be accomplished through several means. The FBI, for instance, identifies economic espionage, clandestine efforts, and malicious foreign influence, targeting companies and universities in the United States, as typical techniques.[25] A successful incident need not always equate to direct loss if the perpetrators are unsuccessful in using the stolen IP. However, the ways in which it can affect a company are not limited to the development of competing products or services.[26] The impact on revenue streams may lead to reduced R&D efforts, paired with an increase in the cost of capital if the IP is seen by investors as not sufficiently protected.

China is central to the risk of IP theft. Former U.S. Treasury Secretary Henry M. Paulson said, "Corporate cybertheft is the most contentious and potentially destructive economic issue we face with the Chinese. It undermines our economic security, gives credence to the sense that China does not play fair, and makes it difficult to find common ground."[27] Assistant Attorney General for National Security John Demers refers to China's "rob-replicate-replace" policy, which seeks to "steal American IP, replicate the product or service in China, replace the American company on the Chinese market, and, if all goes well, on the global market."[28]

This is not just a problem for the U.S. Our survey found that IP theft was behind 11% of the security incidents that caused the longest amount of downtime. This was consistent across different regions.

A timely example of the importance of protecting against IP theft relates to espionage directed towards medical researchers during the COVID-19 pandemic, with many credible allegations that Russian and Chinese hackers targeted vaccine research.[29] These attacks illustrate the non-monetary side of cybercrime. While the economic advantage of being the first company to design a vaccine is calculable, it is harder to put a price on the political value of being the first country to produce such a vaccine.

Incident response costs

It takes an average of 19 hours for most organizations to move from the discovery of an incident to remediation. This typically entails restoring IT services back to normal capacity, removing the threat from the system, and retrieving lost data. In some cases, however, organizations will not consider an incident to be remediated until the source of the incident has been identified or some measure has been implemented to prevent the incident from reoccurring in the future. It takes up the time of eight people, on average, to detect and respond to an IT security incident.

Other hidden costs for businesses that have client data stolen involve offering victims some type of protection or compensation service, such as fraud loss reimbursement or company-sponsored access to credit monitoring and fraud alert services. For instance, after suffering two data breaches (in 2018 and 2020), the Marriott International Hotel established special call centers to respond to clients' concerns. They offered impacted customers free access to credit monitoring and fraud detection programs. The hotel chain provided customers with a one-year free service to monitor websites that are used by cybercriminals to distribute people's personal information in addition to fraud loss reimbursement.

After the 2017 Equifax data breach, which exposed the personal information of 147 million people,[30] Equifax settled the lawsuit with the Federal Trade Commission (FTC), state attorneys general, and the Consumer Financial Protection Bureau for $425 million and agreed to provide benefits to help people affected by the data breach.[31] In addition, U.S. consumers are eligible to receive seven free Equifax credit reports per year through 2026.

Outside assistance

While many cyberattacks can be managed in house, major incidents often require contracting with outside consultants at high rates, forming a significant portion of the cost of a large-scale incident. Only 213 out of 1,332 surveyed organizations reported that they dealt with cyber incidents without third-party support. Typically, they relied on cybersecurity organizations or response teams to help with containment, recovery, and remediation. Whether it was an external response team, specialized cybersecurity company, or legal and public relations assistance, most companies relied on external support. In most of these cases, consultants were used to assist in containment, recovery, and remediation, but in 22% of cases, they also provided public relations assistance.[32] Fourteen percent provided legal assistance.

Consultants: Cyberattacks range from minor attacks that are easily handled in house to major breaches that require a coordinated response involving leadership throughout the organization, lawyers, public relations specialists, and cyber experts, many of whom must be brought in as consultants. As cyberattacks have become more prevalent, so have the consultants who can help remediate a major attack or breach that would otherwise overwhelm a victim organization.

During the NotPetya attack, Maersk hired a consulting firm to help manage its response, bringing in as many as 200 outside personnel at a time to work alongside Maersk's staff.[33] Many consulting firms provide cyber services, and their cyber unit can employ thousands of people, which gives some indication of the size of the market.[34] Consultancies continue to expand to meet demand for their services, with the shortage of qualified experts driving daily rates per consultant into the thousands of dollars.[35] While precise sums are difficult to come by, fees paid to consulting firms are likely to be a significant component of the overall cost of responding to a major incident. In the rare instances where ransomware payments have been made public, Anthem

paid $2.5 million to consultancies after its 2015 breach. The U.K.'s National Health Service spent a total of £73 million on IT support in response to the WannaCry attack, much of which went to outside consultants.[36]

Legal assistance: Potential litigation costs are another source of hidden costs of cybercrime. This includes court filing and administrative fees, deposition costs, attorney's fees, and private investigator fees, as well as discovery production and review costs. Some companies may have the means to finance both an in-house legal counsel team and an outside third-party legal counsel to help advise on cybersecurity incidents and risk management. Even law firms take such steps to evaluate and mitigate risk. The American Bar Association's Cybersecurity Handbook encourages firms to "appoint an individual within the firm (or hire an individual from outside the firm) to serve as a chief information security officer responsible for managing the firm's day-to-day cybersecurity risks," and to determine client-specific data security protocols under the relevant privacy rules.[37]

Financing outside consultants is costly, and not all companies or institutions may be able to finance this approach. One of the most expensive aspects of a major cybersecurity incident is the litigation that can ensue under a range of federal, state, and foreign laws. The 2017 Equifax data breach, for example, resulted in years in court and the lawyers that led the class-action lawsuit against the company were ultimately awarded up to $77.5 million in legal fees.[38] Although that figure is an outlier, breaches often result in class action suits that are complex and time-consuming to defend. Suits resulting from cybersecurity incidents will likely continue to grow, especially as new laws like the EU's GDPR open up new legal remedies for consumers.[39]

Cyber risk insurance

Cyber risk insurance is also becoming normal for big businesses that can reasonably expect to face a cyberattack at some point, but it may be harder to justify for smaller businesses and municipalities that may choose to self-insure rather than add a significant insurance premium.[40] Cyber insurance policies are often exceedingly complex contracts that can easily run to hundreds of pages, and payouts can hinge on precise definitions of terms like "computer system" or "cyber incident" or on specific cybersecurity precautions that were or were not implemented.[41] For these reasons, only 28.4% of claims in 2017 resulted in payment, with an average payout of $188,525, far less than the average $590,000 cost we found for cyberattacks.[42]

In NotPetya, those affected by the hack attempted to collect on policies and were told by their insurers that the attacks would not be covered because of "war exclusion" clauses.[43] These disputes are working their way through U.S. courts and highlight the immaturity of the cyber insurance market, which lacks sufficient data for reliable actuarial models, constantly evolving risks, and contested coverage when compared to more traditional hazards like fires or floods. Still, the market continues to grow, and one estimate puts its overall value at $5.5 billion in 2020.[44] This includes stand-alone cyber policies, as well as protections packaged into standard property and liability policies.

Damage to employee morale

IT security incidents can often have a direct impact on an organization's staff. Not only is their work interrupted, their private information may have been exposed because of a breach. This is what happened in 2014 during the widely covered Sony hack. And while much of the media focus was on the decision whether to release "The Interview" or some of the more scandalous emails leaked, many Sony employees reported increased concern over their personal security. Some employees even received emails threatening violence against them or their families.[45] The exposure of personal information, including Social Security numbers and medical information, led to concerns amongst staff and, eventually, to a class-action lawsuit against Sony for failing to protect their information.[46]

A public scandal such as the Sony hack aired many internal issues, including some related to racism, sexism, and related pay gaps, affecting workplace morale. The studio tried to address the concerns and drop in morale in their staff by setting a hotline for employees that felt "threatened by the release of personal and financial information," providing counseling sessions to address stress and holding a town hall, where leadership figures addressed the situation.[47] Regardless of these measures, months after the hack, employees reported feeling a "leadership vacuum," which was incentivized by a perception of absence from the CEO, resignation of key figures, and the lack of an internal, positive message.[48]

After the Southeastern Pennsylvania Transportation Authority recovered from a cyberattack that derailed its real-time bus and rail information for two weeks, one employee said, "morale is really, really low."[49] The incident affected not only consumer-facing services, but also staff access to the servers where necessary files, projects, and contact information are stored.[50] Addressing staff morale not only helps an organization's recovery and productivity, but also can improve security. Low staff morale is linked to increased malicious insider threats.[51] Disgruntled employees can disrupt operations, delete data, or make public sensitive data to cause harm to their employer.[52]

Effect on Selected Sectors

Government sector

Government services are a tempting target for state actors, cybercriminals, and hacktivists. Economic gain is incentive enough. For instance, between March 2016 and February 2018, three Nigerian cybercriminals, after stealing confidential W-2 tax forms from more than 1,200 individuals, attempted to claim around $16.4 million in fraudulent tax refunds.[53]

But these incidents can have deeper implications than financial loss, as breaches might amount to national security threats involving compromised infrastructure or espionage. The U.S. Cyberspace Solarium Commission claims that "the United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide. Moreover, shortfalls in agility, technical expertise, and unity of effort, both within the U.S. government and between the public and private sectors, are growing."[54]

After the Office of Personnel Management was hacked, SF-86 data on more than 21.5 million individuals was leaked, as well as the fingerprint records of an additional 5.6 million individuals.[55] The national security concerns were profound, as sensitive data was acquired by China.[56]

Government respondents to our survey generally replied similarly to those in other industries. However, their responses diverged from their private sector colleagues in a few areas. Governments appear particularly vulnerable to malicious insider attacks, reporting the highest impact of such attacks among all surveyed industries.[57] Of related interest, many government officials also noted that remote worker and "bring your own device" (BYOD) policies posed particular challenges for their digital security.[58] Their responses also highlight concerns about skill shortages among their security staff and difficulty managing the risks posed by their workers' use of social media platforms and personal business services like Dropbox.[59]

The data also shows that government agencies are less likely to involve their legal departments in either planning for or responding to cyberattacks than is the case for any other industry, and they are also more willing to completely shut down their systems as part of their recovery process.[60] Finally, attacks on government systems are more likely to be publicly disclosed or reported in the media.[61] It should not come as a surprise that IT decision makers in government find damage to brand to be one of the hidden costs they experience to a greater extent than other industries. And that impact has a geographic variation. For government IT decision makers interviewed, 40% of those in the U.S. cited damage to brand as a concern compared to 28% of other government IT decision makers.

The government sector in the U.S. also appears to take longer to rectify the impact of IT security incidents in comparison with their counterparts in other countries and other sectors. For example, while it took, on average, 15 hours to discover the compromise that led to the longest IT security incident in 2019, IT decision makers in the U.S. government reported that it took them 17 hours to discover it. This lengthier timeline extends into the response plan, taking 39 hours from discovery to reach remediation and 45 hours to reach recovery (compared to 28 hours and 38 hours reported for all other IT respondents).

Our survey found that IT decision makers in government are less likely to report that data breaches represent the highest cost for their organization. They are more likely to say that ransomware, phishing, and malicious insider attacks represented the highest cost. This may reflect an unintended consequence of the Federal Information Security Management Act (FISMA).[62] Under FISMA, federal agencies may be inadvertently incentivized to report security incidents in such a way that it will not harm their FISMA compliance score. FISMA requires each federal agency to develop information security plans and report security incidents to the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA). The penalties for a low or failing FISMA grade include censure by Congress, negative

publicity for the agency, and reduced federal funding for agencies.[63] Data breaches are expressly mentioned in FISMA and trigger notification and reporting requirements. In contrast, ransomware, phishing, and insider attacks are not expressly mentioned in the Act.[64]

These findings make intuitive sense in a sector that has struggled publicly with insider leaks, (think Snowden and Manning), is often slower to adapt to novel and more flexible work arrangements than the private sector, and faces more public scrutiny than virtually any other industry. The responses indicate a higher willingness to go temporarily offline, which suggests that government actors face different pressures in responding to cyberattacks.[65]

Healthcare

Medical records often contain financial details and Social Security numbers in addition to confidential and sensitive health information, making the health sector a particularly appealing target for cybercriminals. Hospitals also often rely on poorly secured systems that are vital to their operations, so the healthcare sector has been a ripe target for cybercrime.

Ransomware attacks on hospitals have become commonplace, with regular attacks around the world—from France to Australia—and especially in the U.S.[66, 67] In a typical attack, mid-sized hospitals with limited IT resources are locked out of their systems and forced to pay ransoms that can range from thousands of dollars to millions. These sums certainly add up, but many of the costliest impacts of cybercrime on the healthcare sector have come from broader attacks that have not discriminated among their targets.

The 2017 WannaCry epidemic affected hundreds of thousands of computers but was particularly distressing for the U.K.'s National Health System (NHS). The NHS had to take more than a third of its systems offline either because they had been affected or because they were at risk, greatly slowing performance and patient care at many healthcare facilities.[68] Although the WannaCry attack did not lead to any deaths, more than 19,000 appointments were cancelled, and the lost productivity, system recovery efforts and IT upgrades were estimated to have cost the National Health Service (NHS) £92 million.[69, 70]

NotPetya was also quite costly for the healthcare sector. The attack paralyzed Ukrainian hospitals. In the commercial healthcare sector, the pharmaceutical giant Merck ultimately sustained losses that may exceed $1 billion.[71, 72] The virus also spread from Merck to other parts of the pharmaceutical supply chain and caused delays in the delivery of prescription medications around the world.[73] The 2015 Anthem Breach is another interesting case study. Nearly 80 million records were stolen in the breach, and the insurer ended up spending $2.5 million on consultants, $115 million on security improvements, $31 million to notify consumers, and $112 million for credit protection for those affected by the breach.[74]

NotPetya, WannaCry, and the Anthem breach have been among the most damaging single attacks against the healthcare sector. It appears that state actors may have been responsible for all of them, raising questions about international law and norms protecting healthcare systems. Attacks have also increased during the COVID-19 crisis, with both private and state actors taking advantage of the circumstances to defraud victims and siphon data from researchers.[75] This has resulted in new calls to declare healthcare systems off limits, including the E.U.'s Oxford Statement, but the sector seems likely to remain vulnerable.[76]

Financial sector

In July 2020, the FBI issued a "Flash Alert" to U.S. finance, healthcare, and chemical industries conducting businesses in China about potential targeting by the Chinese government via the state-mandated tax software.[77] According to the FBI, Baiwang and Aisino are the only government-authorized tax software service providers in accordance with China's revised value-added tax in 2018. The malware embedded in the mandatory tax software programs, one of which was aptly named the "intelligence tax," essentially enabled a hidden backdoor into victim networks and systems using malicious software.[78] The FBI reported that this vulnerability likely granted cyber actors access to "conduct remote code execution and exfiltration activities on the victim's network."[79] It is unknown how many companies were compromised. Organizations that use cloud-based email services, especially in the finance and business sectors, are lucrative targets to cybercriminals who conduct business email compromise (BEC) scams.[80]

According to the FBI's IC3, there has been a steady increase in BEC scams since 2014 and from 2014 to 2019 the Internet Crime Complaint Center (IC3) "received complaints totaling over $2.1 billion in actual losses from BEC scams targeting the largest platforms."[81] This is significant because it highlights that BEC scams are growing in volume and users are struggling to maintain the security of their account. As more employees turn to remote working on personal and company devices during COVID-19, as well as conducting virtual financial transactions, this could create a more fertile environment for BEC phishing scams targeting the financial sector.

Cybercriminals are naturally attracted to the financial sector. It is, after all, where the money is. That there have been fewer dramatic successes is a tribute to the intense effort the sector has put into cybersecurity both at individual institutions and collectively. This comes at a cost, however, with spending of up to $3,000 per employee on cybersecurity. A survey conducted in 2018 by the FS-ISAC found that financial institutions spend (depending on their size) between 6% and 14% of IT budgets for defense.

Recommendations for Decision Makers

Global spending on cybersecurity reached almost $145 billion in 2019.[82] Add this to our estimated losses of $945 billion, and cybercrime is now a trillion dollar-plus drag on the global economy. Risk is not distributed equally, and some companies experience no losses while others lose millions. What is worrisome is that fewer and fewer companies can say that they will never experience a damaging hack. Some firms escape loss, while others are damaged. This reinforces the need for adequate planning for cyberattacks.

And despite the fact that becoming a victim of cybercrime is more a matter of *when* than *if*, there is a lot that organizations can do to help prevent IT security incidents or reduce the harm and impact on the organization. There is barely a report on cybersecurity that does not conclude with recommendations for organizations to improve their cyber hygiene and implement known best practices. Some of these best practices include:

1. Uniform implementation of basic security measures
2. Increased transparency within organizations
3. Standardization and coordination of cybersecurity requirements
4. Provide cybersecurity awareness training for employees
5. Develop prevention and response plans

The Center for Strategic and International Studies (CSIS) has published several reports on how organizations can better protect themselves. Although some of the reports are several years old, the recommendations are still valid. Implementing simple cybersecurity measures, such as multifactor authentication and backups are essential and go a long way toward reducing many of the losses from cybercrime.[83] A recent advisory issued jointly by the cybersecurity authorities of Australia, Canada, New Zealand, the U.K., and the U.S. provides their collective recommendations for organizations to avoid common technical missteps when first responding to a cyber incident.[84]

But implementing technical solutions will not solve all problems. Our survey yielded concerning findings regarding some of the struggles that organizations face internally that contribute to making them more vulnerable to cyberattacks. For instance, 507 out of 1,332 respondents considered that lack of user knowledge contributed to the success of the cybercriminals targeting their organizations. One of the biggest challenges is a lack of organization-wide understanding of cyber risk. This makes companies and agencies vulnerable to social engineering tactics. Once a user is hacked, they do not always recognize the problem in time to stop the spread of malware. The increased (and unavoidable) use of personal devices such as smartphones or tablets expands the attack surface and endpoints for attack and complicates the management of cyber defense.

Another facet of this disconnect has to do with how companies respond after an incident. As mentioned earlier, 38% of the respondents said a lack of user knowledge was central for the success of the attacks. And yet, investing in new or different software was the most common modification to processes after a security incident (45%). This is an understandable reaction, but by itself is not sufficient.

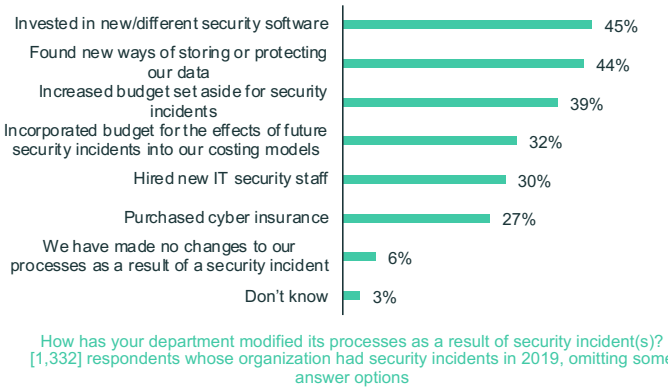

Figure 3. Modification of processes as a result of security incidents.

Besides, without being aware of it, organizations could be setting themselves up for further problems. Large organizations use an average of 47 different cybersecurity tools, and source them from an average of 10 different vendors.[85] This can create interoperability problems and can affect the products' efficiency.[86] Even when different services and products are properly integrated, this can drain resources significantly, making IT professionals devote their time to managing the interoperability of the toolkits that were supposed to make their jobs easier.[87]

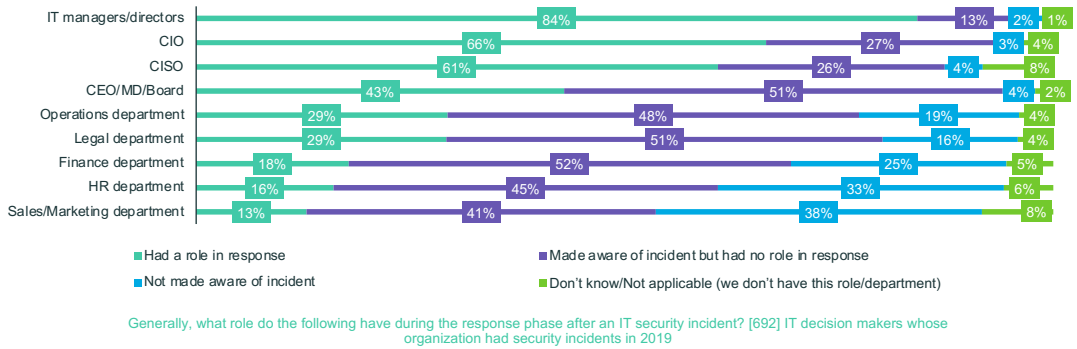

Figure 4. Percentage of organizations that have a plan to prevent and respond to security incidents.

Elaborating prevention and response plans

It is not surprising that ensuring that there is a plan in place for preventing and responding to IT security incidents is key to successfully managing one when the time comes. However, only 44% of the survey respondents say that they have plans in place to both prevent and respond to IT security incidents. Although 32% of decision makers say the organization has a plan to prevent IT security incidents, they do not seem to be as prepared to respond, with only 19% saying a response plan exists. Furthermore, these plans were not regarded as useful or successful. Only 32% of the respondents found their organization's plans to be completely successful in responding to IT security incidents. And, although most (62%) consider them "somewhat successful," it speaks to room for improvement.

Only a small proportion of organizations have a plan to both prevent and respond to IT security incidents

In order to minimize the impact of such incidents, organizations must ensure they have plans in place to both prevent and respond to security incidents. Although it's comforting to see that there are very few organizations who don't have any plans in place, there is still room for improvement. Organizations in Japan are the most likely to not have plans in place for prevention, nor response, which may explain why they're also the most likely to experience the highest impact of cost (slide 15)

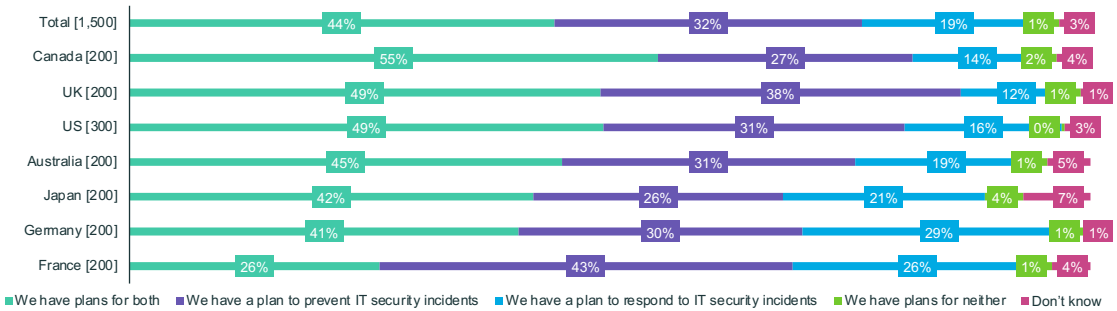

Figure 5. Roles involved in response phase of security incidents.

Lack of communication within the organization

Those organizations that do have plans to prevent or respond to IT security incidents, however, face the problem of communication. Although it is essential that there is an overlap between those creating the plan and those involved in the actual response, communication across an organization and different relevant stakeholders is also necessary.

IT and line-of-business (LOB) decision makers have different understandings of *what*, *why*, and *how* a company or government agency is experiencing an IT security incident. This is likely due to a lack of visibility for LOB executives over what is happening, and not

enough communication across departments. Figures would suggest that LOB decision makers believe there are plans to respond to incidents when, in fact, there may not be. Whereas 42% of IT decision makers say both exist, 47% of LOB decision makers responded positively to the same question.

Unsurprisingly, executives in the IT departments were more aware of the number of investigations carried out, while 18% of LOB decision makers did not know how many were conducted. When it comes to the impact of ransomware or DoS/DDoS attacks, LOB decision makers seem to lack visibility into their actual impact on their organization, contrasted to the evaluation made by IT executives.

Initiatives undertaken after a serious incident highlight the importance of these concerns. Three years after the Equifax breach, the company's CISO reflected that addressing the communication issues with the C-suite and improving the company's cybersecurity awareness culture were some of the most relevant measures put in place.[88]

How IT and LOB decision makers understand the vulnerabilities that can lead to successful cyberattacks is telling. LOB executives see less risk in remote work, BYOD policies, or the increased use of smartphones and tablets—all things that increase the attack surface—than by their IT counterparts. Across departments, respondents indicated that lack of user knowledge allowed an intruder to be successful, which underscores the importance of digital literacy efforts for all employees.

Although senior staff members in the IT department are typically involved in the development of the plans (50% of the survey respondents had their IT director involved, and 45% of the IT managers), it was concerning that just 22% involved the operations department, and only 18% the legal department in response planning. The participation and involvement of the C-suite and the board occurred in less than 36% of the cases. The long list of hidden costs makes it clear that cross-departmental cooperation and communication is essential. Informing other areas about ongoing incidents and developing a multi-stakeholder participation plan enables better risk and crisis management.

This lack of communication extends to the time of responding to an incident as well. There are departments that are not made aware that a cyber incident is happening. Twenty-four percent of LOB decision makers claimed that their departments are directly affected by an IT security incident. If they are not aware of why they are experiencing these incidents, it might lead to confusion across departments. With lack of user knowledge being a root cause for the success of many of these incidents, communication between departments is key in ensuring that they are aware of, and understand, the causes, as well as preventative measures that can be put in place for the future.

Appendices

Appendix A: Cybercrime and COVID-19

The COVID-19 crisis has provided a fertile environment for cybercrime. Not only were criminal actors able to quickly modify their schemes in response to the pandemic, they also take advantage of the quick adoption of remote access infrastructure for work and education. Traditional schemes became "COVID-themed." This represents the highest amount of reported activity in 2020 and includes setting up malicious domains, spam and phishing campaigns, and carrying out fraud schemes for either credential theft, deployment of malware, or gaining access to PII.[89] There has also been an increase in targeting of domestic and international organizations working on the pandemic response. These kinds of attacks primarily look "to collect bulk personal information, intellectual property, and intelligence."[90]

In the U.S., officials from the FBI's IC3 reported that during the pandemic, cybercrime complaints increased from 1,000 to 3,000 to 4,000 daily.[91] Beginning in March, there was a sharp increase in the number of domains being registered that referenced the coronavirus.[92] Although the increase included both malicious and benign domains, the high-risk domains surpassed 5,000 a day during March, while low-risk ones never went over 1,000. This trend in COVID-related domains began declining as the novelty and uncertainty associated with the crisis diminished. By the end of May, the CTC advisory found that the registration of COVID-related malicious domains was under 1,000 a day and continuing its downward trend.[93]

Before COVID-19, the IC3 received more than 1,200 complaints a day from victims on average and approximately 340,000 complaints per year on average over the last five years.[94] That number has only increased since the pandemic as more cybercriminals began targeting the elderly, the healthcare sector, financial institutions, government institutions, and stimulus and paycheck protection programs.[95] Assistant Director of the FBI's Criminal Investigation Division, Calvin A. Shiver testified before the Senate Judiciary Committee in June 2020: "...as of May 28, 2020, the Internet Crime Complaint Center (IC3) received nearly the same amount of complaints in 2020 (about 320,000) as they had for the entirety of 2019 (about 400,000). Approximately 75% of these complaints are frauds and swindles, presenting a challenge for the FBI's criminal program given the sheer volume of submissions."[96]

This increase in cybercrime activity during the wake of COVID-19 is also evidenced in Google's Safe Browsing Service Report, which indicated a steady increase in the amount of phishing sites. These are fake web pages that try to trick users into sharing private information like usernames, passwords, and banking information by appearing to be legitimate websites. According to Google's Safe Browsing Transparency Report on unsafe websites, at the end of January 2020 Google detected 1,690,000 phishing sites. By the end of February, that number grew to 1,695,948, then to 1,798,244 by the close of March and April and showed no sign of stopping as the number of phishing sites swelled to almost 1,900,000.[97]

As organizations moved to remote working in response to healthcare guidelines, they needed to deploy new technologies for remote access and teleworking infrastructure. This move allowed for the exploitation of vulnerabilities that were nonexistent before.[98] The FBI anticipated in early April that cybercriminals would attempt to take advantage of the "increased use of virtual environments by government agencies, the private sector, private organizations, and individuals as a result of the COVID-19 pandemic."[99] The concerns were parallel for the adoption of "edtech," with education systems rapidly going online. UNICEF warns that children are at an increased risk, "vulnerable to online sexual exploitation and grooming, as predators look to exploit the COVID-19 pandemic."[100]

Another facet has to do with criminal activity targeting the relief funds that governments developed to assist their citizens struggling financially during this crisis. In his remarks before the U.S. Senate Committee on the Judiciary on "COVID-19 Fraud: Law Enforcements' Response to Those Exploiting the Pandemic," Michael D'Ambrosio, assistant director of the Office of Investigations of the Secret Service, estimated that potential losses from the $3 trillion CARES Act stimulus package could amount to $30 billion dollars, "[e]ven if we assume a very low rate of fraud, of just 1%."[101]

A different aspect of cybercriminal activity linked to COVID-19 is the increased targeting of medical and research facilities. The cyberattack against the Brno University Hospital in the Czech Republic in mid-March crystallized many of the concerns regarding the security

of medical and research facilities and thrust the issue into the pandemic spotlight. The hospital was reported to have had to shut down its IT network, postponing surgeries and having to reroute patients to other hospitals.[102]

Not long after, Interpol issued a Purple Notice alerting of a "significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response."[103] The FBI and CISA informed that actors affiliated with China targeted U.S. organizations, "attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research."[104] The President of the European Commission publicly stated that China "may have been" behind a number of cyberattacks against European hospitals and that such action "cannot be tolerated."[105]

Appendix B: The Most Costly Types of Cybercrime

Malware and spyware

Based on survey data, spyware and malware (including viruses, worms, spyware, keyloggers, and Trojan horses) cost organizations the most in 2019. Malware facilitates a range of criminal activities, from ransomware and data exfiltration to the active disruption of networks.

Illicit Cybercrime-as-a-Service dealings have allowed malware to simultaneously become more advanced and also more accessible to those without deep technical expertise. As cybercrime markets have grown increasingly sophisticated, they have seen the emergence of specialized vendors who are experts at not only designing malware, but also setting up the necessary infrastructure for an attack.[106] They offer to lease malware to would-be cybercriminals for a fee, creating an environment where a small group of technically minded criminals can focus their full attention on the development of new attack capabilities, and where a large group of less sophisticated actors can easily take advantage of them.

Data breaches

In the first half of 2019, more than 3,800 data breaches were reported, exposing more than four billion records to cybercriminals.[107] One particularly concerning subset of data breaches are those affecting personal health data. This data can often be one of the most valuable forms of data for criminals because of the way it allows for the precise targeting of fraudulent schemes to vulnerable individuals based on their medical histories.[108] As of August 2020, the U.S. Department of Health and Human Services was investigating more than 550 cases of personal health information breaches caused by theft, hacking, IT incidents, or unauthorized access.[109] These cases involve the data of almost 35 million individuals.

Data breaches are mostly the result of external actors, but a recent study found that many are the result of insider attacks. One recent example was the 2019 breach of more than 100 million Capital One records by a software engineer working for Amazon Web Services, who hosted the bank's database.[110] Insiders can also pose a threat to sensitive corporate intellectual

property (IP). An example of this was the case of Tesla in 2018, when an employee abused his/her access to make "damaging" changes to the source code of Tesla's manufacturing operating system, and exported gigabytes of information about Tesla's manufacturing processes to a third party.[111]

Phishing

According to the Anti-Phishing Working Group (APWG), in the first quarter of 2020 more than 165,000 unique phishing sites were recorded.[112] Phishing has become easier in recent years, as Phishing-as-a-Service offerings have emerged on cybercrime markets.[113] Thanks to these offerings, cybercriminals no longer need to have expertise in designing a phishing infrastructure before sending out their campaigns. Instead, criminals can simply buy from vendors who offer their own kits and hosting, and focus on victims (whose contact details are also easily available from the same markets). One research group found more than 5,000 turnkey phishing kits available in the first half of 2019 alone.[114]

Ransomware

Ransomware remains the fastest growing part of cybercrime. During the COVID-19 pandemic, ransomware attacks in general have increased 148% from the baseline levels reported in February 2020.[115] One of the most concerning trends in ransomware is the shift towards targets in the manufacturing industry. Security researchers are beginning to see the emergence of ransomware strains targeting industrial control systems, and millions in ransom has already been paid by industry victims who have fallen prey to these variants.[116] This trend is likely to continue as factories and other industry operators prepare to expand their deployment of vulnerable IoT devices throughout their premises—broadening the attack surface of their network and creating new targets for malicious actors.[117]

Financial cybercrime

Cybercrime continues to impose heavy costs on financial institutions. Today, there are five billion unique user credentials (for example, username and password combinations) available on the darknet to cybercriminals.[118] These pilfered credentials can grant access to corporate networks or bank accounts.[119] There are more than 15 billion pilfered credentials for sale on the darknet, five billion of which are unique first-time identifiers.[120] The FBI's "2019 Internet Crime Report" states: "Some criminals buy credentials on darknet marketplaces, where a single account costs on average $15.43. But the more sought-after banking credentials sell for an average of $71."[121]

Financial institutions have also come under attack by nation states. In 2016, North Korean hackers managed to steal $81 million from Bangladesh's central bank by taking advantage of stolen credentials and submitting false money transfer requests to the Federal Reserve Bank of New York.[122] More recently, in 2018 the same group of hackers managed to steal $20 million from the Mexican bank Bancomext.[123] The scale of the threat facing financial institutions can be most clearly seen in the 2018 arrest of a cybercrime gang leader whose group stole $1.2 billion from more than 100 banks over a period of five years.[124]

Business email compromise

Although banks continue to remain a favorite target of cybercriminals, there has also been an increase in the use of BEC, a special category of identity theft. Typically, these schemes target a company's human resources department or payroll department by posing as an employee asking to change their direct deposit information. Next, the employee's paycheck is wired to a fraudulent prepaid card account. Other forms of BEC scams include spoofed vendor and lawyer email accounts, W-2 form requests, and fraudulent requests for gift cards. This allows for cybercriminals to send emails impersonating any employee—from new hires to the CEO.

Overall, BEC scams present particular challenges to banks, as a wire transfer request may appear to have been submitted by a legitimate customer. However, that person's credentials may actually be exploited by the cybercriminal for nefarious purposes.

In May 2020, one of the world's leading financial services and market-making companies, Virtual Financial, reported that it fell victim to a $6.9 million BEC scam.[125] According to the legal court documents filed by Virtu, hackers infiltrated the CEO's email account and sent several emails impersonating the CEO to the accounting department.[126] The hackers requested "two wire transfers to overseas banks—one in the amount of approximately $3.6 million, the other in the amount of around $7.2 million—for purported capital calls. Believing the requests to be legitimate, Virtu's accounting department complied with the requests."[127] It was only after the accounting department wired the funds that Virtu's internal audit flagged the transfers as potentially fraudulent.

Cryptocurrency theft

The theft of cryptocurrencies continues to be a major trend in cybercrime, with over $4 billion in cryptocurrency stolen over the course of 2019 and almost $1.4 billion stolen in the first five months of 2020.[128] These thefts often occur from exchanges and wallets where users keep their coins, using a combination of tactics including phishing, malware, and insider theft. Another emerging trend is cryptojacking, where malware is installed on victims' computers to remotely mine for cryptocurrencies.[129] Users may not notice when cryptojacking is taking place, but it can slow affected devices and draw electricity costs while the mining takes place.

The use of emerging technical and synthetic media for cybercrime

AI-enabled cybercrime schemes using synthetically generated media are becoming more prevalent.[130] Synthetic media encompasses not only "deep fake" photo and video content, but also false voice and written media.[131] While AI is also being developed as a defensive tool for cybercrime, like automating threat intelligence using machine learning, industry experts are still worried about the offensive uses of AI in cybercrime.[132]

Some experts postulate that deepfakes could become a malicious source for exploitation, disinformation and non-consensual pornography. As facial swapping technology gains more mainstream popularity, some experts are raising concerns that this technology could also potentially be used by criminals for malicious ends like extortion, blackmail, romance fraud, and more.

Appendix C: Who Are the Criminals?

Cybercrime is now a specialized "professional" activity. There are still many unsophisticated new entrants, but if they live in countries where the rule of law is strong, they usually end up in jail. Cybercriminals thrive where law enforcement is weak, whether it is because many countries have still not developed the necessary capabilities to fight cybercrime or because their government decided to turn a blind eye to the activities.

The global reach of the internet means criminals and victims do not need to be located in the same place. As FBI Director Christopher Wray explained at the 2020 National Cybersecurity Summit,[133] "We've got to change the cost-benefit calculus of criminals and nation states who believe they can compromise U.S. networks, steal U.S. financial and intellectual property, and hold our critical infrastructure at risk, all without incurring any risk themselves."

For most countries, the vast majority of cybercrime losses will be attributable to actors outside of their jurisdiction. Cybercrime has become among the most lucrative activities, with data trading and ransomware becoming increasingly popular tools.[134] From January to June of 2020, the victims of the 11 most significant ransomware attacks in Europe and the U.S., in both the private and public sectors, have incurred financial losses of $144.2 million connected to rebuilding infrastructure, paying ransoms, and the creation of new security structures.[135]

Organized cybercrime teams are highly regimented, with team leaders, coders, network administrators, intrusion specialists, data miners, and even financial specialists leading vast organizations of multinational hackers.[136] More recently, some previously unconnected groups have started collaborating with each other in order to increase their activities and profit.[137] In China alone, an estimated 400,000 people work in rapidly growing organized cybercrime networks.[138]

Some countries are hotbeds for cybercrime. A weak rule of law, lack of specialized law enforcement agents, and inadequate resources allow cybercriminals to enrich themselves with impunity. In Nigeria, for example, unemployment, poor implementation of laws, and inadequately equipped law enforcement agencies help explains why cybercrime can flourish.[139] Criminal cyber activity from Vietnam has increased in the last few years, with consensus that the situation has been aggravated in recent years.[140] Rapid economic growth and an inability to absorb talent have led to Vietnam to be considered a "mid-tier cybercrime hub."[141]

Other states, however, have a permissive environment for cybercriminals and use them for state purposes when needed. In Russia, for instance, the complex and close relationship between the state and organized crime makes it into a sanctuary for the most advanced cybercriminals. Allowing criminal groups to pursue their financially motivated schemes and protecting them from law enforcement comes with a price; they are expected to use their skills to support the government's interests. John Carlin, former assistant attorney general for the Department of Justice's National Security Division, said, "Increasingly, you cannot tell which is which when it comes to the criminal and the intelligence agency. So, one day, the same crook may be doing something purely to make a buck. But that same crook may be directed by a trained intelligence operative using the same tools and techniques to steal information from them for the goals of the state."[142] When issuing sanctions against Maksim Yakubets, leader of the cybercrime group Evil Corp, U.S. officials highlighted his "direct assistance to the Russian government's malicious cyber efforts," in addition to his financially motivated crimes.[143]

This symbiotic relationship seems to also be the case in Iran, where cybercriminals act, in many cases, both for private gain and for the government. Recent charges against two Iranian hackers found that in the same "cybertheft campaign," there were instances in which they acted "at the behest of Iran," and sometimes only for financial gain.[144] Mabna Institute hackers stole research from universities, governments, and companies around the world, costing the organizations more than $3 billion.[145]

Some states have directly engaged in cybercrime for their own financial gain. North Korea uses cyber-enabled theft and money laundering, extortion campaigns, and cryptojacking to fund its projects.[146, 147] The hacking initiative is orchestrated by the Reconnaissance General Bureau, North Korea's intelligence agency, and reportedly has 6,000 agents carrying out operations in more than 17 countries.[148, 149] North Korea may have funneled up to $2 billion from cybercrimes against banks and cryptocurrency exchanges to its weapons of mass destruction (WMD) research.[150] Cryptocurrency exchanges are a favored target for North Korea, since they allow the state "to generate income in ways that are harder to trace and subject to less government oversight and regulation than the traditional banking sector."[151] Two 2019 hacks represented the theft of $250 million in cryptocurrency.[152] Ransomware is another preferred tool. By making the ransom cheaper than the cost of backup and restoration, they seek to force companies to pay.[153]

We have discussed how IP theft, as a hidden cost, can represent a significant loss to agencies and companies, as well as pose a national security risk. This form of crime is harder to fight when it is state backed. Economic espionage to benefit national industry has long been a hallmark of China's economic policy. China accounts for roughly 80% of all economic espionage cases in the U.S., and it has cost the U.S. economy around "half a trillion to a trillion dollars of damage."[154, 155] Cyber-theft plays a significant role in making this a successful policy. Typical targets of state-linked Chinese hackers include defense and technology firms, engineering companies, and pharmaceutical and medical device developers spread

out across the U.S., Europe, and Asia.[156] For example, so as to benefit its aircraft industry, China has leveraged its "underground hacking scene, Ministry of State Security or MSS Officers, company insiders, and state directives."[157]

Amid the COVID-19 pandemic, targeting of healthcare and medical research facilities has increased. The president of the EU Commission suggested that China might be behind these operations and remarked that this would not "be tolerated."[158] In a related event, the U.S. Justice Department issued an indictment last July against two Chinese hackers targeting IP, including COVID-19 research. The document alleges they sometimes "acted for their own personal financial gain" and, in some cases, they acted for government agencies.[159] Overall, China has a flourishing cybercrime network but this may be a consequence of its massive state surveillance program, since many of the hackers caught by the Chinese police are offered a choice: work for the state or go to jail.

Appendix D: National Experiences

Our survey found that organizations in different countries assess cyber risk differently. While many of the findings hold true across the world, some outliers help us better tailor plans for increased efficiency. There is no "one-size-fits-all" solution to cyber risk. Although our findings are limited by the locations surveyed (the U.S., Canada, the U.K., France, Germany, Australia and Japan), they provide useful snapshots of variations across countries.

Conducting IT security investigations and the impact of downtime

Organizations conducted an average of 18 IT security investigations in 2019. German, U.S., and UK organizations conducted above average investigations, with French organizations at the lower end of the spectrum, conducting around 15. This might suggest that organizations in France face less of a risk or that they have less regard for it. Thirty-two percent of French organizations report that they did not experience a cyber incident that caused downtime, when that was only true for an average of 26% of the total respondents.

With downtime being a common consequence for around two thirds of respondents' organizations, location appears to make a difference. Forty percent of the companies or agencies in Japan experienced no downtime, while this was only true for 18% of them in the U.S. This could be explained if Japanese organizations implemented better preventative measures—but they do not seem to be doing differently from others in developing prevention and response plans. Another plausible explanation is that organizations in the U.S. are more tempting and lucrative targets.

Although, in some instances, there seemed to be a link between the duration of downtime and the costs associated with it, this was not always true. The average cost of the longest downtime for organizations in both Japan and Germany was above $1 million, and, although Japan's downtime duration was slightly above average at 19 hours, Germany was in the lower spectrum at 14 hours.

Incident response

It took an average of 19 hours for most organizations to move from the discovery of an incident to remediation. This typically entails restoring IT services back to normal capacity, removing the threat from the system, and retrieving lost data. In some cases, however, organizations will not consider an incident to be remediated until the source of the incident has been identified or some measure has been implemented to prevent the incident from reoccurring in the future.

During the average longest IT security incident, 15 hours elapsed before the compromise was discovered. This time of extreme vulnerability was even longer for organizations in Japan, the U.S., and Canada. In the case of Japan, companies and agencies took significantly longer than their counterparts did in other countries to move to remediation, taking 48 hours—20 hours longer than the total average.

Prevention and response plans

We have discussed how the lack of plans for both preventing and responding to IT security incidents is widespread, with only 44% of our respondents stating their organization has both. French organizations scored even lower, with only 26% of institutions boasting prevention and response plans. It is uncommon for an organization to not have any sort of plan in place. Even if they did not have plans for both preventing and responding, they would have one of them in place. Only in Japan did we find a larger percentage of institutions that had neither kind of plan: 4% against an average of 1%.

Limited involvement of the C-suite in developing plans is also a shared experience across the countries. However, it is interesting to note who they decide to involve. While the U.S., Canada, and the U.K. lead in involving the CEO or the board, organizations in France and Germany tended to bring on the CIO, CISO, and CTO to a larger extent.

Communication strategies

Agencies and companies in Canada and Germany were less likely to share information about their most severe IT security incident with anyone outside of their organization. One could hypothesize that increased media reporting would be an incentive for organizations to get ahead of the story and inform the public. However, that is not the case. Although, incidents that occur in the U.S. garner the most media attention—24% of the organizations there responded that their most severe IT security incident was covered by the media (and this was true for an average of 16% of the total surveyed institutions)—22% of U.S. companies and agencies interviewed reported they did not share any information. This was well in line with the average across regions. Communicating with clients and customers does not appear to be a priority in most countries, with no significant discrepancies among the interviewees: only 345 out of 1,332 companies informed their clients that they had experienced a cyber incident.

Appendix E: Case Study—Duke University

To help identify and defend university networks from attackers, Duke University's Office of Information Technology developed the Shared Threat Intelligence for Network Gatekeeping and Automated Response (STINGAR) program for higher education.[160] STINGAR creates locally derived threat intelligence using community honeypot networks across partnering higher education institutions and is designed to counter threats in near real time.[161] For example, at the height of the notorious Mirai botnet attack, STINGAR helped Duke's security team block an average of two billion malicious connection attempts per day.[162]

Once the COVID-19 pandemic began impacting higher education, the STINGAR project observed an initial decline in unique malicious IP addresses (March and April 2020), as faculty, students, and staff moved into a remote learning or working mode. The STINGAR ecosystem uses network sensors (honeypots or other sensors) to detect potential threats, enables the federation of multi-university threat data, and employs network actuators to rapidly block threats in near real time. While the number of unique malicious IP addresses detected has rebounded, the total number of attacks detected by STINGAR remains generally below the levels we were seeing pre-pandemic.

Apart from Russia, China, Iran, and North Korea, other countries with high malicious IP addresses were the U.S., which is indicative that cybercriminals are able to make wide use of the U.S. infrastructure to mask the origins of the attack.[163] (See Figure 6.) Duke hypothesized that the declines were due to (a) the reduction of systems on the participating networks (once faculty, staff and students moved to a remote learning/working scenario, there was less local activity), and (b) a switch in tactics to target home workers and learners via phishing or other social engineering attack.[164]

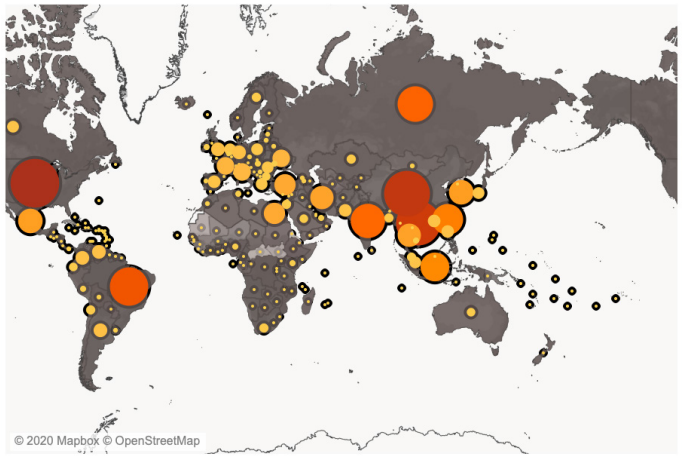

Figure 6. Top Countries with Malicious IP Traffic Per Day in 2019.[165]

China, Russia, North Korea, and Iran are targeting U.S. academic institutions: The STINGAR Project

Among this group of state actors, according to Duke's STINGAR program, from January 2020 to July 2020, the majority of malicious IP address requests appear to have originated from infrastructure hosted in China based on new and unique IP addresses detected.[166]

The leading Autonomous System Numbers (ASN) with organizational ties to China are No.31 Jin-rong Street, with a reported average of 920.5 unique IP addresses,

and CHINA UNICOM, China 169 Backbone with 456. ASN refers to a set of IP routing prefixes managed by network operators for an entity. Jin-Rong Street is also listed on Spamhaus's list of top 10 botnets.

Duke University's STINGAR data shows the ASNs from which attacks originate, providing a source of information on the relative "cleanliness" of networks. Looking specifically at China, Iran, and Russia, Duke's STINGAR threat intelligence data revealed consistent daily activity from these countries through the malicious connection attempts (total attacks, unique IPs, and new attacking IPs). (See Figure 7.) Interestingly, at the time of this writing, no new IP attacks were detected from North Korea since April 2020.

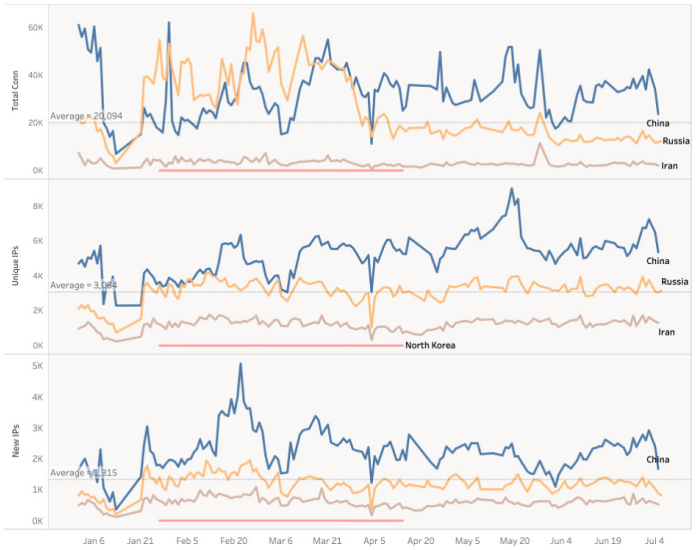

Figure 7. Malicious Traffic from China, Russia, North Korea, and Iran.

Data Analysis

Russia:

- *Total connection daily average of 17,619, unique IP daily average of 3,194.*
- Sharp decline in the number of daily connections at the end of March, with the daily connection number staying lower than normal since the transition. This corresponds with the timing of most higher education institutions moving to a remote learning and working posture.

China:

- *Total connection daily average of 33,292, unique IP daily average of 5,801.*
- Malicious activity from Chinese IPs has largely remained consistent over the past six months. There was a noticeable increase in the number of total connections, unique IPs, and new IPs on May 19 and July 2.

North Korea:

- *Total connection daily average of five, unique IP daily average of 1.*
- Very few malicious connection attempts have been observed from North Korea IPs in this period.

Iran:

- *Total connection daily average of 2,656, unique IP daily average of 1,218.*
- Malicious connection attempts from Iranian IP space have remained consistent throughout the year, with a noticeable spike in late May.

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decision making of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS is ranked the number one think tank in the U.S., as well as the defense and national security center of excellence for 2016 to 2018 by the University of Pennsylvania's "Global Go To Think Tank Index."

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

1 https://us-cert.cisa.gov/ncas/alerts/AA20126A
2 https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf
3 https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1
4 https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/
5 https://www.helpnetsecurity.com/2010/09/08/the-emotional-impact-of-cybercrime/
6 https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds
7 https://docoh.com/filing/8868/0000950103-20-011295/AVP-8K
8 https://www.zdnet.com/article/avon-recovering-after-mysterious-cyber-security-incident/
9 https://www.computerweekly.com/news/252484804/Cosmetics-company-Avon-offline-after-cyber-attack
10 https://www.northamptonchron.co.uk/business/northampton-based-cosmetics-giant-avon-kod-worldwide-cyber-attack-2884686
11 https://docoh.com/filing/8868/0000950103-20-012442/AVP-8K
12 https://d18rn0p25nwr6d.cloudfront.net/CIK-0000008868/c517e612-d1ca-4fdd-8269-d2e3ac963e2a.pdf
13 https://tech.newstatesman.com/security/uk-universities-each-suffering-a-weeks-down-time-a-year-fois-reveal
14 https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/
15 https://www.insurancejournal.com/news/international/2019/07/24/533763.htm
16 https://www.hydro.com/en/media/on-the-agenda/cyber-attack/
17 https://soundcloud.com/csis-57169780/what-keeps-you-up-at-night
18 https://soundcloud.com/csis-57169780/what-keeps-you-up-at-night
19 https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/
20 https://www.wired.com/story/petya-ransomware-ukraine/
21 https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/
22 https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/
23 https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf
24 https://www.reuters.com/article/us-target-consumers/consumers-vent-frustration-and-anger-at-target-data-breach-idUSBREA0D01Z20140114
25 https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states
26 https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
27 Henry M. Paulson, Jr., Dealing with China, p. 390 (2015).
28 https://www.csis.org/blogs/technology-policy-blog/notes-csis-virtual-event-countering-chinese-espionage
29 https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf
30 https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
31 https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
32 VB Survey Q18
33 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
34 https://www.insurancejournal.com/news/national/2019/12/03/550039.htm
35 https://www.theguardian.com/technology/2015/dec/08/cybersecurity-experts-charge-10000-a-day-to-protect-uks-top-firms
36 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf
37 ABA Cybersecurity Handbook pp. 114-115.
38 https://www.washingtonpost.com/business/2019/08/08/lawyers-representing-consumers-equifax-settlement-may-get-more-than-million-is-that-fair/
39 https://mcusercontent.com/0c82d1e732eec64ff4cb3d4b7/files/16898313-4e0c-460a-a9f0-88f4d6d840ad/2020_Class_Action_Survey.pdf
40 https://www.knoxnews.com/story/news/local/2020/06/22/cyber-insurance-helpful-ransomware-attacks-like-knoxvilles/3216039001/
41 https://www.natlawreview.com/article/covid-19-does-your-cyber-policy-cover-remote-working-cyber-risks
42 https://www.bermudareinsurancemagazine.com/contributed-article/cyber-still-small-for-its-age
43 https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html
44 https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/covid-19-crisis-could-be-watershed-for-cyber-insurance-says-swiss-re-exec-59197154
45 https://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html
46 https://www.wired.com/2014/12/sony-getting-sued-former-employees-protecting-data/
47 https://www.hollywoodreporter.com/news/sony-hack-5-things-studio-758450
48 https://www.thewrap.com/sony-entertainment-leadership-vacuum-poor-studio-results-create-tension-insiders-say/
49 https://statescoop.com/philadelphia-transit-system-recovering-from-apparent-cyberattack/
50 https://www.inquirer.com/transportation/septa-malware-attack-employees-riders-app-announcements-20200824.html
51 https://www.fsmatters.com/employees-as-an-internal-cyber-threat
52 https://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf

53 https://www.justice.gov/usao-mn/pr/three-nigerian-nationals-indicted-international-cyber-fraud-conspiracy
54 https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf?mod=article_inline
55 https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/
56 https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine
57 (VB Q2)
58 (VB Q5)
59 (VB Q8, Q10)
60 (VB Q11)
61 (VB Q5)
62 https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma; https://www.gao.gov/key_issues/leading_practices_information_technology_management/issue_summary
63 https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma
64 https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma; https://www.gao.gov/key_issues/leading_practices_information_technology_management/issue_summary
65 https://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf
66 https://www.forbes.com/sites/daveywinder/2019/11/20/infection-hits-french-hospital-like-its-2017-as-ransomware-cripples-6000-computers/#343b5475576e
67 https://www.bbc.com/news/technology-49905226
68 https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
69 https://www.nature.com/articles/s41746-019-0161-6
70 https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
71 https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html
72 https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war
73 https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html
74 https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627
75 https://www.zdnet.com/article/security-warning-state-backed-hackers-are-trying-to-steal-coronavirus-research/
76 https://www.justsecurity.org/70293/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/
77 https://www.ic3.gov/media/news/2020/200728.pdf
78 https://www.ic3.gov/media/news/2020/200728.pdf
79 https://www.ic3.gov/media/news/2020/200728.pdf
80 https://www.ic3.gov/media/news/2020/200707-4.pdf
81 https://www.ic3.gov/media/news/2020/200707-4.pdf
82 The 2019 update to the Australia's Cyber Security Sector Competitiveness Plan by the Australian Cyber Security Growth Network found that the global cybersecurity market was worth around $145 billion.
83 https://www.itworldcanada.com/article/basic-security-measures-could-have-reduced-losses-from-cyber-attacks-says-insurer/435633
84 https://us-cert.cisa.gov/ncas/alerts/aa20-245a
85 https://www.zdnet.com/article/over-half-of-enterprise-firms-dont-measure-the-performance-of-their-cybersecurity-tools/
86 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200127_Cybersecurity_WEB%20FINAL.pdf?FIY72HCWMSJeH3BcIPmHkV65rE2xG3lR
87 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200127_Cybersecurity_WEB%20FINAL.pdf?FIY72HCWMSJeH3BcIPmHkV65rE2xG3lR
88 https://www.bankinfosecurity.com/equifax-whats-changed-since-2017-mega-breach-a-14950
89 https://us-cert.cisa.gov/ncas/alerts/aa20-099a
90 https://us-cert.cisa.gov/ncas/alerts/AA20126A
91 https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
92 https://www.cyberthreatcoalition.org/advisories/2020-05-04-weekly-threat-advisory
93 https://www.cyberthreatcoalition.org/advisories/2020-05-26-weekly-threat-advisory
94 https://pdf.ic3.gov/2019_IC3Report.pdf
95 https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic
96 https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic
97 https://transparencyreport.google.com/safe-browsing/overview?hl=en&unsafe=dataset:1;series:malware,phishing;start:1577836800000;end:1593561599999&lu=unsafe
98 https://www.npr.org/2020/04/03/826129520/a-must-for-millions-zoom-has-a-dark-side-and-an-fbi-warning
99 https://www.ic3.gov/media/2020/200401.aspx
100 https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic
101 https://www.judiciary.senate.gov/imo/media/doc/D'Ambrosio%20Testimony.pdf
102 https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/
103 https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware
104 https://www.ic3.gov/media/2020/200513.aspx
105 https://www.euractiv.com/section/digital/news/von-der-leyen-chinese-cyberattacks-on-eu-hospitals-cant-be-tolerated/

106 https://www.itprotoday.com/cloud-security/malware-taking-new-shape-malware-service
107 https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report
108 https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/
109 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
110 https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
111 https://digitalguardian.com/blog/tesla-data-theft-case-illustrates-danger-insider-threat
112 https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf
113 https://www.bleepingcomputer.com/news/security/phishing-as-a-service-fuels-evasion-methods-email-scam-growth/
114 https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service
115 https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202
116 https://www.zdnet.com/article/cyberattacks-against-industrial-targets-double-over-the-last-6-months/; https://www.infosecurity-magazine.com/news/manufacturing-ransomware-payments/
117 https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/#:~:text=Ransomware%20has%20been%20around%20for,IoT%20ransomware%20is%20relatively%20new.
118 https://www.bankinfosecurity.com/5-billion-unique-credentials-circulating-on-darknet-a-14596?rf=2020-07-13_ENEWS_SUB_BIS__Slot1_ART14596&mkt_tok=eyJpIjoiWldVMlpEYzFPVFExWTJVMCIsInQiOiJKSlVDNE4wSElGalMzUVNvTUxPcllrRU9HSytpb000R3Q4RFwvMFducjNFSVwvM081cE9nY1hvcHViV3N2V0xrR1JLRkZ3WDkzVkR4dDB0Y0xpZkdqb3R1OHpFb2ttMm1hamdOMzEwU1Z0eHBSUTQzdVU1d3JXekh2MkczSjRDb3hNIn0%3D
119 https://www.bankinfosecurity.com/5-billion-unique-credentials-circulating-on-darknet-a-14596?rf=2020-07-13_ENEWS_SUB_BIS__Slot1_ART14596&mkt_tok=eyJpIjoiWldVMlpEYzFPVFExWTJVMCIsInQiOiJKSlVDNE4wSElGalMzUVNvTUxPcllrRU9HSytpb000R3Q4RFwvMFducjNFSVwvM081cE9nY1hvcHViV3N2V0xrR1JLRkZ3WDkzVkR4dDB0Y0xpZkdqb3R1OHpFb2ttMm1hamdOMzEwU1Z0eHBSUTQzdVU1d3JXekh2MkczSjRDb3hNIn0%3D
120 https://www.bankinfosecurity.com/5-billion-unique-credentials-circulating-on-darknet-a-14596?rf=2020-07-13_ENEWS_SUB_BIS__Slot1_ART14596&mkt_tok=eyJpIjoiWldVMlpEYzFPVFExWTJVMCIsInQiOiJKSlVDNE4wSElGalMzUVNvTUxPcllrRU9HSytpb000R3Q4RFwvMFducjNFSVwvM081cE9nY1hvcHViV3N2V0xrR1JLRkZ3WDkzVkR4dDB0Y0xpZkdqb3R1OHpFb2ttMm1hamdOMzEwU1Z0eHBSUTQzdVU1d3JXekh2MkczSjRDb3hNIn0%3D
121 https://pdf.ic3.gov/2019_IC3Report.pdf
122 https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html
123 https://www.wired.com/story/mexico-bank-hack/
124 https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
125 https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/virtu-court-document.pdf
126 https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/virtu-court-document.pdf
127 https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/virtu-court-document.pdf
128 https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#1493a0a755f5; https://www.coindesk.com/crypto-criminals-have-already-stolen-1-4b-in-2020-says-ciphertrace
129 https://www.malwarebytes.com/cryptojacking/
130 https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/
131 https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/
132 https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/
133 https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620?utm_campaign=email-Daily&utm_medium=email&utm_source=stories&utm_content=%5B929332%5D-%2Fnews%2Fstories%2Fwray-announces-fbi-cyber-strategy-at-cisa-summit-091620
134 https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times-bigger-than-walmarts
135 https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-
136 https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity
137 https://securityintelligence.com/the-business-of-organized-cybercrime-rising-intergang-collaboration-in-2018/
138 https://www.mcafee.com/blogs/other-blogs/mcafee-labs/how-chinese-cybercriminals-use-business-playbook-to-revamp-underground/
139 https://ndic.gov.ng/wp-content/uploads/2020/03/NDIC-Quarterly-Q1-and-Q2-2019-Article-The-Impact-of-Cybercrime-on-The-Nigerian-Economy-and-Banking-System-.pdf
140 https://www.cybercrimejournal.com/LuongetalVol13Issue2IJCC2019.pdf

141 https://www.zdnet.com/article/vietnam-on-the-edge-of-becoming-a-mid-tier-cybercrime-hub/
142 https://www.cbsnews.com/news/evgeniy-mikhailovich-bogachev-the-growing-partnership-between-russia-government-and-cybercriminals-60-minutes/
143 https://home.treasury.gov/news/press-releases/sm845
144 https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states
145 https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary
146 https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf
147 https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_cyber_threat_advisory_20200415.pdf
148 http://www.bbc.co.uk/newsbeat/article/32926248/bureau-121-north-koreas-elite-hackers-and-a-tasteful-hotel-in-china
149 https://www.france24.com/en/20190808-cybercrime-north-korea-nuclear-programme-hacking-china-ballistic-missile
150 https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX
151 https://www.cbsnews.com/news/north-korea-skirted-un-sanctions-and-earned-2-billion-using-cyber-attacks-new-u-n-report-says/
152 https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges
153 https://www.nknews.org/2020/08/why-insurance-companies-might-be-stuck-paying-ransoms-to-north-korean-hackers/
154 https://www.justice.gov/opa/information-about-department-justice-s-china-initiative-and-compilation-china-related
155 https://soundcloud.com/csis-57169780/what-keeps-you-up-at-night
156 https://context-cdn.washingtonpost.com/notes/prod/default/documents/ed608b43-ebd6-434e-8819-88f496dfa10f/note/1e7f079b-6864-4353-acb5-f819b26c6bf7.
157 https://www.rollcall.com/2019/10/15/report-underground-hackers-and-spies-helped-china-steal-jet-secrets/
158 https://www.euractiv.com/section/digital/news/von-der-leyen-chinese-cyberattacks-on-eu-hospitals-cant-be-tolerated/
159 https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
160 https://olv.duke.edu/technologies/shared-threat-intelligence-for-network-gatekeeping-and-automated-response-stingar-threat-intelligence-for-higher-education/
161 Duke University, The STINGAR Project, https://stingar.security.duke.edu (This material is based upon work supported by the National Science Foundation under Grant Number NSF1815691 and Grant Number NSF1840034. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.) Authors: Richard Biever, Jesse Bowling, John Board, Mark Delong, Gagandeep Kaur, and Alex Merck. Those interested in learning more about STINGAR or joining the project are encouraged to visit the STINGAR Project site at https://stingar.security.duke.edu. (hereinafter "Duke University, The STINGAR Project, Biever et al.").
162 Duke University, The STINGAR Project, Biever et al.
163 Duke University, The STINGAR Project, Biever et al.
164 Duke University, The STINGAR Project, Biever et al.
165 Duke University, The STINGAR Project, Biever et al.
166 Duke University, The STINGAR Project, Biever et al.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

Methodology
McAfee commissioned independent technology market research specialist Vanson Bourne to undertake the research that this report is based on.

Between April and June 2020, the quantitative study was carried out, interviewing 1,500 IT and line of business decision makers. Respondents came from the US (300), Canada (200), the UK (200), France (200), Germany (200), Australia (200) and Japan (200). Respondents' organizations have 1,000 or more employees and were from all sectors except construction and property. However, only IT decision makers were interviewed in the Government sector.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Additionally, CSIS utilized a survey of open source material on losses accompanied by interviews with Government officials, and an estimate adjusted by national income levels using International Monetary Fund (IMF) income data to determine the cost of cybercrime.

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com