Chapter 7: Data—The Oil of the 21st Century

> If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.
>
> —*Richard Clarke*

Cyber Warfare and Cyber Attacks

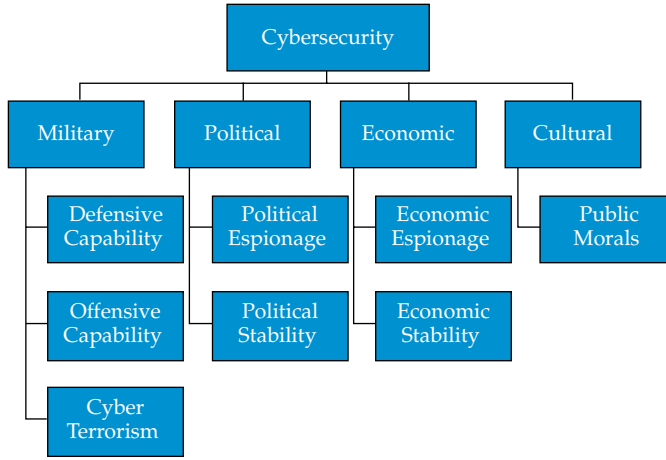
We live in a world where nearly every business is connected to the internet and more than one-half of the people on Earth have online access. This widespread access has opened up the possibility of stealing vital information from both private and public sources and of attacking organizations and putting them temporarily out of business. Cybersecurity has become a major concern in the military, political, economic, and cultural fields, as shown in **Exhibit 1**.

In the military and defense realm, cyber warfare is now a top issue, creating a constant shadow war and arms race between countries and state-sponsored actors. Cyber warfare takes several different forms. As a first line of defense, governments have increased their defensive capabilities and are monitoring the potential cyber vulnerabilities of the software and hardware used for military applications. For example, in 2017, a US Army memo to all service members required them to cease all use of drones from the Chinese company DJI and to uninstall all software from that company because of cyber vulnerabilities in their products (Huang, Madnick, and Johnson 2018). In 2019, the US Department of the Interior followed suit and grounded all drones from Chinese manufacturers, as well as any that contained Chinese parts, because of security concerns (Montague 2019). In 2018, journalists rang the alarm bell when they discovered that the software of a fitness tracking app allowed anyone to locate secret US military bases and follow the patrol routes of US military personnel (Hsu 2018).

But more and more countries are no longer restricting themselves to defensive measures alone. According to public testimony to the US Senate Committee on Armed Services by the then director of National Intelligence James Clapper, more than 30 countries have developed offensive cyber-warfare capabilities. Of course, however, he excluded the United States, making that more than 31 countries.

This chapter is from the book *Geo-Economics: The Interplay between Geopolitics, Economics, and Investments* by Joachim Klement, CFA. For more chapters, go to https://www.cfainstitute.org/en/research/foundation/2021/geo-economics.

Exhibit 1. Types of Cybersecurity Concerns



Source: Huang, Madnick, and Johnson (2018).

The list of cyber attacks by states is getting longer by the day. In 2017, Israeli intelligence officials infiltrated the Kaspersky Lab antivirus software and found evidence of Russian hackers using the software to spy on US businesses (Perlroth and Shane 2017). The cyber attacks of the Russian hacker groups Fancy Bear and Cozy Bear, both of which are widely assumed to be aligned with the Russian military intelligence service GRU, are too numerous to count. The Wikipedia pages for these two groups list 32 publicly discovered attacks (as of January 2021), not counting the ones that were never reported in the media.

The United States and Israel are widely thought to be the origin of the Stuxnet worm, first discovered in 2010, that attacked and damaged the Iranian nuclear program but then got out of control. Iran, in response, has created a cyber army that launched attacks against Israel in 2014 (Marks 2014), managed to create a 12-hour power outage in Turkey in 2015 that affected 40 million people (Halpern 2015), and hacked the email accounts of 90 members of parliament in the United Kingdom in 2017 (*Telegraph* 2017). After the 2019 drone attacks on Saudi Aramco facilities, the United States did not retaliate with missile strikes or any other traditional show of military force as it would have done in the past. Instead, it launched a cyber attack against Iranian infrastructure (Ali and Stewart 2019).

A third component of military cybersecurity concerns is the rising threat of cyber terrorism. Clapper, Lettre, and Rogers (2017) reported that international terror groups, such as the Islamic State, have sought to disclose information

about US citizens to trigger "lone wolf attacks." Terror groups from al-Qaeda to the Islamic State and the Taliban all use the internet to collect information and organize attacks. Some terror groups, such as Hezbollah and Hamas, already have had considerable success with their cyber attacks in the Middle East.

But cyber attacks are also used to try to achieve political goals. Political espionage, such as the Iranian attacks on British members of parliament or the attacks by Fancy Bear on German politicians in 2014 and 2015, are a constant threat to the political process. Increasingly, rather than trying to steal secrets, state-sponsored hackers try to spread misinformation and fake news to influence elections or undermine public trust in politicians and governments. The most prominent example is the alleged Russian operation to influence the 2016 US presidential election (Mueller 2019).

Numerous cybersecurity concerns also exist in countries that have restricted information in some areas of public interest. For example, in Germany, the sale of Nazi memorabilia is prohibited by law, and authorities therefore must monitor the internet for violations of this law and ban sites that offer such goods for sale. Singapore, Lebanon, and Turkey all ban pornographic and adult entertainment sites to protect public morals and maintain public order (Mitchell and Hepburn 2016).

Cyber Attacks Are a Major Business Risk. Although a deeper dive into the details of these cultural cybersecurity issues would be interesting, the focus for the remainder of this chapter will be on economic cybersecurity issues. Economic cyber attacks run the full spectrum from outright espionage, such as the cyber attacks on US engineering and maritime companies to steal intellectual property (FireEye 2018), to stealing data and money and undermining trust in the reliability and stability of information technology (IT) systems.

The list of cyber attacks on businesses is enormous. Coburn, Daffron, Quantrill, Leverett, Bordeau, Smith, and Harvey (2019) reported that a 2018 survey of 1,300 companies in the United States, Canada, United Kingdom, Mexico, Germany, Australia, Singapore, and Japan showed that two-thirds of respondents were targets of cyber attacks on their supply chain. Government entities seem to be less attractive targets, with only 49% reporting a supply chain attack, compared with 82% of biotech and pharmaceutical companies. If successful, these cyber attacks can cause substantial business interruptions:

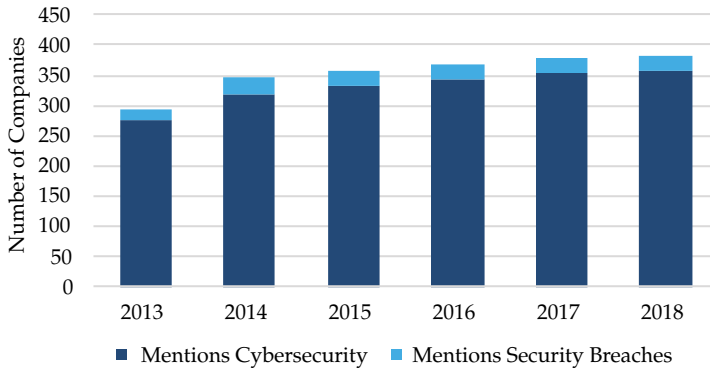
- In 2013, phishing emails stole passwords from a Target Corporation vendor and enabled the hackers to install malware in 1,800 stores. The data breach cost Target $200 million, and profits dropped 46% in the fourth quarter of 2013.

- In 2017, the NotPetya malware infiltrated the systems of a range of companies around the world, destroying hard disks and information. Cadbury reported damages of $147 million, Maersk Line of $300 million, and FedEx of $300 million.
- In 2018, the North Korean WannaCry ransomware infiltrated the network of Taiwan Semiconductor Manufacturing Company, causing damages of $170 million.

Kopp, Kaffenberger, and Wilson (2017) reported that the economy-wide cost of cyber attacks could be substantial. While the contribution of the internet to US GDP was estimated to be somewhere between 3.2% and 6.0% in 2015, the costs of cyber attacks could be anywhere between 0.6% and 2.2% of GDP. This means that in the worst-case scenario, the cost of cyber attacks could almost match the lowest estimate of the benefits of the internet.

Given these potentially large costs, cybersecurity, not surprisingly, increasingly is being discussed by investors and corporate analysts. **Exhibit 2** shows the number of companies in the S&P 500 Index that mentioned cybersecurity issues in earnings calls between 2013 and 2018. In 2018, almost 80% of the companies in the S&P 500 mentioned cybersecurity risks, and 26 companies mentioned security breaches in their systems. This public discussion of cybersecurity issues has two goals. First, businesses have to disclose material risks to their businesses. Given the potentially high cost of cyber attacks, addressing these risks in earnings calls is only natural. Second, and more important, businesses are trying to build public trust by openly discussing their investments in cybersecurity and their efforts to protect their businesses from malicious attacks.

Exhibit 2. Number of S&P 500 Companies Mentioning Cybersecurity in Earnings Calls



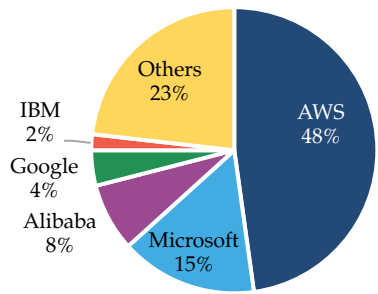
Source: Abbosh and Bissell (2019).

No matter how careful companies are in their efforts to combat cyber attacks, however, they remain vulnerable in two crucial areas. The market for cybersecurity services is dominated by a small number of suppliers, and a security breach in any one of the suppliers could immediately affect a large number of businesses around the world. The infiltration of the Kaspersky Lab software by Russian hackers mentioned earlier is one such example. Kaspersky Lab's anti-malware software is one of the top eight applications on the market, with a market share on Windows systems of 8.1% in 2019 (Liu 2019). In total, these eight providers of anti-malware software cover more than 80% of Windows PCs in the world.

Another area of external concentration risk is in the provision of vital data infrastructure. More and more software providers move their applications onto cloud-computing platforms that not only allow access to data from every mobile device and desktop PC anywhere in the world but also store data in the cloud. Globally, total spending on cloud infrastructure surpassed an estimated $500 billion in 2020, with one-quarter of all businesses spending more than $6 million on cloud services annually (Coborn et al. 2019).

The market for infrastructure as a service is dominated by Amazon Web Services (AWS), which had a market share of 48% in 2018 (Gartner 2019). This means that a severe data breach in Amazon's cloud services would immediately affect a significant share of internet businesses around the world, as **Exhibit 3** shows. In 2018, Amazon got a taste of its vulnerability when its cloud service experienced a series of outages that affected its online store and its Alexa assistant during Amazon Prime Day, the company's second-biggest shopping day of the year. The outages cost Amazon a reported $1.2 million in sales per minute of downtime (Coborn et al. 2019).

Exhibit 3. Market Share of Infrastructure as a Service



Source: Gartner (2019).

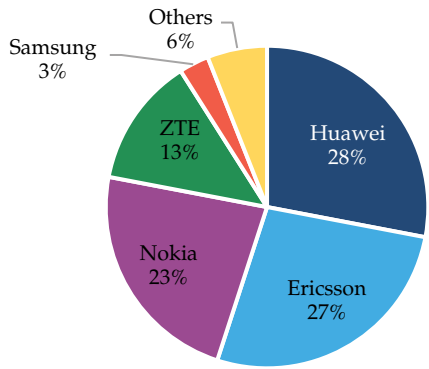
Case Study: From 5G to 6G

Another crucial area for cybersecurity in the coming decade will be the fast-developing communications infrastructure. Starting in 2019, 5G networks were being rolled out around the globe. As in the case of cloud computing, 5G infrastructure is a high-tech product that requires significant know-how and substantial capital to develop. Thus, as **Exhibit 4** shows, the market relies on four different companies, two Chinese (Huawei and ZTE) and two European (Nokia and Ericsson) for wireless telecom infrastructure. Huawei is not only the market leader for 5G infrastructure but also the only manufacturer in the world with sufficient factory capacity to roll out 5G networks in large countries.

Unfortunately, four major Western countries—the United States, Canada, Australia, and New Zealand—have banned Huawei from rolling out 5G networks in their countries because of security concerns (Bryan-Low, Packham, Lague, Stecklow, and Stubbs 2019). In the United Kingdom, Huawei is allowed to operate until 2027, at which point its infrastructure will be banned. Although no proof of Chinese espionage using Huawei equipment has been published, Huawei and other Chinese vendors of 5G technology remain under heightened scrutiny in other countries, including Germany, Japan, and Poland.

This boycott of Chinese hardware poses the risk of creating a technology bifurcation. Because Huawei is the market leader and until early 2019 was the only company with sufficient production capacity, large countries such as the United States face a potential delay of their 5G rollout, compared with China and other countries using Chinese equipment. This delay already puts

Exhibit 4. 5G Market Share Worldwide



Source: IHS Markit.

the United States and its allies on a backfoot, but it also could lead to the use of slightly different technology standards in the West than in China. Both Western companies and Huawei now have an incentive to develop slightly incompatible technological standards to close their markets to competitors.

As a result, the development of the next generation of wireless communication networks, the 6G standard, might move along different paths. When 6G technology is rolled out in the 2030s, countries could be forced to choose between Western and Chinese technology, thus cementing their economic alliances with either side in the form of crucial communication infrastructure.

To clarify the crucial role 6G networks will play over the next decade, we offer this brief introduction to the technology of communication networks.

The main difference between the current 4G, the new 5G, and the future 6G networks is the frequency of the electromagnetic signals they use to transmit information. The 4G networks typically use frequencies between 1 GHz (gigahertz; 1 billion oscillations per second) and 3.5 GHz. The 5G networks will use frequencies between 24 Ghz and 100 GHz. The 6G networks will go beyond that and use frequencies between 100 GHz and 400 GHz (Ma et al. 2018). The advantage of higher frequencies is that more information can be packed into the signal (i.e., offering higher information density), and thus more information can be transmitted per second.

To give you an idea of the difference the frequency makes on information transmission, consider that under the 4G standard, downloading a two-hour movie onto a smartphone that is working efficiently takes approximately 20 seconds. The transmission rate is approximately 150 Mbps (150 million bits per second). Under the new 5G standard, the transmission rate increases to up to 10 Gbps (10 billion bits per second), making downloading three movies in just one second possible. With 6G, the prediction is that it will allow transmission rates of up to 1 Tbps (1 trillion bits per second), which would allow users to download 300 movies in one second.

Obviously, nobody needs to download 300 movies in one second, but new technologies such as autonomous vehicles, a fully connected global Internet of Things (IoT), and artificial intelligence–powered communication technology will all need transmission rates that are beyond the capabilities of 5G (Lee 2019). Thus, if these long-term technological trends are to have any chance of being realized in the next decade, we need to make rapid progress in determining 6G technology standards and developing new hardware that can cope with these demands (Latva-Aho and Leppänen 2019).

These challenges are tremendous because of the nature of physics. Although higher signal frequencies allow higher transmission rates, the problem is that signal strength declines rapidly with distance for higher

frequencies. We are all familiar with this phenomenon in our daily lives when we listen to the radio. Radio signals have very low frequencies, which has the advantage that one can transmit the signal over long distances, and even if many houses or hills are between the sender and the receiver, the signal still arrives in sufficient strength to provide a good listening experience.

Light, in comparison, has much higher frequencies than radio waves, and a simple wall is sufficient to block the signal. In fact, something as ephemeral as water vapor can block light waves after a relatively short distance (that is what happens in a fog). With 6G networks, the first challenge to overcome is developing technologies that can transmit the signals outside a direct line of sight; otherwise, we would need antennas and repeaters literally every few meters in every village, town, and city.

Thus, over the coming decade, the technology race will focus on developing hardware that can combine high transmission rates with long range. Which company will be able to do this best is unclear. For 4G and 5G, the companies involved developed uniform global standards because they all knew they would have to compete with other businesses worldwide, and a unified technological standard would reduce costs. With Huawei boycotted by several countries, it could now design its own 6G infrastructure that is slightly incompatible with the infrastructure developed by Nokia and Ericsson, for example. This would prevent Nokia and Ericsson from competing with Huawei in China and other countries that use Huawei technology. And these slight technological differences would then manifest a slightly different standard for 6G applications in the West and in China, which in turn might affect the ability of businesses to run their applications and software on different 6G networks.

In short, just as railway lines with different gauges hindered international trade and globalization in the 19th century, and differences in radio frequencies forced listeners in different countries to buy different kinds of radios in the 20th century, differences in the communications architecture may hinder trade in the 21st century.

The Vulnerability of Modern Infrastructure

Different technological standards in communications infrastructure not only imply less competition between businesses but also create differences in vulnerability to cyber attacks. Malicious software could damage the infrastructure of one provider but not the other, opening up the possibility for both state-sponsored and private actors to design malware that specifically targets the infrastructure of a single country or an individual provider. Communication infrastructure such as 5G and 6G networks are just a small

part of the overall critical infrastructure in a country, but such infrastructure is increasingly interconnected with traditional infrastructure, such as the power grid. Power stations are monitored using modern data technologies, and drones are used to check nuclear and fossil fuel power plants for damage on a routine basis. The signals of these drones are submitted to ground stations using standard 4G and 5G communications networks.

Already today, with globally standardized infrastructure, a successful cyber attack on a country's electricity grid is probably the biggest economic cybersecurity threat imaginable. To understand how severe the economic impact of a successful cyber attack on a country's electric grid could be, the Cambridge Judge Business School's Centre for Risk Studies interviewed dozens of experts to develop three potential scenarios for a cyber attack on the UK electricity grid (Kelly et al. 2016). This exercise provided an instructive example of the potential economic damage of such a cyber attack on industrial countries around the world.

The difficulty of launching a successful large-scale cyber attack on a nation's infrastructure is that it requires enormous know-how, so at present, doing so seems possible only for state-sponsored actors. Having said that, the previous example of the successful infiltration of Turkey's power network by Iranian agents and the subsequent 12-hour power outage in Istanbul and Ankara reveals that such an attack is not beyond the reach of existing state-sponsored entities. While the Iranian attack on the Turkish infrastructure was short-lived, a more devastating attack is possible. The risk is particularly high if the foreign agent is able to penetrate a country's infrastructure with a Trojan Horse that is not immediately recognizable as malware and can spread within the compromised system and then be activated at will (something that the US–Israeli malware Stuxnet did successfully in Iran).

The potential severity of the impact of malicious software can be seen from the 2003 Northeast Blackout, which hit the United States and Canada. In August, a high-voltage cable in Ohio caused a short in the local grid system. Because of a software bug, the local grid operator, FirstEnergy, did not receive the signal that the grid was down, and electricity was not redirected from the local grid to other grids. This triggered a chain reaction that eventually caused total power failures across the Northeastern United States and the southeast of Canada. Over the subsequent two weeks, a total of 55 million people, among them the entire New York City and Toronto metropolitan areas, faced recurrent power outages, a lack of water supply, and potential contamination of drinking water.

One could even imagine that in a state-sponsored cyber attack, a disgruntled employee of National Grid (the government entity responsible for

the electric grid hardware in the United Kingdom) could act as a spy for the foreign power and install small pieces of hardware in many different substations in a region (substations are the transformers that change the voltage in the high-voltage power cables used for transmission over long distances to the lower voltages used in factories and households).

In this case, a cyber attack would be even more difficult to stop because the individual pieces of hardware at each substation would need to be identified and disabled manually. Because electric substations are regularly checked for vulnerabilities and physically maintained by trained technicians, the attackers would have to be sophisticated enough to install software or hardware that could remain undetected for weeks before it could be triggered simultaneously. A sequential triggering would likely do no harm to the electric grid thanks to the inherent redundancies in the system that avoid a power outage if the individual substations fail.

The Impact of a Massive Cyber Attack on London. As a base case, the Cambridge Judge study assumed three different scenarios for power outages in substations in and around London, targeting the United Kingdom's economic center, as shown in **Exhibit 5**:

- Scenario S1 is a limited attack that takes approximately 3 weeks to compromise 65 electric substations in and around London and triggers a rolling power outage lasting for approximately 1.5 weeks in total.
- Scenario S2 is a more comprehensive attack that has approximately twice the regional footprint, compromises 95 substations, and lasts approximately 3 weeks before it can be resolved.
- Extreme scenario X1 compromises 125 substations for 6 weeks, including those that serve Heathrow Airport, London's largest airport and a major international traffic hub.

Exhibit 5. Scenarios for Cyber Attacks on UK Infrastructure

Case	Type	Number of substations compromised	Length of cyber attack (weeks)	Length of power outage (weeks)
S1	Optimistic case/ quick recovery	65	3	1.5
S2	Conservative case/ average recovery	95	6	3
X1	Extreme case/ slow recovery	125	12	6

Source: Kelly et al. (2016).

In all three scenarios, the power outages in the substations are launched simultaneously, while malicious software in the system is able to spoof the signal to the control center so that no power outage is detected until customers without electricity start to complain in large numbers to the utility company. Because the control center cannot detect the power outage, it must send a field team to the affected substation, taking valuable time.

Once there, the technicians would not likely have the required expertise in cybersecurity to immediately detect the nature of the problem and the malicious hardware. The field team probably would be able to connect power manually after several hours of work, but only after several substations failed would it become clear that this was not an isolated incident; expert teams would then be sent out to identify the problem. Expert engineers sent to the failed substations then would be able to identify the outage as a cyber attack within 12 to 48 hours and determine a quick fix to override failed substations. The malicious hardware in the substations, however, likely would not be found in such a chaotic situation, enabling the attackers to trigger additional power outages over multiple days.

The repeat rolling blackouts would clearly reveal that the cyber attack is not just a software attack but also relies on hardware, thus triggering a search for hardware in the substations. Within several days to one week, the malicious hardware should be detected, starting a chase to find all the installed malicious hardware across the region.

Because correctly identifying the problem takes several days and then removing the malicious hardware takes several days or weeks, the power outages would affect a large number of people. In the most benign scenario, S1, up to 8.9 million people in the United Kingdom would be without electricity on any given day, as **Exhibit 6** shows. Mobile phone connections and other digital communications would be down for up to 8.6 million people at any given time. Because water utilities could not operate properly because of the power outages (water typically is transported to consumers by electric pumps), the freshwater supply would be disrupted for up to 7.9 million people at any one time, and wastewater removal would be compromised for up to 9.6 million people. Given the size of these disruptions, they would likely create significant chaos in London and its surrounding areas, and the military would need to step in for disaster relief to prevent the spread of diseases.

In the more severe scenario, S2, the situation would be even worse, cutting power for up to 11.3 million people and disrupting wastewater disposal for up to 11 million people. In the most extreme X1 scenario, power would be cut for up to 13.1 million people for up to six weeks, causing severe risk of civil unrest. In each of the three cases, approximately one million railway journeys

Exhibit 6. Peak UK Customers Disrupted in an Infrastructure Cyber Attack

Case	Electricity (millions)	Digital communication (millions)	Water (millions)	Wastewater (millions)
S1	8.9	8.6	7.9	9.6
S2	11.3	11.3	10.4	11.0
X1	13.1	12.8	11.8	12.6

Source: Kelly et al. (2016).

a day would be disrupted, bringing London effectively down to walking pace as commuters either stay home or are forced to walk to work. An estimated 150,000 airline passengers per day would see their flights canceled or severely delayed, except in scenario X1, where the successful attack on Heathrow Airport would more than double this number. The traffic disruptions also imply that the processing of agricultural imports would be delayed, creating the possibility of temporary shortages of certain foods in and around London.

The economic costs of such a cyber attack on the electric grid would be tremendous. In the most benign scenario, S1, direct costs to the UK economy are estimated to be £7.2 billion, and knock-on effects from business disruptions would cause another £4.4 billion in costs, for a total cost of £11.6 billion or 0.4% of UK GDP, as shown in **Exhibit 7**. Note that scenario S1 assumes that this cost is due to a relatively brief disruption of the London infrastructure for several hours a day for approximately 1.5 weeks. Because London's financial sector is large, targeting the electric grid would cause the biggest losses to the financial sector. Direct and indirect losses to the financial sector in scenario S1 would add up to an estimated £1.3 billion, compared with £1.2 billion for the retail sector and £700 million for the health-care sector.

For the more severe scenario, S2, with a disruption of business for approximately three weeks, the total costs to the UK economy would be roughly three times as much and sum to £29 billion, or 1.1% of UK GDP. For the most extreme scenario, X1, the costs of six weeks of power disruptions would amount to 3.3% of UK GDP.

Moreover, in each of these cases, the economic shock likely would spread over time. Higher unemployment, lower consumption, a loss of international trade and tourism, and a significant decline in consumer and business confidence all would conspire to lower economic growth in the quarters and years to come. Kelly et al. (2016) estimated that in scenario S1, the economy would return to trend growth after approximately two years, while in the other two scenarios, the recovery could take up to five years. The total lost output over five years is expected to be £49 billion (1.9% of GDP) in scenario

Exhibit 7. Economic Losses to the United Kingdom from a Cyber Attack on the Electric Grid

Case	Direct losses (£ billions)	Indirect losses (£ billions)	Total losses (£ billions)	% of GDP
S1	7.2	4.4	11.6	0.4
S2	18.0	10.9	29.0	1.1
X1	53.6	31.8	85.5	3.3

Source: Kelly et al. (2016).

S1, £129 billion (4.9% of GDP) in scenario S2, and £442 billion (16.9% of GDP) in scenario X1. In short, scenarios S2 and X1 likely would cause a recession in the United Kingdom, while scenario S1 could push a weak UK economy into recession.

The Cost of Data Breaches for Private Companies

A successful cyber attack on critical national infrastructure is a tail risk, but private businesses have to deal with a constant barrage of small-scale attacks every day. Most of these attacks are launched not by state-sponsored actors or sophisticated hacker groups but instead by criminal groups motivated by money. Increasingly, these criminals do not even have to use malicious software to perform their attacks. Coburn et al. (2019) reported that since 2018, an increase has been seen in so-called living-off-the-land tactics that exploit security loopholes in existing software, such as operating systems, and commonly used office software packages. Such attacks cannot be prevented by traditional anti-malware software because they do not deposit code on the targeted systems, and they reduce the risk of legal ramifications for criminals because tracing their origins is more difficult.

Meanwhile, buying malware on the dark web has become cheaper and cheaper, so that even mildly talented hackers can now launch successful attacks against corporations, multiplying the number of potential attacks. Traditional malware software kits can be bought for $600 to $10,000 per month, while zero-day attack kits that enable living-off-the-land attacks cost from $20,000 for Mac OSX operating systems to $80,000 for Google Chrome and Internet Explorer software.

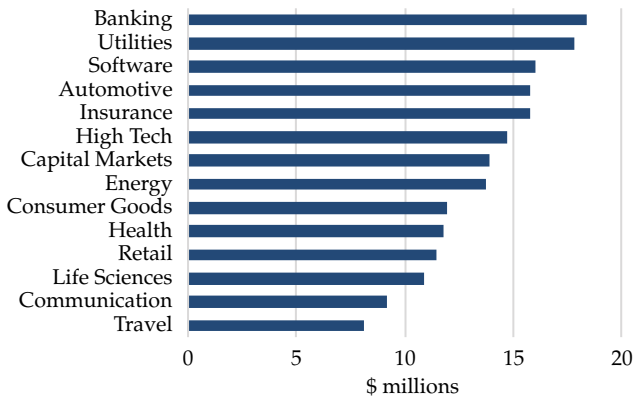
Given this proliferation of cybercrime, the costs for businesses are rising fast. Bissell and Ponemon (2019) reported that each business globally had to deal with an average of 145 successful security breaches in 2018. Successful security breaches were defined as instances when criminals were able to overcome a company's usual firewall defenses and infiltrate their systems.

As cyber attacks and security breaches become more common, the costs for businesses increase rapidly. In 2018, banks were the preferred targets of cybercrime and incurred costs of approximately $18.4 million per company per year. As **Exhibit 8** shows, the damage to other industries is not far behind. Utility companies are another popular target of cybercriminals because of the potential damage that can be caused by shutting down vital infrastructure, and the costs per utility company averaged approximately $17.8 million in 2018. Software, high-tech, and automotive companies typically are targeted by cybercriminals to extract information and customer data that can be used for malicious purposes.

A company's average loss from cybercrime in 2018 was an estimated $13 million, up 12% from the previous year and up 72% in five years (Bissell and Ponemon 2019). The biggest component of these losses was the loss of information (either by losing client data or losing important internal information), which accounted for almost one-half of the losses incurred from security breaches. Business disruption accounted for roughly one-third of the losses, while lost revenue (e.g., from lost customers or lost bids for new orders) accounted for one-fifth of the losses, as **Exhibit 9** illustrates.

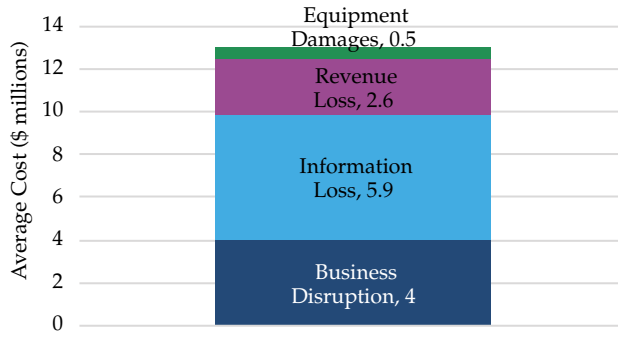
Although the cost for an average company per year does not sound like much, we have to remember that these statistics are averaged over thousands of companies worldwide. Abbosh and Bissell (2019) added everything up and estimated that the total economic loss for global business in the five years from 2019 to 2023 was approximately $5.2 trillion—approximately 2.8% of global corporate revenue and roughly equal to the GDP of the economies of France, Italy, and Spain combined. The estimated forgone revenue over

Exhibit 8. Average Annual Cost of Cybercrime per Company, 2018



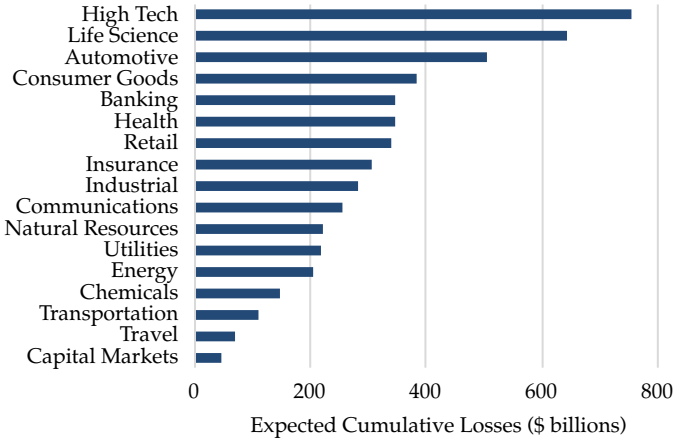
Source: Bissell and Ponemon (2019).

Exhibit 9. Business Impact of Cybercrime



Source: Bissell and Ponemon (2019).

Exhibit 10. Estimated Forgone Revenue Due to Cybercrime, 2019–2023



Source: Abbosh and Bissell (2019).

five years was particularly high for high-tech companies ($753 billion), life sciences ($642 billion), and automotive companies ($505 billion). With the exception of the travel industry and capital markets service providers (stock exchanges and so forth), every industry faces revenue losses from cybercrime in excess of $100 billion over five years. **Exhibit 10** illustrates this finding.

Do Stock Markets Care about Security Breaches?

The majority of security breaches lead to small or insignificant losses for a business. As a result, even those security breaches that are publicly announced

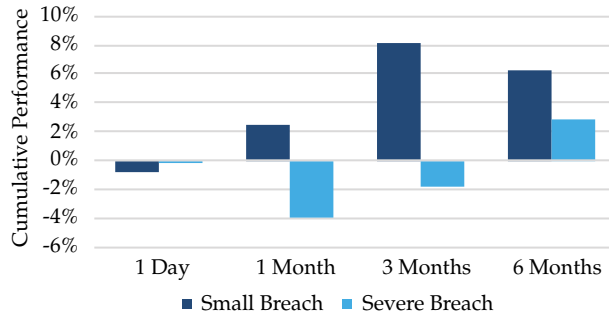
but not consequential for the business at hand likely do not affect a company's share price for long.

Bischoff (2020) collected information on a series of publicly announced security breaches that led to data losses and business disruptions in US listed companies between 2008 and 2018. We replicate this analysis in **Exhibit 11** and differentiate between small- and midsize security breaches, on the one hand, and severe security breaches, on the other. On the actual day of the announcement, the average stock market reaction was rather muted, with a decline in the share price of less than 1%. In the case of small security breaches, that was about what happened. The share price of companies affected by such smaller breaches was virtually indistinguishable from the share price development of companies unaffected by security breaches.

In contrast, severe security breaches can depress the share price of affected companies for several months. One month after the announcement of a severe security breach, the share price of an affected company declined by 4% on average, and after three months, it was still approximately 2% lower. A major driving force behind this delayed share price reaction after severe security breaches is that the main impact on the business in the medium term seems to be a loss of client trust and hence a loss of business that materializes slowly over time.

Abbosh and Bissell (2019) calculated the average revenue growth of companies affected by severe security breaches in the eight quarters after a breach and compared it with the average revenue growth of companies in the same industry that were not affected by cybercrime. The authors covered the time period 2013 to 2018 and selected 460 unique events in 432 companies worldwide. In the two years after a severe security breach, corporate revenues first declined by approximately 10% on average and then recovered slowly.

Exhibit 11. Share Price Response to Data Breaches



Source: Bloomberg; Bischoff (2018).

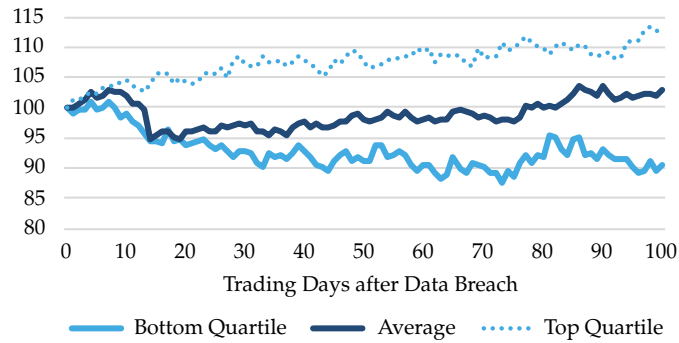
After two years, revenues had returned only to the same level they were when the security breach happened. Meanwhile, the revenues of companies that did not suffer a security breach increased by almost 20% in the same time period.

These averages can disguise big individual differences. **Exhibit 12** shows the average share price development in the six months after a severe security breach, along with the top quartile stocks in the sample and the bottom quartile stocks in the sample. Note that every stock in the sample suffered a severe security breach at time 0 in Exhibit 12, but the companies that saw a significant impact on their business (e.g., through declining revenues or declining profits after a need to invest heavily in IT security) could see their share price drop by 10% or more over six months.

In those extreme cases, the share price could remain depressed for a long time, and losses to investors could be substantial. An example case is the October 2015 leak of consumer data at T-Mobile US, which led to the loss of crucial private information of T-Mobile US customers, including Social Security numbers. Another example is the leak of 1.5 million credit and debit card numbers of customers of Global Payments Systems in 2012. In both instances, customer trust in the companies was shaken, leading to a significant decline in share price.

That markets pay careful attention to the details of a security breach can be seen in the case of Sony. On 26 April 2011, Sony announced that 77 million accounts on the Sony PlayStation Network had been compromised, and some credit card data had been leaked. In response to this leak, Sony shares dropped 31% over the subsequent six months and underperformed the NASDAQ by 23%. On 24 November 2014, Sony announced that 10 million employee records had been hacked over the previous year, leading to the loss of some

Exhibit 12. Share Price Response to a Severe Data Breach



Source: Bloomberg; Bischoff (2018).

Social Security numbers. Apparently, employee records do not count for much because Sony's share price was unaffected by this announcement and rallied 42% in the subsequent six months, outperforming the NASDAQ by 37%.

Could Cyber Attacks Cause a Financial Crisis?

A particularly attractive target for cybercriminals and state-sponsored hackers is the financial system. People like to rob banks because that is where the money is. Given the global financial system's high reliance on the internet and IT in general, the modes of attack and the potential targets are manifold:

- The most basic attack is a distributed denial of service (DDoS) attack on a bank, central bank, or service provider. In a DDoS attack, a large number of bots sends so many requests to a website, or to a server belonging to a financial service provider, that it becomes overwhelmed and crashes or grinds to a halt. Disruptions from DDoS attacks are typically short-lived and cause limited damages. For example, on 10 and 11 August 2011, the Hong Kong Stock Exchange news page suffered a DDoS attack. As a result, the trading of seven stocks had to be suspended because on these two days, the companies reported quarterly results that could not be published properly. Another example is a DDoS attack on three banks in Finland (i.e., OP-Pohjola, Danske Bank, and Nordea) in 2014. Their webpages and systems were disrupted, and online services became temporarily unavailable. One bank could no longer process card payments or cash withdrawals from ATMs (Bouveret 2019).
- Payment fraud using the SWIFT system for interbank payments has become a more popular and lucrative way to attack banks. In these attacks, the SWIFT system is hacked, and a fraudulent order to transfer money to an emerging market bank is sent to the victim's account. The most prominent example of such an attack is the attempt by North Korean hackers to steal $951 million from the central bank of Bangladesh. In the end, the hackers managed to steal *only* $81 million, of which $15 million could be recovered (Corkery and Goldstein 2017). Another incident happened on 24 May 2018, when more than 9,000 computers and 500 servers of Chile's largest bank, Banco de Chile, crashed as hackers tried to steal money from the bank through its SWIFT system. The hackers previously had tried to steal $110 million from Mexico's Bancomext. In the case of the Chilean attack, the losses amounted to an estimated $10 million (Cimpanu 2018).
- The potentially most harmful attacks are those targeting central banks. In 2010, a data breach at the Federal Reserve Bank of Cleveland led to the

loss of details of 122,000 credit cards, while that same year, the Federal Reserve Bank of New York lost proprietary software worth $9.5 million to hackers in a data breach. In 2013, $13.3 million was stolen from the account of the city of Riobamba at the Central Bank of Ecuador, and thieves who launched 21 cyber attacks on the central bank of Russia tried to steal $50 million in 2016 but managed to steal *only* $22 million (Bouveret 2019).

What makes cyber attacks on banks and financial institutions so treacherous is that the financial system is dependent on a highly complex system of interconnected networks with a few central data hubs. The interconnectedness of the financial network means that cyber attacks targeted in one area or at one company can get out of hand and cause significant damage at other institutions. In June 2017, ransomware targeted at Ukrainian companies spread across the border and caused damages in excess of $1.3 billion to international corporations that had business links with Ukraine. In the financial system, the disruption of one major bank could spread across the system if the bank is a counterparty to other banks in financial transactions, creating liquidity and solvency risks.

Alternatively, central hubs such as clearing houses are charged with reducing counterparty and liquidity risks in the derivatives markets. If a clearing house can be put out of service for a prolonged period, millions, if not billions, of derivative contracts might not be able to be settled, creating large uncertainties and counterparty risks across the system. In the worst-case scenario, a successful cyber attack could take a major central bank offline for an extended period, making it difficult or even impossible for commercial banks to cover their liquidity needs. In this case, international central banks might be able to act as interim lenders, but they typically do not have the required data to directly distribute funding to foreign commercial banks. In effect, such a situation would call for an emergency system in which international central banks would provide funding for the largest international financial institutions. In turn, these financial institutions would act as replacement central banks and distribute this liquidity to their business counterparts where needed.

These extreme examples of a disruption of the global financial system demonstrate that a financial crisis could be triggered by cyber attacks. Traditionally, the triggers of a financial crisis are as follows:

- excess leverage in parts of the economy (e.g., the high amount of mortgage debt that triggered the housing crisis and the global financial crisis of 2008, more than a decade ago);

- disruptions in the bank's maturity transformation business (e.g., a run on the bank for cash or short-term financing could leave banks unable to liquidate illiquid long-term assets, as was the case for the British bank Northern Rock in 2007); and
- the procyclical lending behavior of banks that reduces the price of risk (e.g., the willingness of US savings and loan institutions to invest in high-yield bonds in the late 1980s, leading to the savings and loan crisis).

Today, we face an additional trigger for a financial crisis through cybersecurity breaches.

Healey et al. (2018) showed how cybersecurity breaches potentially could lead to a financial crisis through four channels:

- The financial system relies on a few key hubs that process international payments, clear financial contracts, and safeguard assets. A major disruption of any of these key hubs could lead to a widespread breakdown of daily financial activities.
- A breakdown of such key hubs, or more regular but limited outages of everyday banking services such as internet banking or cash withdrawals from ATMs, could undermine public trust in financial institutions and trigger a bank run or significant flows of customer assets from one bank to another, which in turn could lead to a bank default.
- The financial system relies heavily on sensitive customer data. If these data are compromised (not necessarily stolen but maybe just deleted from a bank's system), many banking services will be unavailable for a prolonged period. The restoration of compromised data is typically possible but can take days or even weeks, during which time a bank would not be able to perform some of its services, causing significant economic damage and a severe loss of trust on the part of customers.
- Banks increasingly rely on cloud-based software and, as we have seen, the communication infrastructure is highly centralized and concentrated as well. Thus, an outage of major cloud-computing providers could lead to banks being unable to provide everyday customer services.

Worse yet, unlike traditional triggers of financial crises, cyber attacks can be timed to cause maximum damage. Theoretically, a cyber attack could be so devastating that it could take a central bank or a major clearing house offline for several weeks, triggering a liquidity crisis and even a solvency crisis. It might be easier for criminal actors to instead wait until the financial system is already under stress (say, in a recession or a minor financial crisis) and

then attack vulnerable financial institutions to exacerbate the crisis. In such an environment, trust between financial institutions already would be low. An added cyber attack could create a virtual run on banks that would erode the remaining trust between banks, in a manner similar to the events of autumn 2008, when banks became unwilling to lend to one another in the wake of the Lehman Brothers collapse. Because no one knew who would be next to default on their short-term obligations, banks simply stopped doing business with other banks where possible, and the entire system almost ground to a halt.

Cyber Attacks on Banks Could Be Very Costly for the Entire Economy. The economic losses of such cyber attacks on banks are extremely hard to estimate because they depend very much on the circumstances in which the cyber attack is performed and the nonlinear second-round effects of the attacks (i.e., how quickly and how widely the attack spreads). Bouveret (2019) tried to model the likely impact of such cyber attacks on banks in four scenarios. The "baseline scenario" is one that assumes that cyber attacks happen randomly at the frequency observed between 2011 and 2016 and follow a fat-tailed distribution. In the "severe scenario," the likelihood of an attack happening is approximately twice that of the 2011 to 2016 average. The baseline scenario and the severe scenario assume that cyber attacks remain confined to the targeted financial institution. In a second simulation, Bouveret (2019) assumed that the chance of contagion from one bank to the next is 20%.

Exhibit 13 shows the average loss for the global banking system in the simulations with and without contagion. The baseline scenario without contagion leads to average financial losses to the global financial system of $97 billion, or 9% of the net income of banks worldwide. The losses in any given year would, in 1 instance out of 20 (i.e., a 5% value at risk [VaR]), exceed $147 billion (14% of net income), and the expected shortfall in these cases would be $187 billion, or 18% of net income. Although these numbers look big, they are a fraction of the operational losses banks suffer worldwide, which are estimated at $260 billion to $375 billion each year.

In the severe scenario, however, the potential losses from cyber attacks multiply and become the same as, if not bigger than, operational losses. In the severe case, the average expected loss for banks per year is $268 billion, or 26% of net income, whereas the chance of losses exceeding $352 billion is 5%. In this case, the expected shortfall would be $409 billion. If the cyber attacks are allowed to spread to other banks and institutions, the estimated losses and shortfalls are typically approximately 20% higher, which reflects the 20% likelihood of contagion built into the model.

Given these significant risks to the financial system and the economy overall, financial regulators have focused increasingly on cybersecurity as

Exhibit 13. Estimated Risks from Cyber Attacks on Banks

	Baseline		Severe	
	% of net income	$ billions	% of net income	$ billions
Average loss	9	97	26	268
VaR (95%)	14	147	34	352
Est. shortfall (95%)	18	187	40	409
	With contagion			
	Baseline		Severe	
	% of net income	$ billions	% of net income	$ billions
Average loss	12	127	34	351
VaR (95%)	18	184	43	446
Est. shortfall (95%)	22	229	49	509

Source: Bouveret (2019).

a pillar of financial stability. In June 2016, in conjunction with the Bank for International Settlements (BIS), the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions, the global regulator of payments and securities regulators,[1] issued "Guidance on Cyber Resilience for Financial Market Infrastructures," a document detailing its members' cybersecurity risks and potential ways to mitigate these risks. In 2017, the BIS published reports on the progress made in four jurisdictions, and in the United States, the Financial Stability Oversight Council recommended practical solutions, such as sharing of cybersecurity information between banks and the regulatory harmonization of a risk-based approach to estimate cybersecurity risks.

Major US banks created the Financial Services Information Sharing and Analysis Center (FS-ISAC), which, together with the Payments Risk Council, performs yearly simulations of cyber attacks against payment processes. In recent years, the efforts of the FS-ISAC to prepare for cybersecurity risks have expanded beyond the borders of the United States and now include banks in Europe, Asia, and Latin America. To date, the efforts to protect the financial system are clearly limited, particularly when compared with the increasing importance of cybersecurity.

[1]Yes, regulators have regulators, too.

Blockchain to the Rescue?

Given the rising cybersecurity threats in all areas of the modern economy and the need for the secure transaction of data, we need to devise solutions that are safer than the existing ones. Currently, IT systems are primarily set up in a centralized way, in which a central cloud or a server stores important data. These data are then accessed by individual machines around the world that are connected to the central server by a private or public network. This setup means that if the central server is compromised or taken over by a malicious actor, the entire system is instantly compromised.

Blockchain technology promises a solution to this major vulnerability. In the early 1990s, Haber and Stornetta (1991) created a method to digitally timestamp a document with the help of cryptographic blocks. This method was further developed over time and led to the modern blockchain approach invented in 2008 by the anonymous author who called himself Satoshi Nakamoto in his bitcoin white paper. Bitcoin was the first application to use modern blockchain technology, but cryptocurrencies such as bitcoin are only a small part of the range of blockchain applications.

The basic idea behind blockchain is to create a database that is not centralized but instead is distributed among all the participants who have access to it. To create a blockchain, each participant (commonly called a "node") in the network creates two encryption keys: (1) a public key, which is used by participants to "encrypt" messages and data sent around the network, and (2) a private key, which is used by each participant in the network to "decrypt" the data. Changes made to the database by the different participants are combined in "blocks" that are then encrypted using the public key and sent to neighboring participants in the network. Thus, the blocks are spread around the network through the individual participants and not through a central server.

Once a block is full, individual participants in the network perform what is called a "proof-of-work" operation—essentially a massive number-crunching exercise to provide a verification that the block is genuine. Proof-of-work operations usually are made by brute force and thus are computationally intensive, but they create a solution that is easy to check, thus facilitating verification. This is a crucial step in the blockchain because fraudulent or manipulated data would lead to the incorrect solution and thus a rejection of the block by the other members of the network. Once a member of the network has successfully performed a proof-of-work operation, the solution is sent around the network. If more than one-half of the participants accept the solution, the block is added to the database, and a new block is opened (hence

the name "blockchain"). Once a block has been admitted to the blockchain, it can no longer be altered, providing a permanent record of past transactions.

The blockchain approach offers three advantages:

- The blockchain is decentralized; the entire database is copied to each participant in the network and does not rely on a central server or infrastructure.
- The blockchain is transparent; each participant has a copy of the entire database on her computer, and all past actions can be tracked through the timestamps of the past manipulations saved in each block. These timestamps allow past manipulations made to the blockchain to be traced back to the very first day. At the same time, participants are anonymous in the blockchain because the timestamps are unique to each participant, but the cryptographic keys are not linked to real-world identities.
- The blockchain is secure; changing the data in the chain would lead to a faulty proof-of-work operation and a rejection of the block. Once a block is admitted to the chain, it can no longer be altered.

These three advantages of blockchain technology allow the creation of "smart contracts" and "smart properties," which are secured by blockchains but can be changed as needed by the participants.

The first applications for blockchain were in the financial space with cryptocurrencies such as bitcoin, but applications in finance and in health care, for which data protection is crucial, have since mushroomed. Nevertheless, criminals were—as usual—the first to adopt this technology because it allowed anonymity. Today, black markets for drugs and guns on the dark web operate using cryptocurrencies as payments, while ransomware used in cyber attacks usually demands payment in cryptocurrencies as well (Taylor et al. 2020).

Legal and desirable applications for blockchain are likely to grow exponentially over the coming decade, given that the financial and health-care industries are not the only ones with a need for the safe storage and transmission of data. Fernández-Caramés and Fraga-Lamas (2018) demonstrated that the demand for blockchain applications in the IoT is likely to rise. Smart contracts, primarily based on the Ethereum blockchain technology, execute themselves automatically when certain conditions are met. Such smart contracts can be used in international trade and logistics, particularly with emerging markets, in which traditional credit checks and bank connections are less trustworthy, or with mortgages or in crowd-funding activities, in which monies are released only for specific purposes and when certain conditions are met.

In the future, blockchains will be helpful in such IoT applications as sensing, intelligent transportation, and smart living applications. In agriculture, blockchain technology can enhance food safety by tracking farm animals and feed from a farm to the supermarket and consumer tables. Smart grids rely on blockchain technology to protect against malicious attacks against vital infrastructure, such as the electricity grid or power stations.

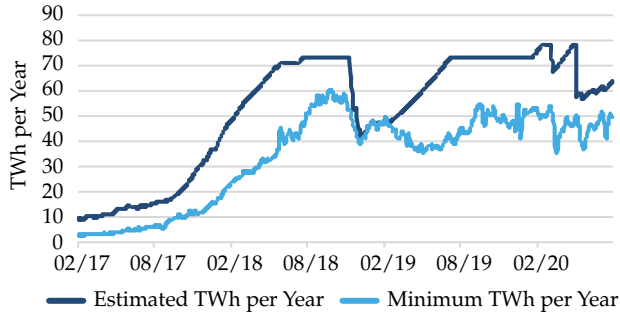
Indeed, Taylor et al. (2020) showed that from a cybersecurity perspective, IoT applications likely will be the main driver for the adoption of blockchain technology. Thus far, blockchain technology has been used in IoT applications to increase data security and to enable a decentralized deployment of firmware, which can be distributed from application to application without the need for a central server. The firmware cannot be manipulated by individual applications because of the blockchain technology, thereby preventing the manipulation of software. Data can be stored securely in a decentralized way or in a central cloud, where access is given only to members of the network with the right blockchain credentials.

Blockchain technology also can be used to protect local wireless systems by storing and monitoring access to the system in a local database. Finally, a manipulation of the web through the Domain Name System (DNS) is impossible if DNS entries are protected by blockchain technology. Thus, malicious actors can no longer hijack a website or a webserver by manipulating the DNS entry of the webpage in a central database.

Blockchain technology also has limitations, however, that make it difficult if not impossible to use in some applications. Most important, many blockchains are incredibly complex and energy intensive. Bitcoin, for example, has a theoretical maximum of seven transactions per second. VisaNet, Visa's electronic payment system, in contrast, can handle up to 24,000 transactions per second. The volume of transactions needed to drive the global system of credit and debit cards alone is way beyond the limitations of blockchain technology as we know it today (Stinchcombe 2018).

Furthermore, because blocks constantly are added to the chain, the storage space requirements grow quickly. In 2019, the length of the bitcoin blockchain surpassed 250 GB. According to *Digiconomist*, mining bitcoin consumed 73 terawatt-hours or trillions of watt-hours (TWh) of electricity—approximately the same as the annual electricity consumption of Austria—and created a carbon footprint of 34.7 megatons of CO_2, approximately the same as Denmark. Per transaction, bitcoin consumed 641 kilowatt-hours (kWh) of electricity because the proof-of-work calculations are so complex and time-consuming. The electricity used per bitcoin transaction would be sufficient to power a US household for more than three weeks, and the CO_2

Exhibit 14. Bitcoin Energy Consumption



Source: Digiconomist.

emitted by this transaction is approximately the same as the CO_2 generated by 761,333 Visa transactions. Furthermore, because the hardware used to work with bitcoin becomes obsolete within one to two years, the electronic waste created by bitcoin miners is approximately the same as the annual electronic waste created by a country the size of Luxembourg, as **Exhibit 14** illustrates.

More modern blockchain technologies such as Ethereum make lesser demands on energy and storage space. As of 2019, Ethereum mining and transactions consumed 8 TWh of electricity per year (approximately the same amount of electricity as Honduras consumes in a year), and each Ethereum transaction consumes enough energy to power an average US household for a day.

Overall, although blockchain technology holds many promises to increase security and prevent major cyber attacks, it is not without limitations or flaws. Before blockchain technology can become a mainstay in our economy and expand beyond specific niche applications, its limitations in terms of energy need and transaction time need to be overcome. Until then, cybersecurity issues will have to be solved by conventional means, implying that the current arms race between cybercriminals and companies will continue.

Conclusions

In a world in which more than one-half of the Earth's population has access to the internet and both civil and military organizations depend on the internet and computer networks for communication, data storage, and information processing, cybersecurity has become a major issue. Cyber warfare and civilian cyber attacks by criminals with pecuniary motives have become a major threat to the economy, the military, and our political discourse.

State-sponsored actors use cyber attacks to undermine trust in organizations and steal both data and know-how. The resulting damage to the economy and individual businesses can be large, and the damage to public trust in institutions and the media is immeasurable.

Although we have not yet witnessed a major cyber attack with a significant economy-wide impact, businesses are constantly struggling with security breaches costing an estimated $13 million per company per year. For banks and other financial institutions, the costs can be even higher. In 2018, the average bank faced annual damages resulting from cybercrime and data loss of $18.4 million, which means that over a five-year horizon, losses from cyber attacks could reach hundreds of billions annually. In fact, model estimates for the global banking system range from $97 billion to $351 billion per year, depending on the scenario. These losses are significant enough to trigger a financial crisis if key institutions such as central banks or clearing houses are hit. But even if the cyber attacks are insufficient on their own to create a financial crisis, they can be timed in such a way as to further destabilize an already fragile economy.

The worst-case scenario in terms of cybersecurity would be a successful attack on the vital infrastructure of a country. If the United Kingdom were to experience repeated outages of the electricity grid around London for several weeks, the direct economic damage could range from 0.4% of UK GDP to 3.3% of GDP. Over five years, the economic loss of such infrastructure outages could be between 1.5% of GDP and 16.9% of GDP, creating a massive recession in the UK economy. Although such attacks on the national infrastructure of a country are unlikely, they remain possible.

Cybersecurity is thus a major concern for investors and businesses alike and will become more important over time as innovations such as the IoT spread. This means that new defensive technologies, including the use of blockchain to protect data, will have to be developed, although significant technological and economic challenges to these methods remain and will have to be overcome.

Bibliography

Abbosh, O., and K. Bissell. 2019. "Securing the Digital Economy: Reinventing the Internet for Trust." Accenture Strategy. https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf.

Ali, I., and P. Stewart. 2019. "US Carried Out Secret Cyber Strike in Iran in Wake of Saudi Oil Attack: Officials." Reuters, 16 October. https://

www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK.

Bischoff, P. "How Data Breaches Affect Stock Market Prices. *Comparitech* (blog). https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/.

Bissell, K., and L. Ponemon. 2019. "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study." Ponemon Institute and Accenture Security. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50.

Bryan-Low, C., C. Packham, D. Lague, S. Stecklow, and J. Stubbs. 2019. "Hobbling Huawei: Inside the U.S. War on China's Tech Giant." Reuters, 21 May. https://www.reuters.com/investigates/special-report/huawei-usa-campaign/.

Bouveret, A. 2019. "Estimation of Losses Due to Cyber Risk for Financial Institutions." *Journal of Operational Risk* 14 (2): 1–20.

Cimpanu, C. 2018. "Hackers Crashed a Bank's Computers While Attempting a SWIFT Hack." *BleepingComputer*, 8 June. https://www.bleepingcomputer.com/news/security/hackers-crashed-a-bank-s-computers-while-attempting-a-swift-hack/.

Clapper, J. R., M. Lettre, and M. S. Rogers. 2017. "Foreign Cyber Threats to the United States." Joint Statement for the Record before the Committee on Armed Services of the United States Senate, 115th Congress, 5 January. https://www.govinfo.gov/content/pkg/CHRG-115shrg33940/html/CHRG-115shrg33940.htm.

Coburn, A. W., J. Daffron, K. Quantrill, E. Leverett, J. Bordeau, A. Smith, and T. Harvey. 2019. "Cyber Risk Outlook." Centre for Risk Studies, University of Cambridge Judge Business School, and Risk Management Solutions, Cambridge, UK. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf.

Corkery, M., and M. Goldstein. 2017. "North Korea Said to Be Target of Inquiry over $81 Million Cyberheist." *New York Times*, 22 March. https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html.

Fernández-Caramés, T. M., and P. Fraga-Lamas. 2018. "A Review on the Use of Blockchain for the Internet of Things." *IEEE Access* 6: 32979–33001.

FireEye. 2018. "Suspected Chinese Cyber Espionage Group (TEMP. Periscope) Targeting U.S. Engineering and Maritime Industries." *FireEye* (blog), 16 March. https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.

Gartner. 2019. "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018." Press release, Gartner, 29 July. https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018.

Haber, S., and W. S. Stornetta. 1991. "How to Time-Stamp a Digital Document." *Journal of Cryptology* 3: 99–111.

Halpern, M. 2015. "Iran Flexes Its Power by Transporting Turkey to the Stone Age." *Observer*, 22 April. https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/.

Healey, J., P. Mosser, K. Rosen, and A. Tache. 2018. "The Future of Financial Stability and Cyber Risk." Brookings Institution, Washington, DC. https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/.

Hsu, J. 2018. "The Strava Heat Map and the End of Secrets." *Wired*, 29 January. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Huang, K., S. Madnick, and S. Johnson. 2018. "Interactions Between Cybersecurity and International Trade: A Systematic Framework." MIT Sloan Research Paper No. 5727-18. MIT Sloan School of Management, Cambridge, MA.

Kelly, S., E. Leverett, E. J. Oughton, J. Copic, S. Thacker, R. Pant, L. Pryor, G. Kassara, T. Evan, S. J. Ruffle, M. Tuveson, A. W. Coburn, D. Ralph, and J. W. Hall. 2016. "Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy." Cambridge Risk Framework Series. Centre for Risk Studies, University of Cambridge Judge Business School, Cambridge, UK. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf.

Kopp, E., L. Kaffenberger, and C. Wilson. 2017. "Cyber Risk, Market Failures, and Financial Stability." IMF Working Paper no. 185 (August). International Monetary Fund, Washington, DC.

Latva-Aho, M., and K. Leppänen, eds. 2019. "Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence." 6G Research Visions 1 white paper. 6G Flagship, University of Oulu, Finland.

Lee, J. 2019. "Moving Toward 6G." Presentation at 6G Wireless Summit, Levi, Lapland, Finland, 24–26 March.

Liu, S. 2019. "Market Share Held by the Leading Windows Anti-Malware Application Vendors Worldwide." Statista. https://www.statista.com/statistics/271048/market-share-held-by-antivirus-vendors-for-windows-systems/.

Ma, J., R. Shrestha, L. Moeller, and D. M. Mittleman. 2018. "Channel Performance for Indoor and Outdoor Terahertz Wireless Links." *APL Photonics* 3 (5): 051601.

Marks, J. 2014. "Iran Launched Major Cyberattacks on the Israeli Internet." *Politico*, 18 August.

Mitchell, A. D., and J. Hepburn. 2016. "Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer." *Yale Journal of Law and Technology* 19 (1): 182–237.

Montague, Z. 2019. "Interior Department Grounds Chinese-Made Drones Amid Review." *New York Times*, 30 October. https://www.nytimes.com/2019/10/30/us/politics/interior-department-chinese-made-drones.html.

Mueller, R. S. 2019. *The Mueller Report: Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: US Department of Justice.

Perlroth, N., and S. Shane. 2017. "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets." *New York Times*, 10 October. https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

Stinchcombe, K. 2017. "Ten Years In, Nobody Has Come Up with a Use for Blockchain." *Hackernoon*, 22 December. https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100.

Stinchcombe, K. 2018. "Blockchain Is Not Only Crappy Technology But a Bad Vision for the Future." *Medium*, 5 April. https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec.

Taylor, P. J., T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. R. Choo. 2020. "A Systematic Literature Review of Blockchain Cyber Security." *Digital Communications and Networks* 6 (2): 147–56.

Telegraph. 2017. "Iran Blamed for Cyberattack on Parliament that Hit Dozens of MPs, Including Theresa May." 14 October. https://www.telegraph.co.uk/news/2017/10/13/iran-responsible-cyberattack-british-parliament/.

