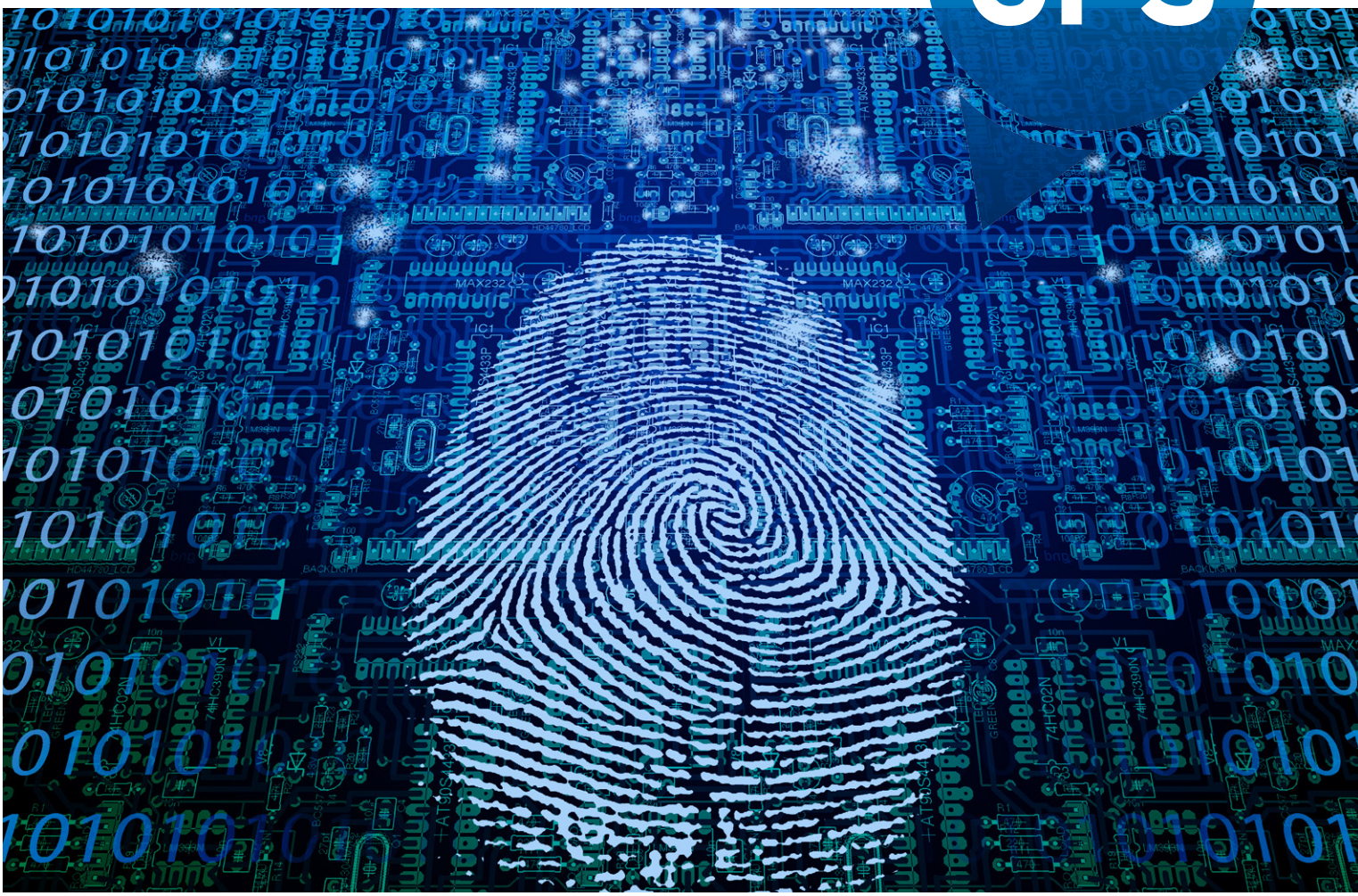
Citi GPS



THE CYBER PROBLEM

Causes and Consequences of the Rise in Cyber Skill Demand

Citi GPS: Global Perspectives & Solutions

March 2023

Primary Authors

Pantelis Koutroumpis is the Lead Economist on the Programme on Technological and Economic Change at the Oxford Martin School. Pantelis's main research interests are industrial economics, innovation, telecommunications economics, and regulation. He is a member of the editorial board of Telecommunications Policy and has published in several journals including the Journal of Economic Literature, Journal of the European Economic Association, and Economic Policy, among others.

Farshad Ravasan is a Research Economist at the University of Oxford. In 2019, he joined the Oxford Martin School and became a core member of the Oxford Martin Programme on Technological and Economic Change. He received his Ph.D. in Economics from the Paris School of Economics.

Taheya Tarannum is a Researcher at the Oxford Martin Programme on Technological and Economic Change. She received her PhD in Economics from the University of Virginia. Her research interest lies at the intersection of digital economics and the study of labor markets. Currently, she is working to understand how adoption of digital technologies affects firms and households. Before joining the Oxford Martin School, she taught as a lecturer at the University of Virginia.

Helen H Krause, CFA is a Managing Director and head of Data Science Insights at Citi Global Data Insights. Previous to Citi, Helen was an Executive Director in Alternative Investment at Morgan Stanly and a Senior Portfolio Manager at BlackRock. She has an MSc in Economics and Finance from University of Warwick and an MSc in Mathematical Trading and Finance from Cass Business School.

+44-20-7986-8653 | helen.krause@citi.com

Anita McBain is a Managing Director at Citi Research and head of ESG Research, EMEA. She joined from M&G Investments, where she was Head of Responsible Investment. Prior to M&G, Anita led sustainability research for an Impact fund and has held various buy-side and sell-side analyst roles in her career. Anita holds an MSt from the University of Cambridge, an MBA from the University of Edinburgh, and a BSc from City University, London.

+44-20-7508-4361 | anita.mcbain@citi.com

Fatima Boolani is a Director at Citi Research and the Co-Head of the U.S. Software Equity Research Team. Prior to joining Citi in 2021, Fatima spent a decade at both UBS and Jefferies in a similar lead analyst capacity, building deep domain expertise in the cybersecurity and infrastructure software sub-disciplines. She began her Wall Street career as an investment banker in the enterprise software sector at Thomas Weisel Partners. She is a graduate of the Ivey School of Business at Western University, where she earned her Honors Business Administration (HBA) degree with Dean's List distinction.

+1-212-816-9115 | fatima.boolani@citi.com

THE CYBER PROBLEM

Causes and Consequences of the Rise in Cyber Skill Demand

As businesses become more digitally connected, their exposure to cyber threats increases. Managing these risks is a complex endeavor due to the rising costs of investment in equipment, software, and cyber talent.

In this report, we focus on the causes and consequences of the increase in cyber skills demand. Our first chapter highlights the factors that have increased companies' exposure to cyberattacks, as well as the costs associated with this exposure. We highlight two notable trends that have drastically changed the landscape and importance of cybersecurity. First, the impact of geopolitics and the emergence of cyberwarfare. Second, consumers' rising attention toward the security of their personal data. In the second chapter, we discuss how global and regional labor markets fare in the face of steep competition for cybersecurity talent. Using information extracted from the profiles of the active cyber professional population, we measure the supply of cyber skills and examine the characteristics of cyber professionals. Our spatial analysis focuses on recruitment difficulties across states and cities. In our last chapter, we turn to regulation, business strategy, and governance. We discuss the importance of compliance and how failure to comply with regulation can substantially increase the cost of a cyberattack.

We evaluate the costs and benefits of strict regulatory measures and explore alternative measures. We argue that cybersecurity is a public good and that firms should implement a resilient cybersecurity defense as their social responsibility.

- Cyberattack costs have started to bite: Apart from the direct costs, supply chain disruptions and reputational damage can be substantial.
- Cyberattack exposure risks and material costs have increased significantly in the healthcare industry.
- Geopolitical risks and the emergence of cyberwarfare have reached new levels, disrupting production networks and causing cross-border economic damage.
- Consumer attention toward privacy and personal data has peaked, magnifying the impact of reputational damage for firms impacted by security breaches.
- Asia is now the second largest market for cyber skills, surpassing Europe.
- Cyber skill demand rose significantly for many managerial positions. One-tenth of cyber job postings also require data privacy knowledge.
- The cyber workforce is relatively young — half of all cyber professionals have less than six years of experience.
- Excluding North America, cyber job openings take longer than other information technology (IT) positions to fill.
- Stringent data breach regulations, which emerged globally through a mix of better enforcement and heftier fines, make non-compliance a non-option.
- Data breach regulation can induce firms to increase investment in cyber skills, but it slows down business creation and increases exit rates.

The Cyber Problem

Cyberattacks are increasing – in number, complexity, and cost– driven by geopolitics and cyber warfare. By sector, there has been a distinct surge in cyber risk in the healthcare industry and cybersecurity is increasingly becoming a concern for firms globally.

75%
of all data breaches in the U.S. are cyber-related

Source: PRC

2021
Jan Feb Mar Apr
May Jun Jul Aug
Sep Oct Nov Dec

287 days
Average time to detect and contain a breach in 2021

Source: IBM

$4.24 mn
Average cost of a data breach in 2021

Source: IBM

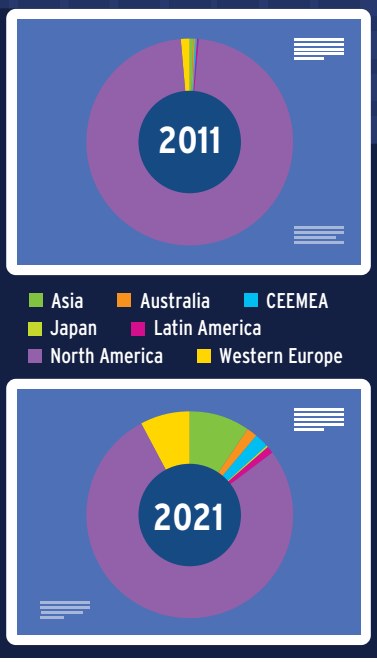
40%
Percentage of total cybersecurity discussions held by non-American firms in 2020

Source: NBER

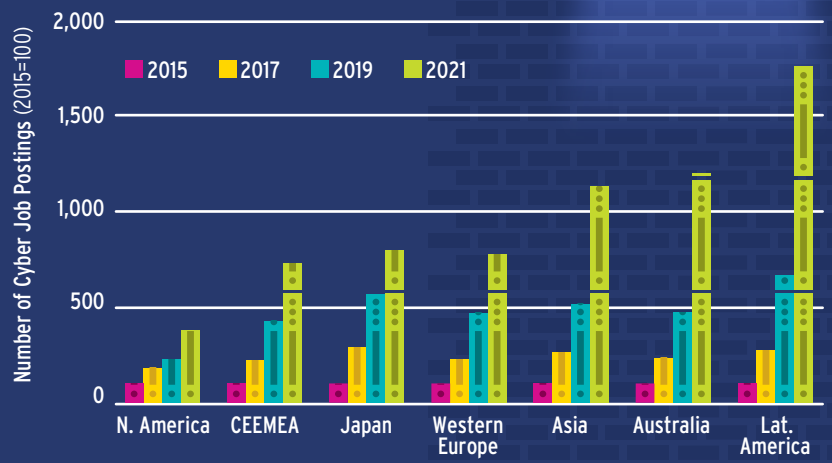
RISE OF DEMAND FOR CYBER SKILLS

Because businesses are increasing their digital footprints at the same time cyberattacks are increasing, the need for a workforce with digital skills is growing – both regionally and by industry.

Regional Demand for Cyber Jobs

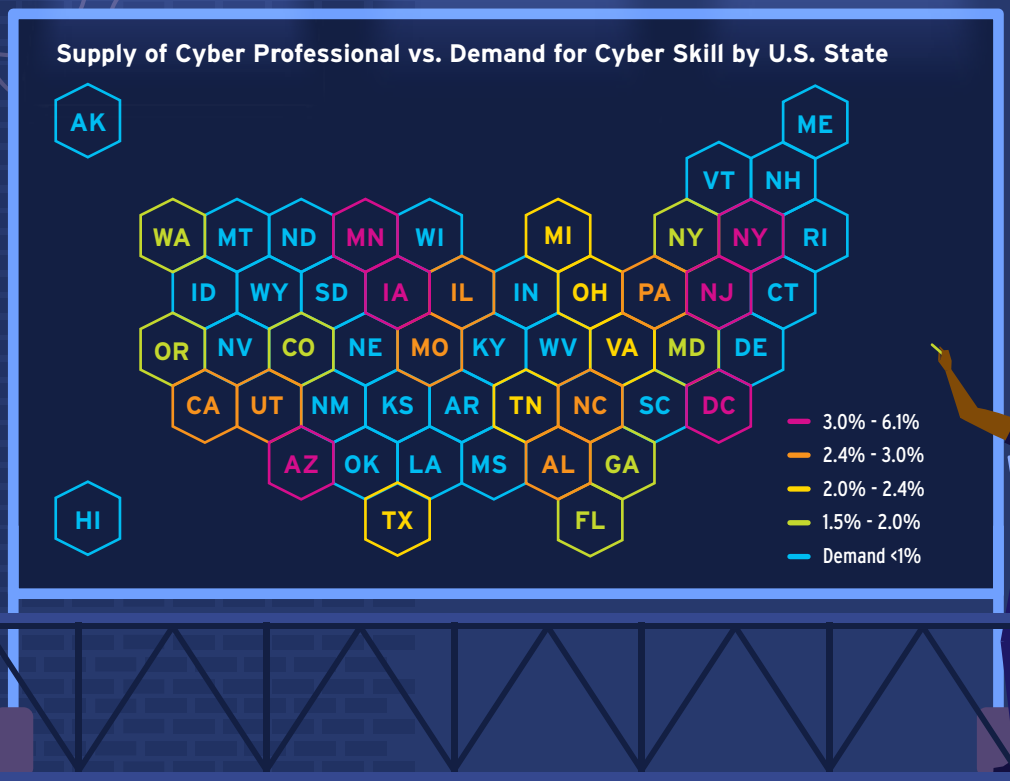


Relative Increase in Demand for Cyber Skills



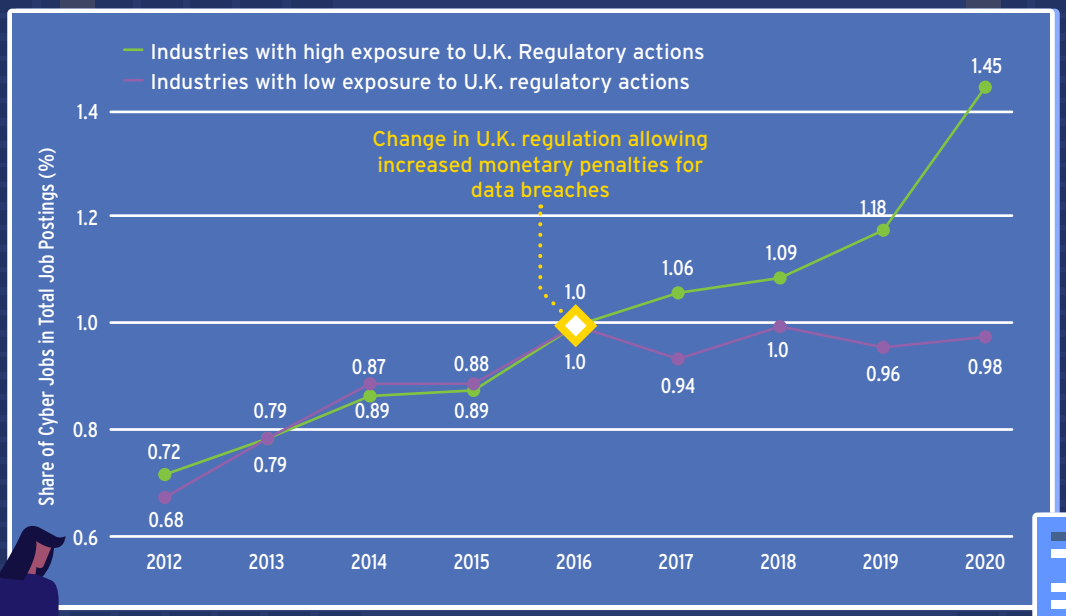
SUPPLY OF CYBER SKILLS NOT MEETING DEMAND

In the U.S., job listing data indicate there is rising demand for workers with cyber skills. In 2021, the average U.S. state saw 2.6 cyber job postings per cyber professional. In addition, compared to IT professionals, the age of the cyber-related workforce is relatively younger and job postings for cyber jobs are open for longer.



ADDRESSING THE MARKET FAILURE IN THE PROVISION OF CYBERSECURITY

Exposure to cyberattacks depends on a firms' own cyber resilience as well as that of its partners and suppliers. The optimal of provision of this public good can be addressed by government intervention via regulations, or by encouraging firms to integrate cybersecurity as part of the corporate social responsibility agenda. Demand for cyber skills rapidly increase in industries highly exposed to enforcement.



Contents

Anatomy of an Economy-Wide Threat

Rise of Cyber Risk

"If you spend more time on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked."

-- Richard Clarke, White House Cybersecurity Advisor, 1992-2003

Cyberattacks: A Brief History

Cyber threats are not new. In fact, the history of cyberattacks goes back to 1834 when a pair of thieves hacked the French Telegraph System and stole financial market data, effectively committing the world's first cybercrime.[1]

In 1962, the Massachusetts Institute of Technology (MIT) set up the first computer passwords to protect student privacy and limit the time students spent on the computer. The MIT computer became the first one to be hacked. Allan Scherr, an MIT student, managed to build a punch card to trick the computer into printing off all of the passwords and used them when he ran out of his allotted time.[2]

Figure 1. The First Password-Protected Computer

Source: MIT

The first computer virus, called RABBITS, appeared in 1969, bringing down the University of Washington Computer Center. In 1974, a variant of RABBITS became the first internet virus that ran over APRANET — an early version of the internet. In 1982, the CIA reportedly blew up a Siberian Gas pipeline by hacking into the network and the computer system of the gas pipeline, conducting the first notable cyberwarfare incident.

In the late 1980s and 1990s, new forms of cyber threats emerged. These included the first Trojan software (a form of malware that captures important information about a computer system or a computer network); the first internet worm (a class of viruses that can replicate themselves unaided by users and spread with information found in an infected computer); and the first large-scale attack on critical network infrastructure, which brought the whole internet down for an hour. In the 2000s, a new type of cyber incident emerged that targeted private companies for financial gain, as opposed to singling out individual users.

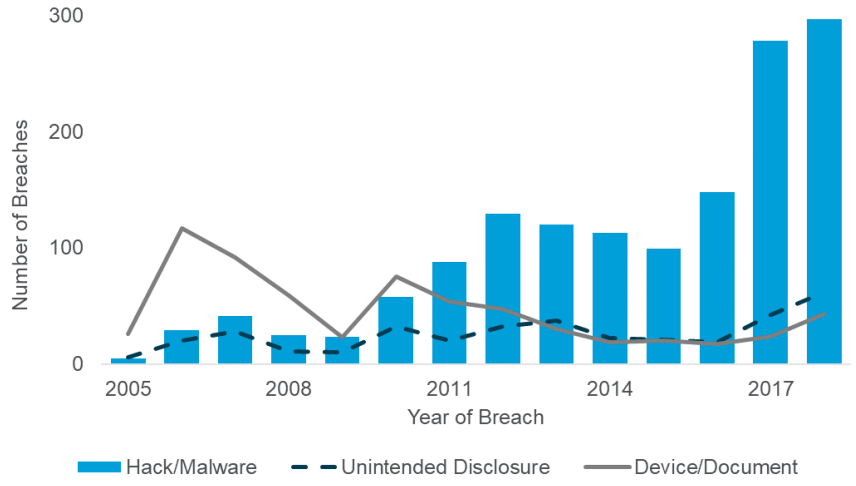
[1] Schneier, "Schneier on Security," accessed December 20, 2022.
[2] Robert McMillan, "The World's First Computer Password? It Was Useless Too," *WIRED*, January 27, 2012.

For instance, TJX, a U.S., retail company, was the object of a massive cyberattack in 2007 that compromised information for over 45 million credit and debit cards, with the estimated damages exceeding $250 million. Since 2010, cyberattacks have become a major source of data breach incidents among companies and organizations.

Incidences of cyber-related data breaches have rapidly increased since 2010. We use information about data breach events from the Privacy Rights Clearinghouse (PRC) dataset to highlight the rising risk of cyberattacks. This data has been collected using reports made to state Attorneys General and the U.S. Department of Health and Human Services offices and includes more than 9,000 data breach incidents since 2005. It covers different types of data breaches, including unintended disclosures, physical data loss and theft, credit card fraud, insider trading, digital hacks, and malware. While cyber-related incidents accounted for a small fraction of data breaches before 2010, they made up three-quarters of all data breaches by 2018.

Figure 2. Rise in Cyberattack Incidents

Cyberattacks are rapidly increasing and cyber-related incidents emerged as the top source of data breaches for companies and organizations from 2010.



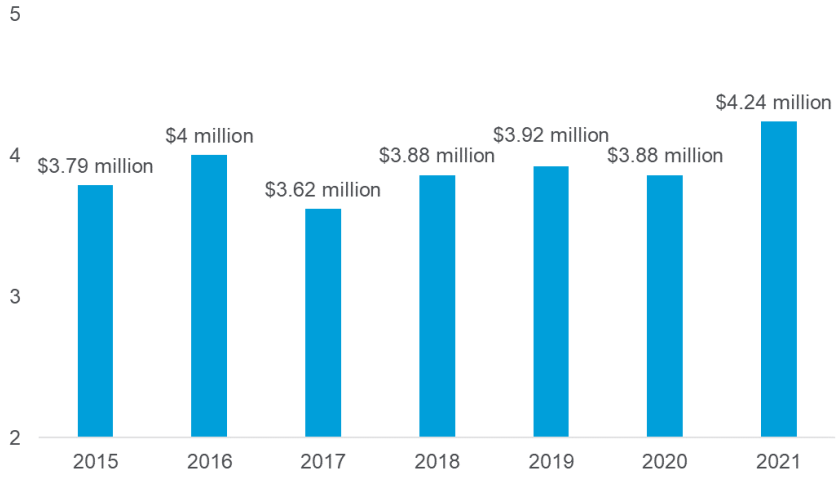
Source: Privacy Rights Clearinghouse, Citi GPS

Rising Costs of Cyberattacks

Apart from their frequency, cyberattacks are also becoming more damaging. According to IBM's *Cost of a Data Breach Report (CDBR) 2021*, the average cost of a data breach has increased significantly since 2015. In 2021, the average cost of each data breach rose to $4.24 million, 12% higher than 2015 levels and 10% higher compared to 2020. The report estimates that a typical breach (excluding very large and very small incidents) compromises 2,000 to 101,000 personal records. On average, the costs of detection, a recovery plan, and post-response actions account for 56% of the total cost of each incident. The remaining cost comes from business losses, such as operational disruption and customer loss.

Figure 3. Rise in the Cost of Cyberattacks

The estimated cost of a cyberattack surged to $4.24 million in 2021, 12% higher than its 2015 level and 10% higher compared with 2020.



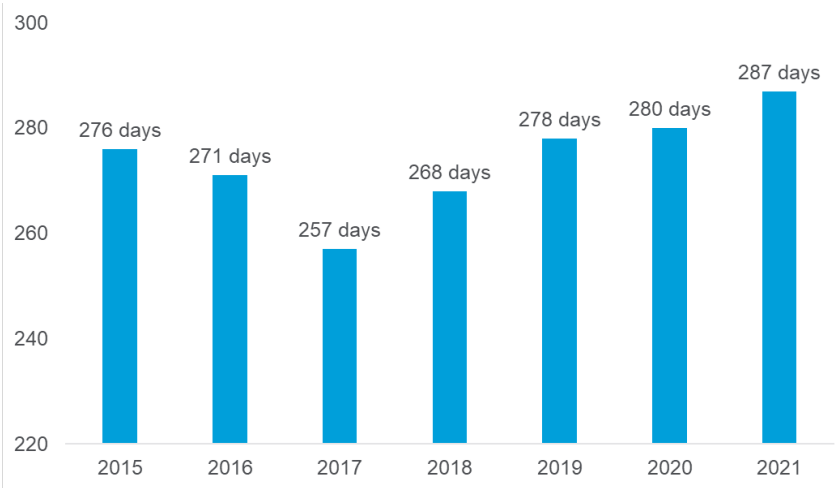
Source: IBM, Citi GPS

Increasing Complexity of Cyberattacks

The trend on time required to recover from cyberattacks indicates that hackers are using more sophisticated methods over time. Although the time to detect and contain an attack decreased between 2015 and 2017, IBM's CDBR report notes it has steadily increased since 2017. On average, it took 287 days to detect and contain a cyberattack in 2021, 30 days longer than the detection period for an average attack in 2017.

Figure 4. Average Number of Days to Detect and Contain a Cyberattack

As cyberattacks are becoming more complex, the time to manage them increases. The average time to detect and contain a cyberattack was 287 days in 2021.



Source: IBM, Citi GPS

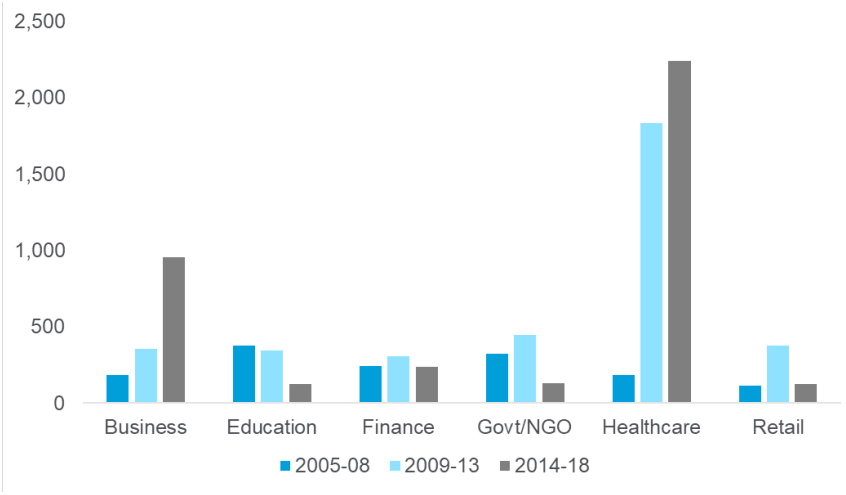
Cyber Risk Across Different Industries

Rising Cyber Risks in the Healthcare Industry

Cyberattacks on firms were traditionally limited to the financial sector and a small number of other industries dealing with valuable personal information. However, that has changed. Digitization across almost every sector has left businesses exposed to rising cyber risks. Thus, cyber vulnerability has become an economy-wide operational risk for businesses across all sectors. Over the past few years, healthcare organizations have experienced the biggest increase in cyber incidents. To increase the efficiency and accessibility of healthcare, the industry has gone through a massive digital transformation since 2010, which could substantially improve the quality of services and lower costs by offering remote communication between patients and medical professionals. But many of these new digital connections lack sufficient security standards, leaving the industry increasingly exposed to cyber risk.

Figure 5. Rise of Cyber Incidents Across Industries

There is a distinct surge in cyber risk exposure in the healthcare industry, while cyberattacks are also increasing in sectors that were not previously exposed to the cyber risk.



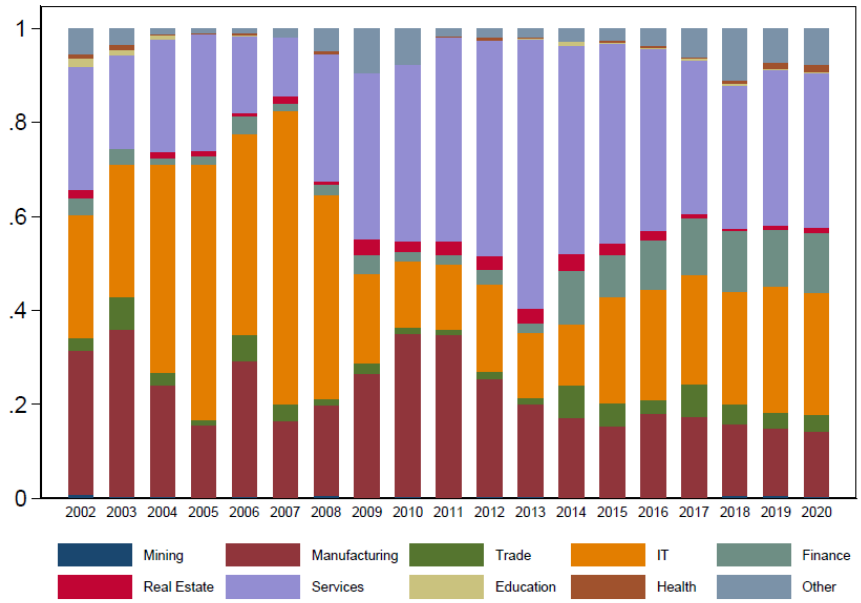
Source: Privacy Rights Clearinghouse, Citi GPS

Market Inattention to Healthcare Cyber Risk

Despite healthcare's importance, key players in the market, such as company CEOs, investors, and analysts, do not seem to pay much attention to its substantial cyber risks. Reviewing the discussion around cybersecurity in transcripts of conference calls from companies across 80 countries, a study by the London Business School shows which industries attracted the most attention from market participants over the past twenty years. During the 2000s, IT firms were the center of cyber attention. In the early 2010s, this attention shifted toward the manufacturing sector and its vulnerabilities to various forms of hacks and malware. During the 2010s, the market focused on service industries and the financial sector, leaving healthcare largely unattended.

Figure 6. Market Attention to Cyber Incidents Across Industries

Discussion around cyber risk shifted from IT and manufacturing sectors toward financial and service businesses. Market attention for healthcare remained limited despite the unprecedented surge in exposure from cyber threats.

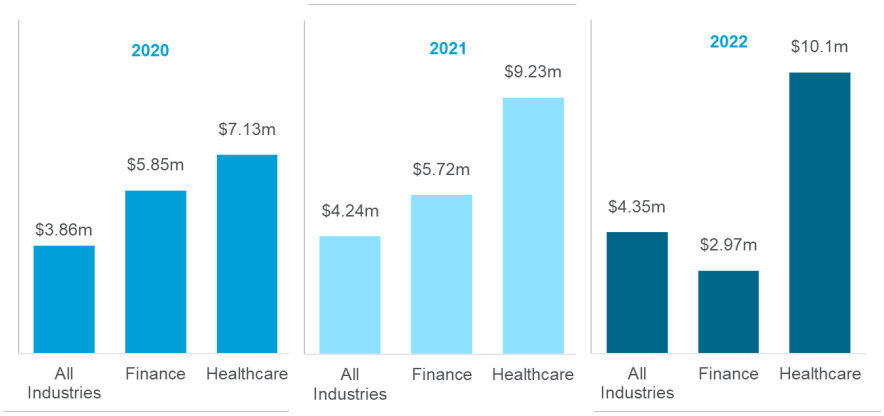


Source: Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," National Bureau of Economic Research (NBER) Working Paper No. w28906, June 2021.

This pattern is worrying, considering that the average cost of a cyberattack in the healthcare industry has been the highest among all industries for the past three years. Moreover, the cost gap with other industries has widened over the same period.

Figure 7. Cost of Cyber Incidents Across Industries

Cyberattacks in healthcare are costlier than others. The cost gap also sharply widened during the past three years.



Source: IBM, Citi GPS

"The world evolves, and the risks change as well, and I would say that the risk that we keep our eyes on the most now is cyber risk."

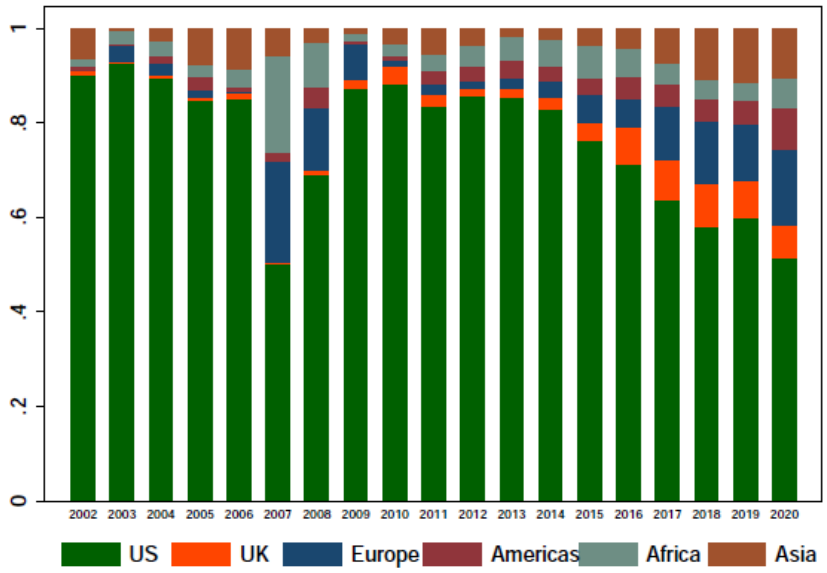
-- Jerome Powell, U.S. Federal Reserve Chairman

The Geography of Cyberattacks

A study by the London Business School looked at the transcripts of conference calls from companies across 80 countries over the past 20 years and found that prior to 2010, the vast majority of cybersecurity discussions originated from U.S.-based firms.[3] However, this has changed drastically, as the number of cybersecurity discussions in Europe, the U.K., Asia, and Africa is steadily increasing. Among European countries, the nations most affected by cyberattacks are France and Germany, which together represent roughly 10% of cybersecurity discussions in firms with headquarters outside the U.S. In 2020, non-American firms generated 40% of all cybersecurity discussions. The trend shows that cybersecurity has risen to become a concern for firms all over the world.

Figure 8. Cyber Risk Around the World

Cybersecurity is becoming a global concern. Before 2010, the majority of cyber risk discussions were linked to U.S.-based firms. This trend has changed and in 2020, non-American firms accounted for 40% of discussions about cybersecurity among market participants during the earnings calls.



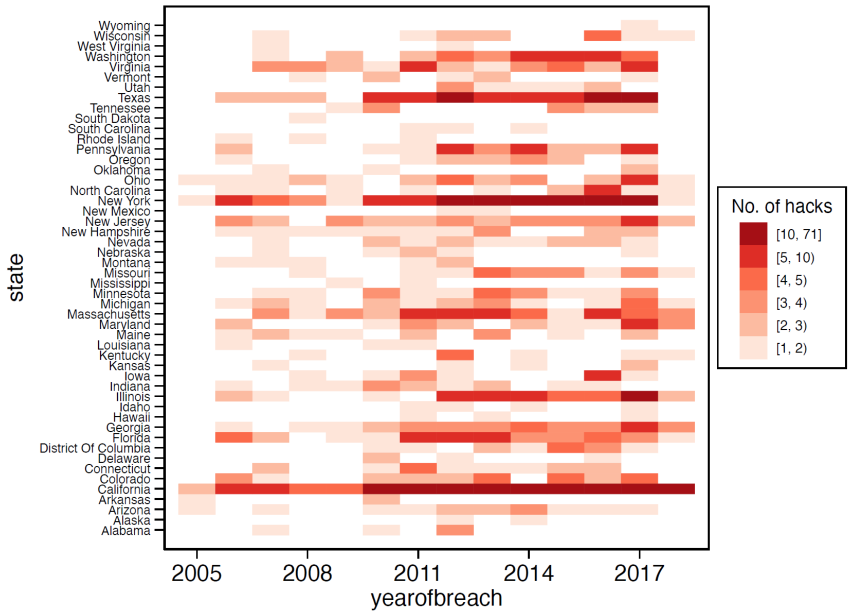
Source: Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," National Bureau of Economic Research (NBER) Working Paper No. w28906, June 2021.

Cyber Risk Across Local Markets

Reviewing the geographic variation of cyber risk within a country also provides interesting insights about distribution. As hackers expand their targets across industries, the intensity of attacks varies across different geographic markets. However, no market is immune to the risk of a cyberattack. Using the PRC data, Figure 9 shows the hacking-related incidents for business organizations reported across U.S. states. Since the early 2010s, hacking-related incidents have increased markedly across all states. One discernible pattern is that states with larger economies are more likely to be targeted by hackers.

[3] Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," National Bureau of Economic Research (NBER) Working Paper No. w28906, June 2021.

Figure 9. Rise of Cyber Incidents Reported Across U.S. States

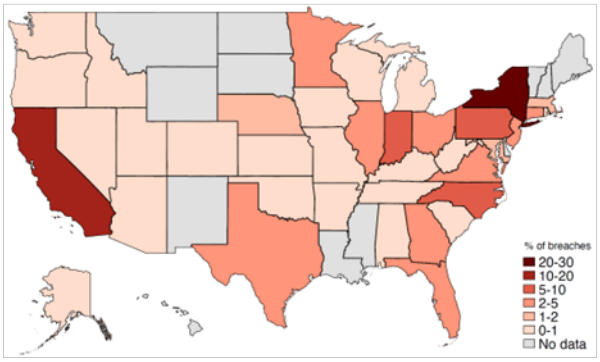


Source: Privacy Rights Clearinghouse, Citi GPS

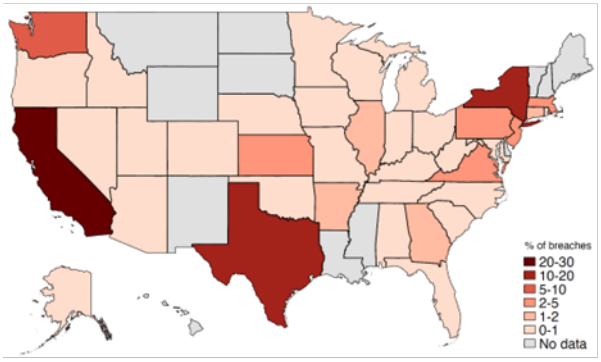
Figure 10 shows how industry-specific threats affect different states. State-level exposure through the IT sector is concentrated in specific geographic markets. Almost one-third of attacks in the IT sector occur in California, followed by Texas (16%), and New York (11.2%). Unlike the IT sector, the risk is spread out more uniformly in the financial sector as well as the wholesale and retail sector — a larger number of states are vulnerable to cyberattacks occurring in those industries. The top-four state concentration ratio is 68% for the IT sector, meaning that 68% of the breaches occurring in the sector are concentrated in those states. The numbers are 51% and 40% for the financial sector and wholesale and retail sector, respectively. Hence, a rise in cyberattacks across service industries or trade sectors is likely to have an impact across many markets.

Figure 10. Data Breaches Across States

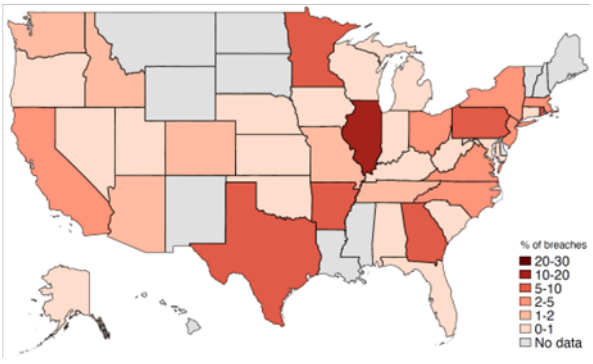
(a) Finance



(b) Information



(c) Wholesale & Retail



Source: Privacy Rights Clearinghouse, Citi GPS

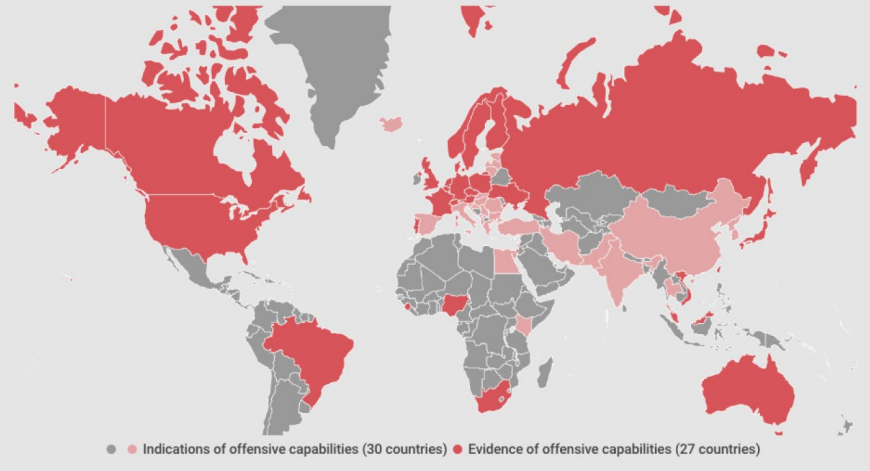
Geopolitics and Cybersecurity

The Hybrid Wars

The rise of offensive cyber capabilities has added a new dimension to war strategy. Several nations now consider cyber as the fifth military domain after land, sea, air, and space. In recent years, investments in these capabilities have grown substantially and have now been made in fifty countries around the globe. This suggests that the futures of geopolitics and cybersecurity are inherently linked.

Figure 11. The Global Cyber Armament

There is evidence on existing offensive cyber capabilities in 27 countries. There are indications that another 32 also possess such capabilities.



Source: digWatch, Citi GPS

The Russian Invasion of Ukraine

The recent invasion, apart from its detrimental human, social, and economic repercussions, shows the importance of cybersecurity in modern conflict. Cyber incidents that followed the initial military events demonstrate two facts. First, they show how cyberattacks have been used in tandem with military actions as coordinated war tactics. Second, they highlight how cyber warfare in local conflicts can expose firms across the world to cybersecurity threats. Since the beginning of the invasion in February 2022, a series of cyberattacks were carried out by threat actors with known and suspected links to the three Russian intelligence services — GRU (the military intelligence service), FSB (the foreign intelligence service), and SVR (the domestic intelligence service).

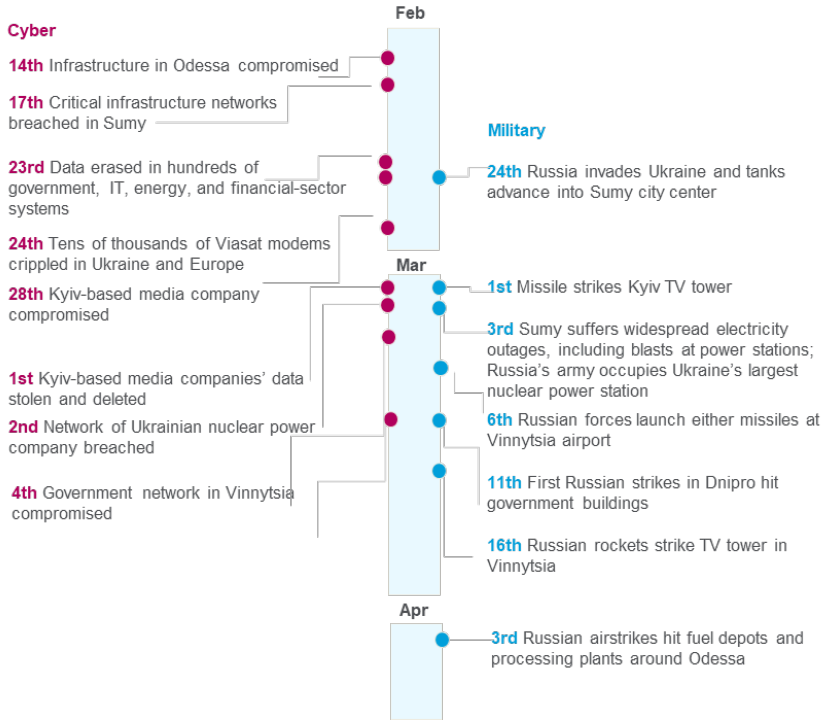
A special report by the Microsoft Digital Security Unit indicates how the cyberattacks were carried out in tandem with the military actions during the first days of the invasion.[4] Cyberattacks almost quadrupled over the period of invasion from the beginning of February through the end of March. The report documents 22 attacks in just the first week of the invasion alone.

[4] Microsoft Digital Security Unit, "Special Report: Ukraine, An Overview of Russia's Cyberattack Activity in Ukraine," April 27, 2022.

A closer look shows that cyberattacks were coordinated with conventional military assaults aimed at similar targets. For instance, as Russian troops began to move toward the border with Ukraine, Nobelium, a Russian state actor, launched a massive phishing campaign against Ukrainians to gain military intelligence. On March 1, 2022, Ukrainian broadcasting infrastructure experienced both a cyberattack and a missile strike. On March 2, 2022, the same happened to Ukrainian nuclear power plants.

Figure 12. Timeline of Russian Invasion of Ukraine

Russian military and cyberattacks have operated in tandem. In many cases, cyberattacks occurred within days or hours of missile strikes on similar targets, indicating the attackers may have overlapping objectives.

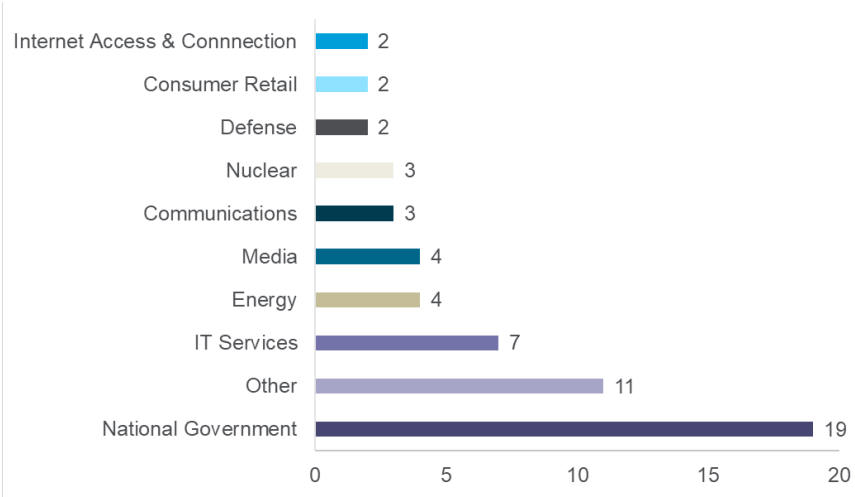


Source: Microsoft, Citi GPS

Figure 13 shows the distribution of cyberattacks across Ukrainian industries. Government entities and public organizations were the main targets of these attacks. Nevertheless, the pro-Russian hackers also attacked key infrastructure and private organizations to disrupt activities and access to services. Among different sectors, IT services were disrupted the most, followed by energy facilities, broadcasting, and retail. The "Other" category represents 11 smaller categories that each experienced an attack during the invasion. The category includes organizations in areas such as local government, agriculture, industrial bases, healthcare, transportation, and finance.

Figure 13. Cyberattacks Across Ukrainian Industries

Apart from government organizations, cyberattacks aimed to disrupt core economic functions by targeting key infrastructure in energy, IT service, communication, and consumer retail.



Source: Microsoft, Citi GPS

How Cyber Warfare Is Different

The unique challenge of cyber warfare compared to traditional conflict is that cyberattacks do not have geographical and temporal boundaries. The report from the Microsoft Digital Security Unit shows that between June 2020 and July 2021, Ukraine was the object of almost 20% of all registered attacks globally by state (not just Russian) actors. Importantly, more than 90% of all Russian-backed cyberattacks targeted NATO allies that openly offered support to Ukraine during the invasion. Many of these attacks were coordinated with traditional espionage activities by the Russian state. For instance, Nobelium, with known links to GRU, successfully carried out targeted data breaches of IT firms serving NATO governments, securing access to their foreign policy positions.

Russia also used cyberattacks to counter the effects of its war sanctions. Since the invasion began, three German wind energy companies have been targeted by cyberattacks. These attacks disrupted Germany's efforts to shift away from Russian fossil fuels. The initial attack targeted ENERCON on the same day as the invasion that started on the February 24, 2022. The other two attacks targeted Nordex and Deutsche Windtechnik during the first and second week of April. Although no group claimed responsibility, existing evidence indicates there are clear links to Russia's invasion. This implies that organizations worldwide are at risk of directly or indirectly being affected by these attacks during the Russian invasion of Ukraine.

Supply Chain Exposure

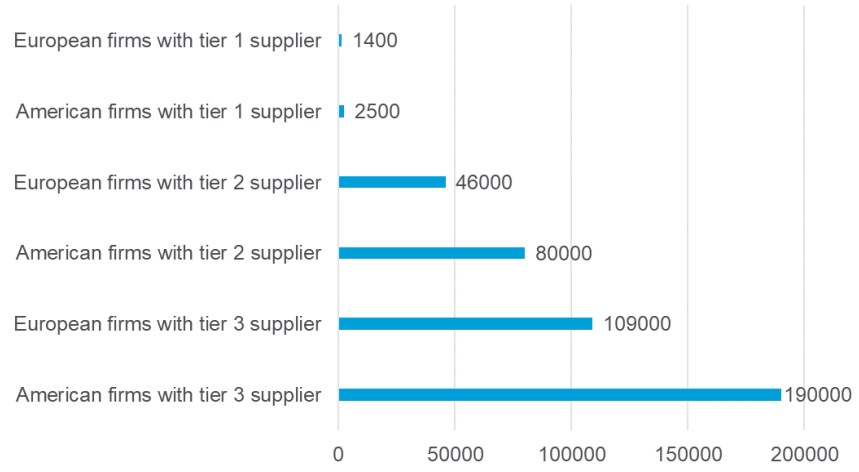
Although individual organizations across the world might be targeted directly by Russian-backed actors, collective supply chain disruptions are the main danger firms face, as they have become increasingly interconnected via global supply chains. According to global supply chain network data from Interos, 1,400 European firms and 2,500 U.S.-based firms have at least one supplier either in Russia or Ukraine.[5]

[5] Interos, "Supply Chain Disruption from the Russian Invasion of Ukraine", February 25, 2022.

However, the number of firms that are linked indirectly to Russian or Ukrainian firms in supply chain networks is significantly larger. There are more than 126,000 European and American firms that have a tier-2 Russian or Ukrainian provider. A tier-2 supplier is an indirect supplier that provides inputs to the firm's direct supplier. Moreover, the 126,000 figure rises to over 300,000 firms when we look at the links via tier-3 providers — i.e., suppliers connected to a firm via two intermediaries in a supply chain network. This implies that firms are very likely to be exposed to disruptions due to an indirect link with a targeted firm.

Figure 14. Exposure to Supply Chain Disruption of Russia's Invasion of Ukraine

More than 300,000 firms across the world are exposed to the supply chain disruption that can be caused by Russian cyber warfare.



Source: Interos, Citi GPS

Russian's NotPetya Supply Chain Attack

Several Russian threat actors have been targeting Ukrainian organizations since the annexation of Crimea in 2014. For instance, IRIDIUM, a threat group linked to GRU, which played a crucial role in Russian cyber warfare during 2022, deployed FoxBlade malware and sandworm during the invasion to target government organizations, critical infrastructure, IT services, transportation, energy grids, and financial sectors in Ukraine. Their most notable activity goes back to the NotPetya supply chain attack, the costliest cyberattack in history, in June 2017.

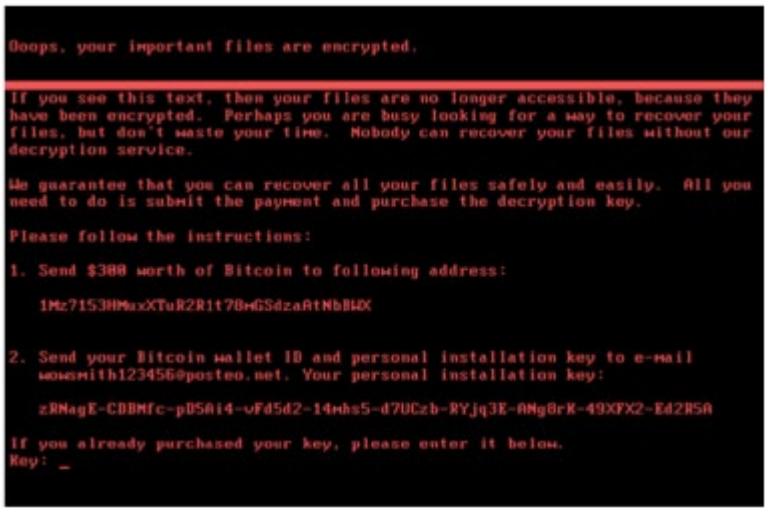
NotPetya targeted Ukrainian organizations but spread rapidly across the world, as it could transmit without administrative access requirements. Initially, it was considered to be a new version of Petya ransomware, which would encrypt the hard drive and make data inaccessible.[6] It would then ask the targeted organization for a Bitcoin payment in exchange for regaining access to the compromised data. However, experts eventually found NotPetya did not keep the decryption code, so decryption of the compromised data was not possible after the attack. In this regard, NotPetya was a form of wiper malware and not a common ransomware threat. The true intention of the attackers was not financial gain but to paralyze the computer networks of Ukrainian banks, firms, and the government.

[6] For more technical analysis, see Karan Sood and Sean Hurley, "NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Threat," Crowdstrike, June 29, 2017.

The global infection started with tax reporting software used by the Ukrainian government. When the software was hacked, it rapidly infected multinational companies with Ukrainian subsidiaries such as FedEx, Merck, Mondelez, Reckitt Benckiser, Nuance, and Beiersdorf, among others. This forced them to halt their operations and triggered a massive disruption in the global supply chain.

Figure 15. The NotPetya Note

Russia's NoPetya supply chain disruption was the most harmful cyberattack in history. Although it initially seemed a variant of Petya ransomware, the attack was not designed for financial gain but only for paralyzing the computer networks of organizations at massive scale.



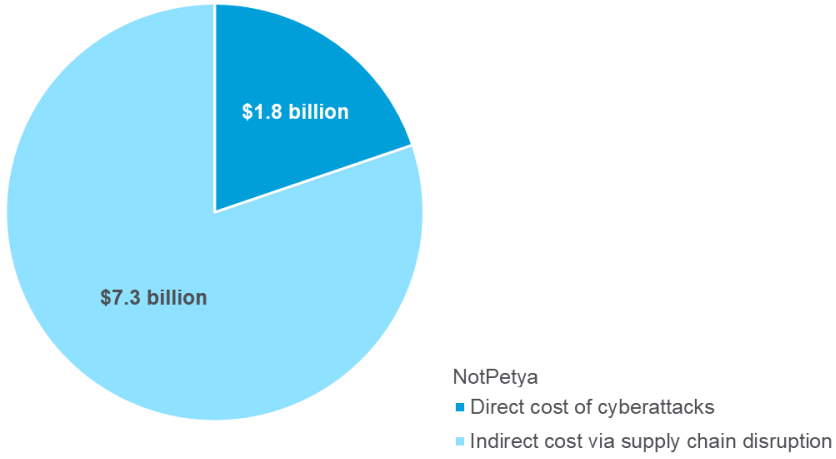
Source: Crowdstrike

The Damage from NotPetya

Economists at the Federal Reserve Bank of New York estimated that the victims infected by NotPetya lost $1.8 billion due to recovery costs and halted operations. However, they also reported that the damage for firms that were not directly targeted but shared ties with a NotPetya-infected provider were a cumulative $7.3 billion. This implies that supply chain disruption accounted for 80% of the total damage of the NotPetya cyberattack.

Figure 16. The Damage of Russia's NotPetya Cyberattack

Supply chain disruption accounted for 80% of the total damaged caused the Russian NotPetya cyberattack.



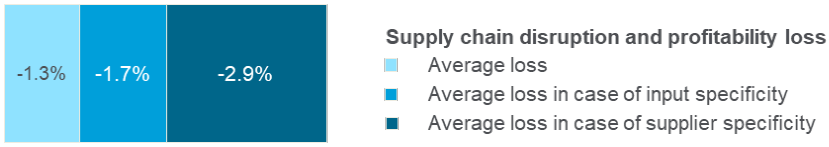
Source: Federal Reserve Bank of New York, Citi GPS

Supply Chain Vulnerabilities

These figures show the importance of supply chain disruption as a major channel that exposes firms to indirect costs of cyberattacks. The economists at the Federal Reserve Bank of New York followed firms whose suppliers were targeted by NotPetya. They found that the profitability of these firms, measured as the ratio of earnings before interest and taxes (EBIT) to total assets, was reduced by 1.3% on average over a period of two years following the attack. They further measured that a firm's profitability declined by 1.7% when its suppliers produced a highly specific input that was only available from a few suppliers. The profitability loss surged to roughly 2.9% when firms' overall supply networks were not well-diversified and relied on only a few suppliers.

Figure 17. Profitability Loss and Supply Chain Vulnerability

Firms with supply chain vulnerability up to 2.9% higher profitability loss after a cyberattack hit their providers.



Source: Federal Reserve Bank of New York, Citi GPS

Firms' Responses to the Russian Invasion of Ukraine

Damage to firms from cyberattacks could increase if cyberwarfare associated with the Russia-Ukraine conflict disrupts the current global supply chain network. The level of damage to a firm will greatly depend on its readiness and the preventive measures it takes to reduce cyber risk exposure. In a recent Gartner poll, over a quarter of organizations in North America and Europe, the Middle East, and Africa (EMEA) said they took some kind of cybersecurity action in response to Russia's invasion of Ukraine.[7] This was the most frequently cited response, ahead of actions related to sanctions, employee welfare, or supply chain risk management. Below, we summarize examples of cybersecurity actions in a few essential steps that allow enterprises to reduce the cyber risk exposure for themselves and their customers.

1. **Know the threat:** Review the known Russian threat actors' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs).

2. **Plan your incident response:** Invest in your incident response capabilities. Cyber incidents can take a long time to detect and contain.

3. **Ensure employees' security awareness:** Promote security awareness among your employees. The majority of cyber incidents are triggered by human error.

4. **Have an offline backup:** During the NotPetya cyberattack, one shipping company had a domain controller in its Ghana office go offline because of a blackout. This lucky coincidence allowed the company to recover its domain controller data.

5. **Monitor your supplier network carefully:** A survey of German supply chain executives conducted by Gartner in 2021 showed that although 80% of the companies had clear visibility into their direct suppliers, only 7% had sufficient information about their indirect suppliers.

[7] Paul Proctor, "How Geopolitics Impact the Cyber-Threat Landscape," Gartner, June 10, 2022.

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

-- Warren Buffet

Reputational Damage

The Long-Term Effects of Cyber Losses

Cyberattacks often impose significant direct costs on firms due to halted operations and costly recovery processes. However, they also come with reputational damage when they lead to a loss of trust by customers and suppliers. Unlike the transitory direct cost of cyberattacks, reputational damage is persistent and can generate substantial losses in the long run.

TalkTalk Incident

One such instance of reputational damage arose from the cyberattack in October 2015 against TalkTalk, a major internet service provider in the U.K.[8] During the attack, data for about 157,000 customers was compromised. These stolen personal records included the full details of 15,656 bank accounts in addition to 28,000 partial credit and debit card records. The company's initial estimate of the attack's cost was £35 million (~$42 million)[9] for an incident response and recovery plan. However, the company's financial statements show they actually suffered a £60 million (~$72 million) loss during the third quarter of 2015. This substantially higher cost was driven by the loss of 95,000 subscribers because of the data breach during these three months. Notably, the company actively tried to limit the pitfalls of the attack by offering a free upgrade to its 500,000 customers.

Quantifying the Impact of a Cyberattack on a Firm's Reputation

A recent academic paper by Pat Akey et al. in 2021 shows a significant drop in corporate reputation after a data breach.[10] The effect is persistent and grows over time. If a firm is initially among the top 25% most reputable corporations, it falls below the median level of reputation two years after the attack.

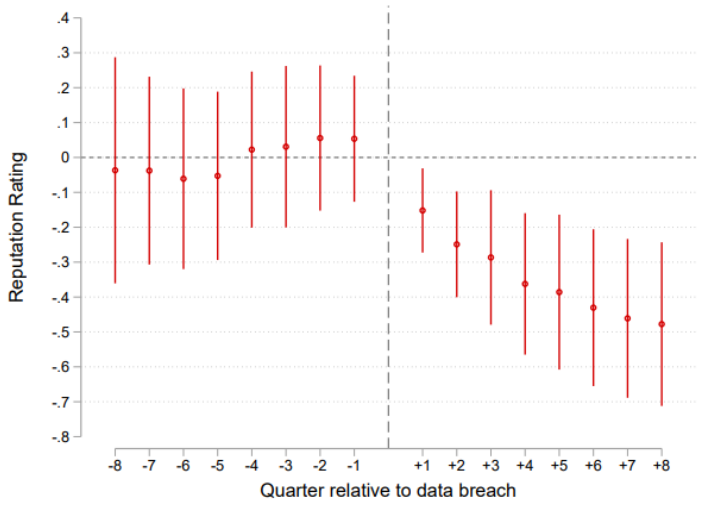
[8] Matt Burgess, 'TalkTalk Hack Toll: 100k Customers and £60m," *WIRED*, February 2, 2016.

[9] All currency calculations are as of February 20, 2023.

[10] Pat Akey et al., "Hacking Corporate Reputations," *Rotman School of Management Working Paper No. 3143740,* March 19, 2018, last revised July 13, 2021.

Figure 18. Reputation Damage Persistent Over Time

A cyberattack can cause devastating reputational damage. If a firm is initially among the top 25% most reputable corporations, its reputation falls below the median level two years after the attack.



Note: the figure plots the evolution of firms' reputation in the eight quarters before and after a data breach. Specifically, the figure plots the coefficient estimates and corresponding confidence intervals for a regression of "Reputation Rating" on dummy variable indicating the distance (in quarters) relative to the data breach.

Source: Pat Akey et al. (2018)

Reputational damage is measured in the study using RepRisk's Reputation Risk Rating (RRR) and translating their letter ratings (AAA to D) into a numerical scale from 1 to 10.[11] It is constructed based on daily reputational risk incidents from 80,000 public sources in 20 languages for roughly 4,000 publicly listed North American companies.

Data breaches negatively affect both profitability and expected growth opportunities for corporation. In the two years following a cyber incident, the study found a firm's return on equity (ROE) declines by 3% to 6% and its price-to-earnings ratio (P/E ratio) falls by 3.13 to 3.38 units. Thus, a cyberattack has lasting effects on a firm's value beyond the direct costs related to the breach.

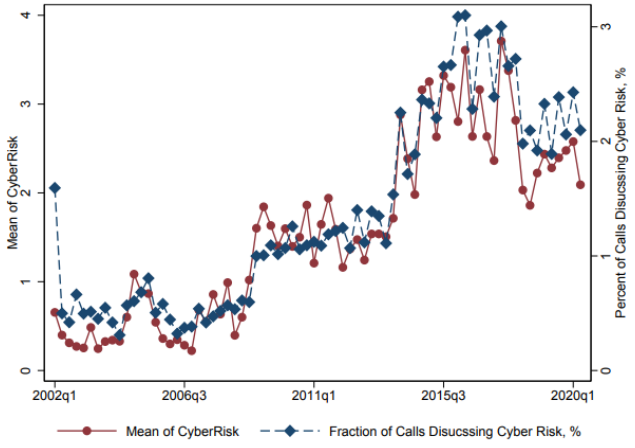
Rise of Public Attention and Reputational Damage

Recent trends indicate that public attention toward firms' cybersecurity policies is increasing.[12] Moreover, sentiments regarding data privacy have strengthened, and firms' stakeholders, like their customers, suppliers, and investors, have become more attentive to data breaches and plans for timely responses. Economists at the London Business School have studied transcripts of conference calls from companies across 80 countries over the past 20 years. They have found that discussion of cybersecurity is rapidly growing. Furthermore, analyzing the tone of discussion using natural language processing, they show that the sentiment surrounding cyber risk is becoming increasingly pessimistic. Their index also shows that the sentiment regarding cyber vulnerability has worsened roughly fourfold since 2002.

[11] FactSet, "RepRisk ESG Business Intelligence," accessed December 20, 2022.
[12] Rustam Jamilov, Helene Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," *National Bureau of Economic Research*, June 2021.

Figure 19. Public Attention to Cyber Vulnerability

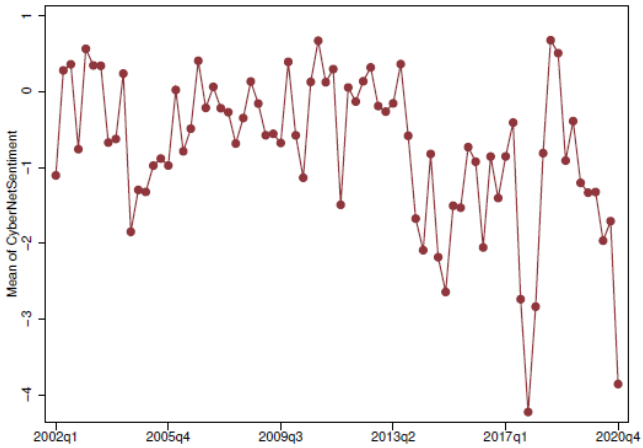
Public attention to firms' cyber vulnerability has gone up steadily during the past 20 years.



Source: Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," National Bureau of Economic Research (NBER) Working Paper No. w28906, June 2021.

Figure 20. Public Sentiment On Cyber Vulnerability

Public sentiment over firms' cyber vulnerability become roughly four-fold more pessimistic since 2002.

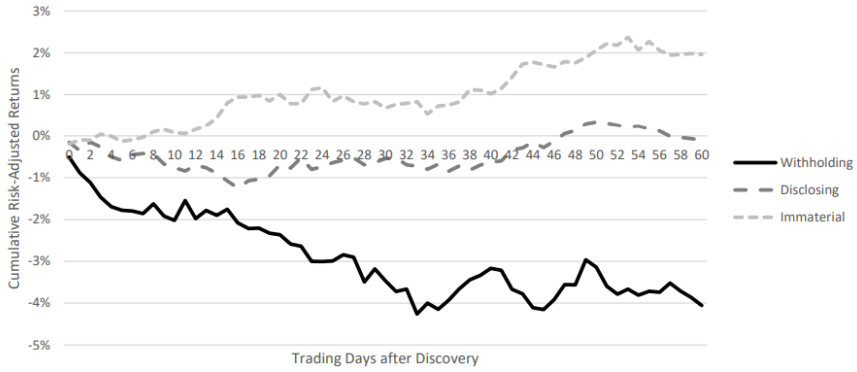


Source: Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," National Bureau of Economic Research (NBER) Working Paper No. w28906, June 2021.

Disclosing Cyber Incidents

Timely disclosure of cyber incidents helps firms to alleviate reputational damage. A joint study by economists at the University of North Carolina and Tel Aviv University showed that firms that immediately disclosed a cyberattack experienced an equity value decline of 0.33%, on average, in the three days after disclosure and 0.72% in the month after disclosure.[13] In contrast, the decline in market values was substantial when firms withheld information and the attack was discovered later by the public. In that case, firms suffered from equity value declines of 1.47% in the three days after the discovery of the attack; this rose to 3.56% in the month after the news broke out.

Figure 21. Sentiment Around Cyber Incidents



Source: Eli Amir, Shai Levi, and Tsafrir Livne, "Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets," Review of Accounting Studies, June 19, 2018.

[13] Eli Amir, Shai Levi, and Tsafrir Livne, "Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets," *Review of Accounting Studies*, June 19, 2018.

Apart from minimizing reputational damage, firms are required by law in many countries to immediately disclose cyberattacks that cause material damage. For instance, in the U.S., 60% of states require breached firms to notify the public as soon as they realize they are breached. However, examining the incidents between 2010 and 2015 reveals that many attacks are not disclosed before investors discovered them from other sources. To put the figures into perspective, compared to the thousands of attacks reported by other sources, only around 300 attacks were disclosed by companies during this period.

Competition for Cyber Talent

Why Cyber Skills Are Important

As the threat and costs of cyberattacks grow, firms seek to invest in cybersecurity personnel as part of their corporate risk management strategies. Recruiting cyber professionals can play an important role in addressing cybersecurity threats. According to the *2021 Cybersecurity Workforce Study* by the International Information System Security Certification Consortium, or (ISC)2, cybersecurity staffing shortages can put an organization at risk.[14] A shortage of workers can have real consequences, such as misconfigured systems, lack of risk assessment, slow patch cycles, oversights, outdated systems, and rushed deployments — all of which increase vulnerability to cyberattacks and data breaches.

The Verizon *2022 Data Breach Investigation Report* finds that 82% of data breach incidents involve a human component.[15] For example, human error can lead to credential theft, phishing, or misconfiguration errors. Hence, having a cybersecurity team is one of the most effective strategies for corporations to protect themselves against cyberattacks.

Notably, while threat prevention and detection tasks can be outsourced, developing internal cybersecurity capabilities is equally crucial for managing risks. Sophos surveyed 119 financial services establishments that were not hit by ransomware in the previous year and did not expect to be hit in the future and asked their IT managers, "Why do you not expect your organization to be hit by an attack in the future?" The top reason for this confidence was having trained IT staff capable of preventing attacks (66%).[16]

Figure 22. Percentage of Cyber Professionals Reporting Consequences of Staffing Shortage

Consequence	% Reported
Misconfigured systems	32%
Lack of risk assessment	30%
Slow to patch critical systems	29%
Oversights in process and procedures	28%
Inability to remain aware of threats	27%
Rushed deployments	27%

Source: Cybersecurity Workforce Study 2021, (ISC)2, Citi GPS

[14] (ISC)^2, " A Resilient Cybersecurity Profession Charts the Path Forward," Cybersecurity Workforce Study, 2021.
[15] Verizon, "2022 Data Breach Investigations Report," 2022.
[16] Sophos, "The State of Ransomware in Financial Services 2022," August 10, 2022.

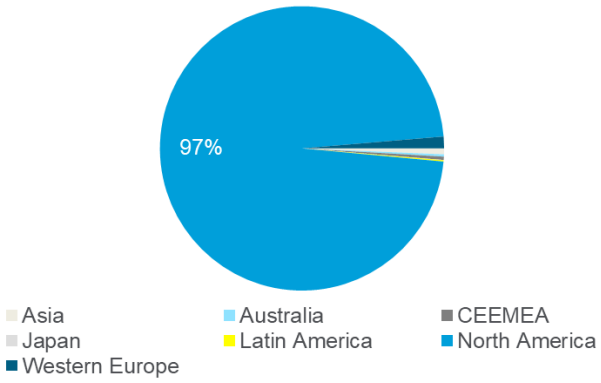
The Rise of Demand for Cyber Skills

With businesses increasing their digital footprints, the need for a more cybersecurity-literate workforce is rising. Traditional job titles do not effectively convey information about cyber skills. Hence, we analyzed text from job advertisements to measure how firms' demand for cybersecurity work is changing. Job postings provide a useful metric because they offer real-time information and capture more nuanced changes in the labor market. For this part of the analysis, we use LinkUp Job Market Data, which curates job listings from employer websites globally.

Global Demand

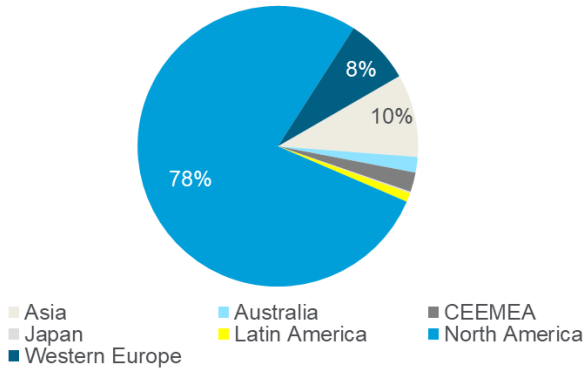
Between 2015 and 2021, the number of cyber jobs advertised by firms grew by a factor of 4.3. At the same time, the number of IT jobs advertised grew 3.5 times and the number of total jobs advertised grew 2.7 times. Although many of these jobs are concentrated in more industrialized regions, such as North America and Western Europe, the market for cyber skills is growing across all parts of the world. Over the same period (2015-21), worldwide information security spending doubled, from $75.4 billion to $157.7 billion.[17]

Figure 23. Regional Demand for Cyber Jobs (2011)



Source: Citi GPS

Figure 24. Regional Demand for Cyber Jobs (2021)



Source: Citi GPS

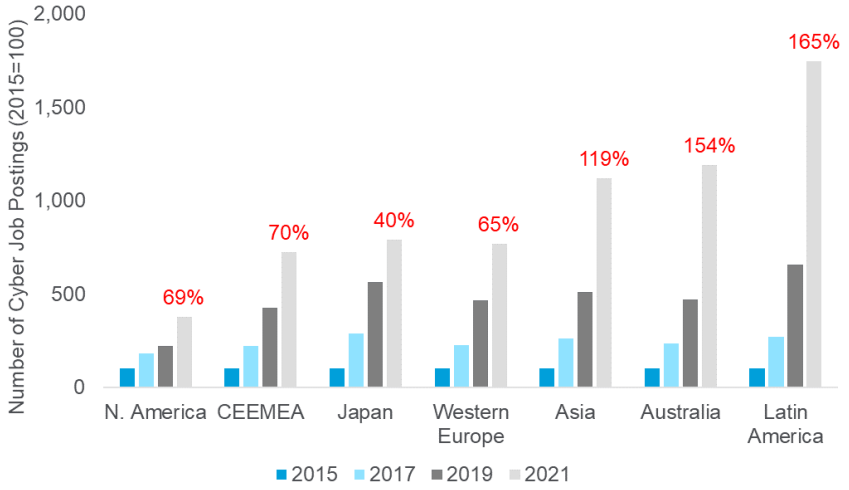
Figure 23 shows the changing composition of cyber job postings across different geographies. Our job posting data covers seven regions, namely Asia; Australia; Central and Eastern Europe, the Middle East, and Africa (CEEMEA); Japan; Latin America; North America; and Western Europe. At the start of the last decade, 97% of cyber job postings globally were in the North American market. Ten years later, 78% of the global job postings are coming from North America. Asia (10%) also surpassed Western Europe (8%) to emerge as the second-largest market for cyber skills, with Singapore, Bangalore, Pune, Gurgaon, and Chennai coming in as the top five Asian cities for cyber job postings. Part of the increased share in regions outside of North America reflects a broader pattern of digital transformation, leading companies to post more jobs online. But the pattern remains the same if we focus on the relative demand growth in the last five years.

[17] Gartner, "Gartner Identifies Three Factors Influencing Growth in Security Spending," October 12, 2022.

Figure 25 shows the number of cyber job postings for each region normalized by the number of cyber job postings in 2016. While North America still represents a large market, other regions are exhibiting faster growth. The COVID-19 pandemic has seemingly accelerated this trend. The numbers in red show the growth of job demand in 2021 compared to levels in 2019. In the post-pandemic period, the fastest-growing demand for cyber jobs came from Asia, Australia, and Latin America.

Figure 25. Relative Increase in the Demand for Cyber Skills

In the post-pandemic period, the fastest-growing demand for cyber jobs comes from Asia Australia, and Latin America. (Numbers in red report growth of cyber job postings 2019-21.)



Source: Citi GPS

Industry-Specific Demand

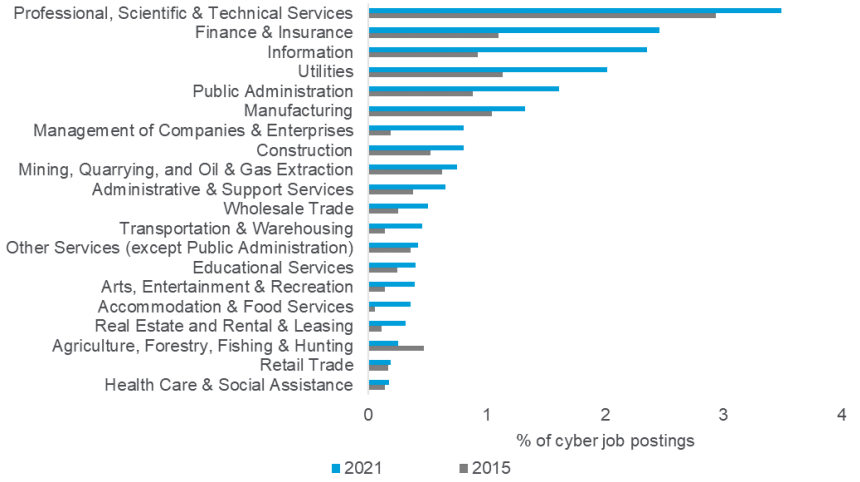
Across different industries, four sectors accounted for 80% of the cyber job postings in 2021 (see Figure 26). The largest share of cyber demand comes from Professional, Scientific, & Technical Services (32%), followed by Finance & Insurance (18%), Manufacturing (16%), and Information (14%). Among the remaining sectors, each accounts for less than 5% of all cyber jobs advertised in 2021.

Figure 26 shows the pattern of demand growth across all sectors between 2015 and 2021. During this period, the average share of cyber job postings out of all job postings in each industry grew from 0.6% to 1% — a 67% increase. The fastest-growing sectors were Information and Finance & Insurance — both doubled their demand for cyber skills during this period. As we show in the first chapter, these are also the sectors suffering from the highest number of data breach incidents.

The group of industries showing the next-largest increase in cyber demand include Professional, Scientific & Technical Services; Management of Companies & Enterprises; Public Administration; and Utilities, which saw demand rise by half a percentage point on average. The Professional, Scientific, & Technical Services sector includes law firms, IT firms, accounting or management consultancies, and advertising agencies. According to a 2022 report by IBM Security, this sector is among the five most-targeted industries by cybercriminals.[18]

[18] IBM Security, "X-Force Threat Intelligence Index," 2022.

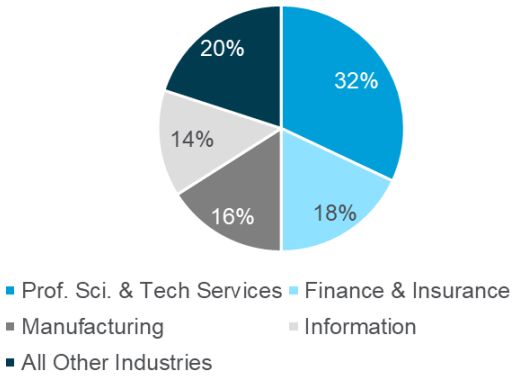
Figure 26. Industry-Specific Demand for Cyber Skills



Source: Citi GPS

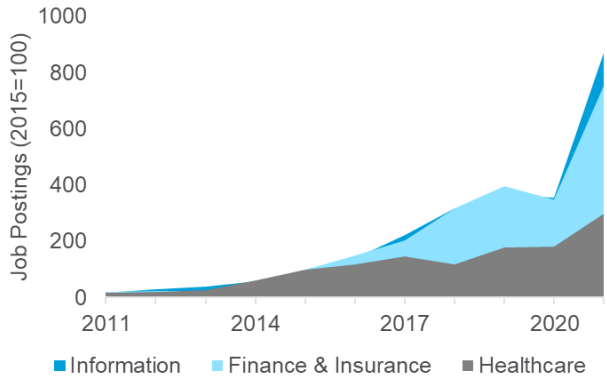
Another sector showing strong demand for cyber skills is the energy sector. Any disruption in this sector can results in high costs trickling through supply chains. Given the energy sector's strategic importance and the 2021 ransomware attack on the Colonial Pipeline, we expect this sector's strong demand to continue.

Figure 27. Demand by Sectors



Source: Citi GPS

Figure 28. Relative Increase in Cyber Demand



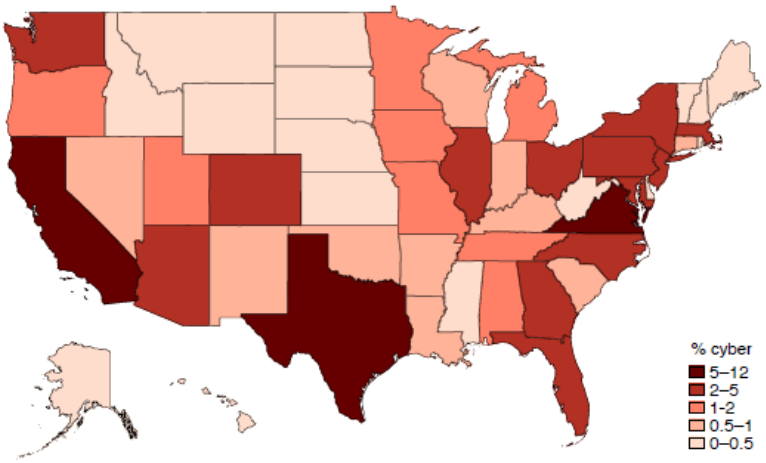
Source: Citi GPS

Interestingly, our analysis shows that the healthcare sector is lagging in terms of its demand for cyber skills. It is not surprising that the share of healthcare cyber job postings is still low given the large number of workers the sector employs in general. However, healthcare cyber job postings are also rising slowly over time relative to other industries. Although the healthcare sector experienced a large number of attacks in recent years (see Figure 28) and the overall demand for cyber jobs has more than doubled from 2015 to 2021, healthcare's cyber job posting growth is only one-third of that of the fastest-growing sectors, such as Finance & Insurance.

Demand Across Locations

As demand grows across different industries, the geographic market of cyber skills could also change. Businesses choose their locations based on agglomeration benefits and costs of production. As the cost of cyberattacks rises, employers might favor different locations for hiring cyber talent. Businesses could also relocate based on their cost of doing business or the availability of skilled workers. In this section, we examine the U.S. market closely to understand how the demand for cyber skills varies across geographies. Later, in a subsequent section, we take into account the supply side by examining the location of cyber professionals.

Figure 29. Demand for Cyber Skills Across the U.S. Market (2021)

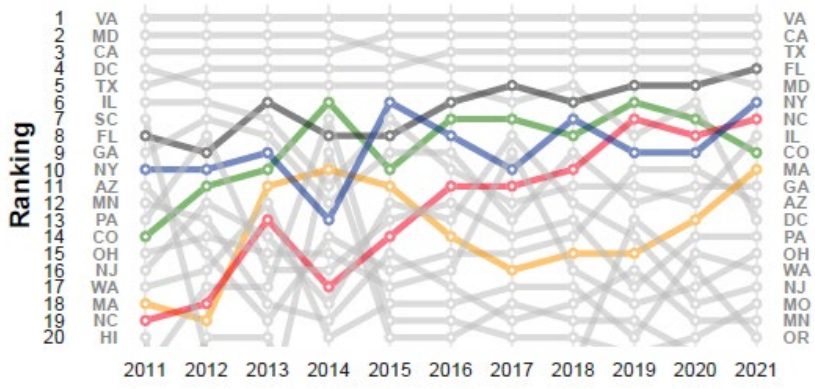


Source: Citi GPS

Figure 29 shows the concentration of cyber job postings across U.S. states in 2021. California, Texas, and Virginia came in at the top, each accounting for at least 9% of all cyber jobs advertised. Traditionally, the Virginia-D.C.-Maryland area had the highest concentration of cyber jobs because of the presence of the defense industry and government agencies. In recent years, other states have also emerged as new hubs of cyber jobs.

Figure 30 shows the full cyber job opening dynamics in U.S. states over the last ten years. The vertical axes show the ranking of U.S. states based on their share of cyber job postings at the start and end of the period. Among the top five states in 2011, only D.C. and Maryland have moved down in the rankings. This could reflect rising real estate costs in the D.C. metro area that are forcing firms and workers to reconsider their locations.

Figure 30. Cyber Demand — Ranking of U.S. States



Source: Citi GPS

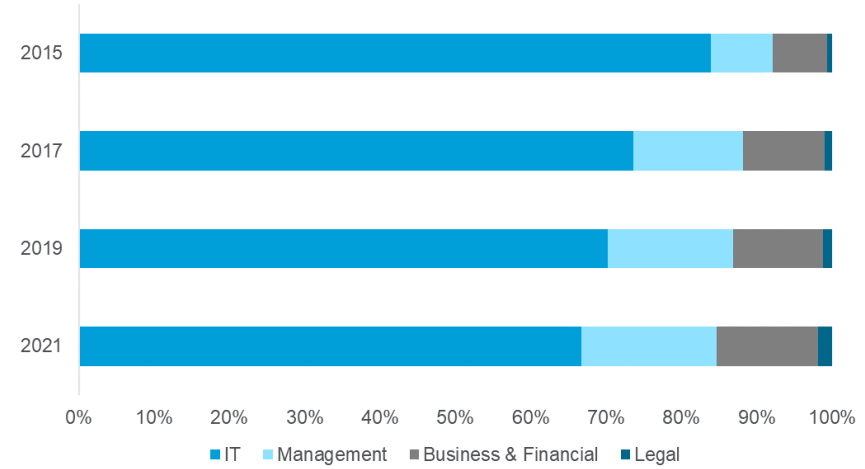
The emerging locations of cyber demand are highlighted in color. North Carolina is the most notable among them. It is now the seventh-largest market for cyber skills. Florida and New York have also moved up in ranking. By 2021, each of these states accounted for 4% to 4.6% of all cyber job postings. Among other states, Colorado and Massachusetts now make the list of the top ten states.

Occupational Demand

A large share of jobs requiring cyber skills belong to the larger group of IT-related occupations, such as IT Managers, System Administrators, Database Administrators, System Analysts, and Network Support Specialists. In 2015, the IT occupation group accounted for 84% of all cyber job postings. However, other occupation groups have seen a rising demand for cyber skills in recent years. In Figure 31, we report the share of cyber job postings across four occupation groups, namely Computer & Mathematical (IT in short), Management, Business & Financial, and Legal.[19] Between 2015 and 2021, the share of cyber job postings of non-IT occupation groups increased from 14% to 33%. The largest increase was for managerial occupations, which now account for 18% of cyber job postings. Legal occupations are also showing fast-growing demand for cyber knowledge.

[19] These categories correspond to O*Net occupational groups 15,11,13, and 23, respectively.

Figure 31. Occupation-Specific Cyber Demand



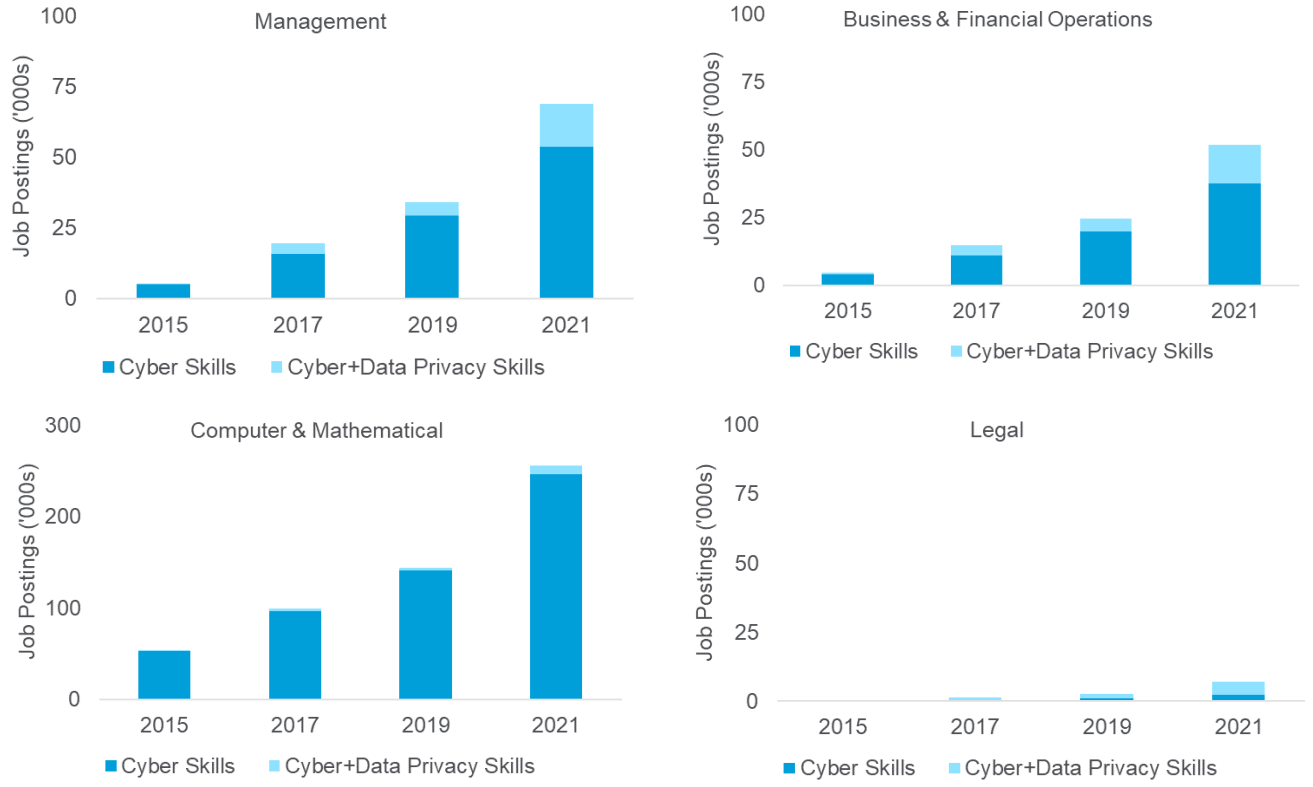
Source: Citi GPS

The changing regulatory environment accounts for some of the increased demand for cyber skills. In the final chapter, we discuss how data protection laws can change the burden on firms, requiring them to pay more attention to cyber risks. In this regard, the EU's General Data Protection Regulation (GDPR) played a pioneering role when it came into effect in May 2018.

Figure 32 shows the increased demand for roles requiring knowledge of data protection and privacy based on job postings. The figure reports the number of cyber and data privacy-related job postings (in thousands) for each of the four occupation groups. In 2015, only 2% of cyber job postings required data privacy-related skills. By 2021, 11% of these job postings required such knowledge.

Privacy-related knowledge is in especially strong demand for Management, Business & Financial, and Legal occupations. In 2021, 22.1% of cyber job postings advertised for Management positions required an understanding of data privacy-related issues. These figures are 27.7% and 6.5%, respectively, for Business & Financial and Legal occupations, whereas only 3.5% of Computer & Mathematical occupations require data privacy-related skills.

Figure 32. Demand for Cyber and Data Privacy Knowledge



Source: Citi GPS

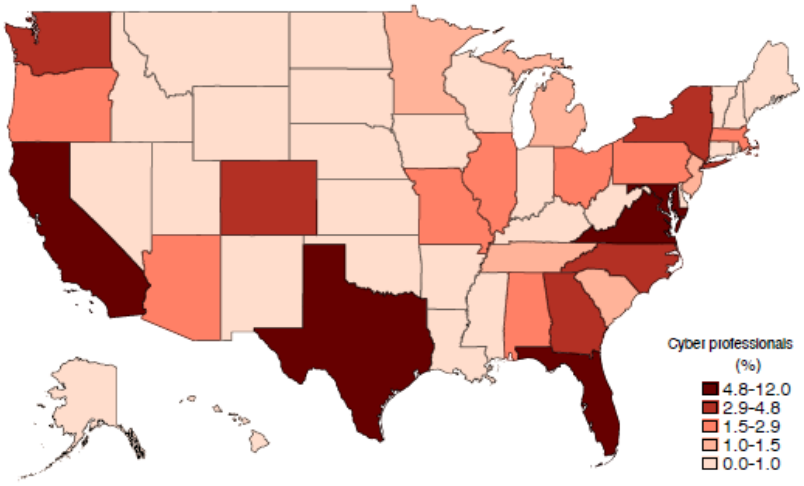
Supply of Cyber Professionals

We next turn our focus to the supply side of cyber skills in the U.S. to understand how such skills are distributed geographically. A rich dataset extracted from LinkedIn profiles of cyber workers helps us gain insights about their location choices and other characteristics.

Location of Cyber Professionals

Figure 33 shows the percentage of cyber professionals residing in each U.S. state. The states ranking at the top are Virginia (11.1% of all cyber professionals), California (9.4%), Texas (9%), Maryland (7.1%), and Florida (5.4%). Note that these are also the states accounting for the most cyber-related job postings (Figure 30). Workers with cyber skills are slightly more concentrated than all professionals. The top eight states account for 50% of all professional workers, whereas this number is 55% for cyber professionals.

Figure 33. Location of Cyber Professionals



Source: Citi GPS

Characteristics of Cyber Professionals

We calculated years of experience for cyber professionals as well as for all IT professionals. Figure 34 shows the cumulative percentage of workers by years of experience, measured by the number of years-since their graduation.

The median cyber professional has 5.7 years of experience, meaning that 50% of cyber professionals have less than six years of cyber experience. In the case of IT professionals, the median number of years of experience is over 1.6 times higher at 9.4. This comparison suggests that the workforce is relatively young for cyber-related positions. Only 18% of the cyber workforce has at least 15 years of experience, whereas 32% of IT professionals have this level of experience. For 20-plus years of experience, the gap is almost double — only 11% of the cyber workforce has at least twenty years of experience, whereas 21% of the IT workforce does.

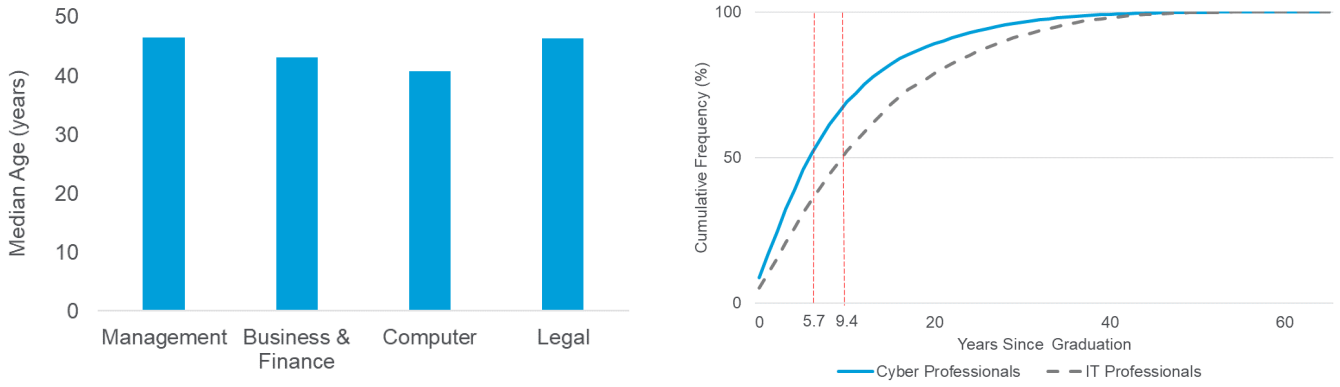
One implication of having a relatively younger workforce with cyber skills is that there are fewer workers available who can assume senior roles requiring these skills. As we discuss in the previous section, in recent years we have seen a surge in demand for cyber skills outside IT and other technical roles.

In general, these occupations also require more experience than IT occupations. For example, the average age for IT-related occupations is 41 years, whereas the average ages for Management, Business & Finance, and Legal occupations vary from 43 to 47 years (Figure 34).[20] This means that the supply scarcity is more acute for mid- or high-level cybersecurity positions. As a result, retaining talented cyber professionals should be a top priority for most employers.

[20] Labor Force Statistics from the Current Population Survey (2021).

Figure 34. Median Age by Occupation and Cumulative Distribution of Years of Experience

The workforce is relatively young with only half of cyber professionals having at least six years of experience.



Source: Citi GPS, Labor Force Statistics

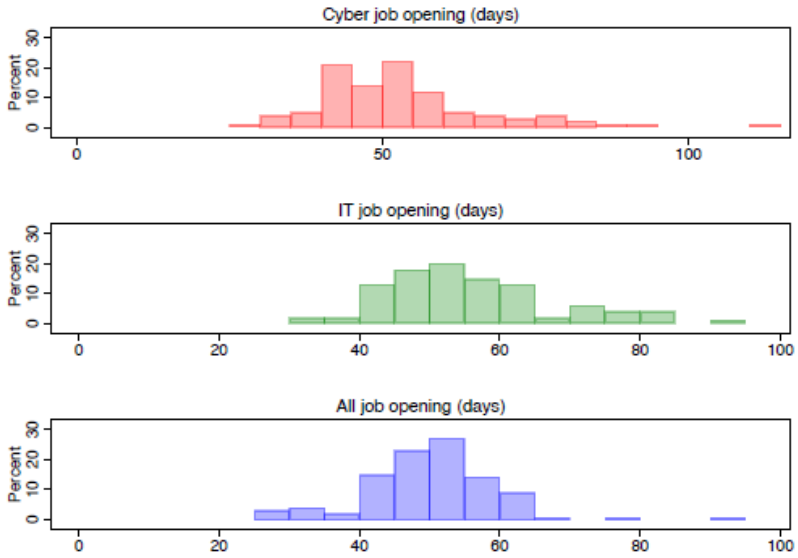
Recruiting Difficulties

In this section, we explore the implications of firms' competition for skilled cyber workers. If the rising demand outpaces the supply of cyber skills, it will take longer for firms to fill vacancies, or some vacancies will remain unfilled. We check two indicators to understand the nature of cyber skill shortages. Our first measure looks into the duration of job advertisements to understand whether it takes longer to recruit cyber professionals. Our second measure examines the demand-supply ratio to understand how acute the skill shortage is across markets.

Cyber Job Opening Times

We calculate the number of days for which a job is advertised. We refer to this period as "job opening duration." Figure 35 shows the distributions of mean job opening duration for around 100 large cities across the globe. The average job opening time is 50 days for all job postings, whereas the average is around 54 days for cyber job postings and 56 days for IT job positions. Although the averages are in the same range, the distributions of cyber and IT have a longer right tail, meaning that there are some job postings with longer opening duration than usual. The 90th percentile is 72 days for IT job postings and 75 days for cyber job postings.

Figure 35. Job Opening Duration



Source: Citi GPS

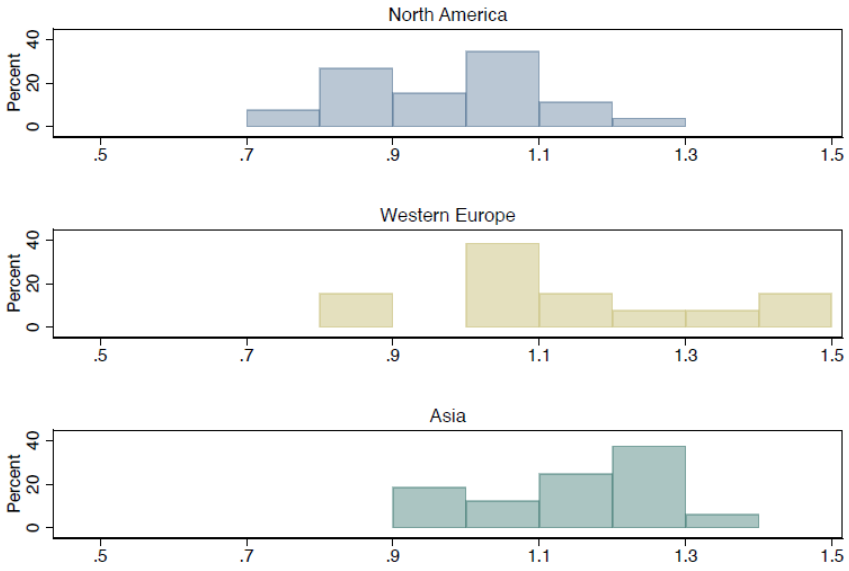
We compare the largest three markets: North America, Western Europe, and Asia. In Figure 35 we plot relative job opening duration, which is the duration of cyber job opening time normalized by the opening time duration for all job postings. The figure shows whether cyber job postings have a longer duration compared to all job postings.

We find that the North American market is rather efficient. Only 17% of cities have longer durations (by 10%-30%) for cyber job postings than for all job postings. In contrast, the data for Western Europe and Asia depict a more long-tailed distribution. The average is slightly below one for North America, meaning that cyber job postings have almost the same duration as all other job postings. Cyber job opening time is 16% and 24% longer for average cities in Western Europe and Asia, respectively. In at least half of the cities in Western Europe, cyber job postings are advertised for 10-50% longer periods than all job postings. The European cities with the longest cyber job opening times are Madrid, Copenhagen, London, Milan, and Brussels. For Asian cities, the relative job opening time is even longer.

As we discussed at the beginning of this chapter, Asia is one of the regions with the fastest-growing demand for cyber skills. We find that 71% of the Asian cities in our sample have 10-40% longer advertisement periods for cyber job postings. The Asian cities with the longest cyber job opening times are Kuala Lumpur, Manila, Delhi, Singapore, and Jakarta.

Figure 36. Relative Job Opening Duration

The North American market is relatively efficient. By contrast, cyber job opening time is on average 16% and 24% longer in Western Europe and Asia, respectively.

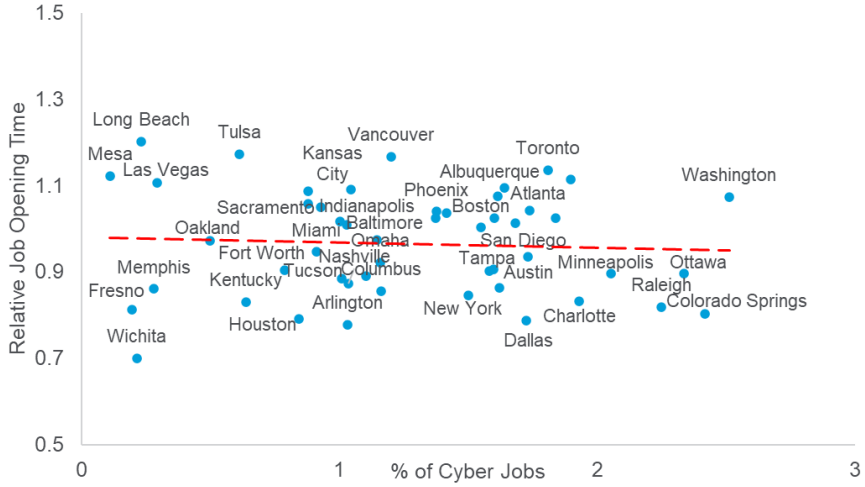


Source: Citi GPS

Finally, we assess the relationship between market size and job opening duration for the mature North American market. We find almost no correlation between the share of cyber job postings and the duration for which cyber jobs are advertised. Within the North American region, we do not observe any pattern suggesting that the cities with higher cyber demand need longer to hire workers.

Figure 37. Relative Opening Time and Market Size

The figure plots relative job opening duration for cyber jobs against the size of the market. The market size is measured in terms of the share of cyber job postings out of all job postings in the city.



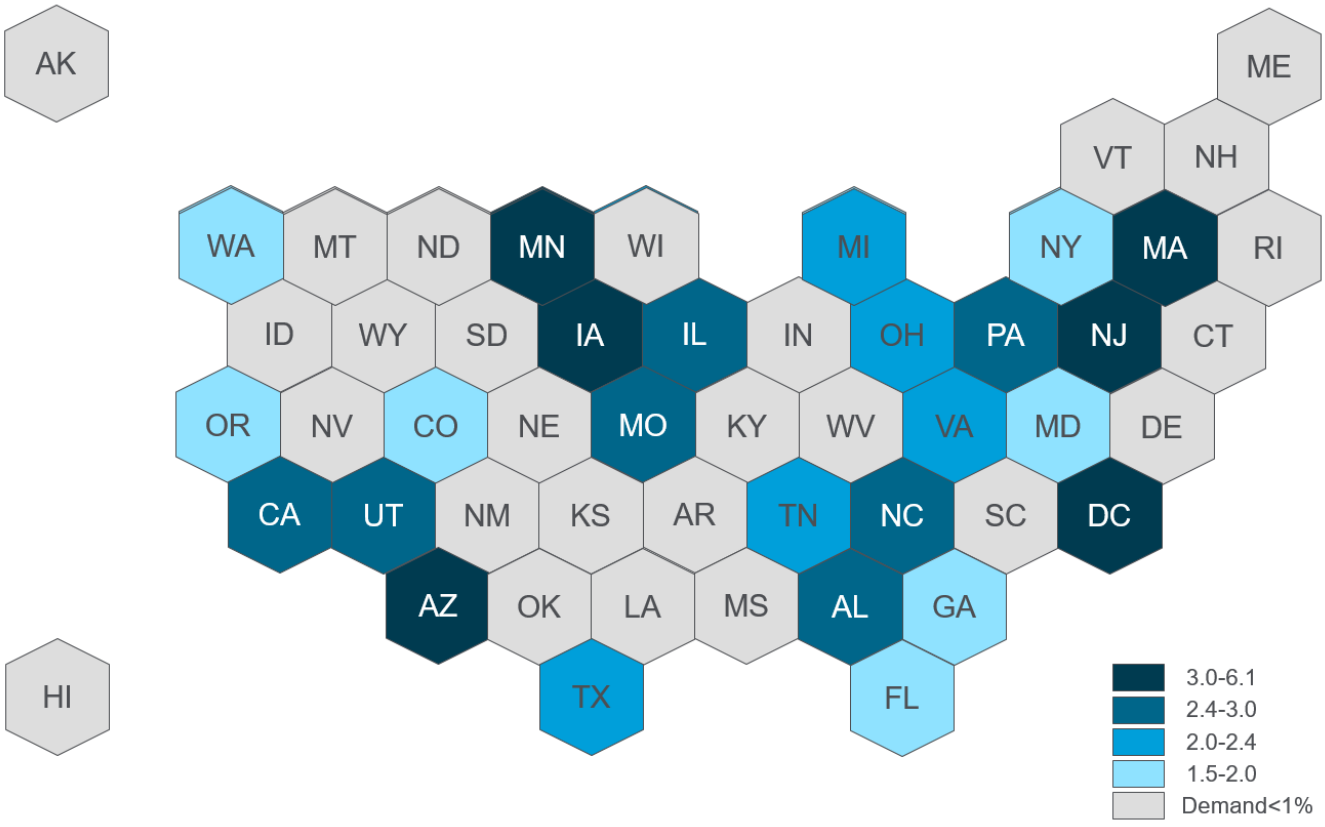
Source: Citi GPS

Does the Supply Match the Demand?

We compare the demand for cyber skills in 2021 — as measured by cyber job postings — with the supply of cyber professionals. The average U.S. state has 2.6 cyber job postings per cyber professional. Figure 38 shows how the ratio of job postings per cyber worker varies across all 50 states and Washington, D.C. We focus on the states accounting for at least 1% of all cyber job postings nationally.

In 2021, the average U.S. state saw 2.6 cyber job postings per cyber professional. The states shown in blue or dark blue report higher concentrations of these job postings. Among these locations, Washington, D.C. is an exception since most cyber professionals working there live outside of D.C. itself. Most others are established markets for cyber positions, such as California, Arizona, Massachusetts, or Illinois. Among the growing markets, North Carolina shows an acute skill shortage, with around three cyber jobs posted per worker. The states in grey or light blue are the ones with relatively better demand-supply ratios. Notably, Florida, Georgia, Colorado, Oregon, and Washington state show 1.5-2 job postings per cyber professional, which is well below the average.

Figure 38. Supply of Cyber Professionals Versus Demand for Cyber Skills (U.S. States)



Source: Citi GPS

To sum up, we review two indicators to gauge the impact of the rising demand for cyber skills. Across regional markets, we find that the recruiting time for cyber jobs, as reflected in job opening duration, is comparable with all other jobs in North America. For other regions, the market seems to move more slowly. Especially for one of the growing regions, Asia, cyber job opening times are relatively long across key cities.

Across the U.S. market, we do not find any systematic pattern suggesting that larger regional markets face more difficulties in hiring for necessary skills. Our second indicator, the demand-supply ratio, shows that some of the growing markets (e.g., North Carolina) have acute skill shortages while other large markets, such as Texas, Virginia, and Florida, have low to moderate skill shortages. In general, across all states, businesses demand more cyber skills than can be filled by the current pool of workers.

This rise in the demand for cyber talent is also evident from wages and compensation for cyber professionals. In the U.S., the median cash compensation for Chief Information Security Officers (CISO) rose 23% from 2020 to 2022 (the median figures were $584,000 in 2022, $509,000 in 2021, and $473,000 in 2020). The median total compensation, including any annualized equity grants or long-term incentives, also increased by 24% during the same period (to $971,000 in 2022 from $784,000 in 2020).[21] Moreover, employers give hiring bonuses in cash or equity (with respective median values of $175,000 and $400,000) to lure these professionals.

[21] Heidrick & Struggles, "2022 Global Chief Information Security Officer (CISO) Survey," accessed December 21, 2022.

Business Strategy for Managing Cyber Risk

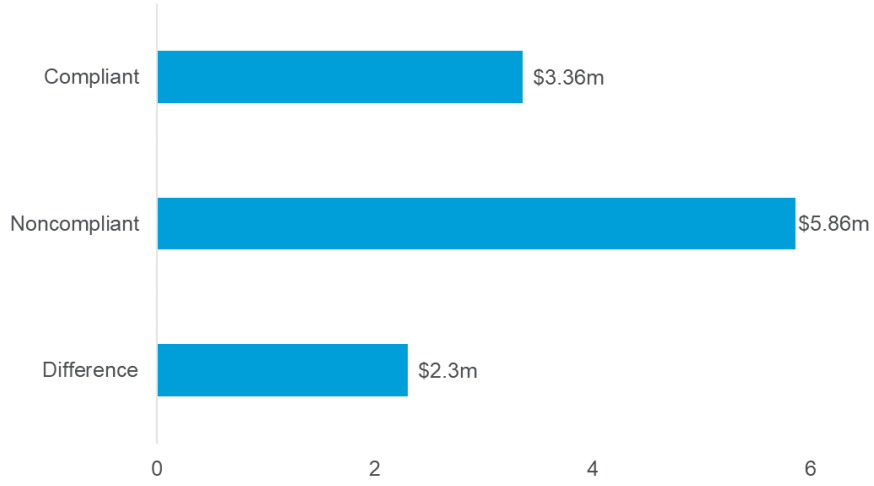
Compliance and Cyber Risk

Cost of Noncompliance

An IBM report shows that noncompliance with data protection regulations amplifies the data breach costs of a cyberattack.[22] If compliance authorities find that companies lack good cybersecurity practices or appropriate safety measures to prevent breaches, the authorities are more likely to take strict legal measures and impose harsher penalties. The average data breach cost for noncompliant organizations is $5.65 million, compared to only $3.35 million for organizations with low levels of compliance failure. The $2.3 million difference highlights the importance of compliance with cybersecurity regulations.

Figure 39. Cost of Noncompliance with Data Protection Regulations After a Cyberattack

Firms that fail to comply with data protection regulations experience 51.1% higher cyberattack costs because of fines, penalties, and lawsuits.



Source: IBM Security, Citi GPS

Moreover, the risks and costs of noncompliance are rising. Over the past few years, the data protection regulatory environment has become increasingly stringent, with a growing number of countries implementing data protection and privacy regulations. According to UNCTAD, 71% of countries in the world already have such legislation, and another 9% are drafting such laws. On May 25, 2018, the General Data Protection Regulation (GDPR) was enacted across the European Union and the U.K. Since then, several countries and jurisdictions have adopted similar data privacy laws, such as the California Consumer Privacy Act (CCPA).

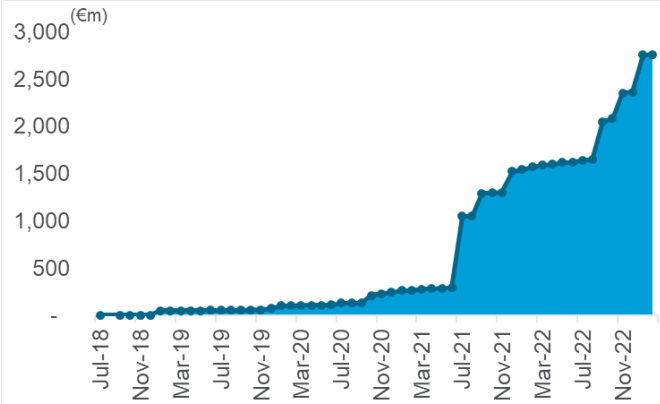
Reviewing the total fines for noncompliance indicates that the passage of the GDPR significantly increased both the risk and the cost of noncompliance for businesses across European countries. This is because the maximum fine increased substantially under the GDPR. Under the latest rule, an organization could be charged for an amount of up to €20 million (~$21 million) or 4% of its annual global turnover, whichever is higher. The law also makes it mandatory for data controllers to notify data protection authorities as well as affected individuals within 72 hours of becoming aware of a breach.

[22] IBM Security, "Cost of a Data Breach 2022 Report," July 27, 2022.

Figure 40 shows that not only have fines become more frequent across European countries since 2018, but their amounts have also increased. The last two years saw a particularly notable surge. While the cumulative amount of issued penalties by January 2020 totaled €100 million (~$106 million) for 169 GDPR cases, it increased to €1,671 million (~$1,767 million) for 1,233 cases by August 202

Figure 40. Course of Overall Sum of Fines (Cumulative)

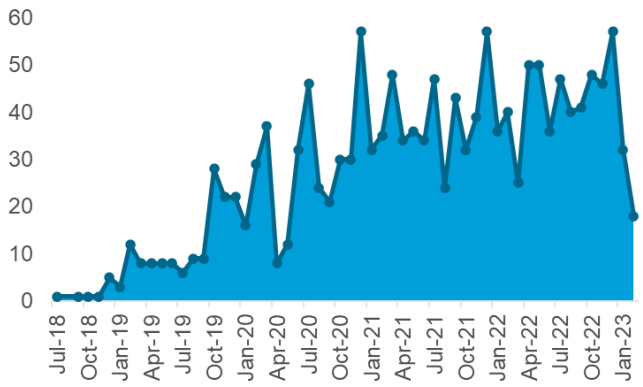
The cost and risks of noncompliance are rising, with the number of fines has surging since 2021.



Source: Citi GPS, CMS.Law GDPR Enforcement Tracker

Figure 41. Sum of Fines Per Month (Non-Cumulative)

The cumulative number of fines increased to 1,233 cases in August 2022 vs. 169 in Jan 2020.



Source: Citi GPS, CMS.Law GDPR Enforcement Tracker

Notably, 247 of the European cases were related to data breaches and insufficient technical and organizational measures related to information security. The same scenarios applied to many of the mega-fines of €1 million (~$1.1 million) or above. The highest fine, issued to British Airways, was due to a 2018 cyberattack that breached names, email addresses, and credit card details of more than 400,000 of its customers. Reviewing other mega-fines for data breach cases reveals that, apart from those that risked customers' financial data, companies that lost or endangered customers' medical records were subject to the highest penalties.

Figure 42. Top 10 Highest GDPR Fines for Data Breaches Since 2020

Organization	Country	Date	Amount (€)
British Airways	UK	2020-10-16	22,046,000
Marriott International (Lodging including hotels)	UK	2020-10-30	20,450,000
Meta Platforms	IRELAND	2022-03-15	17,000,000
Cosmote Mobile Telecommunications	GREECE	2022-01-27	6,000,000
OTE Group (Telecommunications)	GREECE	2022-01-27	3,200,000
Capio St. Göran (Health care provider)	SWEDEN	2020-12-03	2,900,000
DEDALUS BIOLOGIE (software solutions for medical analysis)	FRANCE	2022-04-15	1,500,000
Aleris Sjukvård (Health care provider)	SWEDEN	2020-12-03	1,463,000
Ticketmaster (ticket sales and distribution company)	UK	2020-11-13	1,405,000
AOK (health insurance company)	GERMANY	2020-06-30	1,240,000

Source: Citi GPS

How Data Protection Enforcement Differs Across European Countries

The GDPR was enacted across various European countries in 2018. Nevertheless, its enforcement substantially differs across the region. For instance, in Spain, Agencia Española de Protección de Datos (AEPD) has significantly increased the number of fines issued but has kept the amount of the fines rather low. While Spain ranks first in the number of penalties with 471, the sum of fines only amounts to €56 million (~$59 million). In contrast, France has issued only 28 fines, but they total €271 million (~$287 million). This highlights the two strategies that European countries have used to ensure compliance with GDPR — increased enforcement and increased penalties.

Increased Enforcement Versus Increased Penalties

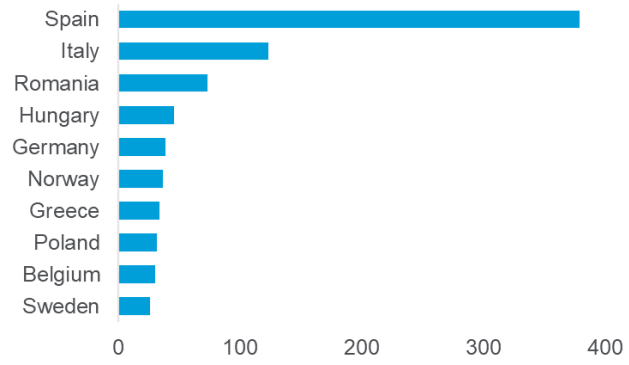
A study by a research team at the Oxford Martin School of the University of Oxford examines the effectiveness of these two strategies. The researchers looked into two periods of data protection enforcement by the Information Commissioner's Office (ICO) in the U.K. Between 2015 and 2018, the ICO adopted an aggressive enforcement campaign to increase firms' compliance with the data protection regulation. During this period, the ceiling of fines stayed relatively low. However, the ICO changed its strategy after the enactment of the GDPR, which substantially raised the ceiling of monetary penalties. Since then, the ICO has relied more on mega-fines but decreased its frequency of issuing monetary penalties.

The researchers also focused on the trend of cybersecurity hirings during these two periods, as hiring cyber talent is one of the most effective ways firms can reduce the risk of data breaches and stay compliant with information security standards. They find that both approaches can be effective if they are well-designed, but each strategy has clear advantages and disadvantages.

While the impact of mega-fines is substantially stronger in bringing firms closer to compliance, frequent-but-smaller penalties have a more widespread and monogenous impact across firms of different age and financial strength.

Figure 43. Europe: Number of Fines Per Country

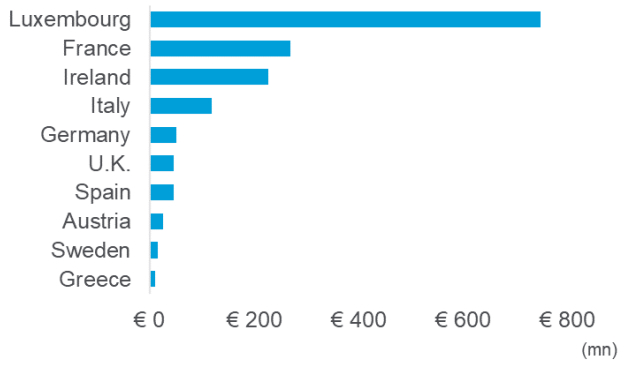
Countries such as Spain have significantly increased the number of fines issued while keeping the amount of fines relatively low.



Source: CMS.Law GDPR Enforcement Tracker Report, Citi GPS

Figure 44. Europe: Sum of Fines Per Country

Countries such as France rely on fewer but larger sums of fines.



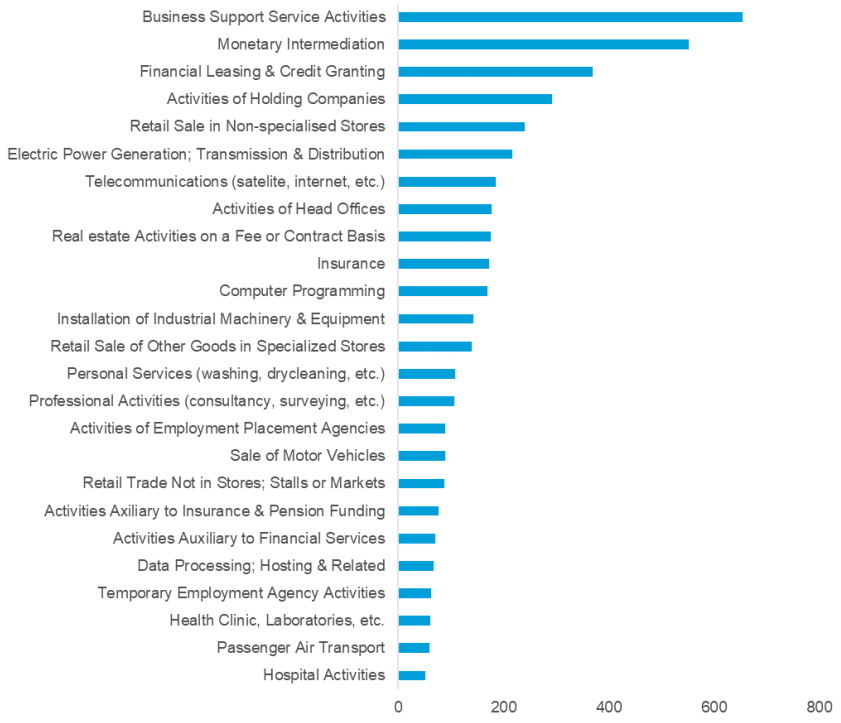
Source: CMS.Law GDPR Enforcement Tracker Report, Citi GPS

Which Industries Are Most Exposed to Enforcement?

Businesses in different sectors are exposed to different degrees of compliance risk. This is partly because firms in some industries deal with more valuable and sensitive personal data than others. Traditionally, financial information on customers' credit and debit cards was among the most valuable, and thus most expensive, personal data to lose. Recently, medical records, owing to their potential sensitive contents, brought regulators' attention to ensuring their protection.

Oxford Martin School researchers reviewed around 5,800 data protection cases in the U.K. to shed light on which businesses face the most customer complaints and resulting actions from regulators.[23] The "business service activities" sector comes at the top of the list. This sector includes a wide variety of businesses, but many of them are specialized information brokers, such as Jobzooma Ltd. (a job recruiting platform). The sector of financial activities such as leasing, credit granting, insurance, and real estate activities comes next. Retail and utility companies are also often exposed to data protection enforcement. Finally, complaints regarding healthcare providers and businesses account for another significant segment of data protection cases.

Figure 45. Data Protection Enforcement Across Different Industries



Source: Oxford Martin School, U.K. ICO, Citi GPS

[23] Pantelis Koutroumpis, Farshad Ravasan, and Taheya Tarannum, "(Under) Investment in Cyber Skills and Data Protection Enforcement: Evidence from Activity Logs of the UK Information Commissioner's Office," July 23, 2022. Available at SS

Cybersecurity as a Public Good

A firm's exposure to cyberattacks not only depends on its own cyber resilience, but also on its partners' and suppliers' resilience to cyber risk. In other words, a firm's cyber hiring can also improve its partners', suppliers', and customers' cyber safety. In this sense, cybersecurity is a public good, and its provision should be a collective and coordinated decision.

So how do we address market failure in the provision of cybersecurity? There are two approaches to ensure the optimal provision of a public good. One is government intervention via regulations that oversee firms' data protection and security. The second is encouraging firms to integrate cybersecurity as a part of their corporate social responsibility (CSR) agenda. Both are important to highlight because cyberattacks can have substantial social impacts. For instance, the ransomware attack in May 2021 that led to the Colonial Pipeline's shutdown for six days left 88% of Washington D.C. without gas supply.

When it comes to government intervention, there is always a trade-off between the benefits and adverse effects of regulation. The cost of regulation also includes compliance cost, operational uncertainty, and costly hirings to adapt to the new regulatory environment. Research by economists at the University of Oxford examined this trade-off in the context of stronger data protection regimes adopted by the U.K. data protection authority.[24]

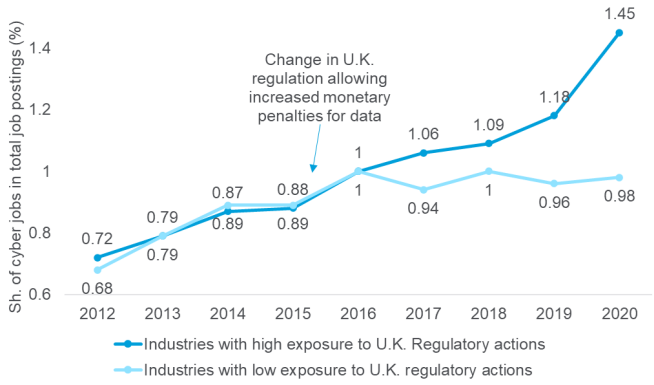
As already discussed, the U.K. has one of the strongest regulatory environments around data privacy, with the Information Commissioner's Office (ICO) overseeing compliance with the Data Protection Act (DPA), GDPR, and Privacy and Electronic Communications Regulations (PECR). Researchers compared industries with high and low exposure to ICO enforcement and found that the high-exposure industries experienced a 26-52% increase in the demand for cyber skills following the introduction of stronger data protection regimes.

Figure 46 and Figure 47 show the demand for cyber skills across the two types of industries. The top panel reports normalized shares of cyber job postings, clearly showing a break in the trend in recent years. The bottom panel reports the actual share of cyber job postings, revealing that high-exposure industries initially had a lower demand for cyber skills.

[24] Ibid.

Figure 46. Data Protection Enforcement and Demand for Cyber Skills

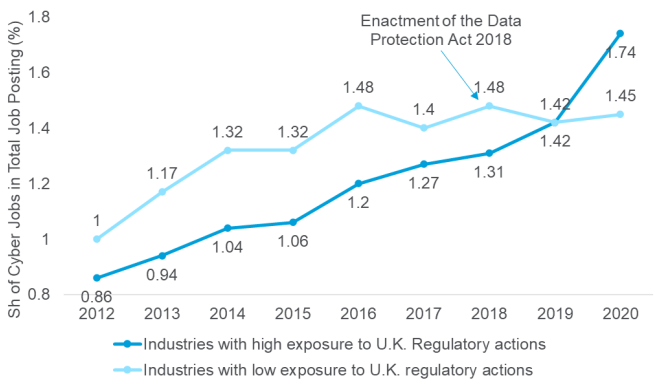
Highlighting UK ICO's greater discretion to issue monetary penalties.



Source: Citi GPS, Oxford Martin School

Figure 47. Data Protection Enforcement and Demand for Cyber Skills

Highlights the enactment of the Data Protection Act of 2018

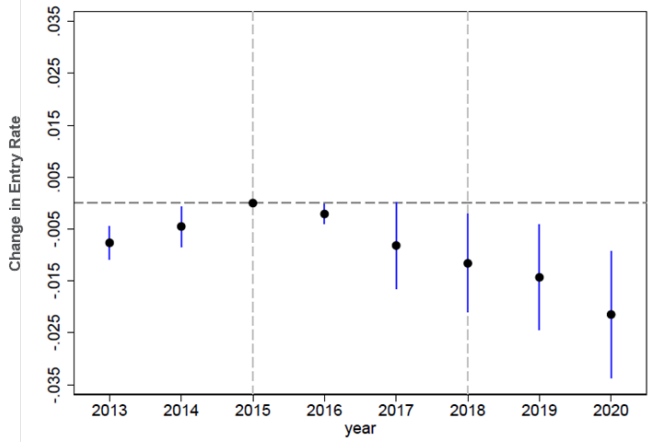


Source: Citi GPS, Oxford Martin School

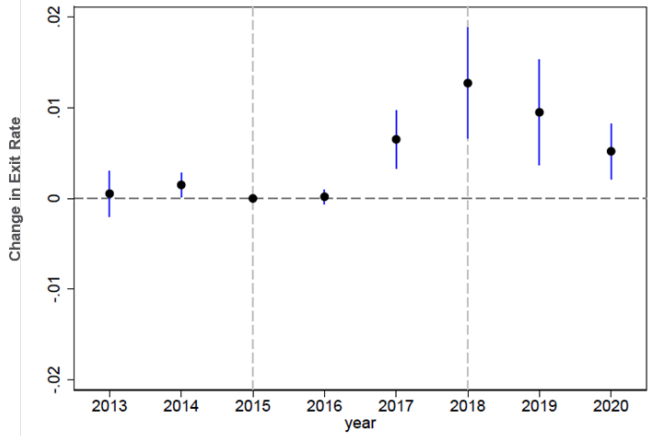
Although there is a compelling case for stronger data protection regulation, it comes at a cost. The aforementioned study examines the entry and exit rates of the industries with high and low exposure to ICO enforcement. The entry rate to high-exposure industries slowed down significantly by up to 1.4 percentage points after the legal changes. Similarly, the exit rate increased by up to a percentage point. These findings highlight the trade-off — stronger data protection laws are effective in increasing investment in cybersecurity, but at the same time, they could slow down firm creation.

Figure 48. Impact of Data Protection Regulation on Firm Entry and Exit

The top panel shows the differences in entry rates for high vs. low exposure industries. The downward turn means the entry rate in high-exposure industries falls below the entry rate of the low-exposure industries. The blue line shows the confidence interval of the estimates. The bottom panel shows the differences in exit rates for the high vs. low exposure industries. High-exposure industries have a relatively higher exit rate under strict regulation, but the difference is getting smaller.



(a) Entry rate



(b) Exit rate

Source: Pantelis Koutroumpis, Farshad Ravasan, and Taheya Tarannum, "(Under) Investment in Cyber Skills and Data Protection Enforcement: Evidence from Activity Logs of the UK Information Commissioner's Office," July 23, 2022.

Not all businesses experience the same adverse effects of regulation. The California Consumer Privacy Act (CCPA) limits firms' ability to access personal data. A recent study on the CCPA found that this adversely affects firms that rely on external data to develop their products.[25] In contrast, the study found that firms with in-house data from a large customer base thrive in the new environment, enjoying a higher return on assets.

The evidence presented so far highlights the importance of considering alternative tools to strict regulatory measures, which is the topic of the next section.

[25] Mehmet Canayaz, Ilja Kantorovitch, and Roxana Mihet, "Consumer Privacy and Value of Consumer Data," Swiss Finance Institute Research Paper No. 22-68, June 2, 2022.

From Cyber Risk to Cyber Resilience

The Growth of Responsible Investment

Anita McBain
Head of EMEA ESG Research
Citi Research

ESG stands for environmental, social, and governance investing. Investors who adopt or utilize this acronym to describe an investment style can demonstrate an approach to integrating non-financial disclosures that align to a specific environmental or societal issue.

Examples include the reduction of greenhouse gases to align with a net-zero emission strategy; addressing the lack of gender or racial diversity within their portfolio companies; or analyzing board governance of financially material issues such as climate action, biodiversity loss, and supply chain management.

The UN Principles of Responsible Investment (UNPRI) describe the many approaches now deployed under the banner of ESG investing as sustainable investing, socially responsible investing, responsible investing, impact investing, and thematic investing, among others.[26]

ESG Integration

For many investors, the adoption and integration of non-financial disclosures can be a proxy for management quality by demonstrating how well a company has understood and then mitigated a future risk. Key drivers to pursue an ESG strategy can include asset owner demands for transparency and traceability, regulatory pressures for greater disclosures, inter-generational wealth transfer, and the recent arrival of "big data" analyzed using artificial intelligence and machine learning. Big data has revealed many new investment opportunities, and investors operate in an era of "data superabundance."

For many investors, the starting point when assessing risk is understanding how risks manifest, including whether they could arise from changing regulations or a threat of litigation if a company is found to be in breach of a local environmental or human rights law. Investors also look at reputational risk, such as from negative images posted on social media implicating a company in an illegal activity linked to effluence, waste, modern slavery, or environmental pollution, for example.

The risks described above are potentially financially material, and it is incumbent on asset management teams to demonstrate that they have assessed these future risks to understand how well-positioned a portfolio or investee company is at mitigating and managing them. Investors today wish to understand the resilience of their investee companies in the face of future risk from climate change, biodiversity loss, food insecurity, energy prices, employee attraction and retention, supply chain management, and cybersecurity.

Cyber Risk's Sector-Agnosticism

Cyber risk can impact any company in any sector or geography that holds or processes confidential personal or financial data. It is often described as a governance issue, and if financially material, it should be incorporated into an enterprise risk management (ERM) framework. Companies that retain and process confidential personal data related to finance, health, or identity can be at risk of a data breach.

[26] Principles for Responsible Investment (PRI), "An Introduction to Responsible Investment: What is Responsible Investment?" accessed November 14, 2022.

If sensitive data is widely disseminated or falls into criminal possession, individuals might be at risk of having funds or identities stolen and, in more extreme cases, fall victim to personal demands from criminals who are intent on extracting a financial reward.

This short chapter discusses the importance of cyber governance failures for investors who have widened the scope of their ESG analysis and integration. The chapter also references the work of the UNPRI, which defines responsible investment as "*a strategy and practice to incorporate environmental, social, and governance factors in investment decisions and active ownership*."

The Financial Materiality of a Cyberattack

Today, many investors consider a cyberattack or the exfiltration of confidential client data to be a serious and financially material event. If data is exposed and then unlawfully possessed, it has the potential to cause a major disruption to business operations and personal employee and customer security. This can be further compounded by legal fines, reputational damage, and disciplinary action from local regulators, all exacerbated by negative media headlines and vocal employee and customer dissatisfaction.

Personal security, or human security, is an issue highlighted by the ongoing conflict in Eastern Europe that has seen over 5 million people displaced. To achieve human security, individuals require reliable access to food, energy, and water. Human security also encompasses access to health systems and modern medicine, nutritious food, freedom from forced labor, and, in a modern society, freedom from the threat of online predators and exploitation.

Companies' protection of their employees' and customers' identities is a new aspect of delivering personal security. Companies that invest insufficiently in robust and resilient cyber defense technology put their digital infrastructure at risk and can undermine their business credibility with key suppliers, consumers, employees, peers, and other stakeholders. Companies possessing weak or inadequate cyber infrastructure may face a less-than-forgiving regulator or government that prohibits payment as part of a ransomware attack.

These threats are financially material, and companies must be able to credibly demonstrate that they understand them. They must also be able to prove they have sufficiently robust technology to protect key stakeholders, deliver on personal security, and ultimately protect their business from cyberattacks.

Since the invasion of Ukraine, there has been a notable shift from terrestrial land warfare to cyber warfare, and many companies worry that it is not a matter of if they will suffer a cyberattack, but when. The World Economic Forum has long cautioned that cybersecurity risks and data breaches will have a major impact on the worldwide operations of businesses, as the attacks, which are often transboundary, are global in nature.[27]

[27] David Paul, "Cybersecurity Risks a Major Global Threat, World Economic Forum Warns," *DIGIT News*, January 11, 2022.

For many businesses, new responsibilities have arisen under the remit of the chief information security officer (CISO), with the inclusion and mapping of cyber risk often embedded within the ERM framework and routinely discussed at the executive level. This is exactly the sort of engagement that an active investor might wish to be informed about to identify where the ERM framework prioritizes cyber risk and what level of board oversight has been attributed to its successful delivery.

The COVID-19 pandemic accelerated a move toward greater online corporate activity amid the shift to remote work and the increasing frequency and complexity of business communications. The digitalization of everyday activities has benefited remote workers but increased the need for vigilance, as online systems are stress-tested daily. Notably, remote work also delivers benefits across the demographic spectrum, making jobs available to a broader array of workers, some of whom may be more cyber-literate than others. This highlights discrepancies within firms around cyber awareness and exposes areas of potential weakness.

Fostering employee awareness of heightened cybersecurity protocols deployed in the office, at home, and on the move is now embedded into many online corporate training modules, especially those concerning systems at risk of infiltration. The high-profile ransomware attack in May 2021 of the U.S. Colonial Pipeline, which immobilized computer systems that managed the pipeline billing infrastructure and disrupted gas, diesel, and jet fuel distribution for 17 U.S. states, resulted in U.S. President Joe Biden declaring a state of emergency.

Managing Cyber Risk with Active Engagement

The trust of, and dependency on, cloud-based and remote digital systems by companies, governments, and civil society has fundamentally shifted global interactions and operations across time zones and jurisdictions. While cloud-based and remote digital system capabilities create new opportunities for companies to meet the demands of an increasingly global, interconnected, online, and generally younger consumer base, they also expose all users to more pernicious forms of cyber risk and data breaches.

As highlighted by the UNPRI, which gives an investor's point of view, "there is a strong business case to actively engage with portfolio companies to understand how they are managing cyber risk, now considered a governance issue, and an area where executive oversight is essential."[28]

For many investors, having confidence that a portfolio company is managing all risks, whether cyber-related or climate-related, requires clear board oversight and ownership. Investors routinely evaluate the skills and competency of the individuals responsible for delivering on climate-related risk, and companies should expect the same level of scrutiny to be applied to cybersecurity-related risk.

Cybersecurity Governance

Investors have several reasons to engage with portfolio companies on their digital and cyber technology. A breach could be financially material and reputationally debilitating if confidential data is exposed and disseminated, resulting in penalties. Penalties can range from fines to, in the worst-case scenario, criminal convictions for obfuscation in the event of a data breach, as happened with Uber's former head of security in 2016.

[28] PRI, "Governance Issues: Introduction," July 24, 2018.

In a report on cybersecurity governance, the UNPRI identified and named the key cyber threats that investors need to be aware of.[29] These range from malware and web-based attacks to ransomware, insider threats, and phishing. Since employees can accidentally or intentionally disclose confidential data, robust and rigorous internal controls are necessary to prohibit and remediate suspicious activity. Investors keen to build a coherent engagement strategy can reference the UNPRI resources to develop a framework to understand portfolio companies' fluency in cyber risk, including any early detection measures in place to thwart imminent attacks and remediate a breach.

If a portfolio company is unable to explain its cyber infrastructure, it is reasonable for an investor to request the appointment and deployment of a cybersecurity expert to deliver a robust cyber resilience strategy. This constitutes an active engagement strategy with measurable outcomes that can be evidenced over a defined timeframe; for example, 18 months to three years.

Non-Financial Costs of Cyberattacks

Advances in desk-based and mobile technology dramatically improve employee efficiency, satisfaction, cohesion, work life balance, and productivity as the global workforce moves towards a more hybrid approach. Yet, employees can find themselves exposed to more sinister forms of digital and cyber threats, as the sophistication of online attacks evolves faster than the speed of security measures to prevent an attack.

The financial burden of a cyber breach can reach into thousands and sometimes millions of dollars. This is compounded by the reputational damage, legal costs, and regulatory fines that can result. The impact is not just financial — for individuals that find themselves implicated in a security breach, there could be an impact on mental health and well-being, which is further exacerbated if the breach results in disciplinary action, suspension, and fines.

How portfolio companies protect employees' mental health and well-being extends to the cybersecurity training and education they offer regarding online activity, both company-related and personal.

Growth in Cyber Solutions

The growth in demand for cyber solutions and cyber defense has been a focus for European governments. The 2022 U.K. National Cyber Strategy set out a comprehensive approach to tackling emerging cybersecurity threats. Pillar 2 of the U.K. Strategy is "Cyber Resilience," and the U.K. government has deployed cyber centers to offer preparedness and advice.

Remote work has also accelerated the routine transmission of sensitive company data on handheld devices by an increasingly mobile workforce as they travel between countries and work across a diverse array of technological infrastructure.

Technological solutions can effectively streamline business operations, aligning actions to corporate goals and dramatically improving efficiency, quality, and productivity. As companies increase their reliance on automation and technology, they also need to increase their reliance on cyber solutions and be more alert to malicious cyber intentions.

[29] Ibid.

The increase in digitalization is one of the reasons the UNPRI highlights the need for signatories to demonstrate an awareness of cyber risk and how it can impact portfolio companies. Backed by $121 trillion of assets under management, the UNPRI has been a vocal ally in its efforts to promote cybersecurity awareness.

Forward-Looking Investor Engagement

Investors keen to engage with portfolio companies on cyber risk can take a number of steps to assess the sophistication and business relevance of a cyber strategy. Staff training, a critical first line of defense, is often the most time-efficient way to identify and prevent a data breach. Simulation dummy attacks can help prepare staff by building risk familiarity and vigilance into everyday activities. Training also evidences a credible employee awareness strategy if having to explain or demonstrate risk mitigation activities to shareholders or regulators.

If a company does fall victim to a cyberattack, regulators often want to know how long the company took to detect and respond to the breach, as well as the response time upon detection and the promptness of escalation to the relevant regulatory authority.

Investors seeking to understand a company's cyber risk preparedness should seek clarification on how the company defines reporting lines such that if an employee detects a breach, they can act with immediacy, confidence, and urgency. A clearly articulated and well-communicated incident response plan is a crucial element of cyber resilience.

We lay out some questions investors can ask today:

- Does the company launch dummy attacks for employees to familiarize themselves with suspicious activity?
- How often does the company update its cyber training employee module, and what does it use for the updates? How does the company stay informed and up-to-date on the latest information?
- How does the company prove that employee training reflects the latest cybersecurity knowledge, and does it work with cybersecurity experts? If so, who?
- How often do staff complete cyber training? Is it monthly, quarterly, or yearly? What is the reason for the monthly, quarterly, or yearly decision?
- How does the company demonstrate "cyber hygiene" at all levels of the organization?
- Has confidential data ever been exfiltrated and if so, how quickly did the company respond to the attack and within what timeframe?
- What were the learning outcomes from past attacks, and was the company able to identify how the attacks originated?
- In the event of a data breach or attack, do staff have clear instructions on how to escalate?
- How often does the company conduct penetration testing of firewalls, and does it work with any experts on this?

- How are employees working in the cyber risk and resilience function trained to safeguard personal information in the event of a breach?

Cybersecurity: Automation and Outsourcing

Practical Commercial Solutions Will Likely Come From Private Sector

Fatima Boolani
U.S. Software Analyst
Citi Research

Outside of public-private sector partnerships to develop cyber talent through collaborative avenues like vocational training, higher-ed training initiatives, and standardized certifications, the most pragmatic approach to addressing the cyber talent shortage may be to leverage products from private-sector product vendors, such as those incorporating automation and AI, that offer more headcount-efficient defense.

Increasingly, we see a rising appetite for outsourcing security services and leveraging external consultants in the cybersecurity realm. Such outside experts may offer deeper expertise, better headcount return on investment (ROI), more effective around-the-clock security operations management, and more expansive cross-industry risk management. But this opportunity, too, is being "software-enabled" — i.e., usurped by software product platforms rather than professional services firms relying mostly on human labor.

Working Smarter, Not Harder: Automation Versus Labor-Intensity

The security operations center (SOC) has long been the backbone, or "mission control room," of an organization's ongoing cybersecurity strategy, both in terms of breach detection and incident response. The SOC's modus operandi in the pursuit of these objectives has always been gathering and analyzing data from across an organization's internal IT footprint — users, networks, endpoints, servers, databases, applications, websites, and email inboxes — as well as from external sources and threat intelligence feeds. Yet, the task at hand has become more challenging due to the "Great Dispersion" of these attack vectors amid trends toward digital transformation and hybrid work.

The resulting decentralization of organizations has metastasized the cyberattack surface — the set of points on a system where an attacker can try to enter. This has overwhelmed often under-staffed, under-resourced SOCs, which must now contend with skyrocketing volumes of alerts, signals, events, and suspicious emails. Meanwhile, in this vastly more distributed network environment, malicious actors are enjoying an offensive attack advantage indifferent to the size of their victim organizations, as these organizations' adoption of novel technologies introduces new cyber blind spots, and thus incremental roads of incursion.

Along with the talent shortage, these factors are exposing the increased depth of skills now required of cyber defense and SOC personnel. Current trends have also laid the groundwork for the technology disruption we have begun to see in the modern, more analytically anchored SOC, including (1) security incident event management (SIEM), (2) SIEM + user entity behavior analysis (UEBA), (3) SIEM + UEBA + security orchestration automation response (SOAR), and (4) SOAR + extended detection response (XDR).This is driving vendors across the infrastructure software spectrum to rush to stake their claims in these areas. Indeed, Citi Research's proprietary research has shown that investments in security analytics operations toolsets (encompassing SIEM, XDR, network detection response, traffic analysis, incident orchestration response, threat hunting, and intelligence) remain optimistic and enjoy a relatively high priority sequence in the Chief Information Officer (CIO) organization.

Product Platform for the Majors...

We concede that cybersecurity efficacy is increasingly a data analytics and data management problem. This is especially true as IT environments become more complex and multi-modal. Yet, there is little consensus on which vendor(s) are primed for wallet share leadership (and conversely, relegation) in the overdue modernization of the SOC. This debate stems from a combination of:

1. **Public cloud (infrastructure as a service (IaaS) vendors muddying the pricing waters:** This occurs given their underlying infrastructure elasticity and ability to process a data deluge at massive scale.

2. **Emergent categories muddying the terminology waters:** The recent emergence of an extended detection response (XDR) solution category promises centralized data collection, event/incident correlation, forensic analyses, and tailored responses to compromises across the entire dispersed IT infrastructure of users, devices, networks, and clouds. Such cross-vector visibility and attack response purview is intriguing, but requires integration and upkeep with myriad control points, and thus third-party competitor vendors. The delta in functionality from what security incident event management (SIEM) has been attempting to achieve for years is also contentious. At present, the commercial awareness of XDR's spans anywhere from an SIEM super-set and complementary augment, to an outright replacement.

3. **Sector consolidation bringing disciplinary consolidation, new angles:** Cybersecurity, performance monitoring, and networking vendors branching beyond their respective core domains, are aggressively moving to holistically tackle cyber defense efficacy (and budgets) in the SOC. Breaking operational and financial barriers to threat data ingestion and anomaly comprehension, these tie-ups have been a precursor to, and evangelizer of XDR ("big picture", "connect the dots" attack view) aspiring to dent mean-time-to-detection (MTTD) on security compromises irrespective of where they originate.

4. **Heightened demands for SOC workflow automation muddying the functional waters:** While reducing mean-time-to-respond (MTTR) naturally follows suit on MTTD reduction, it demands greater process and workflow automation against alert barrage and an overwhelmed, scarce SOC staff. Such requirements have consequently birthed the SOAR sub-segment within the security analytics market. This capability increased in prominence for SIEM, XDR, and to a lesser extent ITSM vendors, as security incidents, concurrently exploiting multiple enterprise IT systems, require a coordinated response.

Putting it all together, we anticipate that as XDR matures in awareness, adoption, and productization and "XDR ecosystems," led by a select group of cybersecurity vendors, will likely emerge as the most viable solution to the cyber talent shortage. This will be especially true in the large enterprise tier, with vendor standardization occurring where most of the event data is generated — i.e., with the vendor who owns the control point from which the most critical mass of event data is generated and/or collected, or the vendor/platform enjoying the greatest "telemetry gravity" and deployment pervasiveness. This in turn brings the high-fidelity signals and necessary automation needed to do more with less.

…Software-Enabled Services for the Masses

For the mass market, the picture is somewhat nuanced. The appetite to outsource security operations continues to increase, and the small/medium business segment of the market is particularly vulnerable given the low levels of investment in security operations and high attack susceptibility. But even this segment is likely to see the total cost of ownership benefits of what we would characterize as a long-tailed services-to-software conversion runway within the labor-intensive security services arena.

As mentioned, the preponderance of today's "next-gen" security product platforms — especially in the network and endpoint cybersecurity sub-disciplines — have an analytically-focused, forensically-driven, and proactive response-oriented product DNA that has traditionally been consumed as a service and thus fell in the domain of labor-intensive managed services providers. Additionally, these same modern analytically-grounded defense platforms in many cases have a cadre of incident management and breach assessment service professionals on staff, ready for "front-line" remediation and response — yet another territory of specialized security consultancies.

Considering the turnkey threat hunting and malware analysis functionalities, deep "in-app" investigative and attack reconstruction abilities, and staggering intelligence collection scale these software platforms boast, we believe a steady appropriation — or rather software-enablement — of upwards of $30 billion of human-capital intensive managed security/consulting-centric services dollars is plausible over the next several years. The front-line intelligence these vendors can filter back into their product's intellectual property is another added, and comparative advantage. This is further reinforced by cybersecurity seeing the most active integration and "solutionization" of AI and machine learning principles, given the sheer volume of telemetry and data.

Streamlining Workflows Can Go a Long Way Too

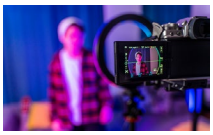
While the promise of SOAR has yet to be fully realized, this is an open opportunity for cybersecurity as well as IT Operations, and more horizontally-focused robotic process automation vendors to drive response automation and alleviate manual efforts of SOC personnel.

The featurization of SOAR capabilities within security analytics is mostly a fait accompli, as evidenced by the rapid consolidation that has occurred since the segment's emergence in mid 2010s, but we think its eventual home remains an open-ended question that could be the wildcard of success for XDR aspirants, contenders, and new entrants alike.

SOAR rather intuitively resides in XDR and SIEM systems at present, but vendors in these domains have done little to move the commercial needle so far. We believe RPA (robotic process automation) and ITSM (IT helpdesk, ticketing) focused players could become "dark horse" alternatives and category expanders in this market, where respective workflow creation/automation/management intellectual property is especially pertinent to the breach response orchestration and event triage automation challenges that define SecOps. These players' broader, vendor-agnostic purviews of information technology assets and infrastructure environments is an added benefit and could indeed be expansive to their total addressable market.

As our premier thought leadership product, **Citi Global Perspectives & Solutions (Citi GPS)** is designed to help readers navigate the most demanding challenges and greatest opportunities of the 21st century. We access the best elements of our global conversation with senior Citi professionals, academics, and corporate leaders to anticipate themes and trends in today's fast-changing and interconnected world.

All Citi GPS reports are available on our website www.citi.com/citigps

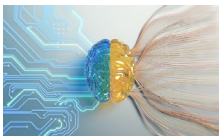


The Creator Economy
Getting Creative and Growing
March 2023

Generative AI
ChatGPT and Search
February 2023

Supply Chain Finance
Uncertainty in Global Supply Chains Is Going to Stay
January 2023

State of Global Electric Vehicle Adoption
A Trip Around the World
January 2023



Disruptive Innovations IX
Ten More Things to Stop and Think About
December 2022

Antimicrobial Resistance
The Silent Pandemic
December 2022

Climate Finance
Mobilizing the Public and Private Sector to Ensure a Just Energy Transition
November 2022

Food Security
Tackling the Current Crisis and Building Future Resilience
November 2022

Energy Transition: Vol 1
Mixed Momentum on the Path to Net Zero
November 2022

Energy Transition: Vol 2
Building Bridges to Renew Momentum
November 2022

China's Inward Tilt
The Pursuit of Economic Self-Reliance
October 2022

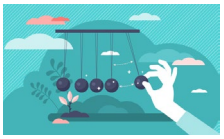
Philanthropy v2.0
Reinventing Giving in Challenging Times
October 2022

Food and Climate Change
Sustainable Foods Systems for a Net Zero Future
July 2022

Home of the Future 2
PropTech – Towards a Frictionless Housing Market?
June 2022

Global Supply Chains
The Complexities Multiply
June 2022

Space
The Dawn of a New Age
May 2022



Investing for Outcomes
Why Impact Is Relevant Beyond Impact Investing
April 2022

Metaverse and Money
Decrypting the Future
March 2022

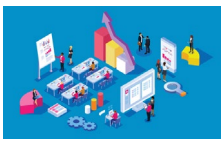
Global Art Market Disruptions
Pushing Boundaries
March 2022

Women Entrepreneurs
Catalyzing Growth, Innovation, and Equity
March 2022

Eliminating Poverty
The Importance of a Multidimensional Approach
February 2022

Global Supply Chains
The Complicated Road Back to "Normal"
December 2021

Philanthropy and the Global Economy
Opportunities in a World of Transition
November 2021



Education: Learning for Life
Why L&D is the Next Frontier in Global Education
November 2021

Home of the Future
Building for Net Zero
October 2021

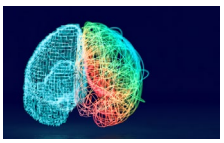
Global Carbon Markets
Solving the Emissions Crisis Before Time Runs Out
October 2021

Disruptive Innovations VIII
Ten More Things to Stop and Think About
October 2021

Holistic Digital Policy
Nation States Must Lead in Building Equitable Human-Centric Digital Economies
October 2021

Biodiversity
The Ecosystem at the Heart of Business
July 2021

Natural Gas
Powering Up the Energy Transition
July 2021



Technology at Work v6.0
The Coming of the Post-Production Society
June 2021

Hard to Abate Sectors & Emissions
The Toughest Nuts to Crack
May 2021

Future of Money
Crypto, CBDCs and 21st Century Cash
April 2021

Systemic Risk
Systemic Solutions for an Interconnected World
April 2021

The Global Art Market and COVID-19
Innovating and Adapting
December 2020

Bitcoin
At the Tipping Point
March 2021

If you are visually impaired and would like to speak to a Citi representative regarding the details of the graphics in this document, please call USA 1-888-800-5008 (TTY: 711), from outside the US +1-210-677-3788

IMPORTANT DISCLOSURES

NOW / NEXT

Key Insights regarding the future of Cyber Risk

GLOBAL REACH

In 2015, only 2% of cyber job postings required data privacy-related skills. By 2011, 11% of these job postings required such knowledge. / The changing regulatory environment will continue to drive the demand for roles with knowledge of data protection and privacy, especially for managerial positions.

LABOR MARKET

To solve the mismatch between the demand and supply for cyber skills sustained public-private partnership is being utilized to enhance talent and availability is key. / In the future, private-sector product vendors with robust built-in AI/automation that offer a higher and more headcount-efficient defense may help companies "work smarter, not harder" in tackling cyber risk.

TECHNOLOGY

To solve the mismatch between the demand and supply for cyber skills sustained public-private partnership is being utilized to enhance talent and availability is key. / In the future, private-sector product vendors with robust built-in AI/automation that offer a higher and more headcount-efficient defense may help companies "work smarter, not harder" in tackling cyber risk.