OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

The Cyber Problem

Causes and Consequences of the Rise in Cyber Skill Demand

Prepared for Citi GPS

By:
Pantelis Koutroumpis
Farshad Ravasan
Taheya Tarannum

October 12, 2022

Note: The background cover is produced by DALL.E 2, a new AI system that can create images and art from a description in natural language. We asked DALL.E to generate a picture for "The cyber problem. Causes and consequences of the rise in cyber skill demand"

Disclaimer

The authors have no conflict of interest with the firms, data owners or countries/regions discussed in this report. All errors are ours.

Copyright

Contact

34 Broad Street,
OX1 3BD,
Oxford,
United Kingdom
pantelis.koutroumpis@oxfordmartin.ox.ac.uk

Changelog

v1.0	2022-09-15	Draft prepared

Table of Contents

1 Executive Summary

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 driving factors that led to higher exposure and costs of cyberattacks. We highlight two notable trends that drastically changed the landscape of cybersecurity and its importance. First, we examine the impact of geopolitics and the emergence of cyber warfare. Second, we study the rising attention of customers toward the security of personal data. In the second chapter, we examine how global and regional labor markets fare in the face of steep competition for cybersecurity talents. Using information extracted from the profiles of the professionally active 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 regulations, business strategy, and governance. We discuss the importance of compliance and how failure to comply 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.

Key Insights:

- Cyberattacks costs have started to bite: Apart from the direct costs, supply chain disruptions and reputational damage, can be substantial.
- Exposure risks and material costs have increased significantly in healthcare.
- The geopolitical risks and the emergence of cyber warfare have reached new levels, disrupting production networks and causing cross-country economic damages.
- Consumer attention towards privacy and personal data has peaked, magnifying the impact of reputational damages for affected firms.
- Asia is now the second largest market for cyber skills, surpassing Europe.
- Cyber-skills' 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 the cyber professionals have less than six years of experience.
- Excluding North America, cyber-jobs take longer than other IT positions to fill.
- Data breach regulations make non-compliance a non-option, as stringent regulations emerged globally through a mix of better enforcement and heftier fines.
- Regulation can induce firms to increase investment in cyber skills, but it slows down business creation and increases exit rates.

2 Anatomy of an Economy-Wide Threat

2.1 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*

The brief history of cyber crimes. Cyber threats are not new. In fact, the history of cyber attacks 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.

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

Figure 1: The first password-protected computer

In 1962, the first password-protected computer was set up in MIT. It was also the first computer to be hacked.

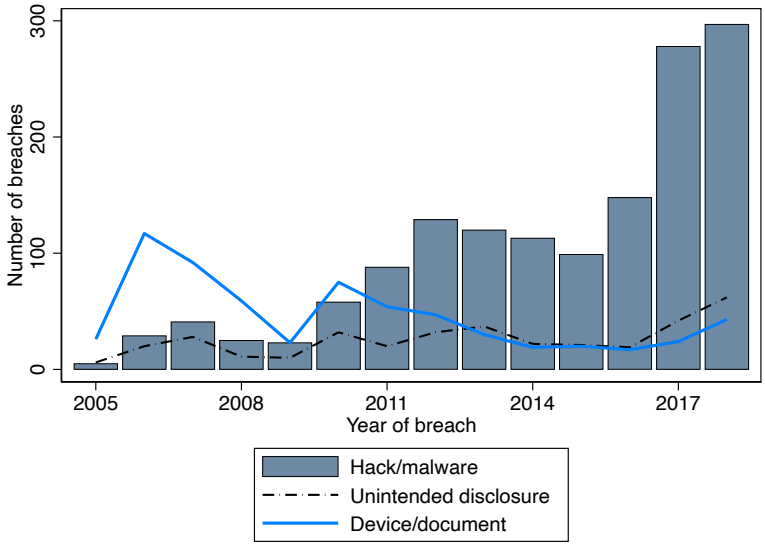
A first computer virus, called **RABBITS**, appeared in **1969**, bringing down the University of Washington Computer Center. In **1974**, a variant of RABBITS became the first internet virus that ran over APRANET – an early version of the Internet. In **1982**, the CIA blew up a Siberian Gas pipeline 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. This 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 that brought the whole Internet down for an hour. In the **2000s**, we saw a new type of cyber incident that substituted individual users as the target of their attacks with private companies for financial gain. For instance, TJX, a retail company, was the object ot a massive cyberattack in 2008 which compromised information for 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.

Incidents of cyber-related data breaches have rapidly increased since 2010. We use the 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 the reports to state Attorneys General and the US Department of Health and Human Services offices and includes more than 9,000 data breach incidents since 2005. It includes different types of data breaches, such as 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, by 2018 cyberattacks accounted for three quarters of all data breaches,.

Figure 2: Rise in incidents of cyberattacks

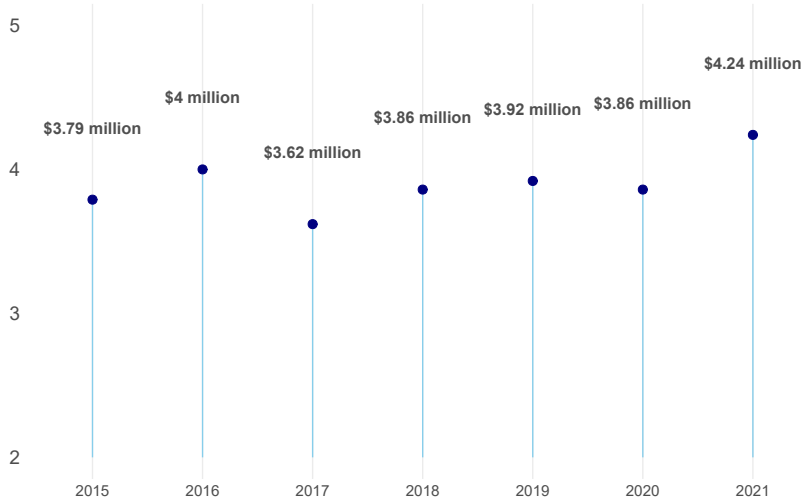


Cyberattacks are rapidly increasing and cyber-related incidents emerged as the top source of data breaches for companies and organizations since 2010.
Source: PRC

The cost of cyberattacks is rising. Apart from their frequency, cyberattacks are also becoming more damaging. According to the IBM CDBR 2021 report, the average cost of a data breach has increased significantly since 2015. The average cost of each breach rose to $4.24 million in 2021, 12% higher than its 2015 level and 10% higher compared to 2020. The report estimates that a typical breach (excluding very large and very small

incidents) compromises 2,000-101,000 personal records. On average, the costs of detection, recovery plan, and post response account for 56% of the total cost of each incident. The remaining cost comes from business losses, such as operational disruption and customer loss.

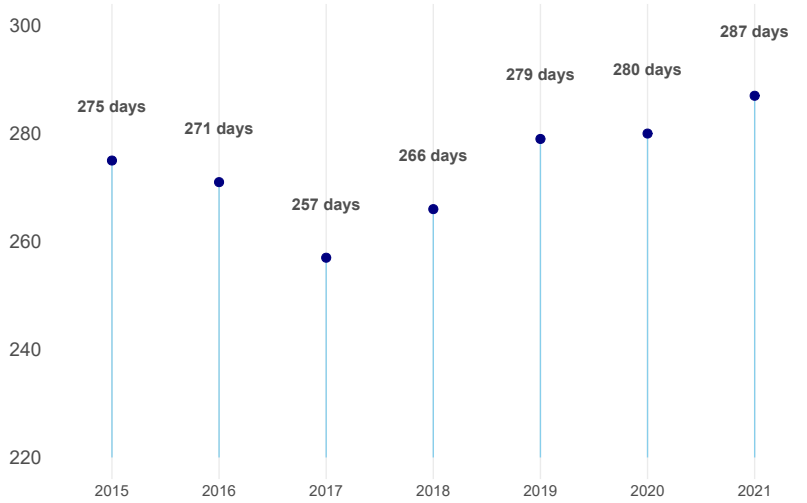
Figure 3: Rise in the cost of cyberattacks



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

Cyberattacks are becoming more complex. The trend on the required time to recover from cyberattacks indicates that hackers are using more sophisticated methods over time. Although the time to detect and contain an attack was decreasing between 2015 and 2017, it began to steadily surge since 2017. On average, it took 287 days to detect and contain a cyberattack in 2021, 30 days longer compared to the detection period for an average attack in 2017.

Figure 4: Rise in the complexity of cyberattacks

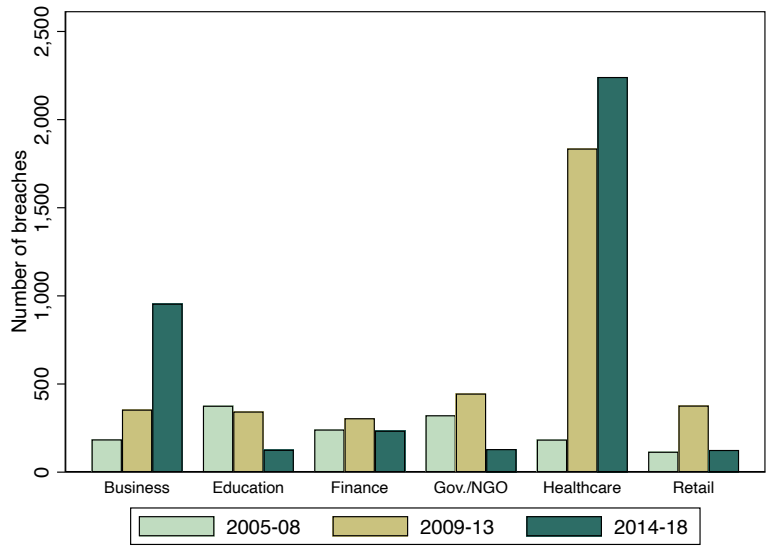


As cyberattacks are becoming more complex, the time to manage them increases. The average time to detect and contain a cyberattack was 287 days in 2021. Source: IBM

2.2 The Cyber Risk across Different Industries

Cyber risks surge in the healthcare industry. Cyberattacks were traditionally limited to firms operating in the financial sector and small number of other industries dealing with valuable personal information. However, that has changed recently. Digitization in businesses across almost every sector left them exposed to rising cyber risks. Thus, the cyber vulnerability has become an economy-wide operational risk for businesses across all sectors. During the past few years, healthcare organizations experienced the highest increase in cyber incidents. Since 2010, the healthcare industry has gone through a massive digital transformation, in an effort to increase patient access to healthcare and to improve its efficiency. This could improve the quality of services and lower costs by offering remote communication between patients and medical professionals. But many of these new digital connections lacked sufficient security standards, leaving the industry exposed to high cyber risk on the verge of its digital transformation.

Figure 5: The rise of cyber incidents across industries

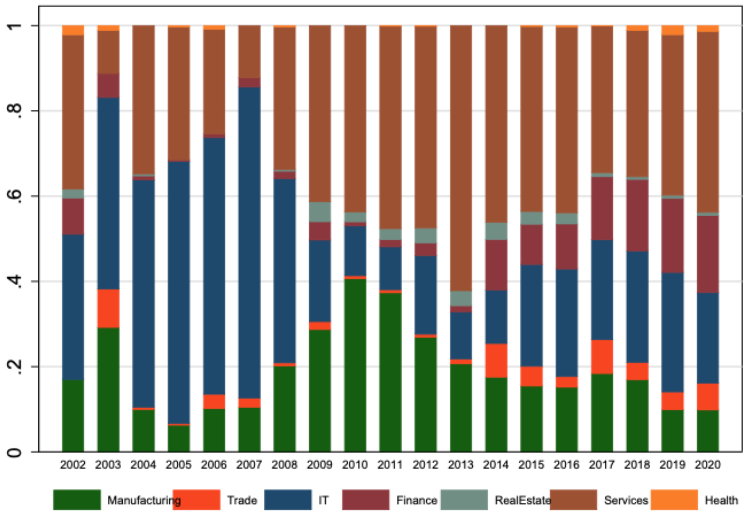


There is a distinct surge in cyber risk exposure in the healthcare industry, while cyber attacks are also increasing in sectors that were not previously exposed to the cyber risk. Source: PRC

Lack of market attention to rising cyber risk in healthcare. Despite its importance it seems that the key players in the market, such as company CEOs, investors, and analysts, do not pay much attention to the substantial cyber risks in healthcare. Reviewing the discussion around cybersecurity in transcripts of conference calls from companies across 80 countries shows which industries attracted more 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 towards manufacturing and their production vulnerabilities to the various forms of hacks and malware. During the

2010s, the market focused on the service industries and the financial sector, leaving healthcare largely unattended.

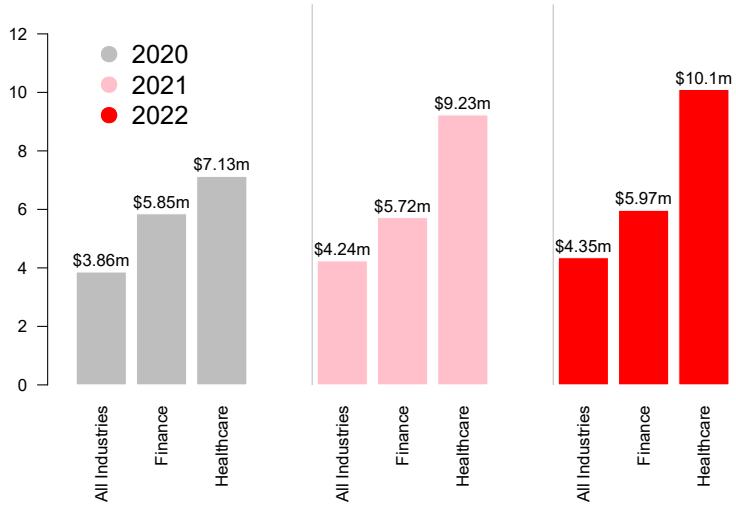
Figure 6: Rise of cyber incidents across industries



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: NBER

The pattern is more worrying, considering that the average cost of a cyberattack in the healthcare industry was the highest among all industries for the past three years and also widened its gap with other industries.

Figure 7: Rise of cyber incidents across industries



Cyberattacks in healthcare are more costly than others. The cost gap also sharply widened during the past three years.
Source: IBM

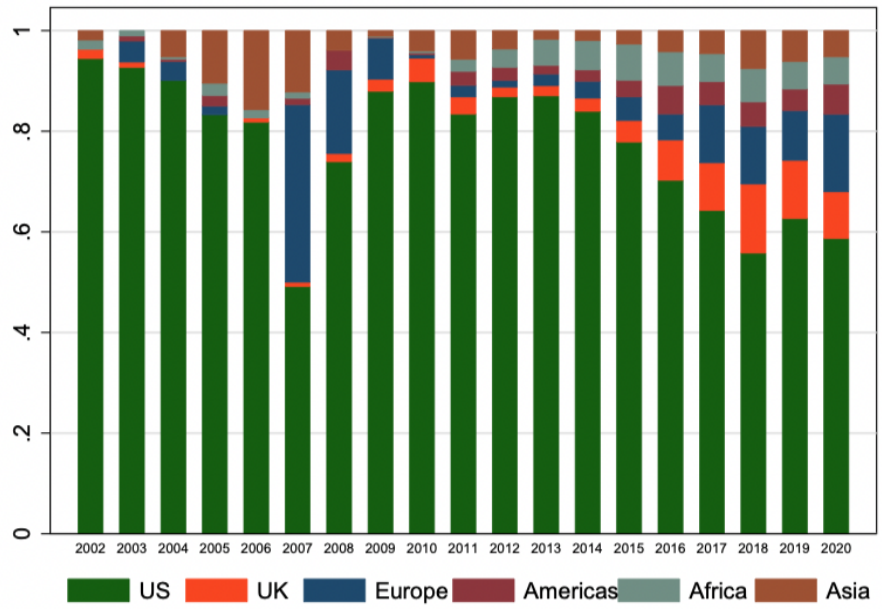
2.3 The Geography of Cyberattacks

"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
Federal Reserve Chairman

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 US-based firms. However, this trend has been changing drastically, as the number of cybersecurity discussions in Europe, the UK, Asia, and Africa are steadily increasing. Among the European countries, the most affected countries are France and Germany and together they represent roughly 10% of cybersecurity discussions in firms with headquarters outside the US. In 2020, 40% of all cybersecurity discussions were generated from non-American firms. The trend shows that cybersecurity has risen to become a concern for firms all over the world.

Figure 8: Cyber risk across the world



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

Cyber risk across local markets. Reviewing the geographic variation of cyber risk within a country also provides interesting insights. 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 US states. Since the early 2010s, hacking-related incidents increased markedly across all states. A discernible pattern is that states with larger economies are more likely to be targeted by hackers.

Figure 9: Rise of cyber incidents reported across US states

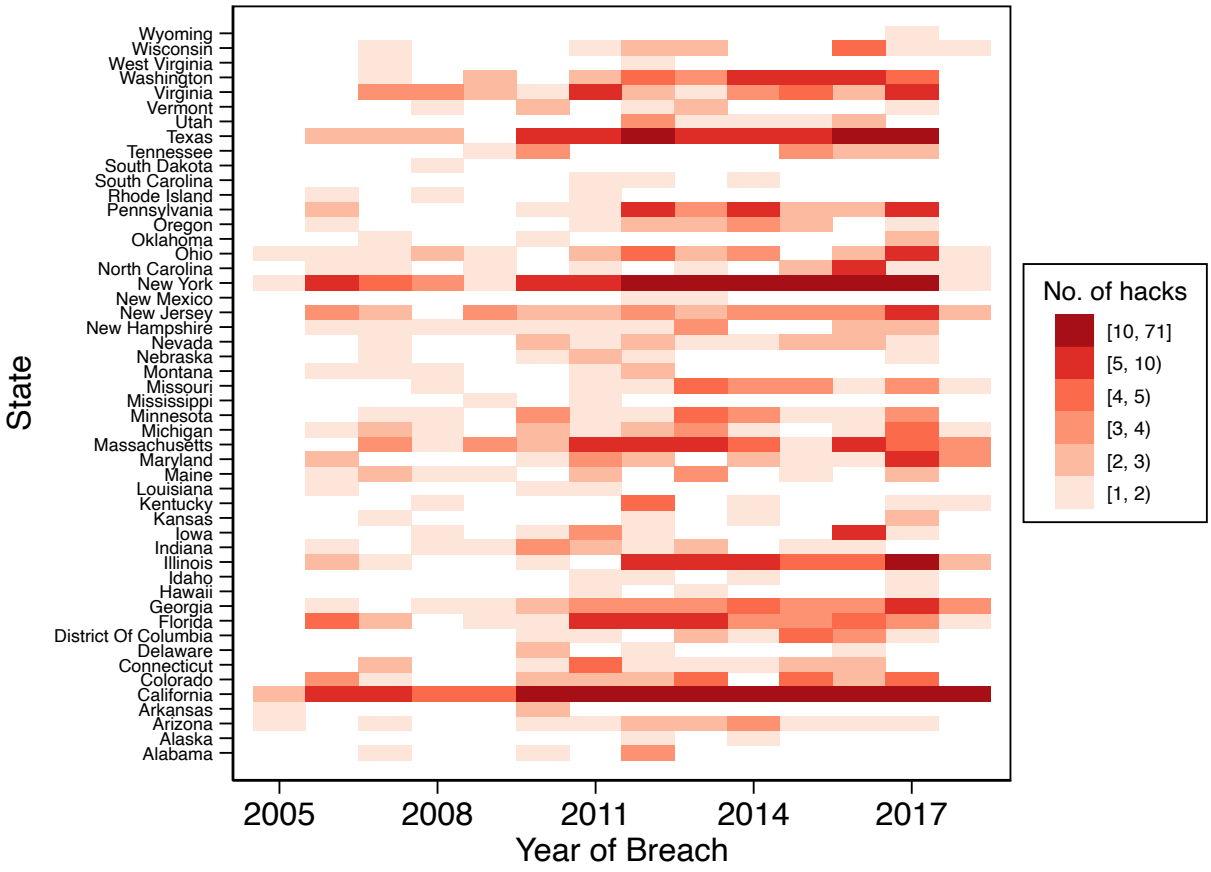
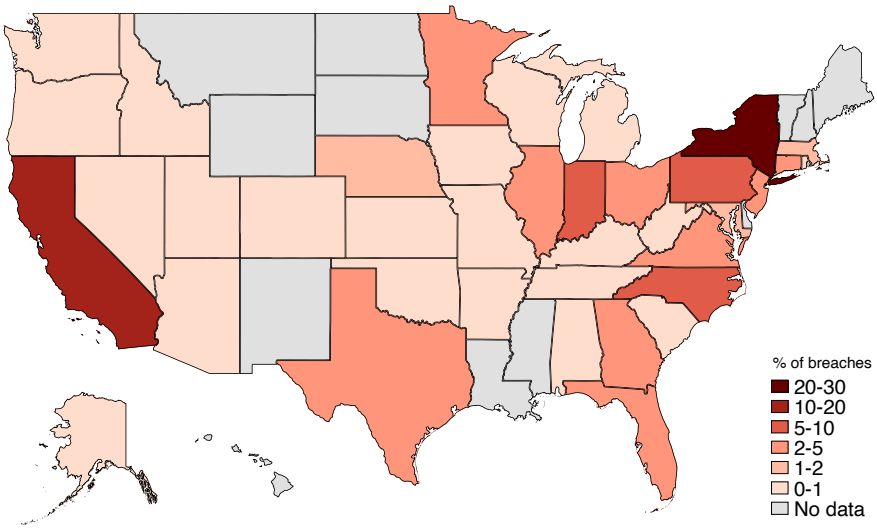


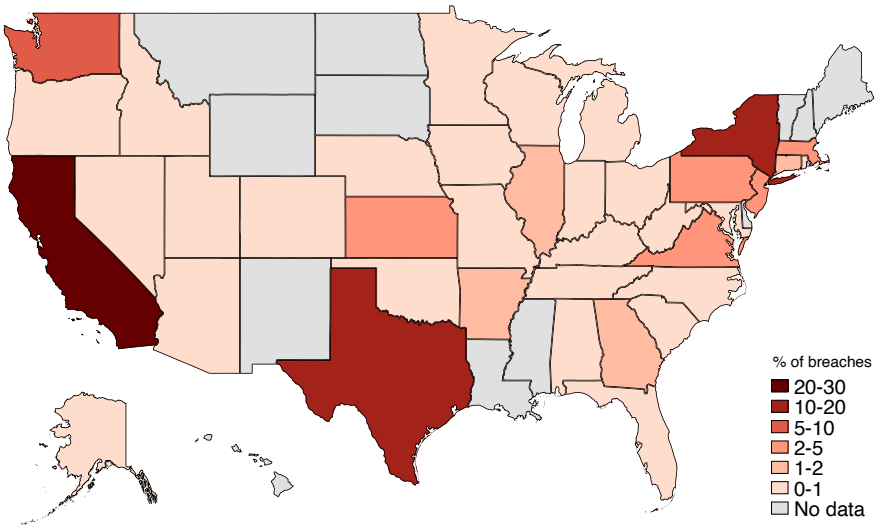
Figure 10 shows how industry-specific threats affects different states. State-level exposure through the IT sector is concentrated in specific geographic markets. Almost one-third of attacks in the IT sector occurs in California, followed by Texas (16%), and New York (11.2%). Unlike the IT sector, the risk is more uniformly spread for 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

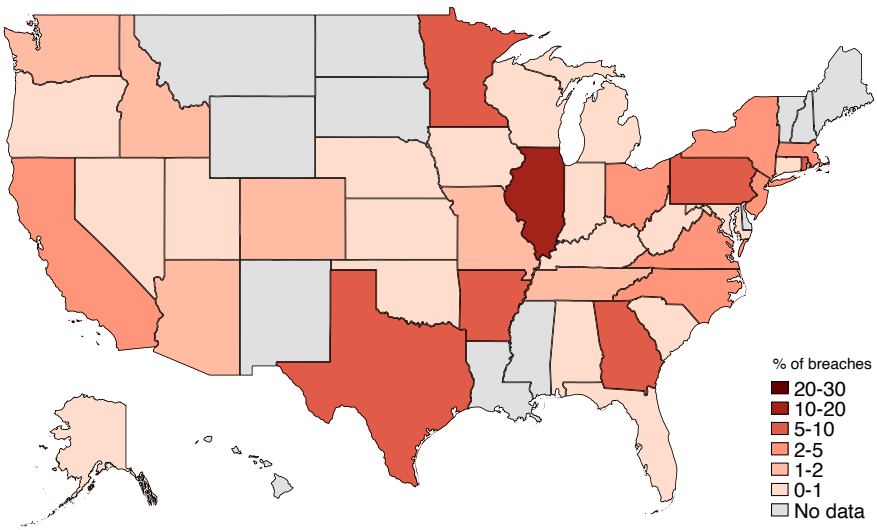
(a) Finance



(b) Information



(c) Wholesale & Retail

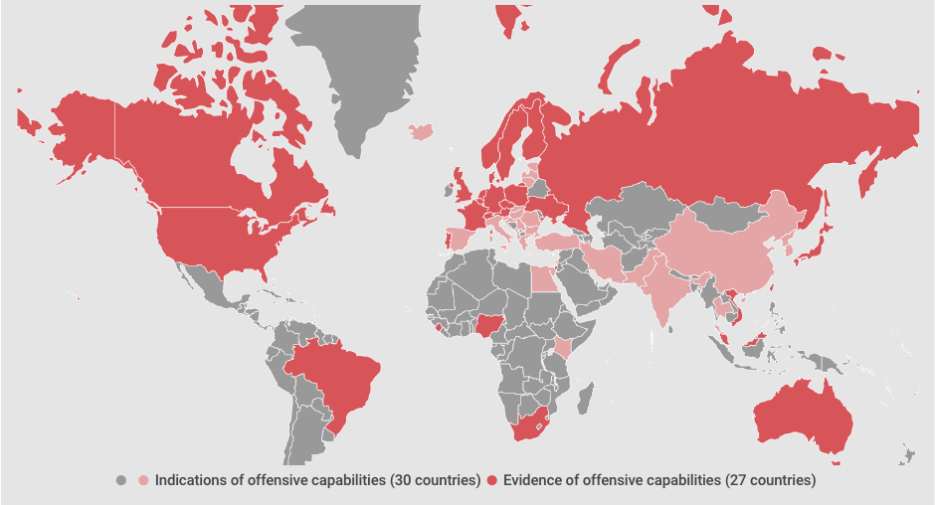


2.4 Geopolitics and Cybersecurity

> *"In the shadow of the invasion, it has become evident that hybrid warfare is the new reality, and geopolitics and cybersecurity are inextricably linked."*
>
> *– Paul Proctor*
> *Distinguished Vice President Analyst at Gartner*

The hybrid wars: The rise of offensive cyber capabilities have added a new dimension in war strategies such that several states consider cyber as the fifth military domain after land, sea, air, and space. In recent years investments in these capabilities have grown substantially and are now present in around fifty countries all over the globe. This situation suggests that the future of geopolitics and cybersecurity are inherently linked.

Figure 11: The Global Cyber Armament



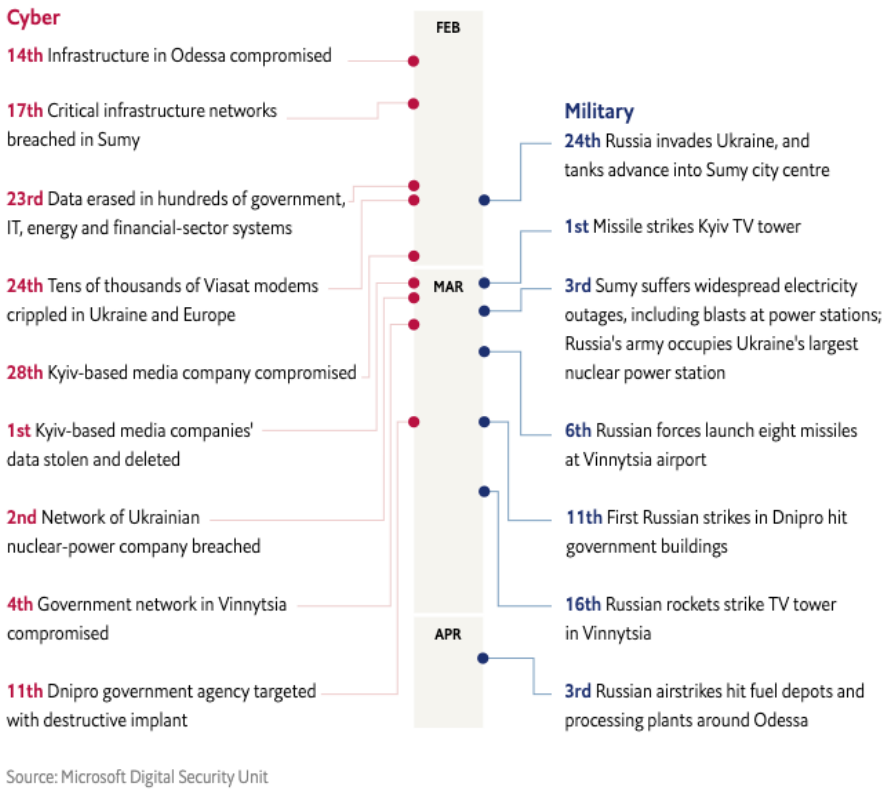
There is evidence on existing offensive cyber capabilities in 27 countries. There are indications that another 32 also possess such capabilities.
Source: digWatch

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. The 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 February 2022, when the invasion began, a series of cyberattacks were carried out by threat actors with known and suspected links to the three Russian intelligence services namely GRU (the military intelligence service); FSB (the foreign intelligence service); and SVR (the domestic intelligence service).

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

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

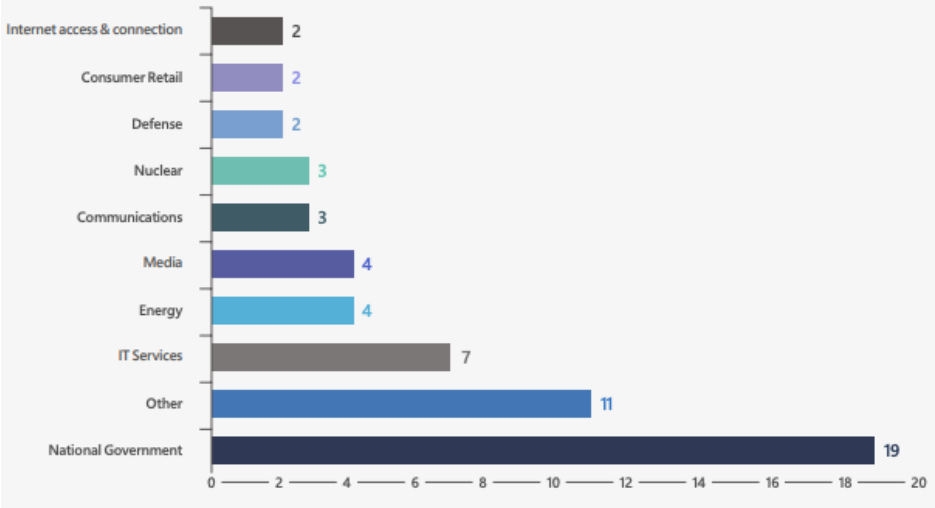
Figure 12: Timeline of Russian invasion of Ukraine



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

The chart shows the distribution of cyberattacks across Ukrainian industries. The government entities and public organizations were the main targets of these attacks. Nevertheless, the pro-Russian hackers also attacked the key infrastructure and private organizations as well to disrupt activities and access to services. Among different sectors the IT services were disrupted the most, while energy facilities, broadcasting and retail come next. The 'Other' represents eleven other categories that each experienced an attack during the invasion. This list includes organizations such as local government, agriculture, industrial bases, healthcare, transportation, and finance.

Figure 13: Cyberattacks across Ukrainian industries



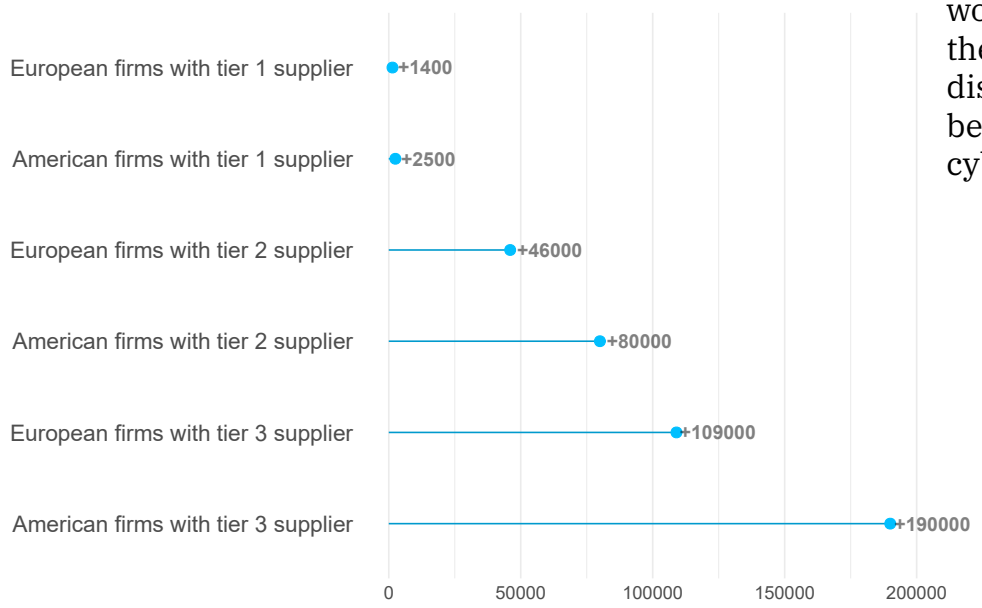
Apart from government organizations, cyberattacks aimed to disrupt core economic functions by targeting key infrastructure in energy, IT services, communication, and consumer retail// Source: Microsoft

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 Microsoft Digital Security Unit shows that between June 2020 and July 2021 Ukraine was the object of almost almost 20% of all registered attacks by state 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 attached were coordianted 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.

Nevertheless, 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 cyber attacks. These attacks disrupted Germany's efforts to shift away from Russian fossil fuels. The initial attack targeted Enercon in the same day as the invasion that started on the 24th of February. The other two attacks targeted Nordex and Deutsche Windtechnik during the first and second week of April. Although no group has claimed responsibility, the existing evidence indicates that 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, the collective supply chain disruptions are the main danger that firms face as they have become increasingly interconnected via global supply chains. According to the global supply chain network data from Interos, 1,400 European firms and 2,500 US based firms have at least one supplier either in Russia or Ukraine. 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. Tier-2 is an indirect supplier that provides inputs to the firm's direct supplier. This number rises to over 300,000 firms when we look at the links via Tier-3 providers. That are suppliers connected to firm via two intermediaries in supply chain network. This implies that firms are very likely to be exposed to these disruptions due to an indirect link with a targeted firm.

Figure 14: Exposure to supply chain disruption of Russia's invasion of Ukraine



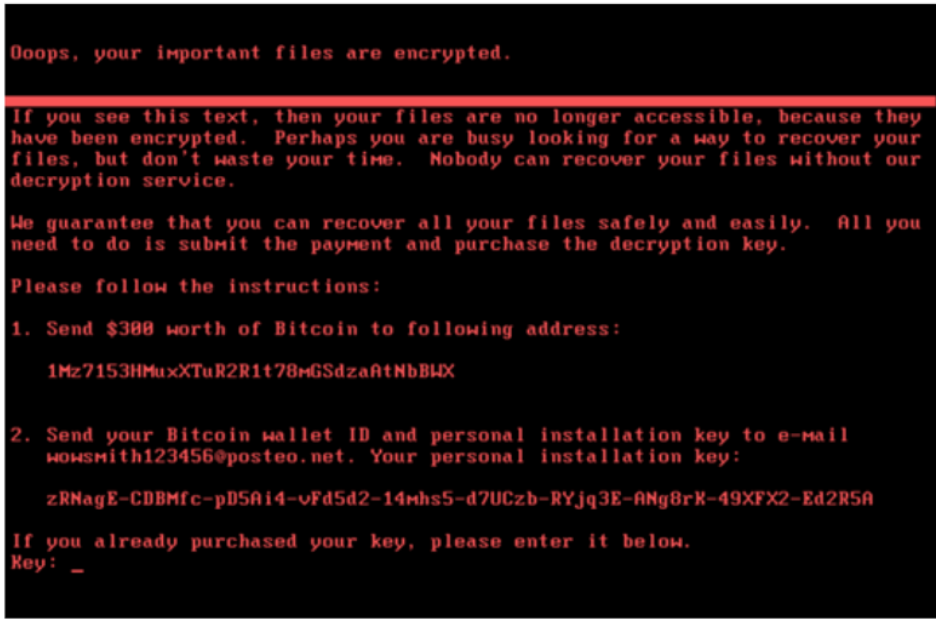
More than **300,000 firms** across the world are exposed to the supply chain disruption that can be caused by Russian cyber warfare

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 the past few months, has deployed FoxBlade malware and sandworm during the invasion to target government organizations, critical infrastructure, IT services, transportation, energy grids and financial sectors in Ukraine. But their most notable activity goes back to the NotPetya supply chain attack, the most costly cyberattack in history, in June 2017.

NotPetya brutally hit Ukrainian organizations but it also 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 (See the technical analysis here). 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 does not keep the decryption code. This implies that the decryption was not possible after the attack. In this regard, NotPetya was a form of wiper malware and not a common ransomware type of threat. The true intention of the attackers was not financial gain but to paralyze the computer networks of Ukrainian banks, firms, and government.

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

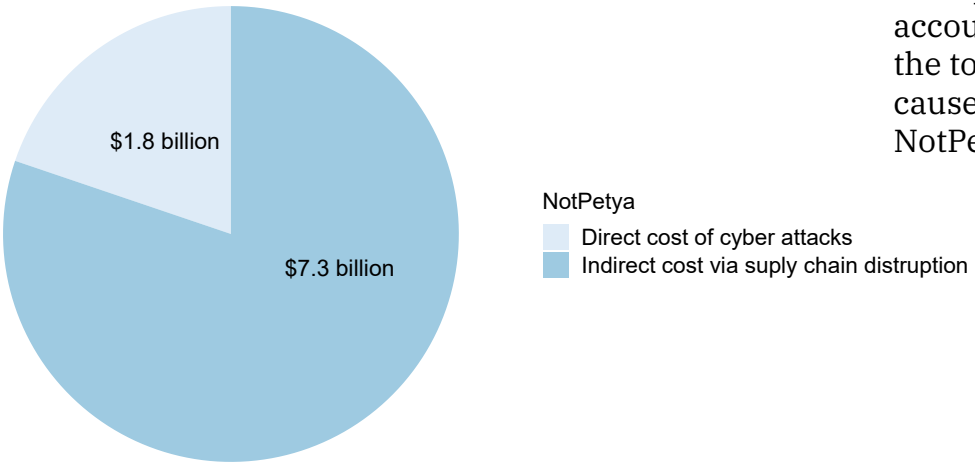
Figure 15: The NotPetya note



Russia's NotPetya supply chain disruption was the most harmful cyberattack in history. Although it initially seemed as 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: Microsoft

The damage of 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 provider that was infected by NotPetya suffered a cumulative $7.3 billion loss. This implies that the supply chain disruption accounted for 80% of the total damage of the NotPetya cyberattack.

Figure 16: The damage of Russia's NotPetya cyberattack

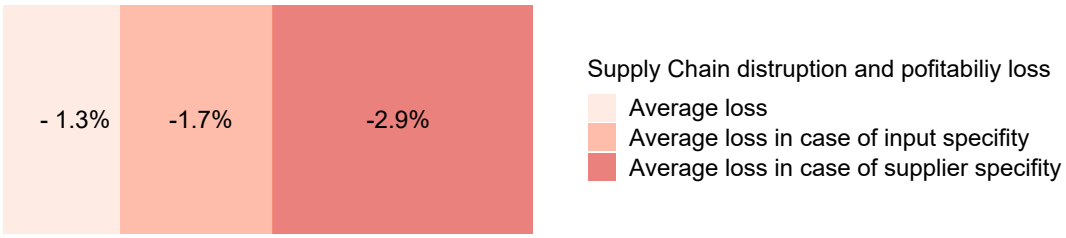


The supply chain disruption accounted for **80%** of the total damage caused by Russian NotPetya cyberattack

Supply chain vulnerabilities: These figures indicate 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 (measured as the ratio of earnings before interest and taxes (EBIT) to total assets) of these firms was reduced by 1.3% on average over a period of two years following the attack. They further measured that their profitability declined to 1.7% when these firms' suppliers produced a highly specific input that is only produced by few firms. The figure surges to roughly 2.9% when firms' overall supply networks are not well diversified and they only rely on few suppliers.

Figure 17: Profitability loss and supply chain vulnerability

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



Firms' response to the Russian invasion of Ukraine: The damage can be higher if the current global supply chain network is disrupted by the cyberwarfare of Russia-Ukraine conflict. This greatly depends on the firms' readiness and preventive measures taken to reduce their cyber risk exposure. In a recent Gartner poll, over a quarter of organizations in North America and EMEA said that they took some kind of cybersecurity action in response to Russia's invasion of Ukraine. This was the most frequently cited response, ahead of actions related to sanctions, employee welfare or supply chain risk management. Below we summarize the 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. **Incident response:** Invest in your incident response capabilities. Cyber incidents can take a long time to detect and contain.
3. **Employees' security awareness:** Promote the security awareness among your employees. The majority of cyber incidents are triggered by human errors.
4. **Have an offline backup:** During the NotPetya cyberattack, one of Maersk's domain controllers in their Ghana office went offline because of a blackout. Only thanks to that, Maersk could restore its networks.
5. **Monitor your supplier network carefully:** A survey of German supply chain executives conducted by Gartner in 2021 shows that although 80% of the companies had a clear visibility of their direct suppliers, only 7% of them had enough information about their indirect suppliers.

2.5 Reputational Damage

> *"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 Buffett*

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

TalkTalk incident: One great example of reputational damage is related to the cyber attack in October 2015 against TalkTalk, a major internet service provider in the UK. 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 cost was £35 million in incident response and a recovery plan. However, the company's financial statements show that they suffered a £60 million loss during the third quarter of 2015. This substantially higher cost is driven by the loss of 95,000 subscribers because of the data breach during these three months. It is worth noting that the company actively tried to limit the pitfalls of the attack by offering a free upgrade to its 500,000 customers.

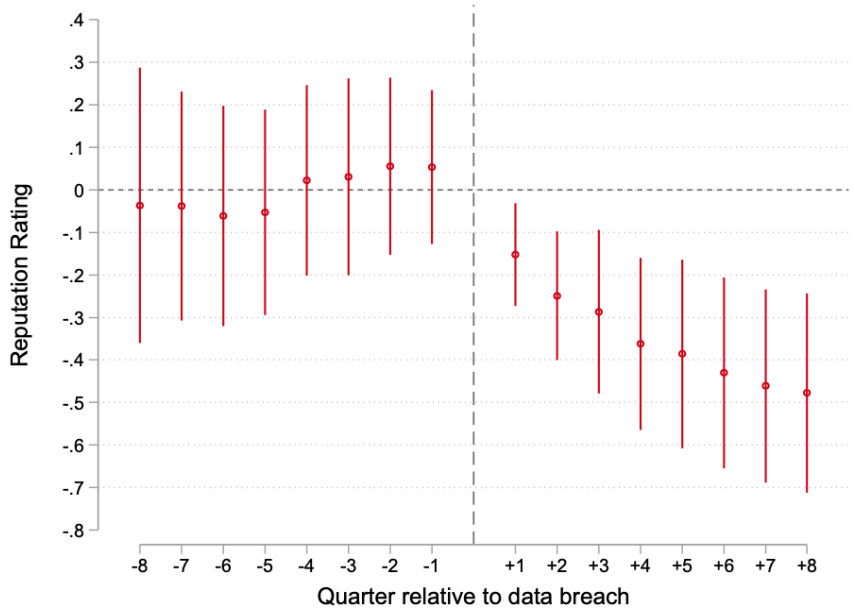
Figure 18: TalkTalk reputational damage

TalkTalk lost slightly less than 100,000 customers and £60 million due to the severe reputational damage of a cyberattack in 2015

What is the impact of a cyberattack on firm's reputation?

A recent academic paper shows a significant drop in corporate reputation after a data breach. 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.

Figure 19: Reputation damage persists over time



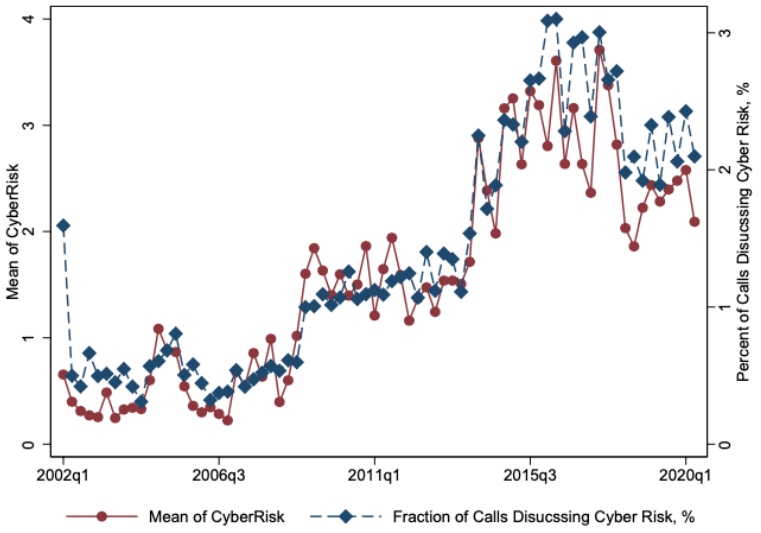
Reputational damage: A cyberattack can cause a devastating reputational damage. If a firm is initially among the top 25% most reputable corporations, its reputation falls below the median level two years after the attack.

The reputation damage is measured by Reputation Risk Rating (RRR) from RepRisk index. The rating is measured on a scale of 0 to 10 and ranges from 9.25 to 9 when we move from top 25% towards the median. 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.

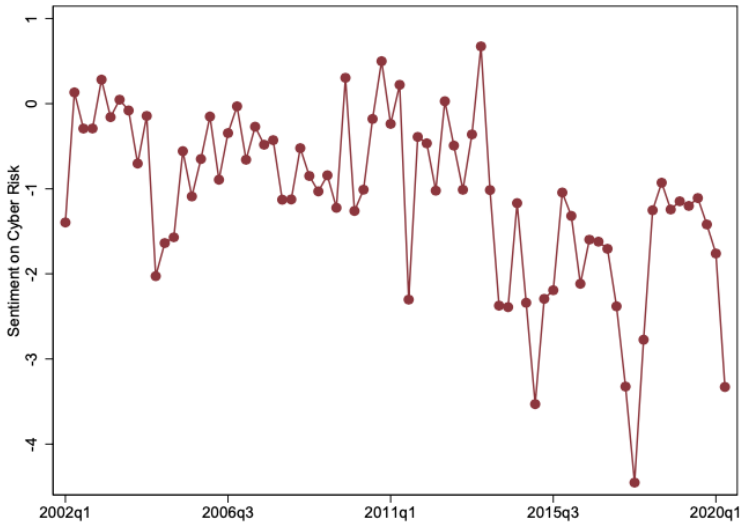
Long-term value effects: Data breaches negatively affect both the profitability and the expected growth opportunities. In the two years following a cyber incident, firms' return on equity (ROE) declines by 3% to 6% and price-to-earnings ratio (P/E ratio) by 3.13-3.38 units, Thus, a cyberattack has lasting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

The rise of public attention and reputation damage. The recent trends indicate that public attention towards firms' cybersecurity policies is increasing. Moreover, there are stronger sentiments on data privacy and firms' stakeholders, like their customers, suppliers and investors, become more sensitive about data breaches and the plans for timely responses. Economists at the London Business School have studied the transcripts of conference calls from companies across 80 countries over the past 20 years. They have found that the discussion over 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 over cyber vulnerability increased roughly fourfold towards more negative sentiments since 2002.

Figure 20: Attention and sentiment around cybersecurity



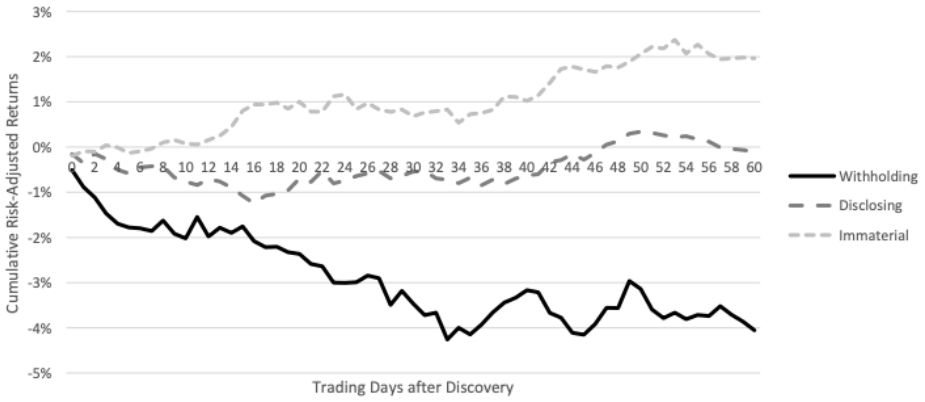
Public attention increasing. The public attention to firms' cyber vulnerability has gone up steadily during the past 20 years.



Public sentiment growing negative. The public sentiment over firms' cyber vulnerability became roughly four-fold more pessimistic since 2002.

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

Figure 21: Sentiment on cyber incidents



Timely disclosure of cyber incidents helps to limit the reputational damage after a cyberattack. The market also reacts positively if a firm manages to successfully defend itself without any material damage during a cyber incident.

Apart, from the potential reputational damage, firms are required to immediately disclose cyberattacks that cause a material damage. For instance, in the US, 60% of the states require breached firms to notify the public as soon as they realize they are breached. However, examining the cyber incidents between 2010 and 2015 sheds light on the fact that many attacks are not disclosed before investors discover them from other sources. To put the figures into perspective, in comparison to the thousands of attacks reported by other sources, there are around only 300 attacks that are disclosed by the companies during this period.

3 Competition for Cyber Talents

3.1 Why are Cyber Skills Important?

As the threat and costs of cyberattacks grow, firms seek to invest in cybersecurity personnel as part of their corporate risk management strategy. 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.[1] 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 Data Breach Investigation Report 2022 finds that 82% of data breach incidents involve a human component.[2] Human errors could lead to the use of stolen credentials, phishing, or a misconfiguration error. Hence, having a cybersecurity team can be one of the most effective strategies for corporations to protect themselves against cyberattacks.

It is important to note that, 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 do 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%).[3]

Table 1: 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, $(ISC)^2$.

[1] $(ISC)^2$ Cybersecurity Workforce Study, 2021.
[2] The 15th annual Verizon Data Breach Investigations Report (2022).
[3] The State of Ransomware in Financial Services 2022. Sophos.

3.2 The Rise of Demand for Cyber Skills

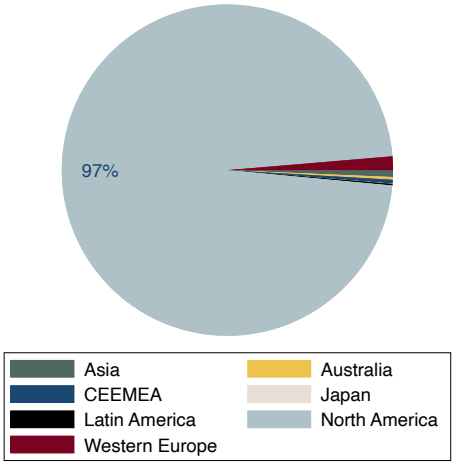
With businesses increasing their digital footprint, the need for a workforce with more sophisticated and varied roles is growing more than ever. Traditional job titles do not portray this information sufficiently. Hence, we analyze texts from job advertisements to measure the extent to which firms' demand for cybersecurity tasks 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.

3.2.1 Global Demand

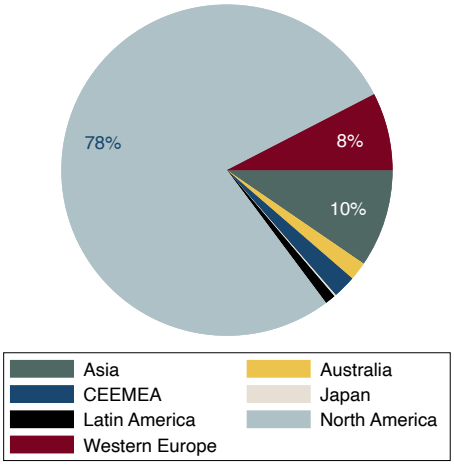
Between 2015 and 2021, the number of cyber jobs advertised by firms grew 4.3 times. At the same time, the number of IT jobs advertised grew 3.5 times and the number of total jobs advertised grew 2.7 times. Although a large number of these jobs are concentrated in more industrialized regions, such as North America or Western Europe, the market for cyber skills is growing across all parts of the world.

Figure 22: Regional demand for cyber jobs

(a) 2011



(b) 2021



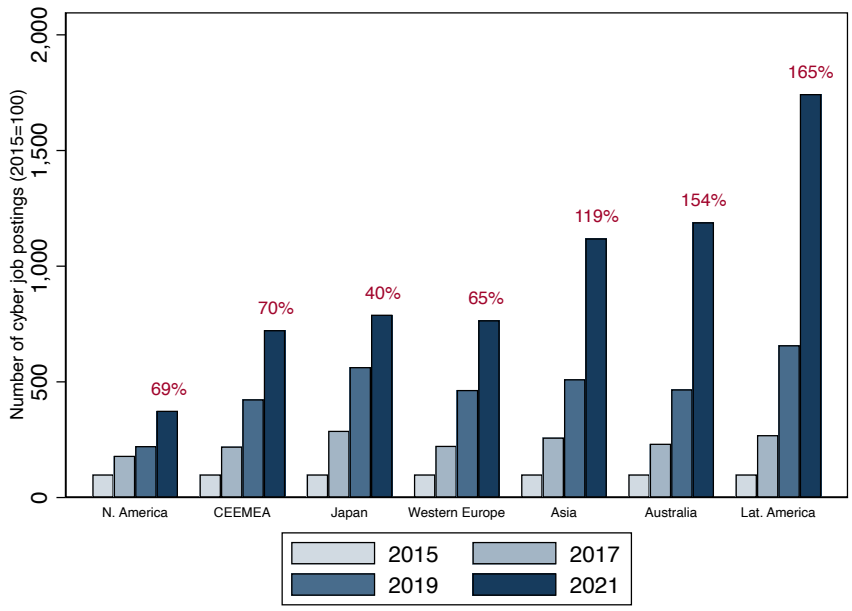
Figures 22a and 22b show the changing composition of cyber job postings across regions. Our job posting data covers seven regions, namely Asia, Australia, Central and Eastern Europe, Middle East and Africa (CEEMA), Japan, Latin America, North America, and Western Europe. At the start of the last decade, 97% of these jobs were advertised in the North American market. Ten years later, 78% of the global job postings are coming from North America. Asia (10%) surpassed Western Europe (8%) to emerge as the

second largest market for cyber skills. Part of the increased share of other regions could also reflect a broader pattern of digital transformation which leads 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.

Figure 23 shows the cyber job postings for each region normalized by the number of cyber job postings in 2015. While North America still represents a large market, other regions are growing faster. It appears that the COVID-19 pandemic has accelerated this trend. The numbers in red show the growth of job demand in 2021 compared to the levels of 2019. In the post-pandemic period, the fastest-growing demand for cyber jobs comes from Asia, Australia, and Latin America.

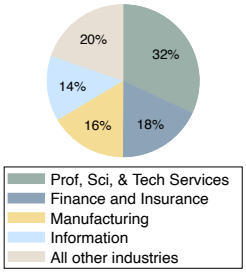
Asia has surpassed Western Europe to emerge as the second largest market for cyber skills.

Figure 23: 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 from 2019-2021)

Figure 24: Demand by sectors (2021)



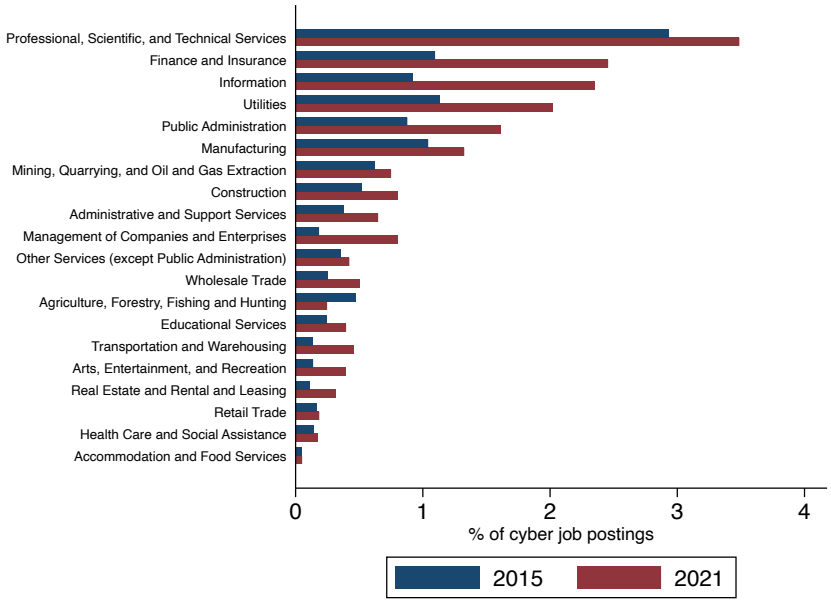
3.2.2 Industry-Specific Demand

Across different industries, we find four sectors accounting for 80% of the cyber job postings in 2021 (Figure 24). The largest share of cyber demand comes from Professional, Scientific, and Technical Services (32%), followed by Finance

and Insurance (18%), Manufacturing (16%), and Information (14%). Out of the remaining sectors, each accounts for less than 5% of all cyber jobs advertised in 2021.

Figure 25 shows the growth pattern of demand across all sectors between 2015 and 2021. During this period, the average share of cyber job postings out of all job postings in the industry grew from 0.6% to 1% which amounts to a 67% increase. The fastest growing sectors are Information and Finance and Insurance – both doubled their demand for cyber skills during this period. As we show in the first chapter, these are also the sectors subject to the highest number of data breach incidents. The next group of industries in terms of increased cyber demand include Professional, Scientific, and Technical Services, Management of Companies and Enterprises, Public Administration, and Utilities, which grew by half a percentage point. The Professional, Scientific, and 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.[4]

Figure 25: Industry-specific demand for cyber skills

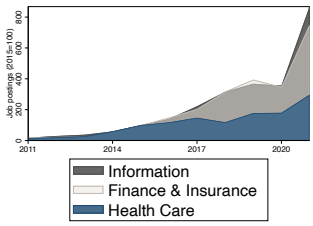


From 2015-2021, the average share of cyber job postings grew from 0.6% to 1%.

[4] X-Force Threat Intelligence Index 2022. IBM Security.

Another sector showing strong demand for cyber skills is the energy sector. Any disruption in this sector can have a high cost trickling through supply chains. Given its strategic importance and the recent ransomware attack on Colonial Pipeline, we expect this trend to continue.

Figure 26: Relative increase in cyber demand



Interestingly, our analysis shows that the health sector is lagging in terms of its demand for cyber skills. It is not surprising that the share of cyber job postings advertised in this sector is still low given the large number of health care (and other types of) professionals employed by this sector. However, the number is also growing slowly over time relative to other industries. Although the health care sector experienced a large number of attacks in recent years (see Figure 26), the demand growth is only one-third of the fastest-growing sectors, such as Finance or Information.

3.2.3 Demand across Locations

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

Figure 27: Demand for cyber skills across the US market (2021)

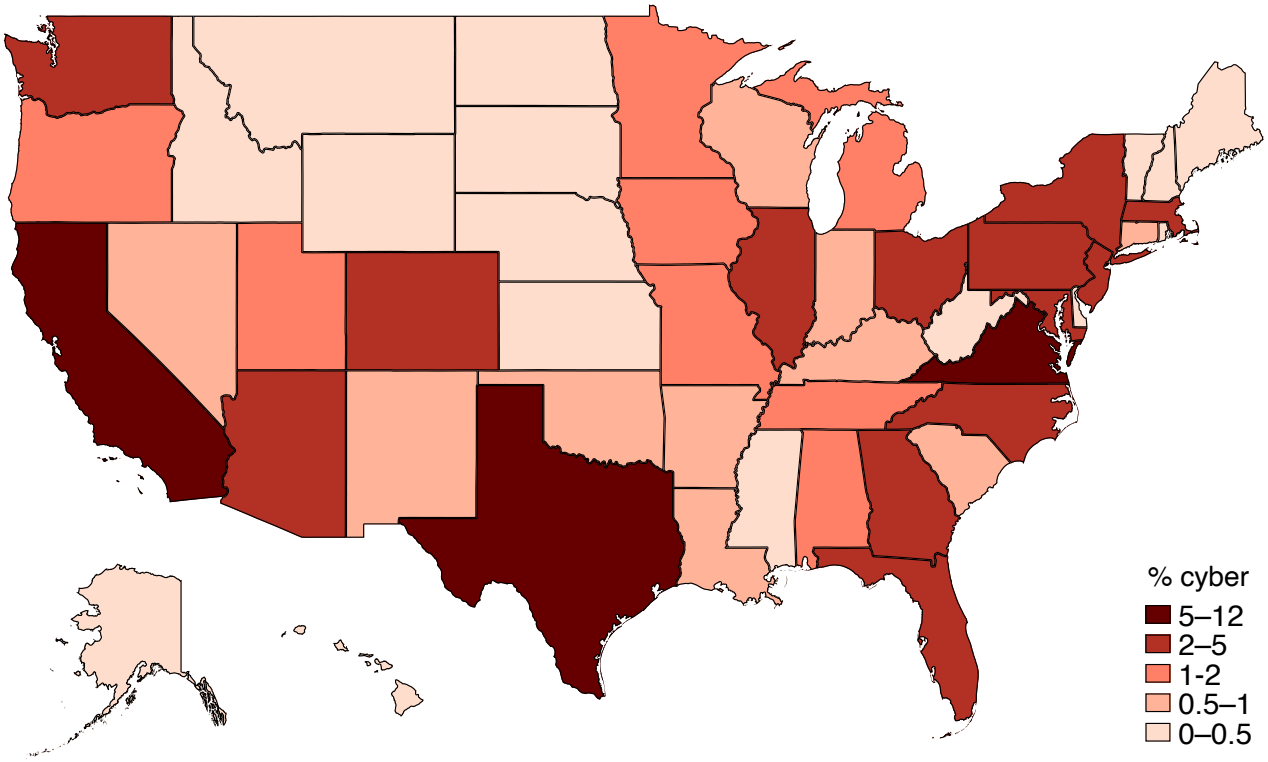
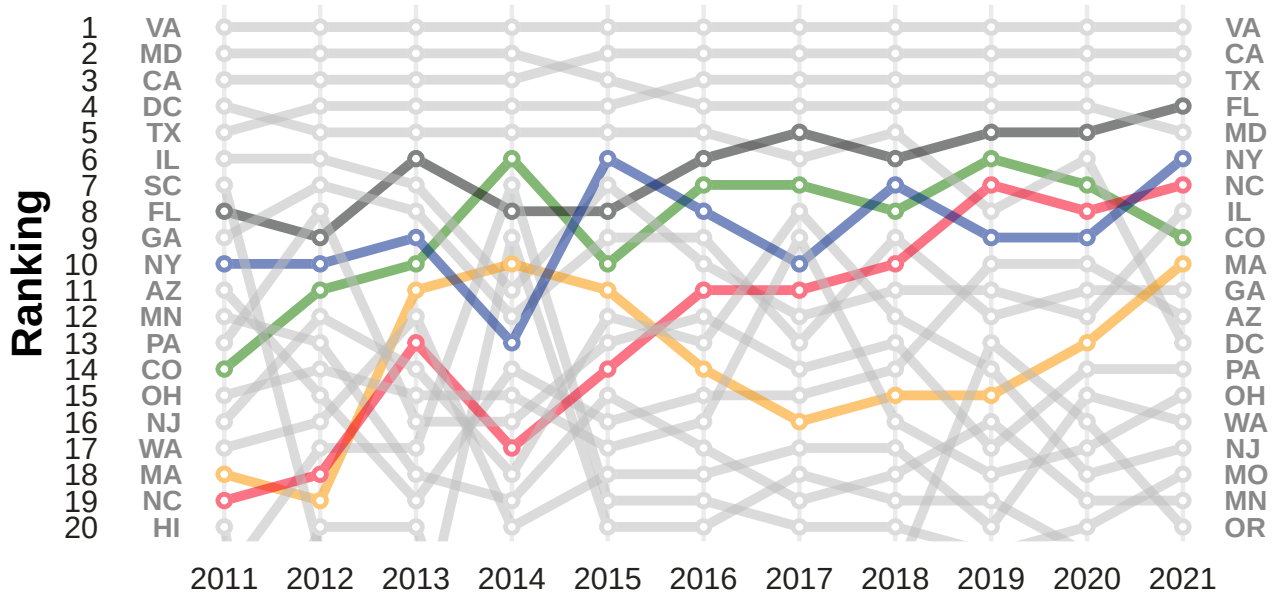


Figure 27 shows the concentration of cyber job postings across US states in 2021. California, Texas, and Virginia came at the top, each accounting for at least 9% of all the cyber jobs advertised. Traditionally, the Virginia-DC-Maryland area had the highest concentration of cyber jobs because of the presence of the defense industry and government agencies. In recent years, other states have also emerged as new hubs of cyber jobs.

Figure 28 shows the full dynamics of US states over the last ten years. Each vertical axes shows the ranking of the US states based on their shares of cyber job postings at the start and end of the period. Out of the top-five states in 2011, DC and Maryland have lost their importance. This could reflect the rising real estate cost in this metro area that is forcing firms and workers to reconsider their locations.

Figure 28: Cyber demand – Ranking of US states



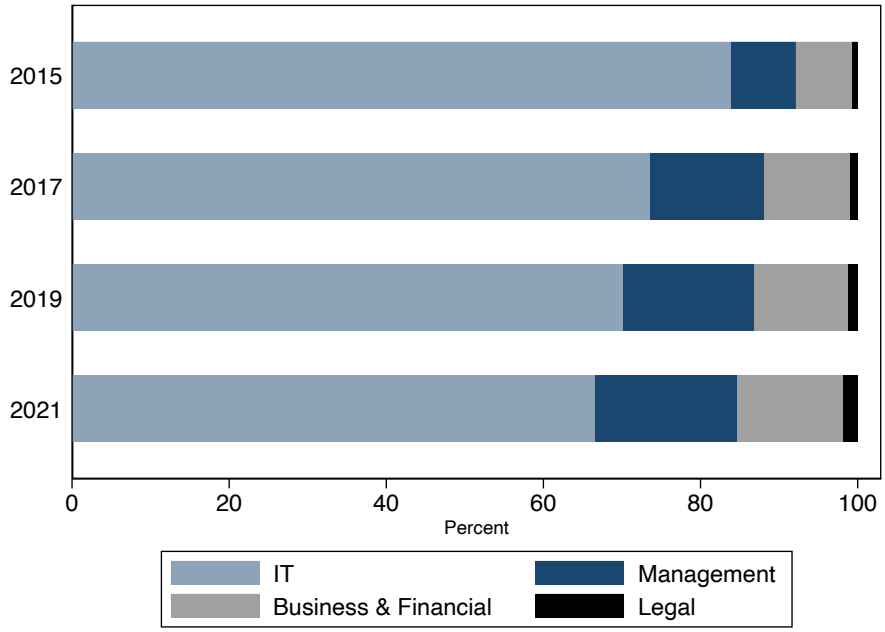
The emerging locations of cyber demand are highlighted in color. North Carolina is the most notable among them. It is now the seventh largest market for cyber skills. Florida and New York have also grown ahead in ranking. By 2021, each of these states accounted for 4-4.6% of all cyber job postings. Among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

3.2.4 Occupational Demand

A large share of the jobs requiring cyber skills belongs to the larger group of IT-related occupations, such as IT Managers, System Administrators, Database Administrators, System Analysts, or 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 29, we report the share of cyber job postings across four occupation groups, namely Computer and Mathematical (IT in short), Management, Business and Financial Operations, and Legal Occupations.[5] Between 2015 and 2021, the share of cyber job postings of non-IT occupation groups increased from 14% to 33%. The largest increase is for managerial occupations which now account for 18% of cyber job postings. Legal occupations are also showing a fast-growing demand for cyber knowledge.

[5] These categories correspond to Onet occupation groups 15, 11, 13, and 23, respectively.

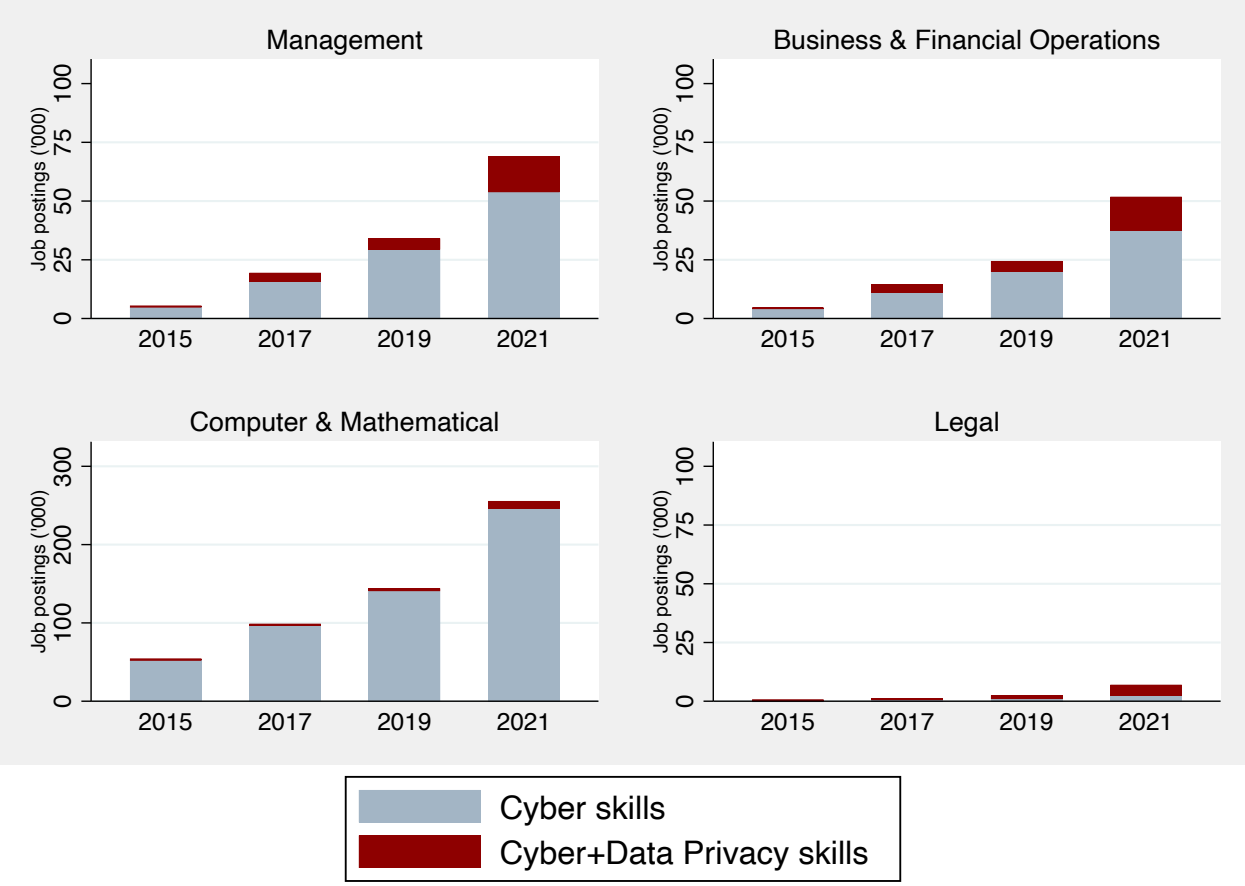
Figure 29: Occupation-specific cyber demand



A large number of managerial positions now require cyber skills. The next figure shows that the demand is also high for data privacy related skills – one-tenth of cyber job postings also require knowledge of data privacy issues.

The changing regulatory environment also accounts for some of the increased demand for cyber skills. In the last 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 GDPR adopted by the European Union played a pioneering role when it came into effect in May 2018. In Figure 30, we see an increased demand for roles with knowledge of data protection and privacy. 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 the cyber job postings required data privacy related skills. By 2021, 11% of these job postings required such knowledge. Privacy-related knowledge is in greater demand for management, business and financial, or legal occupations. In 2021, 22.1% cyber job postings advertised for managerial positions require an understanding of data privacy related issues. These figures are respectively 27.7% and 6.5% for business and financial operations and legal occupations, whereas only 3.5% of IT occupations require data privacy related skills.

Figure 30: Demand for cyber and data privacy knowledge



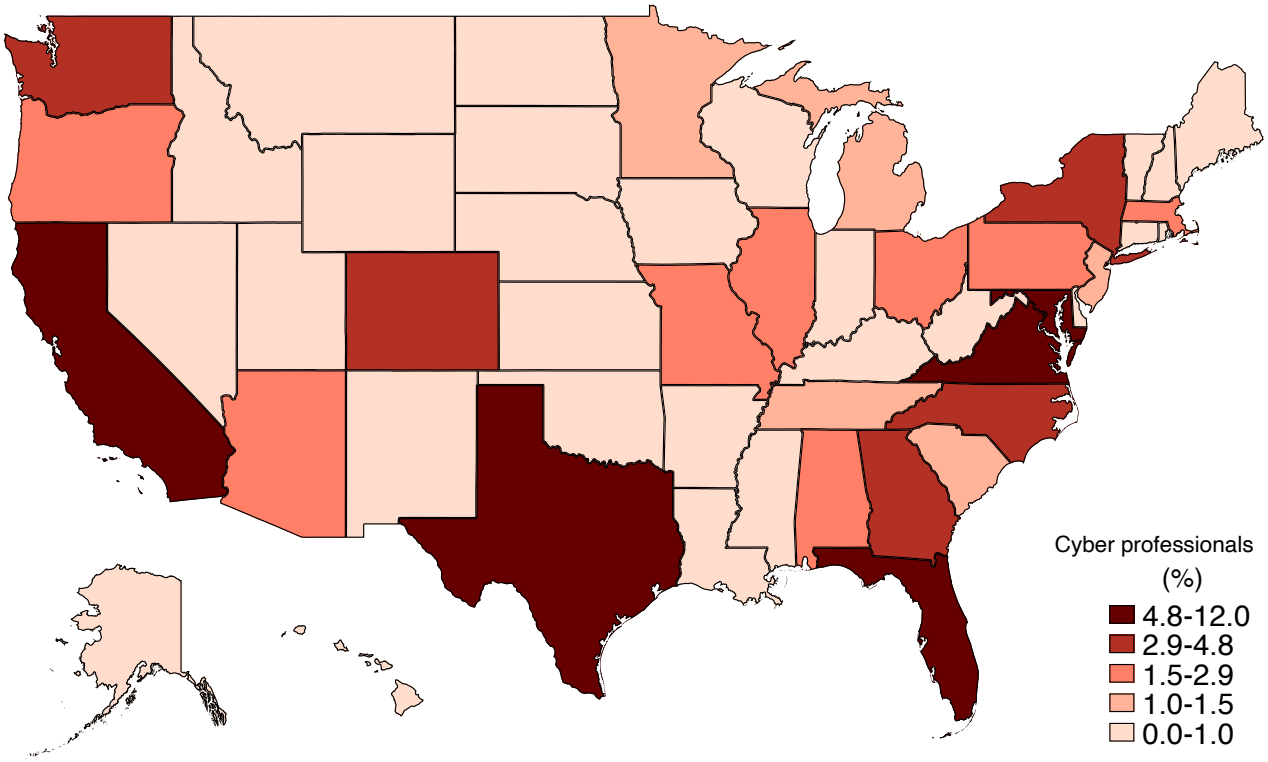
3.3 Supply of Cyber Professionals

We next turn our focus to the supply side of cyber skills. We check the availability of cyber professionals in the US to understand how the supply of cyber skills is distributed across space. A rich dataset extracted from LinkedIn profiles of workers helps us gain insights about their location choices and other characteristics.

3.3.1 Location of Cyber Professionals

Figure 31 shows the percentage of cyber professionals residing in each state. The states ranking at the top are Virginia, Texas, California, Maryland, and Florida. 11.1% of all cyber professionals are located in Virginia, 9.4% are in California, and another 9% are in Texas. Note that these are also the states accounting for most of the cyber-related job postings (see Figure 28). Workers with cyber skills are slightly more concentrated than all types of workers. The top eight states account for 50% of all professional workers, whereas this number is 55% for cyber professionals.

Figure 31: Location of cyber professionals



3.3.2 Characteristics of Cyber Professionals

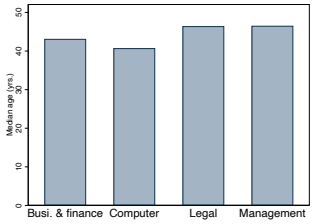
We calculate years of experience for cyber professionals as well as for all IT professionals. Figure 33 shows the cumulative percentage of workers with work experience measured by the number of years passed since graduation.

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

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

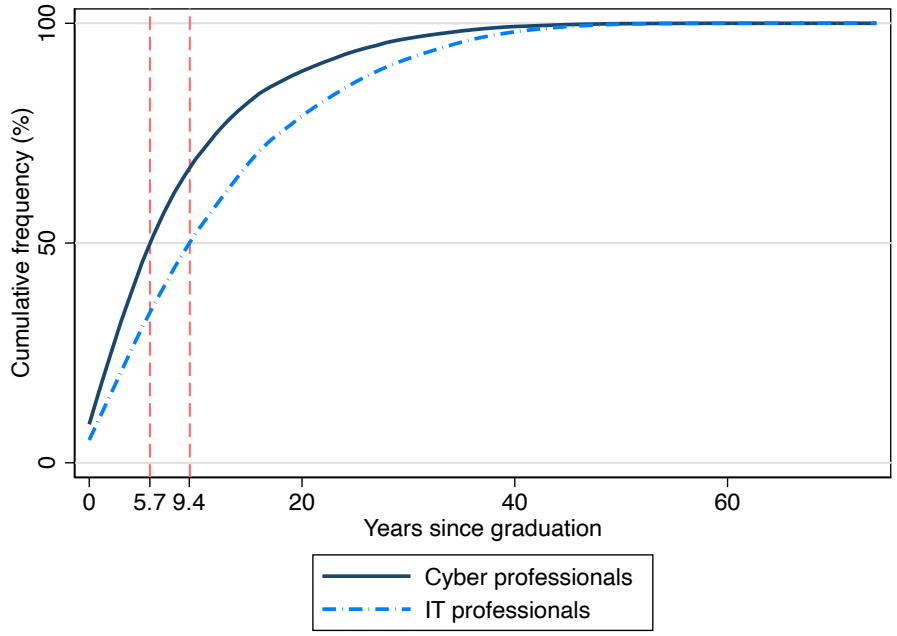
In general, these occupations also require more experience than IT occupations. For example, the average age for IT-related occupations is 41 years, whereas the average age for managerial, business and finance related, or legal occupations vary from 43-47 years (Figure 32).[6] This means that the supply scarcity is more acute for mid- or high-level cybersecurity positions.

Figure 32: Median age by occupation (Source: LFS 2021)



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

Figure 33: Cumulative distribution of years of experience



3.4 Recruiting Difficulties

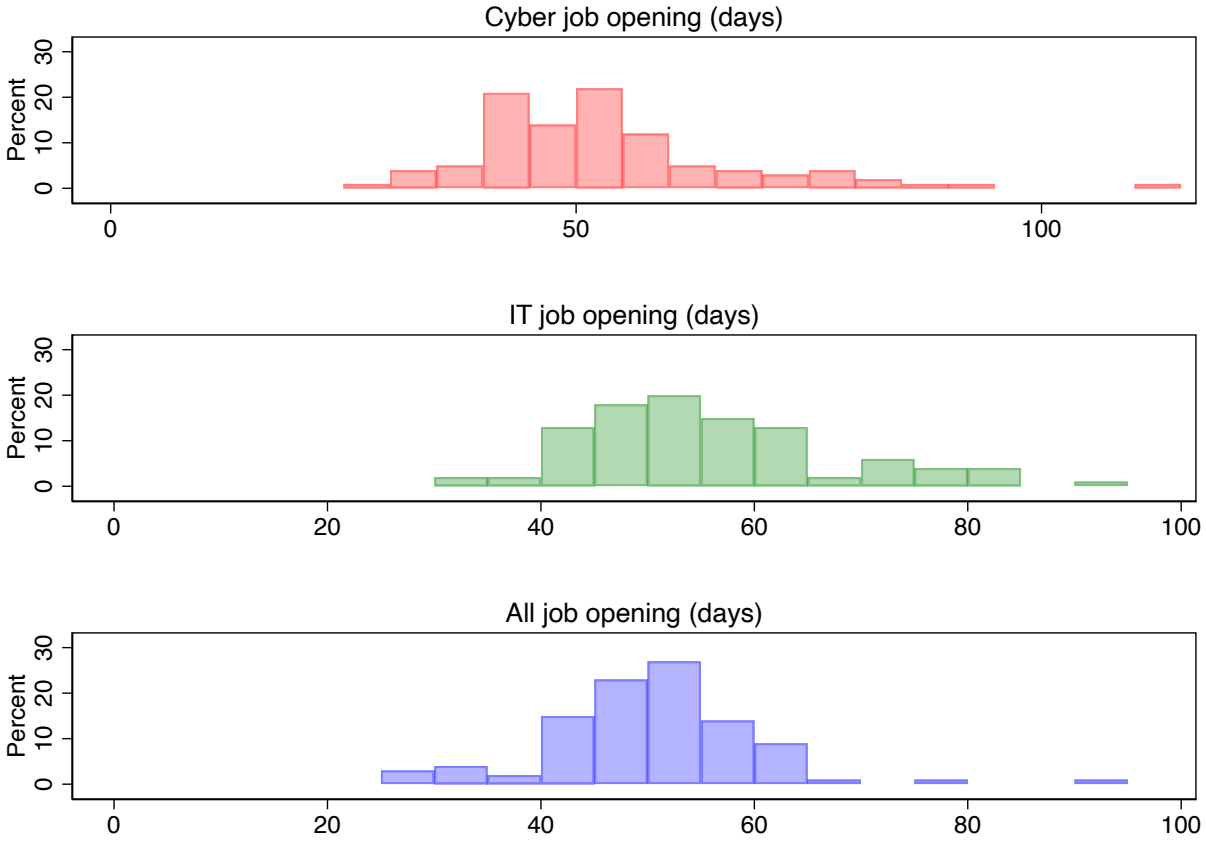
In this section, we explore the implications of firms' competition for acquiring cyber skills. If the rising demand outpaces the supply of cyber skills, it will take longer for firms to fill the vacancies, or some vacancies will remain unfilled. We check two indicators to understand the nature of cyber 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.

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

3.4.1 Cyber Job Opening Time

We calculate the number of days for which a job is advertised. We refer to this period as job opening duration. Figure 34 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 postings. 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.

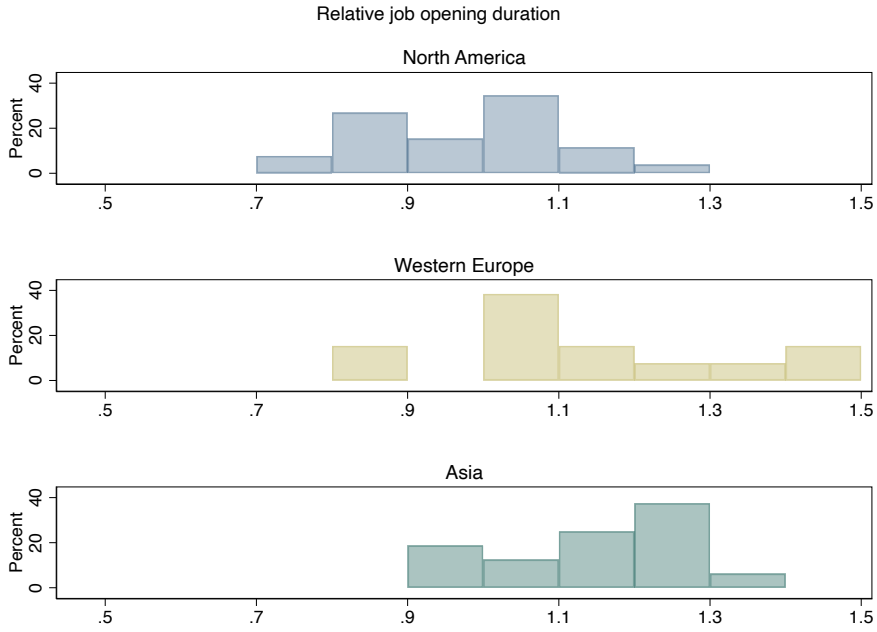
Figure 34: Job opening duration



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. It 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 10-30% longer durations for cyber job postings. In contrast, the data for Western Europe or Asia depicts a

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 compared with the duration for all job postings. For Asian cities, the relative job opening time is even longer. As we have discussed at the beginning of this chapter, Asia is one of the regions with faster-growing demand for cyber skills. We find that 71% of the Asian cities in our sample have 10-40% longer advertisement periods.

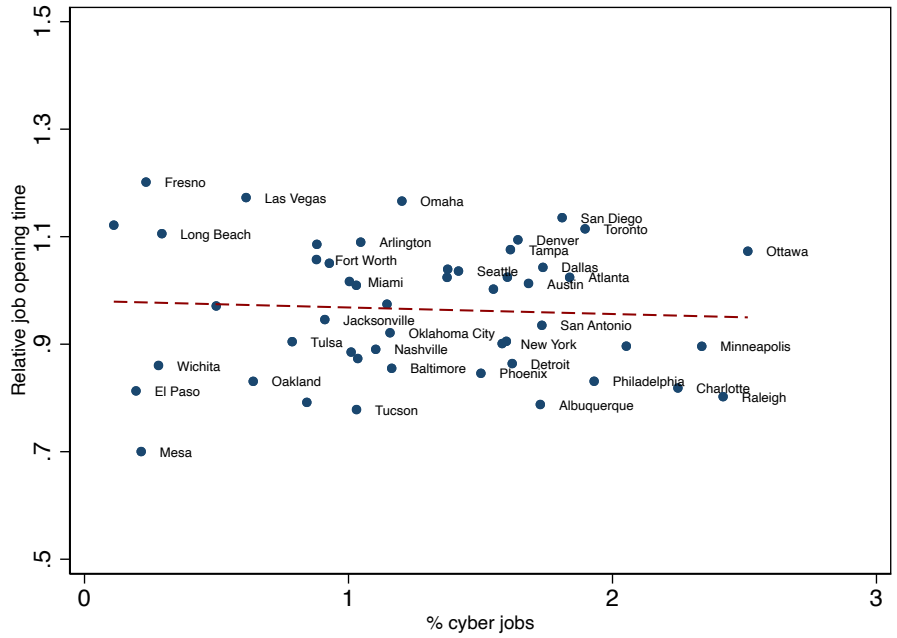
Figure 35: Relative job opening duration



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

Finally, we check 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 to suggest that the cities with higher cyber demand need longer to hire workers.

Figure 36: Relative opening time and market size



The figure plots the 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 a city.

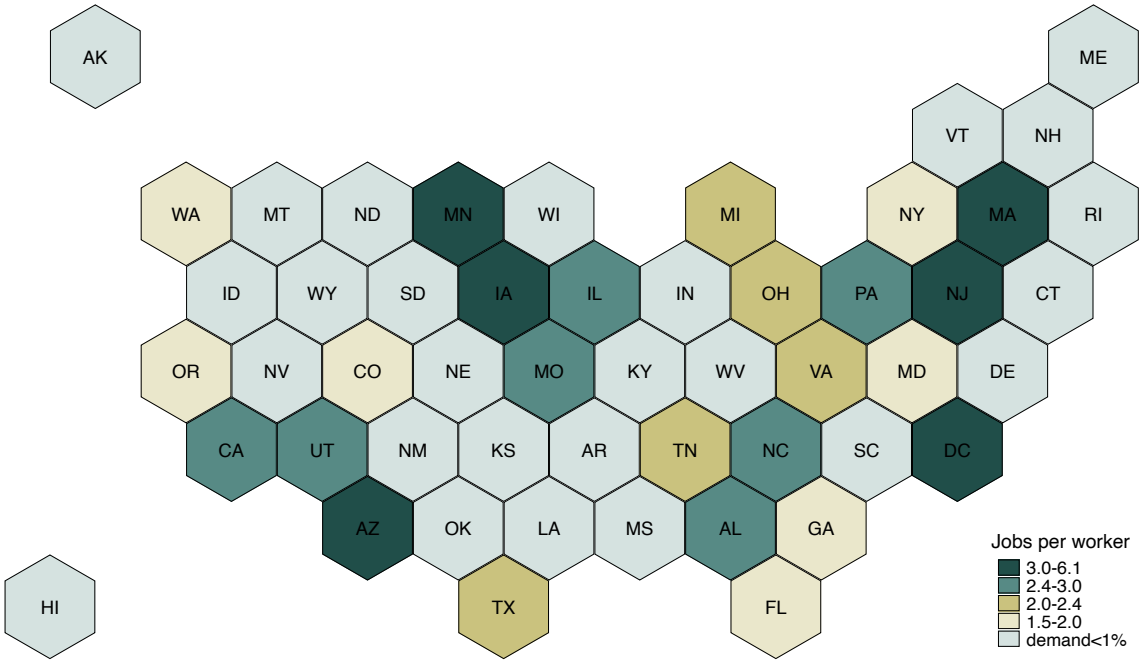
3.4.2 Does the Supply Match the Demand?

We compare the demand for cyber skills in 2021 as measured by the cyber job postings with the supply of cyber professionals. The average US state has 2.6 cyber job postings per cyber professional. Figure 37 shows how the ratio of job postings per cyber worker varies across all fifty states and DC. We focus on the states accounting for at least 1% of all cyber job postings nationally.

In 2021, the average US state saw 2.6 cyber job postings per cyber professional.

The states shown in green or dark green color report a higher number of job postings per cyber professional. Among these locations, DC is an exception since most of the cyber professionals working there live outside the DC area. For others, most of these are established markets, 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 yellow or light yellow are the ones with a relatively better demand-supply ratio. Notably, Florida, Georgia, Colorado, Oregon, and Washington state show 1.5-2 job postings per cyber professional which is well below the average.

Figure 37: Supply of cyber professionals to demand for cyber skills (US states)



To sum up, we review two indicators to gauge the impact of the rising demand for cyber skills. Across the 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 slowly. Especially for one of the growing regions, Asia, we see cyber job opening time is relatively long across key cities.

Across the US market, we do not find any systematic pattern to suggest that larger markets face more difficulties in hiring 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, or Florida, have low to moderate skill shortages. In general, all the states show that businesses demand more cyber skills than can be filled by the current pool of workers.

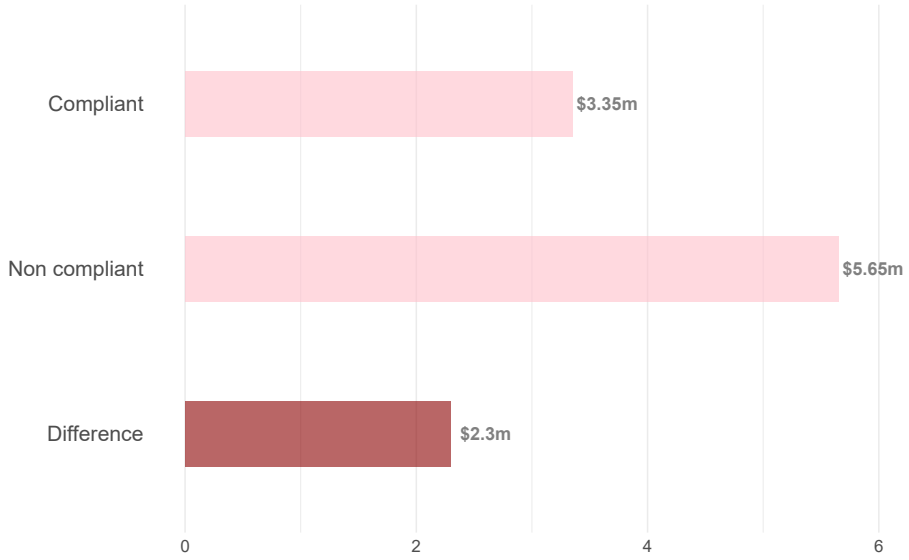
4 Business Strategy for Managing Cyber Risk

4.1 Compliance and Cyber Risk

Cost of noncompliance.

An IBM report shows that the failure to comply with data protection regulations amplifies the data breach costs of a cyberattack. If the compliance authorities find that companies lack in good practices and do not have appropriate safety measures to prevent breaches, they are more likely to take strict legal measures and impose harsher penalties. The average data breach cost for noncompliance organizations is $5.65 million, compared with only $3.35 million in organizations with low levels of compliance failures. The $2.3 million difference, which amounts to 51.1% higher cost, sheds light on the importance of compliance with cybersecurity regulations.

Figure 38: Cost of in-compliance with data protection regulations after a cyber attack



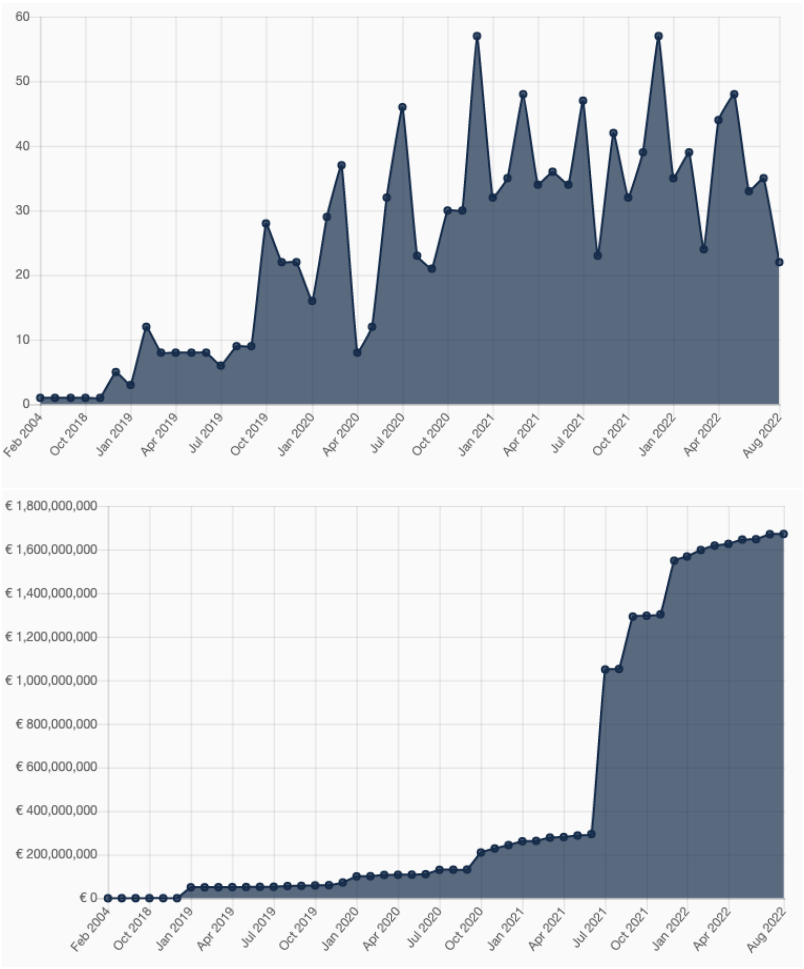
Firms that fail to comply with data protection regulations experience a 51.1% higher cost of a cyberattack because of fines, penalties, and lawsuits. Source: IBM

The risk and cost of noncompliance is increasing. During the past few years, the data protection regulatory environment became increasingly stringent. At the same time, an increasing number of countries have legislated data protection and privacy regulations. According to UNCTAD, 71% of the countries in the world already have such legislation and another 9% are drafting such laws. On 25 May 2018, the General Data Protection Regulation (GDPR) was enacted across the European Union and the UK. 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 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 or 4% of its annual global turnover, whichever is higher. The law also makes it mandatory for the data controllers to notify data protection authorities as well as affected individuals within 72 hours of becoming aware of a breach. Figure 39 shows that not only did the fines become more frequent since 2018 across European countries, but the amount of fines also increased. In particular, the surge was notable during the last two years. While the cumulative amount of issued penalties by January 2020 totalled €100 million for 169 GDPR cases, it increased to €1,671 million for 1,233 cases by August 2022.

Figure 39: The risk and cost of noncompliance is increasing



The fines related to data protection and privacy became more frequent across European countries since the passage of GDPR in 2018 . Moreover, the amount of fines has also increased since then, with a substantial surge during the past two years following the onset of the pandemic. While the cumulative amount of issued penalties by January 2020 totalled €100 million for 169 GDPR cases, it increased to €1,671 million for 1,233 cases by August 2022.

It is important to note that 257 of the European cases were related to data breaches and insufficient technical and organizational measures related to information security. The same reason applies to many of the mega-fines of €1 million or above. The highest fine issued for British Airways was due to a 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.

Table 2: Top 10 Highest GDPR Fines for Data Breaches since 2020

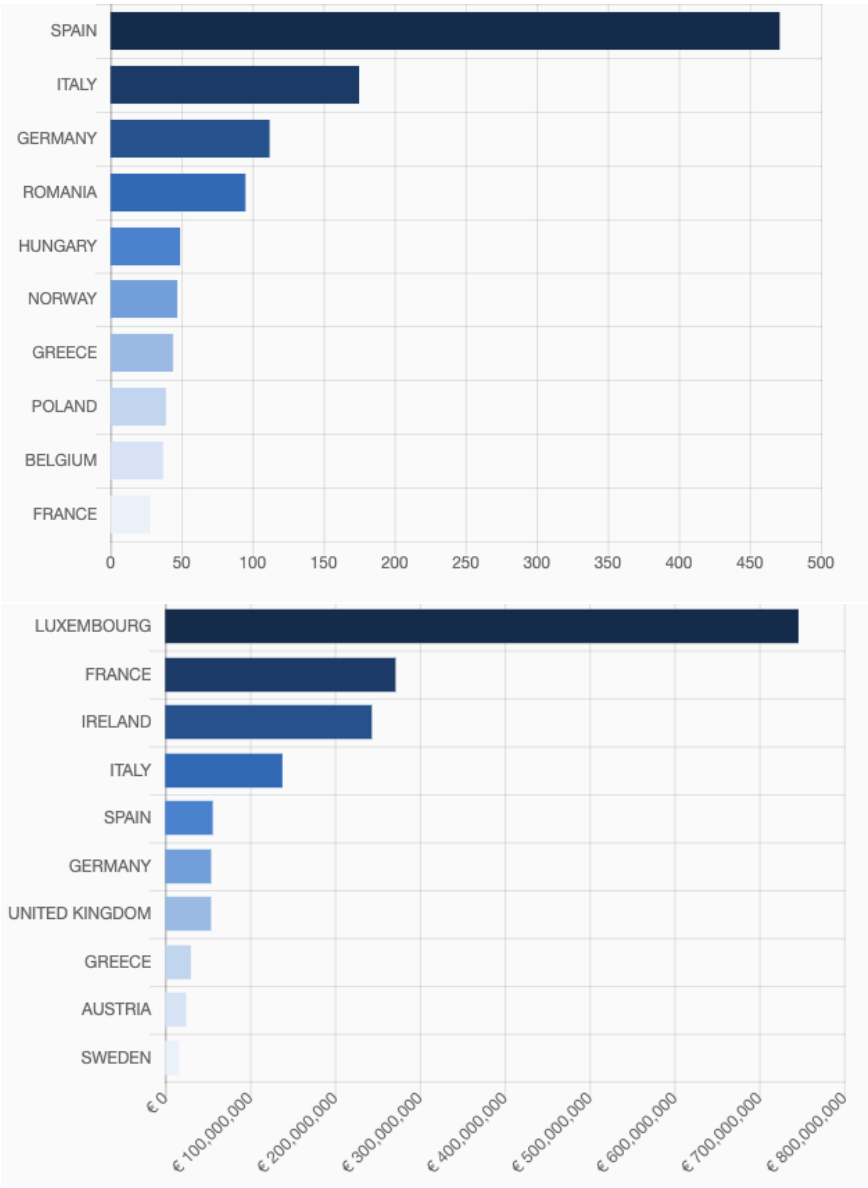
Organization	Country	Date	Amount (€)
British Airways	UK	2020-10-16	22,046,000
Marriott International (Lodging including hotels)	UK	2020-10-30	20,450,000
Meta Platforms	IRELAND	2022-03-15	17,000,000
Cosmote Mobile Telecommunications	GREECE	2022-01-27	6,000,000
OTE Group (Telecommunications)	GREECE	2022-01-27	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

How data protection enforcement differs across European countries. The GDPR was enacted across different European countries in 2018. Nevertheless, the enforcement of the GDPR substantially differs across Europe. 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 fines rather low. While Spain ranks first with 471 penalties, the sum of fines only amounts to €56 million. In contrast, France has issued only 28 fines but the sum of them amounts to €271 million. This highlights the two strategies that European countries have used to ensure compliance with GDPR – increased enforcement vs. increased penalties.

Increased enforcement vs. 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. They look into two periods of data protection enforcement by the Information Commissioner's Office (ICO) in the UK. 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 the enactment of the GDPR, which substantially raised the ceiling of monetary penalties. Since then, the ICO relied more on mega-fines but decreased the frequency of issuing monetary penalties. The researchers focus on the trend of cybersecurity hirings during these two periods, as hiring cyber talents is one of the most effective ways firms can reduce the risk of data breaches and stay com-

pliant 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, the frequent-but-smaller penalties have a more widespread and homogeneous impact across firms of different age and financial strength.

Figure 40: Difference in data protection enforcement strategies across European countries



The enforcement of the GDPR substantially differs across the Europe. Countries such as Spain have significantly increased the number of fines issued while keeping the amount of fines rather low. In contrast, there are countries, such as France, that relied on fewer but larger sums of fines. This highlights the emergence of two strategies that European countries have used to ensure the compliance with the GDPR, namely increased enforcement and increased penalties.

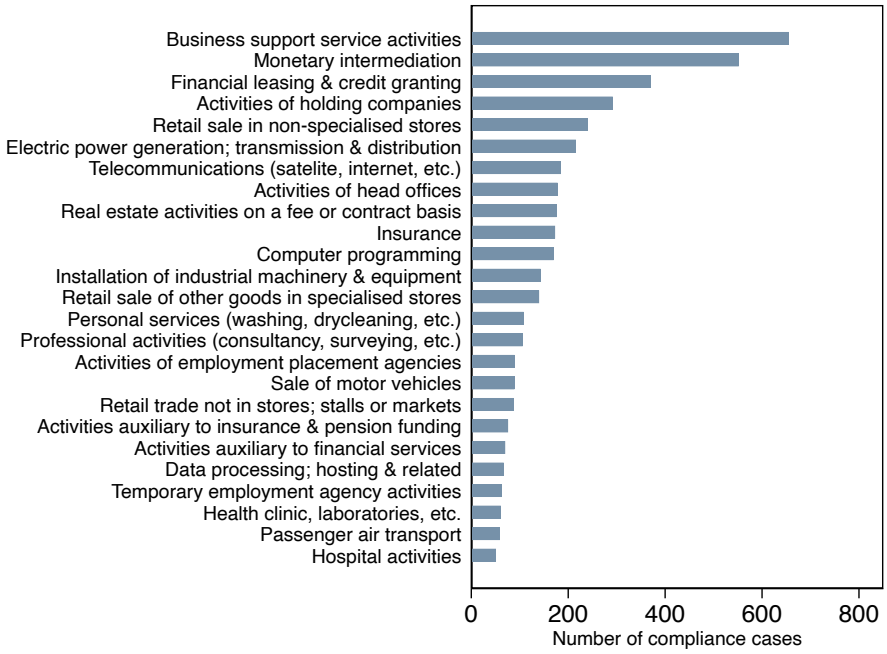
Which industries are more exposed to enforcement?

Businesses in different sectors are exposed to a different degree of compliance risk. One explanation lies in the fact that 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 more expensive personal data to lose. Recently, medical records, owing to their potential sensitive contents, brought regulators' attention to ensuring their protection.

The Oxford Martin School research reviewed around 5,800 data protection cases in the UK to shed lights on which businesses face more customer complaints and resulting actions from regulators. 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 Equifax (a credit rating agency) or 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 health care providers and businesses account for another significant segment of data protection cases.

Figure 41: Data protection enforcement across different industries



The noncompliance risk differs across industries. 'Business service activities' comes at the top and includes businesses that are specialized information brokers. Financial activities, retail and utility companies, and health-care providers are among the top 25 categories that are most exposed to data protection enforcement. Source: Authors' calculation using ICO data.

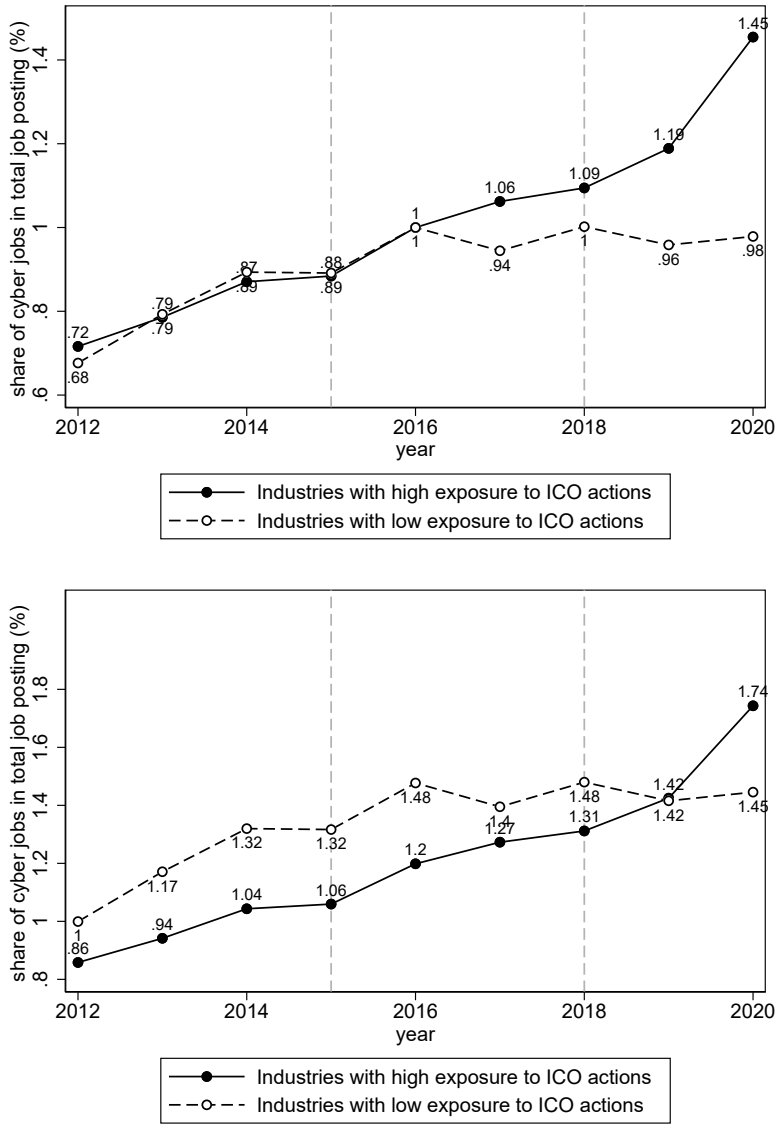
4.2 Cybersecurity as a Public Good

A firm's exposure to cyberattacks not only depends on its own cyber resilience but also on how resilient its partners and suppliers are to cyber risk. In other words, a firm's cyber hirings 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. **How to 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 approach is encouraging firms to integrate cybersecurity as a part of their corporate social responsibility (CSR) agenda. This is important to highlight because cyberattacks can have substantial social impacts. For instance, the ransomware attack in May 2021 that led to Colonial Pipeline's shut-down 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 UK data protection authority.

As already discussed, the UK has one of the strongest regulatory environments, with the Information Commissioner's Office (ICO) overseeing compliance with the Data Protection Act (DPA), General Data Protection Regulation (GDPR), and Privacy and Electronic Communications Regulations (PECR). Researchers compare industries with high- and low exposure to ICO enforcement and find that the high exposure industries experience a 26-52% increase in the demand for cyber skills following the introduction of stronger data protection regimes. Figure 42 shows 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 which shows high-exposure industries initially had a lower demand for cyber skills.

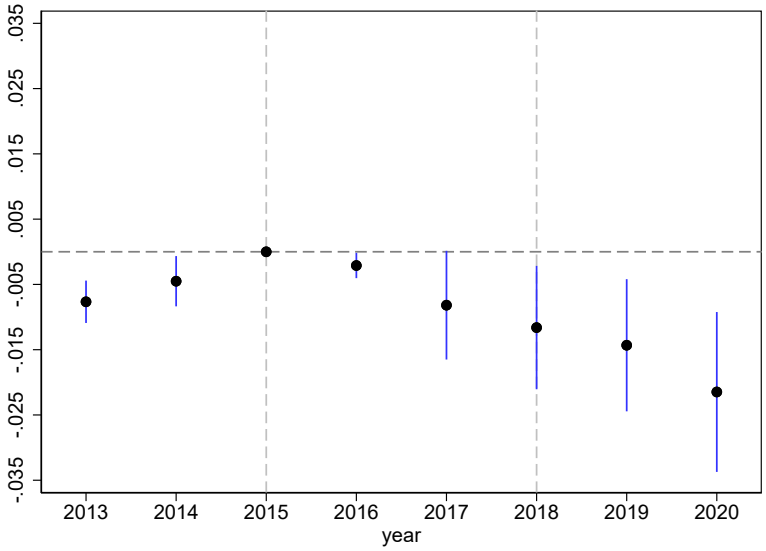
Figure 42: Data protection enforcement and demand for cyber skills



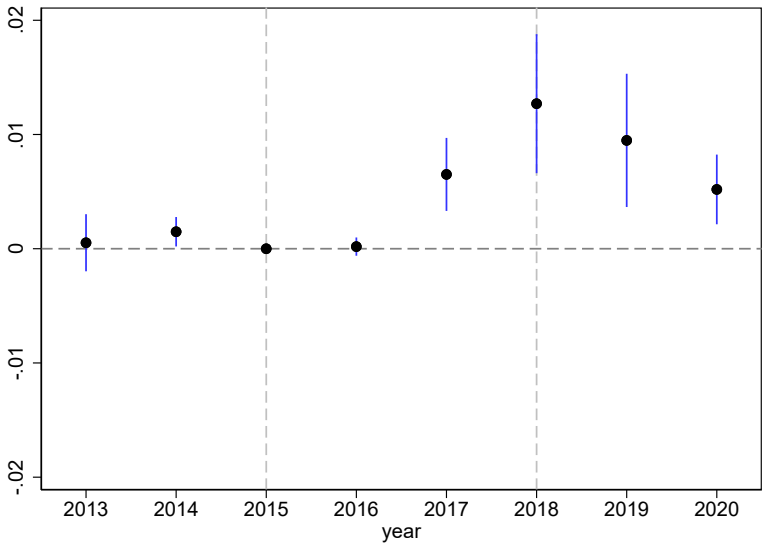
Demand for cyber skills rapidly increases in industries highly exposed to enforcement following the introduction of stronger data protection environments. The first dashed line shows a change in the rule that gave the UK Information Commissioner's Office greater discretion to issue monetary penalties. The second line shows the enactment of the Data Protection Act 2018 which raises the ceiling of the penalty. Source: SSRN

Adverse effect on firm dynamics. Although there is a compelling case for stronger data protection regulation, it comes with 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 43: Impact on firm entry and exit



(a) Entry rate



(b) Exit rate

The top panel shows the differences in entry rates for the high vs. low exposure industries. The downward turn means the entry rate in high-exposure industries consistently 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.
Source: SSRN

Not all businesses are affected in the same way by the adverse effect of regulation. A recent study on the California Consumer Privacy Act (CCPA) examines this issue. The CCPA limits firms' ability to access personal data. This adversely affects firms that rely on external data to develop their products. In contrast, 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.

4.3 Cyber Resilience as a Frontier ESG Theme *by Anita McBain*

4.4 Cybersecurity: Automation and Outsourcing *by Fatima Boolani*