TECH ACCORD

Securing a shifting landscape: Corporate perceptions of nation-state cyber-threats

WRITTEN BY The Economist INTELLIGENCE UNIT

About the research and acknowledgements

Securing a shifting landscape: Corporate perceptions of nation-state cyber-threats is a report from The Economist Intelligence Unit, sponsored by the Cybersecurity Tech Accord. Kim Andreasson is the author of the report and Michael Gold the editor, with support from Wade Islan and Kosi Ogbuli. The research is based on a survey of 524 executives conducted in November and December 2020 and input from leading security experts. All survey respondents are in senior roles and familiar with their organisation's cyber-security strategy.

Survey respondents come from Asia-Pacific, Europe and the US, with a minimum of 150 respondents in each region. They all sit at director-level or above and come from companies with more than US$500m in global annual revenue. A wide range of industries are represented in the survey, led by IT and technology, retail and consumer goods. Half of respondents are from IT/tech or cyber-security functions. See the appendix for a full breakdown of the survey demographics.

To better understand the perceived challenges of nation-state cyber-threats, in particular during times of disruption and in the wake of significant incidents, interviews were conducted with experts and supplemented with wide-ranging desk research. Our thanks are due to the following for their time and insights:

- **Charles Carmakal**, senior vice-president and chief technology officer, Mandiant, a division of FireEye
- **Mark Montgomery**, senior director, Center on Cyber and Technology Innovation, Foundation for Defense of Democracies, and senior advisor, Cyberspace Solarium Commission
- **Marietje Schaake**, president, CyberPeace Institute and international policy director, Cyber Policy Center, Stanford University

A note from the Cybersecurity Tech Accord

Recent nation-state attacks require a new call for defences and dialogue

The Cybersecurity Tech Accord serves as the voice of the technology industry on matters of peace and security in cyberspace. Amid increasingly sophisticated cyber-attacks and geopolitical tensions in the digital domain, we aim to capture the values of our industry on security through four simple principles: **stronger defence, no offence, capacity building** and **collective action**. We put our users and customers first and stand against corrupting technology products to cause harm to innocent civilians and organisations.

Launched in 2018, the Cybersecurity Tech Accord brings together a wide array of technology companies, including software developers, hardware manufacturers, social media platforms and many more—everything from silicon to the selfie. Our coalition includes nearly 150 global technology companies committed to fundamental cyber-security principles for responsible behaviour on the part of industry to keep our customers safe and to improve trust in the digital ecosystem.

Nation-state attacks: An escalating problem too big to ignore

Like nearly every year before it for the past decade, 2020 set a new high-water mark for significant cyber-incidents, including an increasing number of nation-state attacks. These incidents included attacks not just on businesses, but also against hospitals and other healthcare infrastructure amid an ongoing pandemic. One such incident, a ransomware attack against a hospital in Germany, even caused the first-ever recorded death as a direct result of a cyber-attack. Perhaps most concerning, the SolarWinds hack, which came to light only in December, was a nation-state attack which corrupted the routine update of business software—crossing a new threshold by exploiting a process which has long underpinned the security and reliability of so many digital products and services and, in doing so, undermining overall confidence.

As a result of these increasing numbers of sophisticated attacks, organisations today of all sizes are finding themselves having to defend against highly advanced threats while conducting business online. This trend is driven in no small part by increased investment in the development of malicious cyber-capabilities by the most advanced threat actors: nation states. As cyberspace has emerged as a unique fifth domain of conflict (alongside air, land, sea and space), governments around the world have worked to build up their cyber-arsenals. And in a digital environment without clear borders, these tools can and have been used against a wide range of targets, often including private organisations.

A survey for perspective and a call for action

The data in this report captures how private-sector leaders and security experts across different industries from around the world are grappling with the rise of nation-state threats online, how they have seen these threats evolve and where they see the trends going. The results are sobering. Not only do private-sector leaders increasingly recognise nation-state threats as posing significant risk to their organisations, but the problem is only expected to get worse in the years ahead. This marks a fundamental shift in security planning. While every organisation historically has had to give at least some consideration to its security practices—both physical and digital—it is unprecedented that private organisations on this scale should have to steel themselves against attacks from the most sophisticated actors: governments.

Throughout the report, you will hear from interviews of leading thinkers and security experts—including one from a division of FireEye, a Cybersecurity Tech Accord signatory—about the meaning of the survey data and the nature of escalating nation-state threats online. The survey also brings forward specific recommendations about how to get ahead of these challenges, but fundamentally we feel that enduring solutions will be those that turn the tide on escalating state threats online. More than anything else, this will require co-operation across stakeholder groups to help set and enforce meaningful expectations—asking companies to think more expansively about their roles and governments to think more inclusively about theirs. Our own commitment is to help strengthen and advance industry responsibility, and similarly applaud multi-stakeholder initiatives like the Paris Call for Trust and Security in Cyberspace, which bring together governments, industry and civil society around shared values and principles for a free, secure and rights-respecting online world.

Executive summary

Cyber-security is rarely far from the headlines, but reporting tends to focus on big events rather than a general growth in attacks and the evolving domain of conflict. As the world becomes more interconnected, nation-state incursions that steal, destroy or damage information, or that spy on or embarrass their targets, are a growing concern among policymakers and corporate executives alike, with more countries facing accusations of either conducting or sponsoring such attacks. The shifting landscape of state-sponsored threats—and how stakeholders respond to them—will have a major impact on how firms operate and what they perceive to be the best way to mitigate threats. This is crucial as cyber-attacks increasingly target new sectors and different types of data.

This report assesses corporate perceptions of nation-state cyber-threats. It finds that companies have become aware of the challenges posed by such threats and are concerned about them; however, their ability to respond to evolving risks may be lacking. The key findings are:

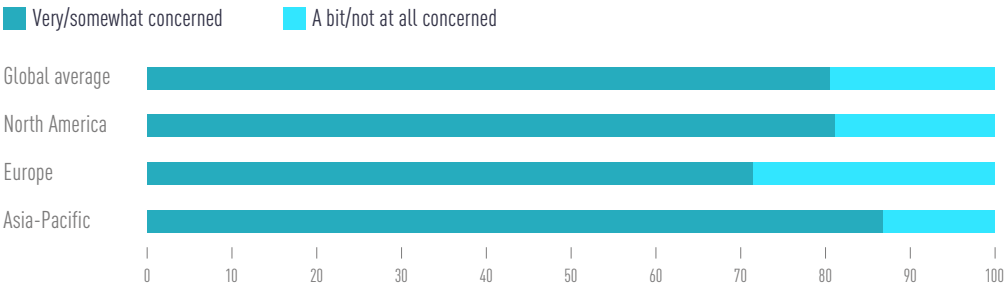
- **Firms' confidence in their ability to handle nation-state threats may be overstated.** Companies recognise the threat posed by nation-state attacks and demonstrate a high degree of confidence in their ability to face them. This confidence may be inflated, however, according to experts interviewed for this report.
    - Executives in Asia show a subtle but noticeable trend of both greater concern and greater readiness than their European and North American counterparts.
- **Concerns over nation-state threats have evolved to encompass more factors.** Cyber-attacks were once primarily viewed as a financial risk. Now, however, nation-state attacks also often target confidential materials and other important information (such as medical data), as highlighted by recent sophisticated breaches. Our survey respondents recognise this shift and view nation-state actors as a rising future threat.
- **Greater political will, at home and abroad, is crucial to combating the issue.** Executives and experts view stronger cyber-security legislation and regulation as key ways to cultivate a safer cyber-environment, followed closely by stronger international agreements, which have been elusive to date.
- **The covid-19 pandemic has led to growing opportunities for cyber-incursions, especially to gain a foothold in the vaccine race.** Experts interviewed for this report all note an increase in foreign actors trying to exploit weaknesses to gain access to sensitive pandemic-related data, particularly in sectors such as healthcare.

01. Chapter 1: Overconfidence amid rising threats

In the survey conducted for this report, eight in ten executives say they are concerned about their organisation falling victim to a nation-state cyber-attack.[1] There is no shortage of recent high-profile examples to stoke their fears. In December 2020 an attack exploited business software provided by SolarWinds, an IT company; those who use its software were exposed to the attack.[2] According to *The New York Times*, the government itself appears to have been the primary target.[3] In the same month, the European Medicines Agency was also subject to a cyber-incursion that stole covid-related data.[4]

Figure 1: States of concern

"How concerned is your organisation about falling victim to a nation-state cyber-attack?", overall and by region



Source: The Economist Intelligence Unit

"The SolarWinds supply-chain attack caused the industry to rethink how they manage third-party risk," says Charles Carmakal of Mandiant, a division of FireEye, a cyber-security company. "What's different from previous nation-state attacks was the level of sophistication and scale of this operation."

[1] Note: The survey was conducted prior to the disclosure of the SolarWinds attack.

[2] "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", FireEye Threat Research, December 13th 2020.

[3] David E Sanger, Nicole Perlroth and Julian E Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm", *The New York Times*, January 2nd 2021.

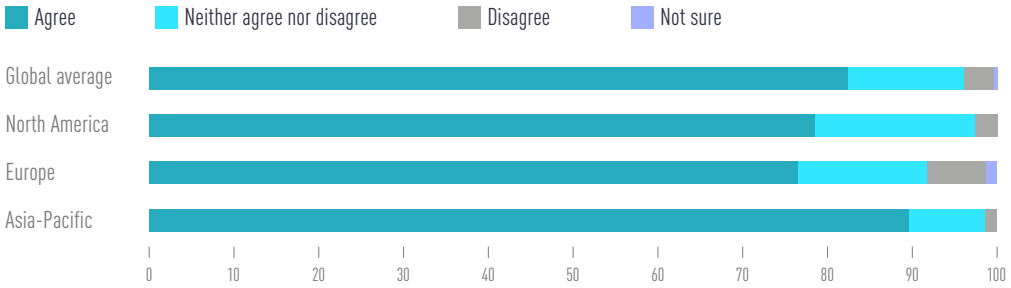
[4] "Some data from last month's cyber attack leaked online, says EU drugs regulator", Reuters, January 12th 2021.

The growing concern among executives is illustrated by the fact that eight in ten also say nation-state cyber-attacks are advancing faster than defences, a finding supported by Mark Montgomery, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, a non-profit organisation in Washington, DC, and senior adviser to the Cyberspace Solarium Commission (CSC), established by the US Congress to investigate cyber-security threats. "The risk is growing significantly because adversaries' access to tools and interconnectivity of our systems are going up exponentially," he notes. "The only risk mitigator is our investment in cyber-security defence, and that's generally linear."

Covid-19 has also expanded the attack surface. In our survey, almost eight in ten say the pandemic has increased the likelihood of a nation-state cyber-attack on their organisation. The International Criminal Police Organization (INTERPOL), which tracks cross-border crime, has noted a rapid uptick in the number of cyber-attacks during the pandemic as organisations deploy remote systems and networks to support work-from-home.[5] According to Mr Carmakal, "During the covid-19 pandemic we have seen cyber-espionage activities by multiple governments to try and learn everything they can about vaccine development and R&D," a trend also noted by the other experts interviewed for this study.

Figure 2: The enterprise at risk

"Corporate efforts to combat cyber-attacks should focus more on nation-state actors", % agreeing, overall and by region



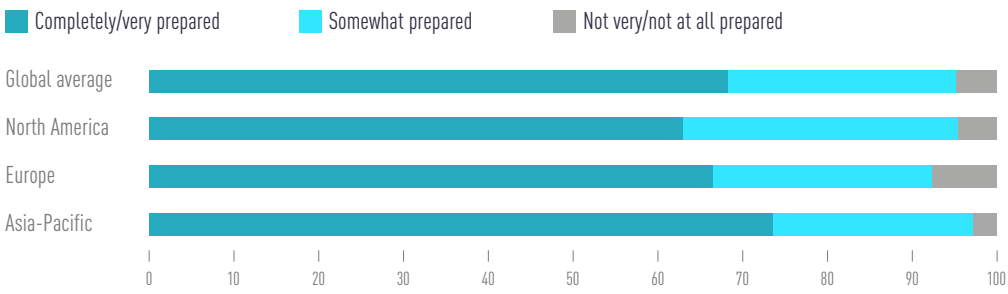
Source: The Economist Intelligence Unit

[5] "INTERPOL report shows alarming rate of cyberattacks during COVID-19", INTERPOL, August 4th 2020.

Nation-state cyber-attacks have shifted the risk consciousness for organisations, which were previously dealing with a largely physical threat landscape. Indicative of this new mindset, roughly seven in ten executives feel their organisation is very or completely prepared to handle nation-state cyber-attacks. However, Marietje Schaake, president of the CyberPeace Institute and international policy director of Stanford University's Cyber Policy Center, calls this a "false sense of security", in part because until an attack occurs, organisations tend to be confident that they will not become a victim. Mr Carmakal notes that not all organisations are actually the intended target of nation-state attacks, so many do not have tangible experience of dealing with such threats. "Nation-state threat actors are very focused and persistent with their targeting," he says. "Organisations that have been previously compromised by nation-state actors tend to be better prepared for future attacks, as they learn from prior security incidents and improve their defences." Even non-targets may end up as collateral damage, though, as malware attacks can spread far beyond their intended victim.

Figure 3: Prepared or overly confident?

"To what extent is your organisation prepared to deal with a nation-state cyber-attack?", overall and by region



Source: The Economist Intelligence Unit

02. Chapter 2: Prime targets and the ever-evolving threat environment

Cyber-attack methods are multifaceted, ranging from emails asking for personal information (phishing), to denial of service (DoS) attacks meant to render websites unavailable. The same is true of the objectives, which range from simple fraud and data theft to sophisticated attacks on infrastructure. Survey respondents view individual hackers seeking financial gain (22%) and organised cyber-crime groups (22%) as the two gravest cyber-threats to industry, while nation-state actors only rank fourth (12%). However, the threat from nation-state actors is forecast to rise to second place (18%) in the next five years, behind organised cyber-crime groups. The threats posed by nation-state actors can multiply as advanced tools and technologies developed by nation-state actors can later be repurposed by less advanced users.

With some exceptions, nation-state actors do not seek pure financial gain, as other types of hackers often do. Survey respondents generally recognise this, viewing the leak of confidential materials and loss of crucial information as the top potential consequences of a nation-state cyber-attack on their organisation. "If you go back ten years, banks would be experiencing the most cyber-criminal activity because that's where the money was," says Mr Montgomery. "Now a wider variety of industries are vulnerable to malicious behaviour because their data can be monetised."

Facing unintended consequences

The geographical origins of nation-state attacks are also more complicated than might be assumed from front-page headlines. The CSC views China, Russia, Iran and North Korea as the top perpetrators of nation-state attacks.[6] Yet many countries develop offensive capabilities and engage in attacks—a trend that can have unintended consequences, often because a piece of malware designed for a specific target can spread throughout the supply chain as other organisations also become exposed to it. The US National Security Agency, for example, developed a malware tool named WannaCry that was purportedly later stolen and used by North Korea to extract money from organisations.[7]

[6] Cyberspace Solarium Commission website.

[7] "'WannaCry' Ransomware Attack Reveals Government Possession of Attack Tools", *Government Technology*, May 16th 2017.

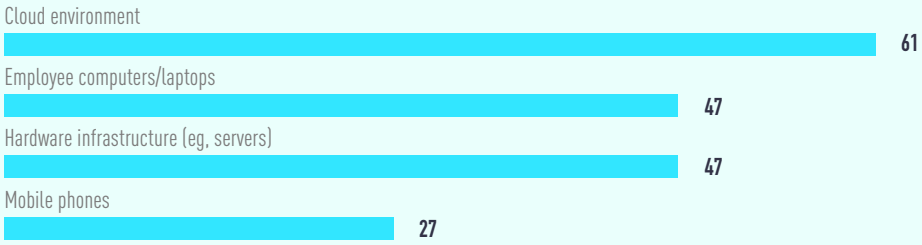
Opportunities and challenges of emerging technology

Newer technologies, especially artificial intelligence and machine learning (AI/ML), can offer new opportunities to defend against attacks by virtue of quickly recognising data patterns. In the survey, respondents cite AI/ML and cloud computing as the emerging technologies that would be best deployed to counter nation-state cyber-attacks directed towards private organisations. Such technologies can also be a vector for threats, however, as malicious actors can use these emerging tools just as anyone else can.[8] "These technologies offer a vast opportunity but also expose you to increased risk if an adversary develops tools for their own offensive capabilities," says Mr Montgomery.

It used to be conventional wisdom that data stored locally—rather than in the cloud—was safer due to its nearby physical presence. Recently, however, many organisations have determined that cloud providers can provide greater cyber-security than they themselves can. This, in turn, has led to a renewed interest among attackers, a trend recognised by our survey respondents, six in ten of whom believe their cloud environment will be the area where a nation-state cyber-attack will most likely occur, far ahead of local servers. One reason may be that cloud adoption has increased rapidly over the years and users are unaware of security details. Underscoring this point, in January 2021 the Cybersecurity & Infrastructure Security Agency, a unit of the US Department for Homeland Security, issued an alert about various cyber-attacks against organisational cloud environments due to poor "cyber hygiene".[9]

Figure 4: Searching for backdoors

"Through which of the following types of infrastructure do you think a nation-state cyber-attack would most likely enter your corporate network over the next five years?", % of respondents



Source: The Economist Intelligence Unit

[8] "The evolution of cloud security: perception vs reality", bitglass.

[9] "Attackers Exploit Poor Cyber Hygiene to Compromise Cloud Security Environments", Cybersecurity & Infrastructure Security Agency, January 13th 2021.

03. Chapter 3: In search of solutions, at home and abroad

The complexities and sophistication of nation-state threats demand a response at multiple levels, including government and the private sector. Our respondents themselves are primarily focused on increasing investment in cyber-security-related technical measures (44%), improving training and education of employees (37%) and designating a person or team to be in charge of cyber-security across the organisation (31%).

Yet corporate action alone is not sufficient to stop the threat. Four in ten respondents say their country provides a high level of protection against nation-state cyber-attacks directed towards private organisations and a slightly higher number (46%) report leveraging discussions with or intelligence provided by governments to stay abreast of developments in the nation-state cyber-threat landscape. Specialised government-supported entities, known as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs), founded to support one or more industries, often provide threat insights to member organisations. The European Union Agency for Cybersecurity, for example, maintains a list of more than 500 such entities across the region that share information and co-operate in the face of an attack.[10]

Official efforts to support organisations remain incomplete, however, as almost six in ten executives say their country only offers a medium or low level of protection. To reduce nation-state attacks on private organisations, respondents point to the need for stronger cyber-crime legislation at the national level as the top broad initiative they would like to see, and regulations to strengthen the overall ecosystem resilience against nation-state threats as their top desired specific government action. Ms Schaake sums up the sentiment: "We need democratic governments to step up regulation. I would not consider that heavy-handed; I think it's more a matter of catching up."

Greater co-operation as the holy grail and biggest challenge

The international arena also lacks sufficient political will to tackle cyber-security generally and nation-state attacks specifically. Although there are several international frameworks and norms-based initiatives,[11,12] they cover only a limited set of countries and have no enforcement mechanism. "International co-operation is becoming increasingly difficult as political systems differ and technological competition between countries intensifies," says Ms Schaake. "It's difficult to arrest individuals when it comes to nation-state attacks," adds Mr Carmakal. "Many of the operators are protected by their host nations and do not travel to countries with extradition laws with the United States."

This is a problem that the private sector would surely like to see ameliorated; almost one-half of survey respondents see more international economic co-operation as the top geopolitical change that could most reduce nation-state cyber-attacks on private organisations, followed closely by more international political co-operation. These two approaches could represent promising avenues for building consensus around international agreements while creating mandatory norms, if even at a basic level.

[10] CSIRTs Network website.

[11] "Details of Treaty No.185", Council of Europe Treaty Office website.

[12] Paris Call for Trust and Security in Cyberspace website.

04. Conclusion: A call to action in a new cyber-landscape

It has become clear that nation-state cyber-threats and their attendant breaches are unavoidable. Instead of trying to protect everything, many organisations have in recent years defaulted to a risk-management mindset of trying to protect the most important data and information in the company rather than trying in vain to protect everything.[13] Moreover, an ad-hoc, company-by-company approach leaves many gaps.

There is a need for actions that can both strengthen defences and reduce the incentives for nation-state attacks, starting with greater political will and partnerships between both the private sector and governments and between countries. Many countries have tried public-private partnership (PPP) models to resolve the challenge, but to little avail. "The asymmetry of power between the private and public sectors is a problem," says Ms Schaake, who points out that businesses provide most of the infrastructure and hold most of the data on which governments rely. "I don't think that corporations have the same incentives as, for example, public officials, to share information and ensure accountability."

Yet government action—or the lack thereof—is also to blame. The CSC has not given up hope: it is encouraging the US government to work more closely with the private sector to defend national infrastructure and help build PPPs, according to Mr Montgomery. "I think we're much further along [compared with past efforts]. Because there's been so much criminal behaviour and so much recognition of inappropriate nation-state behaviour, corporations are starting to understand the need for greater collaboration." Whether this sense of urgency can be extended to the international arena—critical to ensuring appropriate cyber-norms and behaviours across borders—remains to be seen.

The way forward: Five key steps

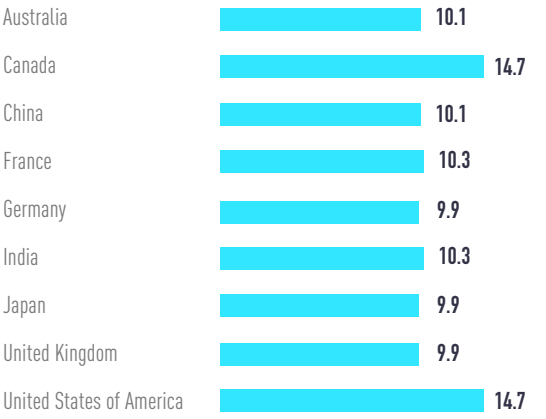
1. **Realise the extent of the problem.** Even when alert levels appear high, prominent examples of purported nation-state attacks show that many organisations need to realise that the threat may be larger than their current ability to defend themselves.
2. **Recognise the evolving nature of the threats.** Given that recent nation-state cyber-attacks increasingly target confidential materials and crucial information across a wider range of sectors, organisations across industries must prepare for potential attacks on types of data they would not have previously expected.
3. **Identify potential pain points within the organisation.** The covid-19 pandemic illustrates the ability of malign, sophisticated and foreign actors to exploit gaps. These weaknesses should be clearly identified and addressed, even though the most sophisticated attackers will find a way in if they work hard enough.
4. **Create partnerships for the future.** Political and business leaders need to co-operate more proactively to craft both domestic and international agreements on cyberspace norms.
5. **Encourage governments to do more.** Companies can work with governments to increase transparency around nation-state threats, raise awareness of the issue and build capacity to deal with it.

[13] "Locking down the value of data", Grant Thornton, 2017.

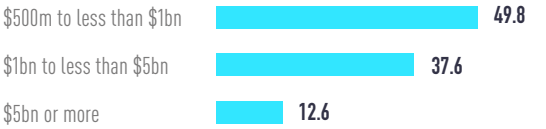
Appendix: Survey results

All figures represent % of respondents.
Figures may not add up to 100% in some cases due to rounding or because more than one option could be selected.

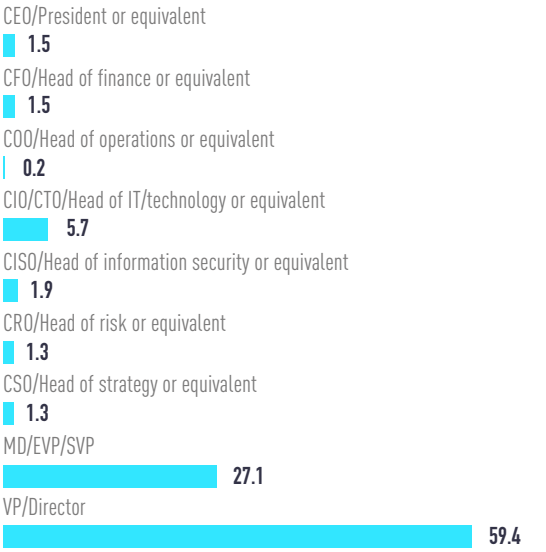
Q1. In which country are you personally located?



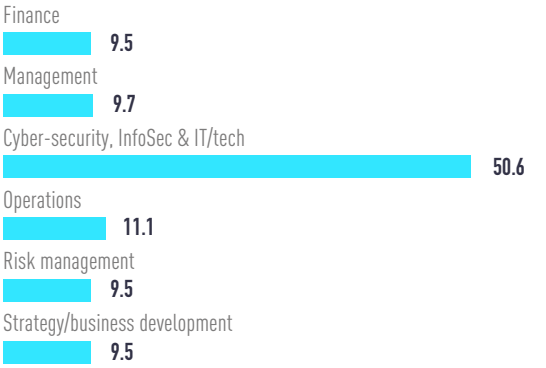
Q2. What is your organisation's annual global revenue in US dollars?



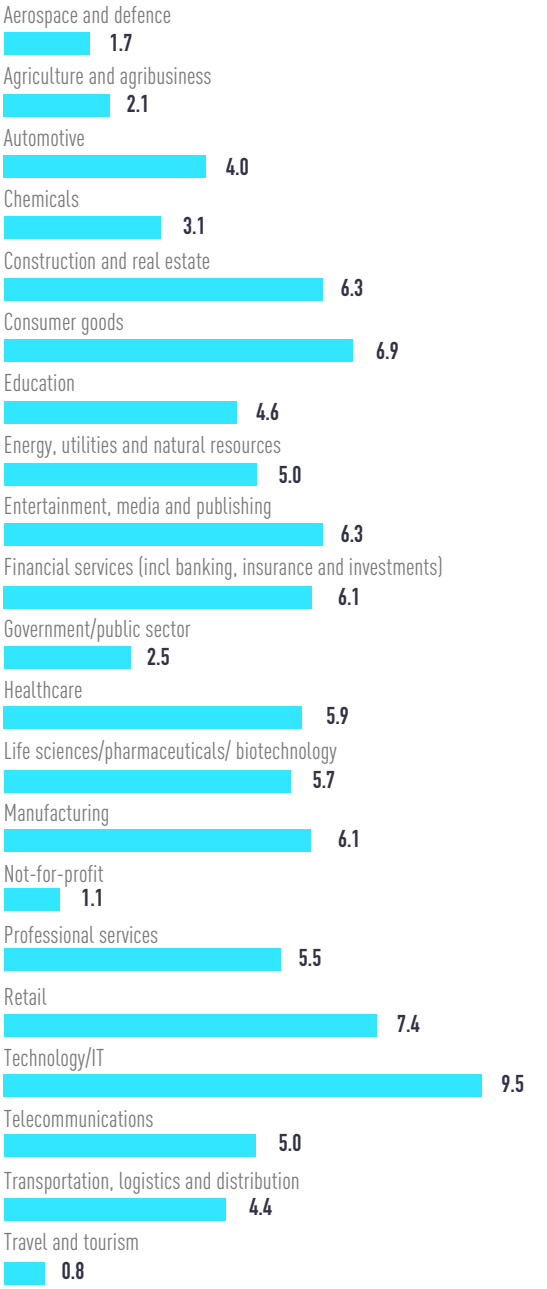
Q3. Which of the following best describes your title?



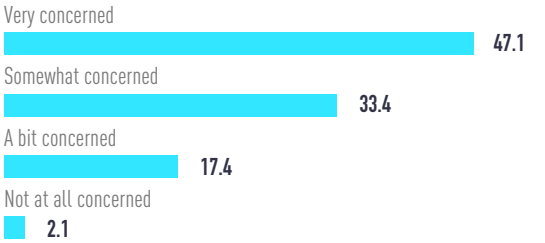
Q4. Which of the following best describes your main functional role?



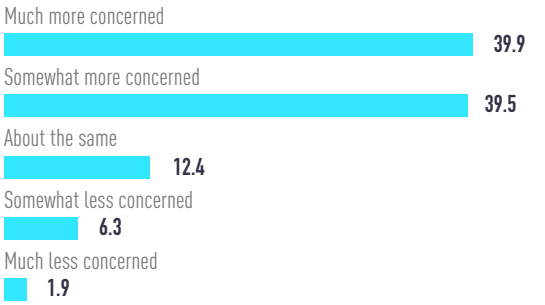
Q5. What is your organisation's primary industry?



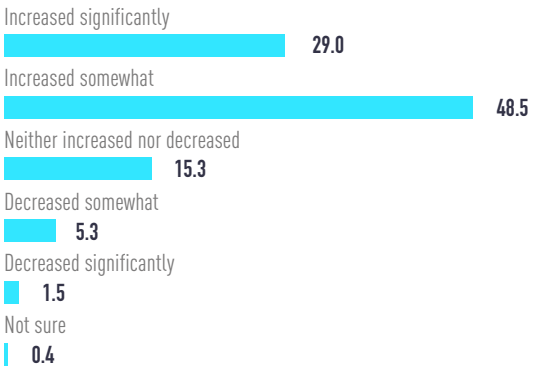
Q6. How concerned is your organisation about falling victim to a nation-state cyber-attack?



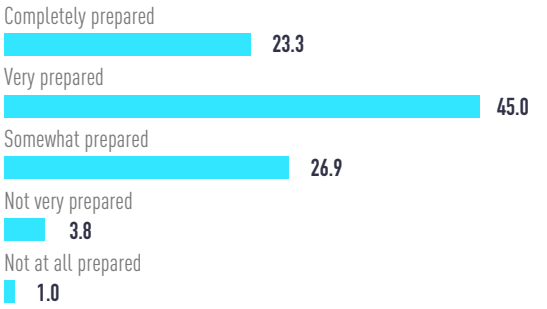
Q7. How much more or less concerned is your organisation about falling victim to a nation-state cyber-attack today compared with five years ago?



Q8. In your opinion, to what extent has the covid-19 pandemic increased or decreased the likelihood of a nation-state cyber-attack on your organisation?

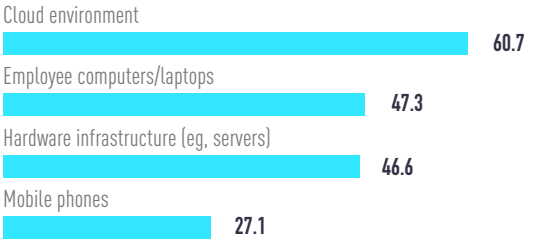


Q9. To what extent is your organisation prepared to deal with a nation-state cyber-attack?



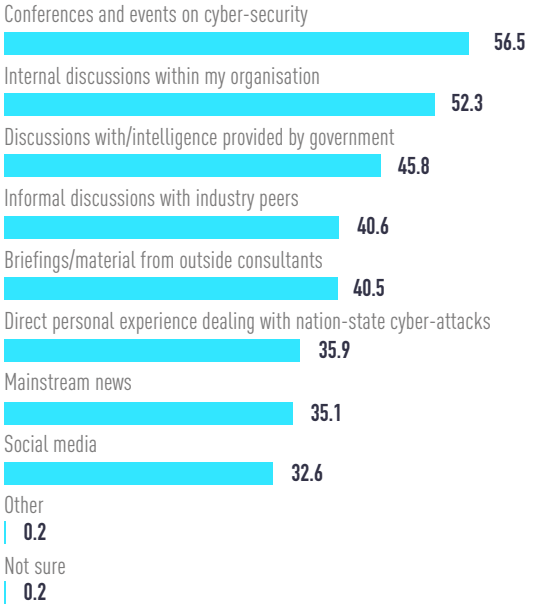
Q10. What steps has your organisation taken to prepare for a potential nation-state cyber-attack?

Q11. Through which of the following types of infrastructure do you think a nation-state cyber-attack would most likely enter your corporate network over the next five years?

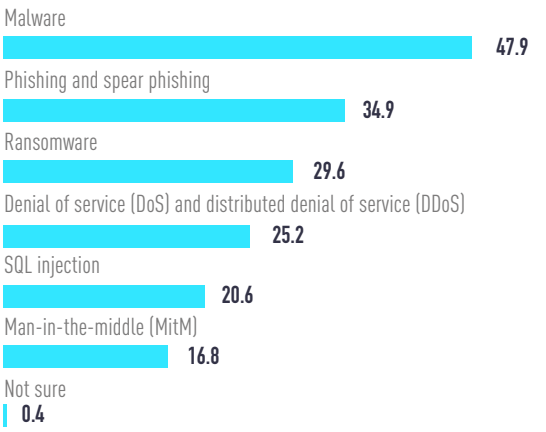


Q12. What are the most concerning potential consequences of a nation-state cyber-attack on your organisation?

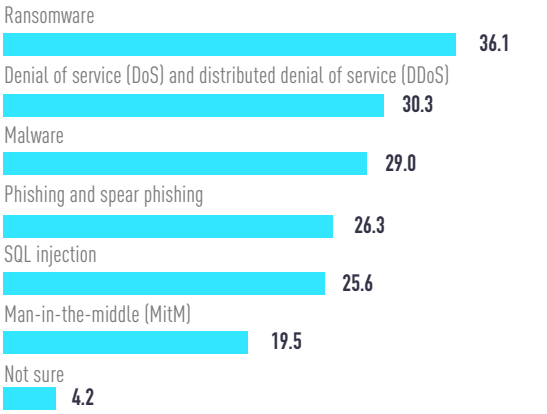
Q13. How do you personally stay abreast of developments in the nation-state cyber-threat landscape?



Q14a. What is the most common form of nation-state cyber-attack facing your organisation today?

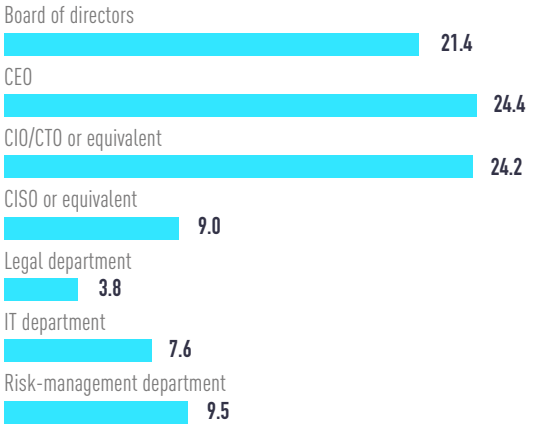


Q14b. What do you think will be the most common form of nation-state cyber-attack facing your organisation five years from now?

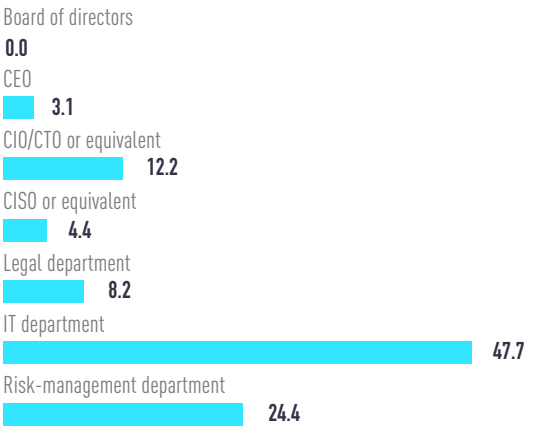


Q15. What are the main objectives of your organisation's overall cyber-security strategy?

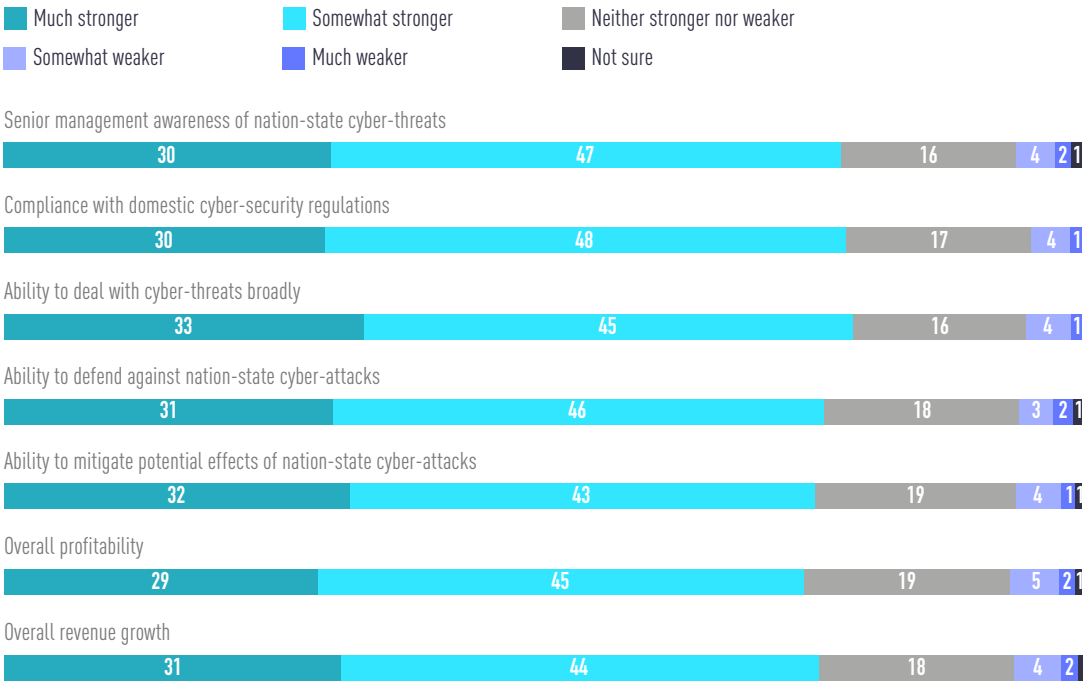
Q16a. Who is primarily responsible for setting your organisation's overall cyber-security strategy?



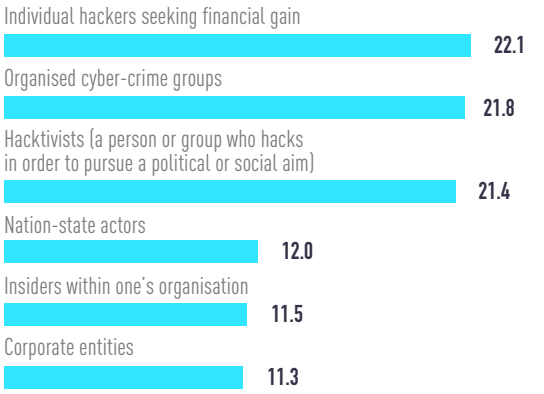
Q16b. Who primarily manages your organisation's cyber-security strategy on a day-to-day basis?



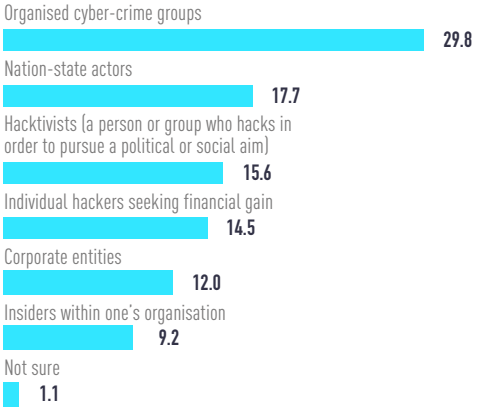
Q17. From your perspective, how does your company compare to its closest competitors in the following areas?



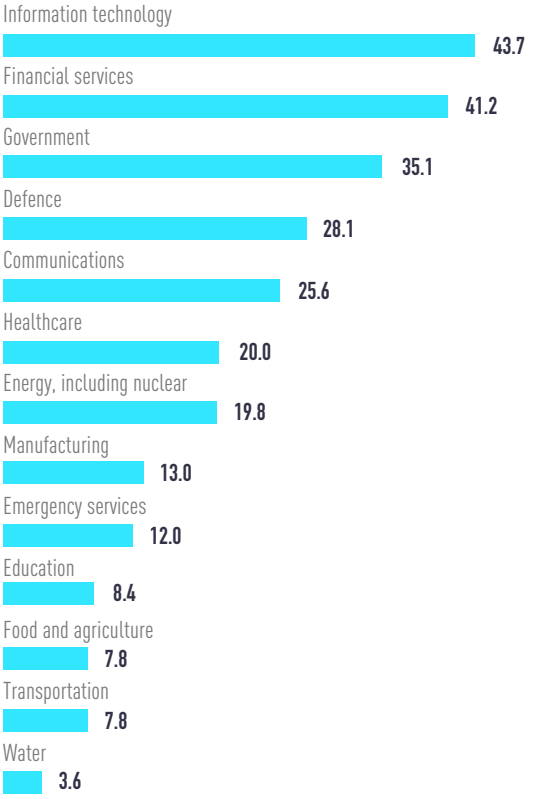
Q18a. Which of the following actors present the gravest cyber-threat to your industry today?



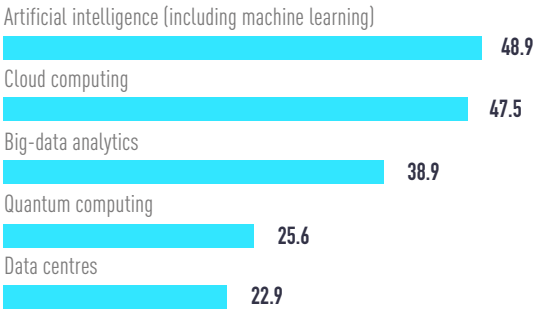
Q18b. Which of the following actors do you think will present the gravest cyber-threat to your industry five years from now?



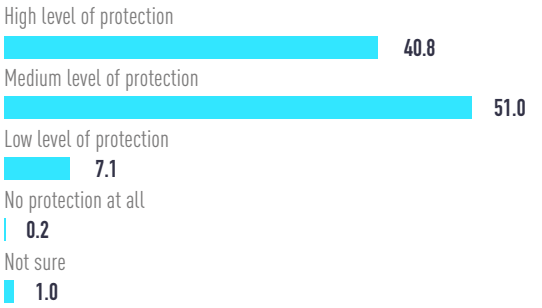
Q19. In your opinion, which sectors are most vulnerable to a nation-state cyber-attack?



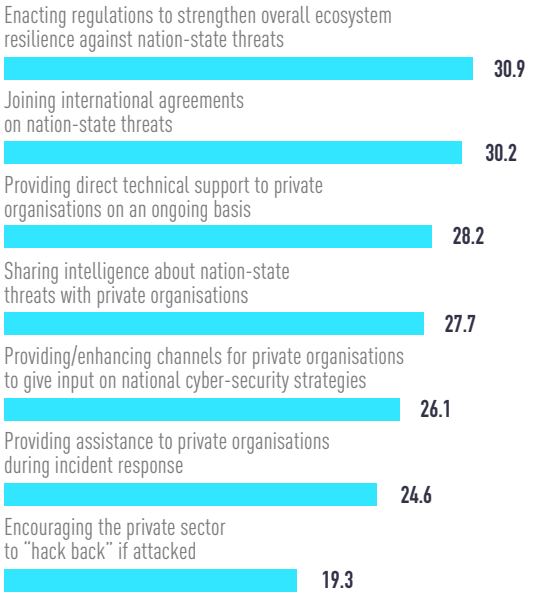
Q20. Which of the following emerging technologies do you think would be best deployed to counter nation-state cyber-attacks over the next five years?



Q21. To what extent do you believe your country's cyber-security strategy provides protection against nation-state cyber-attacks directed toward private organisations?

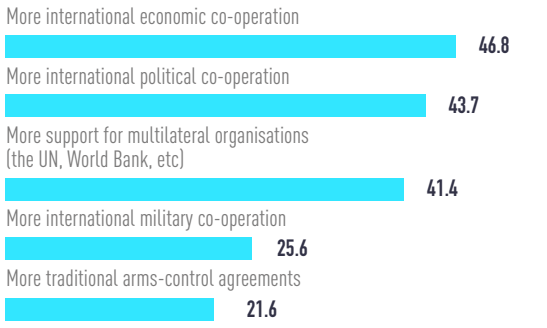


Q22. What specific government actions at the national level could most likely reduce nation-state cyber-attacks on private organisations?



Q23. Which broad initiatives at the global level could most likely reduce nation-state cyber-attacks on private organisations?

Q24. What changes in the overall geopolitical landscape could most likely reduce nation-state cyber-attacks on private organisations?



Q25. To what extent do you agree or disagree with the following statements?