



Data protection ecosystems:

Unlocking strong digital economies



Written by:

The Economist INTELLIGENCE UNIT



Foreword

Welcome to **Data protection ecosystems: Unlocking strong digital economies**.

At WhatsApp, our highest priority is to protect the private communications of people who rely on WhatsApp in a world where cyber attacks occur every minute of the day. Strong security is essential not only because it protects people's most private communication, but because it helps millions of businesses have confidence that when communicating with their customers, their chats are secure.

In 2020, the COVID-19 pandemic forced our personal and work interactions almost entirely online. Businesses couldn't welcome customers into their stores. Doctors, lawyers, government workers and millions of other service providers couldn't be in the same room as the people who rely on them. WhatsApp helped keep lines of communication open and our economies running.

Going remote accelerated a trend in business -- how do we protect against the risks of an increasingly interconnected, digital world?

The Economist Intelligence Unit report helps bring to light that businesses around the globe are putting security first and need simple solutions that keep their data secure. There are three lessons for business leaders and policy makers:

First, we all must acknowledge the severity of the cyber threat.

The data in Figure 2 of this report highlight just how prevalent cyber attacks on organizations of all sizes have become. The people responsible for these cyber attacks are not amateurs; they are increasingly part of sophisticated criminal networks and well-resourced foreign governments. The financial costs to an organization of implementing robust data protection practices are dwarfed by the potentially catastrophic consequences of severe data breaches that are becoming more common every year. Any organization that handles personal or commercial data is a potential target.

Second, organizations need access to encryption technology that can secure their most sensitive data.

Companies that can easily take advantage of encryption at rest and encryption in motion technology will serve their customers well. Additionally, businesses should ask themselves before collecting data if they really need it, and why.

Which brings me to my final point: policy makers must embrace technology that keeps our communications secure in the face of ever-present cyber threats. WhatsApp, Apple iMessage, Signal, Viber and many other organizations use end-to-end encryption for the simple reason that it is the best technology available to ensure that people's private communications remain private. The ability to communicate privately is not only essential to people's lives; it is becoming increasingly essential to their livelihoods. The case study in this report on the role encryption plays in the success of innovative businesses like Fred IT Group (*Case study 1: A role for secure communication*) only strengthens my belief that our economic prosperity will become ever more dependent on tools like WhatsApp's end-to-end encryption in the coming years.

To protect our economies and our human rights in equal measure, we have to be clear-eyed about the threats we face in the digital age, and the trade-offs required to overcome them. As our society develops rules, security must be held high. WhatsApp will continue to do our part to provide simple, reliable, and secure communications to two billion people and business users around the world.



Will Cathcart
Head of WhatsApp



Contents

2 About the research

4 Executive summary

6 Introduction

Different data divisions

Moving from data to data protection

10 Digital threats as the new normal

From cyber breaches to better data management choices

Case study I: A role for secure communication

A starting point

Suggestions for improvement

17 Tracking awareness across the board

Case study II: A concern to both David and Goliath

Small and weak links

23 Surprising motivations as a driver towards data protection

The trust factor

Case study III: Regulatory approaches

29 Conclusion

Key takeaways

31 Appendix

About the research

Data protection ecosystems: Unlocking strong digital economies

is a report from The Economist Intelligence Unit, commissioned by WhatsApp, exploring the data-protection landscape around the world and the benefits and challenges that come with it as organisations increasingly operate digitally.

Kim Andreasson is the author and Jason Wincuinias is the editor of this report. Both can be reached at asiaperspectives@economist.com.

The report's analysis is based on a survey of 400 people conducted from February to April 2020. Half the respondents came from developed economies (Australia, Germany, the UK and the US) and the other half from developing nations (Brazil, India, Indonesia and Mexico). About 60% of respondents work at companies with revenue of US\$1bn or greater. Roughly 75% of survey takers were board members or C-suite whereas 25% were at director level and above. IT and technology (35%), general management (34%) and finance (12%) were the most common functions represented, while IT and technology (31%) and financial services (13%) were the most represented industries. The vast majority (92%) of organisations in the survey have operations in countries outside of their home country. All survey takers were familiar with their company's approach to managing customer data and the design and testing of the systems that protect it. Complete demographics can be found in the appendix.

We would like to thank all interviewees and survey respondents for their time and insight (listed alphabetically by surname):

- **Eduardo Araral**, associate professor, Lee Kuan Yew School of Public Policy
- **Alicia Bárcena**, executive secretary, Economic Commission for Latin America and the Caribbean (ECLAC), UN
- **Nigel Cory**, associate director, Information Technology and Innovation Foundation
- **Rahul Matthan**, partner, Trilegal
- **Mark Montgomery**, executive director, Cyberspace Solarium Commission
- **Paul Naismith**, founder and CEO, Fred IT Group
- **Michelle Price**, CEO, AustCyber
- **Andrew Stott**, former CIO, UK Government

Executive summary

The vast sums of data generated daily create new business opportunities and challenges for organisations across the world. Many commercial and public entities use data to improve services and internal operations, as well as sharing it for commercial or public-service delivery. Data then becomes an economic lynchpin; therefore cyber threats, as well as complexities of complying with data-related regulations that are clearly needed to protect consumers and businesses, have emerged as significant issues within digital development (a term used as a catchall for new technological tools and benefits within business and daily life). Grappling with these is integral to unlocking strong digital economies. Cyber attacks have increased in both scope and frequency, and the covid-19 pandemic has highlighted this challenge as organisations had to move rapidly to remote work and now rely on digital tools more than ever.

That shift is likely to have permanence. And if organisations are to reap the full benefits of digital development, cybersecurity will be a central issue—now and in the future.

Increasing need for secure data

Data exchange is an ever-growing part of public, private and corporate life, be it browsing, buying or basic communication. Remote work during, and likely after, the pandemic, is set to intensify cybersecurity needs, prompting organisations and consumers to turn to technical tools, such as virtual private networks (VPNs) or cloud services, and measures such as firewalls and end-to-end encryption.

Different types of information present varying levels of sensitivity

Not all data are created equal and certain types are inherently more sensitive than others. Considering scope or volume of data collected can help organisations determine what is adequate, relevant and necessary for their business.

Optimising for protection

Leadership understands that protecting data is a challenge that needs to be met. Risks to data carry corresponding threats to economic activity and business reputation. Company policies that prioritise consumer protection and organisational accountability show a slightly greater likelihood to engender consumer trust than do policies aimed purely at regulatory compliance. Meeting customer expectations is a critical competitive consideration and a majority of surveyed executives say that encryption is a core business requirement in the country where they are located.

Education as much as regulation

Regulatory approaches to data protection vary greatly across the world and discrepancies in application can be seen through the different approaches from small and large organisations. One-size-fits-all regulations, typically targeting multinational companies, can burden smaller organisations, which are greater in number and at the heart of most national economies. Soliciting input from a diverse range of affected stakeholders on any new regulation, as well as publicly explaining its goals and any trade-offs, should boost consumer trust, enhance employee awareness and, ultimately, ensure business compliance. Part of data protection is technical; the rest depends on people and their practices.

Introduction

From demographics and health information to credit card details and addresses, consumers today regularly share valuable pieces of their life through the data they exchange with private and public organisations through all kinds of transactions. How these data and the people who provide it are protected is vital to the development of a healthy digital economy.

While data can be used to find new business opportunities and improve public services, data protection is also emerging as a key concern at the individual and organisational levels. Regulations and customer expectations can vary greatly among jurisdictions, leading to a complex environment to leverage data while managing it properly.

As a result, all kinds of organisations are redesigning data strategies to meet demand, especially in light of disruption such as the covid-19 pandemic, which has forced many people to work from home. Many organisations, however, would also benefit from realising the current threat environment, enhancing awareness among all employees, integrating data protection—to meet regulatory and customer expectations—and, in the process, identifying the amount of data actually required.

“A lot of organisations, particularly at the larger end of the spectrum in, terms of global reach but also how many employees they have, are starting to get the sense that data protection is something that they do need to focus on,” says Michelle Price, CEO of AustCyber, an Australian cybersecurity growth network established in 2017 as an independent, not-for-profit institution. Recognition may be the easy

part; what matters more, she highlights, is “whether or not organisations fully understand that within their different strategies and business plans.”

A World Economic Forum study highlights “cyber attacks and data fraud” as the third most pressing concern for business in the current climate; only the structural risks of a prolonged global recession or surging bankruptcies resulting from it rank higher¹.

According to the survey conducted for this report, data protection is considered “very important” to 78% of organisations today, a figure that rises to 82% when respondents are asked to look ahead to three years from now. Respondents in Mexico showed the biggest jump between these periods, rising from 70% to 94%.

Ms Price also envisions data protection becoming more important. “Because of the covid-19 pandemic, more organisations in the next 12 months will become conscious of what they need to do from a business-strategy and business-planning perspective.” One reason is that more companies and public entities are likely to recognise the critical nature of data protection to their value and supply chains. “If they can’t demonstrate how they are protecting data, the integrity of that data, access to that data, and that they are following compliance and audit requirements, then they’re not going to survive in the medium to long term,” says Ms Price. Her indication is that the pandemic will have lasting consequences on business operations and that organisations should consider that recently instituted digital measures will remain fully or partially enacted in the future.

¹ World Economic Forum, COVID-19 Risks Outlook A Preliminary Mapping and Its Implications, May 2020

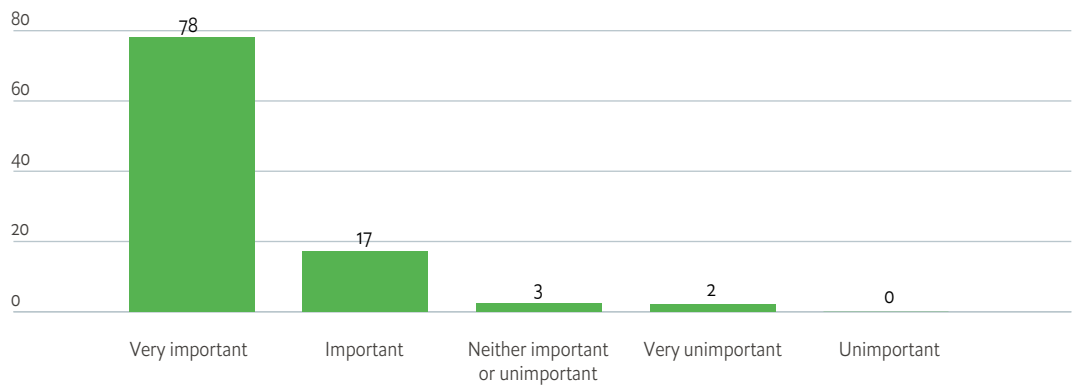


Figure 1: Perceptions on protecting data

How important is the role of data protection in your organisation today?

Data protection today

(%)

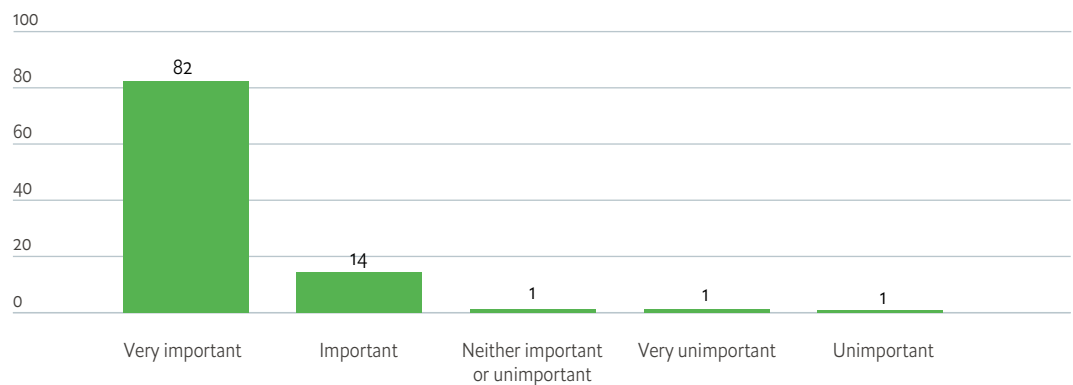


Source: The Economist Intelligence Unit

How important is the role of data protection in your organisation in three years time?

Data protection in three years

(%)



Source: The Economist Intelligence Unit

Different data divisions

There are three stages of data, carrying various types of risk and requiring different needs for protecting it. Some data are more valuable in terms of sensitivity, therefore requiring greater attention from a security perspective.



At rest: information stored on a server, database, in the cloud or on a local device.



In transit: data in motion via email, message systems, internet uploads and downloads, or over mobile networks, including Wi-Fi.



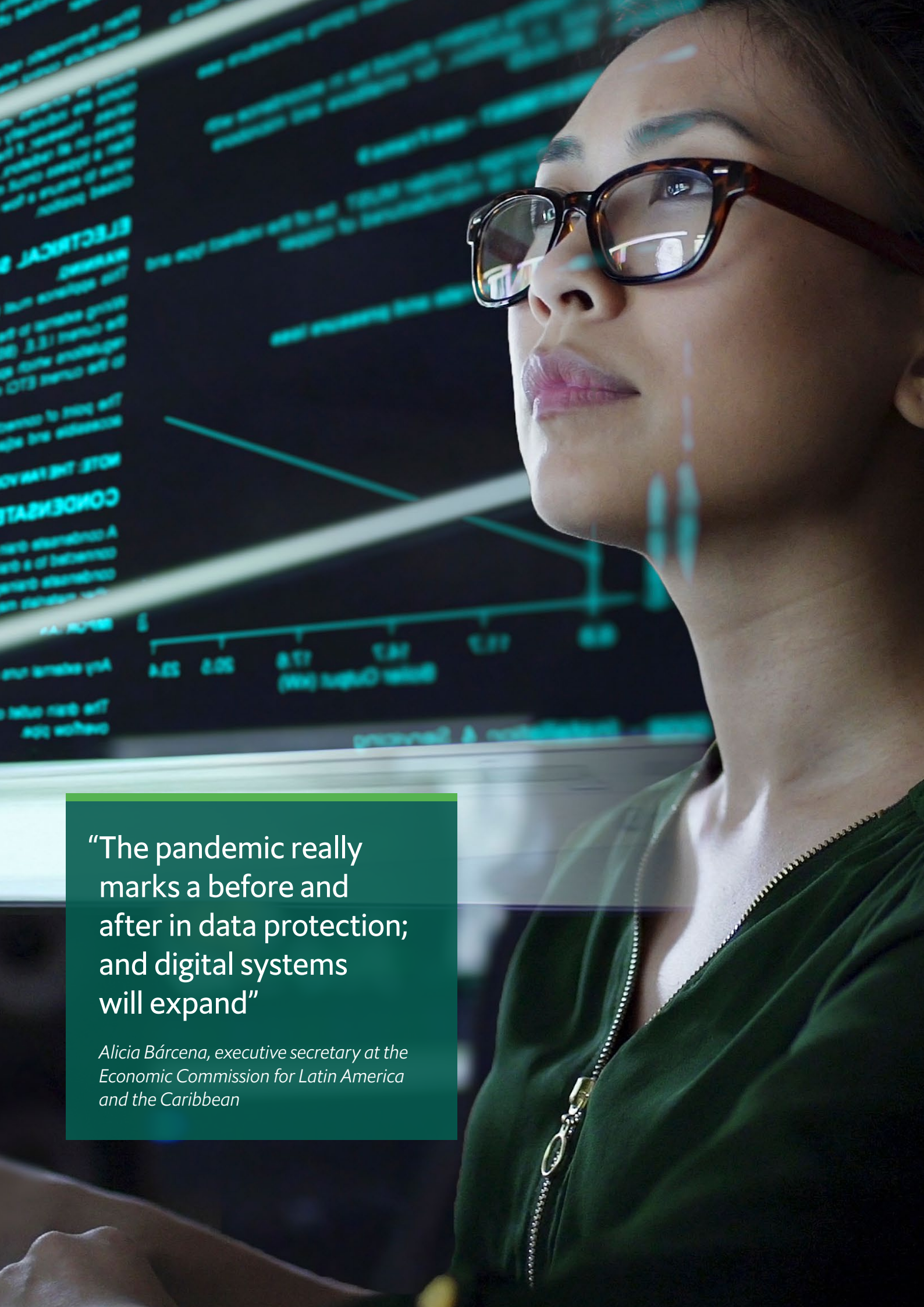
In use: information being used by a computer or mobile device, including office applications, cloud and mobile apps, and databases.

Moving from data to data protection

Broadly, digitisation has emerged as a key tool for organisations to counter business fallout from the pandemic and seize opportunities. “Maintaining many socio-economic activities during covid-19 has depended on the economy being digital; the pandemic has accelerated digitisation even further,” explains Alicia Bárcena, executive secretary at the Economic Commission for Latin America and the Caribbean, which is part of the UN.

“The pandemic really marks a before and after in data protection; and digital systems will

expand,” explains Ms Bárcena. “This requires greater protection of information not only for people, but also for companies in both technological and non-technological sectors as they see the advantages in digital transformation.” Data protection is therefore essential, given rapidly increasing digital adoption, and has hence risen to the top of cybersecurity discussions in the boardroom as well as being recognized more widely as underpinning post-pandemic economic recovery, as the World Economic Forum report mentioned earlier highlights.



“The pandemic really marks a before and after in data protection; and digital systems will expand”

Alicia Bárcena, executive secretary at the Economic Commission for Latin America and the Caribbean

Digital threats as the new normal

The primary reason for concern is that attacks are frequent. About a fifth of survey takers (22%) say these occur daily, with another one in five (20%) noting weekly attacks. INTERPOL, an inter-governmental police group, has also noted a rapid uptick in the number of cyber attacks during the covid-19 pandemic as organisations deploy remote systems and networks to support work-at-home activities and other support channels.² Many organisations have come to realise the importance of securing their data, although the challenge may be greater for small and medium-sized enterprises (see Case study II).

The cost of cyber crime was already steadily increasing pre-pandemic, which has been well documented. What’s less known is that improved cybersecurity can also decrease the cost of doing business and by extension create new revenue opportunities.³

“There is a commercial imperative to have best-in-class data protection,” says Nigel Cory, who is associate director at the Information

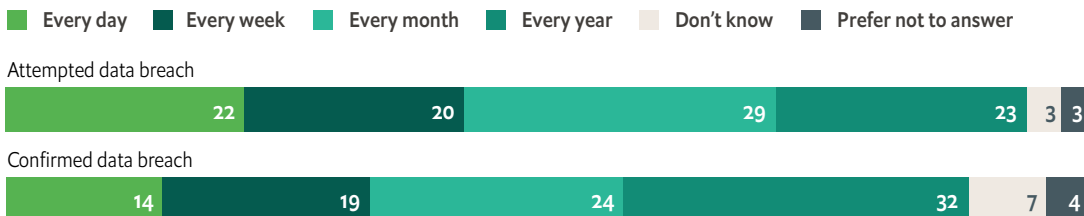
Technology and Innovation Foundation, a Washington, DC, think-tank. “It can serve as the basis to create a competitive advantage.” Globally, 90% of survey respondents would agree with that outlook, agreeing or strongly agreeing with the statement “cybersecurity is a core business requirement in the country where I am located”. The rate edged up slightly in Brazil (94%) and Indonesia (96%).

The most common form of attack is malware (42%), followed by phishing and spear phishing (39%), as well as denial-of-service and distributed denial-of-service attacks (34%), according to survey takers, a finding that aligns with those of INTERPOL—although the forms of attack can also be conflated.

“The starting point is phishing, because they need the phishing to get access,” explains Paul Naismith, CEO of Fred IT Group, Australia’s largest dedicated IT solution provider to the pharmacy industry. “Ransomware attacks have definitely been on the rise, as that business model has been successful,” he adds.

Figure 2. Regular cyber attacks reported

How often does your organisation experience an attempted and confirmed data breach?
(%)



Source: The Economist Intelligence Unit

2 INTERPOL, INTERPOL report shows alarming rate of cyberattacks during COVID-19, <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
3 Accenture, Ninth Annual Cost of Cybercrime Study, <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>

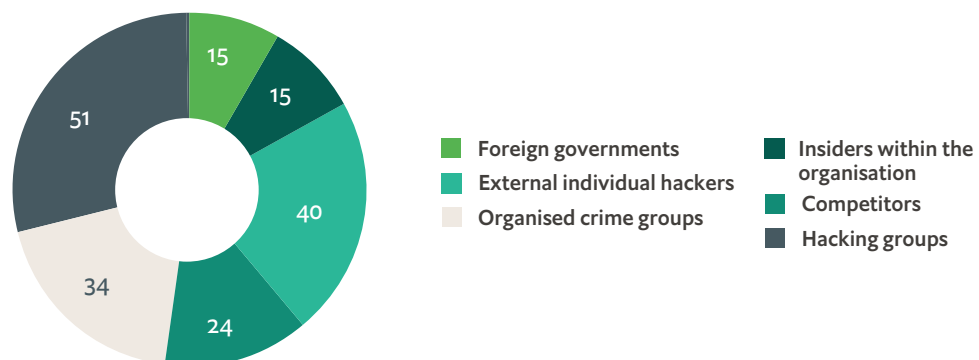
In 2016, a hospital in Los Angeles had to pay a ransom of US\$17,000 to an unknown attacker in Bitcoin, a cryptocurrency, in order to unlock personal data.⁴ “Attackers value health information because they know how personal it is and it’s not like you can change your medical past,” explains Mr Naismith. “So we’ve seen a huge increase in ransomware attacks in all sorts of healthcare, whether it be hospitals or, in my case, pharmacies.” Healthcare is particularly an example of where collecting or holding only personal data that is “adequate, relevant and limited to what’s necessary”⁵ could be a mitigating solution. One of the most sweeping regulatory regimes already in force, the EU’s General Data Protection Regulation (GDPR) embraces the concept. It sets out that data collection should follow safeguards that “ensure that technical and organisational

measures are in place to ensure, in particular, the principle of data minimization.”⁶

In the survey, hacking groups are believed to be the most common form of attacker (cited by 51%), followed by external individual hackers (40%) and organised crime groups (34%). Foreign governments (15%) and insiders within the organisation (15%) are, conversely, seen as the least likely attackers, despite newspaper headlines touting such challenges. Only 6% of respondents in the US cited insiders as a concern. Respondents in Germany and India gave the most diverse set of answers to the question of attack sources—hacking groups were still their top answer but respondents in these countries gave more weight to organised crime or foreign governments than in other countries.

Figure 3. Who is responsible?

Who do you believe are the most common actors behind such attacks? Please select up to two.
(%)



Source: The Economist Intelligence Unit

⁴ LA Times, Hollywood hospital pays \$17,000 in bitcoin to hackers; FBI investigating, <https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html>

⁵ EU GDPR, Article 5 (Principles relating to processing of personal data)

⁶ EU GDPR, Recital 156

The nature of attacks inherently makes tracking their source tricky. “It’s not usual for fraudsters to put a ‘thank you’ to the source of the data when they commit a fraud,” says Andrew Stott, former CIO in the UK Government. “You can sometimes find out [who conducted an attack] but it’s messy and takes a long time. What data an organisation—with which you deal—has stored on you is the easy part; but it’s much harder to find out who that organisation passed data on to and what they are doing with it,” he says, pointing out weak links in the system. Mr Stott predicts that the issue will go up on political and regulatory agendas over the next few years.

From cyber breaches to better data management choices

“Most of the attention in organisations is about confidentiality and the risks of data breach, and showing that you’ve taken reasonable steps against data breach,” says Mr Stott. “There’s less often focus and concern about how data is being used and whether it’s being used for the purposes for which it was collected.” Increasingly, however, organisations are starting to realise the varying value of the data they hold. Research from Grant Thornton, a global professional services company, suggests that 20% of data holds 80% of the risk.⁷

A focused approach on limiting data collection to what is adequate, relevant and necessary and securing what is valuable could be far more efficient in identifying and protecting potentially weak links in data at rest and in motion. This is imperative, given the

notion that cyber attacks are inevitable; especially as adversary actors deploy new methods and tools to gain access to sensitive information. Healthcare is again an example of an industry where the data being handled is often sensitive and where privacy issues were at the forefront even before digitalisation. The Health Insurance Portability and Accountability Act (HIPAA), a US regulation enacted in 1996, allows for fines that range from US\$100 to over US\$4m for any instance of misuse—due to fraud or negligence—including acquisition, access, disclosure or subsequent use of patient data that’s unrelated to normal treatment and administration. The regulation also generally requires encryption for data transmissions.

“We’re seeing variations on attacks in the last short period of time, even in the last 12 months, where it’s a combination of ransom ... but at the same time the new twist is, unfortunately, they’re also talking data out,” says Mr Naismith. “Even if your systems are good enough to be restored, they will ransom you to not release your data onto the web. And it’s that combination that’s very difficult for people to recover from, especially if you’re a healthcare provider and your healthcare data is possibly turning up on a public website.”

Given the amounts of data being collected, it’s clear that the importance of data security is not just in healthcare but in all industries, as evident by newspaper headlines around the world concerning data privacy and data loss. “It’s really become front-and-centre, and that’s only going to increase over the

⁷ Grant Thornton, Locking down the value of data, <https://www.grantthornton.global/en/insights/cybersecurity/value-of-data-hub/>

next three years as there's more and more challenges," adds Mr Naismith. "But to get the benefit of any data, and certainly health data, you've got to get it as close as you can to the point of value. And in this case, that's with the practitioner when they're with the patient."

For sensitive data, many firms are turning to end-to-end encryption, not because of regulatory requirements, but to ensure safe transmission to customers. HIPAA requires encryption, although it doesn't specify a technology or protocol. Online communication and payment platforms increasingly advertise use of an end-to-end

protocol, which blocks third parties from accessing data in transit. Only senders and recipients have a key to decrypt the data.

"There is a clear market demand for highly secure services, which includes encryption," says Mr Cory, who predicts we will see more encryption services in the future as it relates to digital trade. "It is a commonly used tool to use and secure data in order to create competitive advantages." At the same time, he believes more needs to be done to seize the benefits, especially regarding data-governance awareness.



Case study I: A role for secure communication

End-to-end encryption, virtual private networks (VPNs) and secure cloud computing are fundamental keys to data security, especially as people started working remotely during the covid-19 pandemic. “To really get the value out of data, you’ve got to actually get it very close to real-time and very close to the source of value,” says Paul Naismith, CEO at Fred IT Group, Australia’s largest IT solutions provider for pharmacies. “That has been driving a lot of the digitisation in healthcare and that’s a real challenge because the further that data gets away from secure places and gets closer to the consumer to use, the more challenging it is to keep it secure.”

Finding the balance between technology that allows data to be secure and accessible while being easy enough for consumers to use has therefore emerged as the holy grail for organisations, especially those holding sensitive information about people such as the financial services and healthcare industries. “That interface of trying to get the value of data—the health value of data—right to the end-consumer, the patient, on their device in a way that they’re happy with and keeping it secure is the biggest challenge,” explains Mr Naismith.

A starting point

Many governments have responded by creating regulations to secure data in various forms, most notably spearheaded by the EU’s General Data Protection Regulation (GDPR).

“I think there are obviously good practices to reduce the potential impact of data breaches, including encryption, not holding data that you no longer need, fuses on firewalls that notice large amounts of data being exfiltrated, separation of datasets at rest and having separate control regimes for those,” says Andrew Stott, former CIO in the UK Government. “I think that it’s become more visible thanks to the GDPR.”

In the Economist Intelligence Unit survey, 87% of executives also say that encryption is a core business requirement in the country where they are located. A similar number say their organisations limit access to data for cybersecurity reasons by technical and non-technical means.

“There are certain requirements and compliance for us to meet around security,” agrees Mr Naismith about the situation in Australia. “But it doesn’t often extend down to consumer use, and it’s [in] those new areas that we need to make sensible choices if there’s no regulation in place.”

“There is a whole set of relatively new types of attacks that are difficult for organisations to, I think, understand and will tend to blur accountability,” adds Mr Stott. “Supply-chain attacks are becoming more prevalent, and yet something pretty standard in the software and IT services industry is that the supplier doesn’t take any liability.” Indeed, several high-profile cyber breaches over the past decade have involved attacks

on the weakest link in the ecosystem to target the biggest organisations. “The local data-centre storage often has the latest available technology and tools to secure it,” says Mr Naismith. “The biggest challenge is the in-transit data and having end-to-end encryption, regardless of the technology used.”

Suggestions for improvement

“Businesses are reliant on the broader cyber ecosystem,” says Mark Montgomery, executive director at the Cyberspace Solarium Commission (CSC). To fend off attacks, he recommends four solutions. The first is VPNs, which enable users to use public networks to send and receive data as if their devices were connected to a private network. Second is improved cyber hygiene. Examples include two-factor authentication, in which users are identified by two different means, and 16-digit passwords to limit the effect of brute force attacks that can easily break short passwords. Third, is better security among cloud service providers, as it is not ubiquitous throughout the industry. The fourth is enhanced regulations relating to the Internet of Things (IoT), especially during the current pandemic. “Many people work from home and their household devices are vulnerable,” Mr Montgomery says. “There needs to be better basic security levels for these devices, starting with Wi-Fi routers.” In the US, the National Institute of Standards and Technology already provides guidelines, but

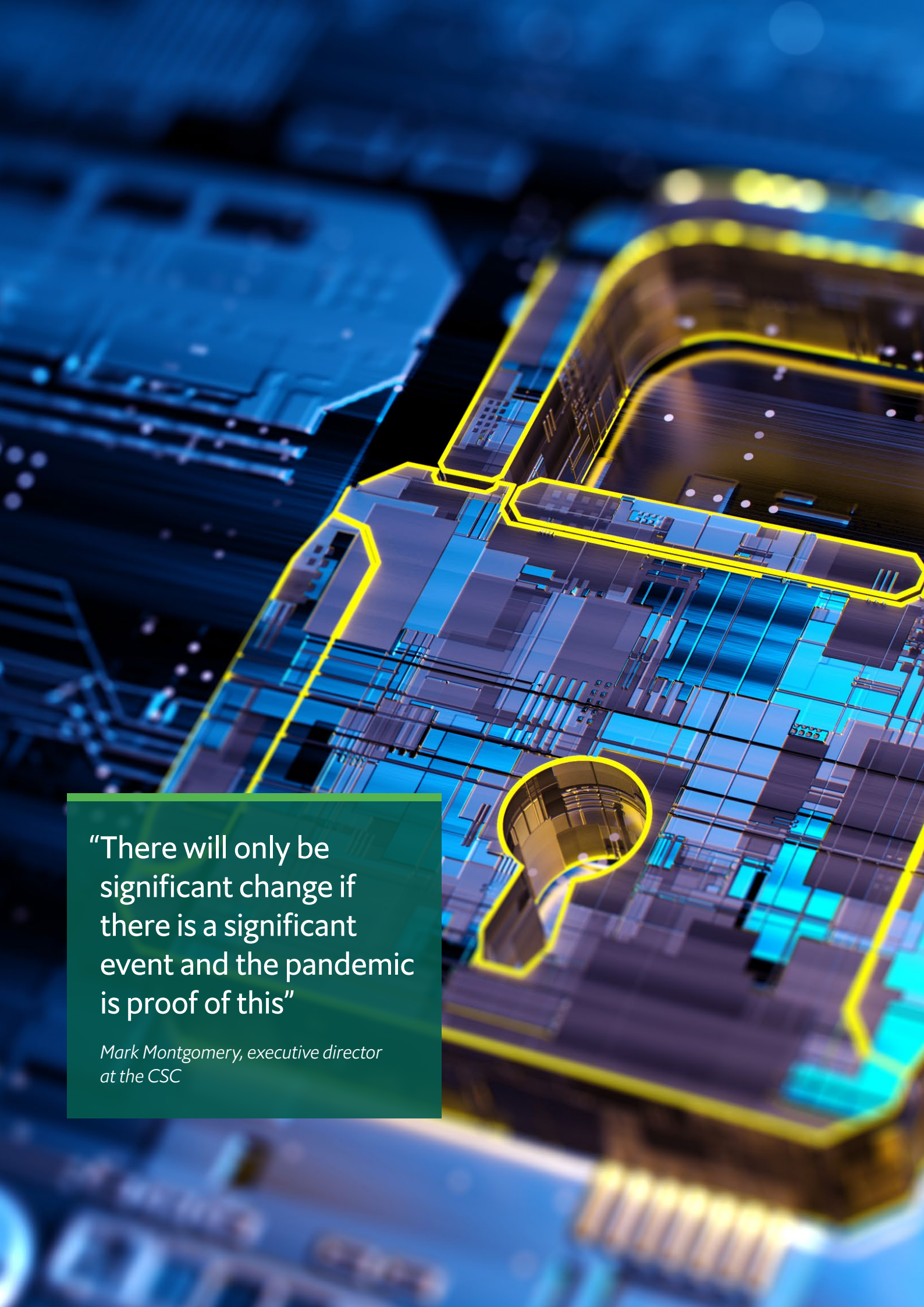
they are simply recommendations and don’t go far enough, according to Mr Montgomery.

In March 2020 the CSC released a report containing 82 recommendations organised into six pillars, which included a number of legislative proposals.⁸ Notably absent from the list is the topic of end-to-end encryption—the Commission couldn’t reach a consensus given the various benefits and challenges, in part relating to the question of enabling access to law enforcement and its potential consequences for unintended uses. Mr Montgomery does, however, believe that the technology has a role to play moving forward. “Encryption is already ubiquitous in the private sector, especially with data at rest.” In 2020, four of the top six messaging apps—ranked by monthly active users—employ end-to-end encryption, representing about 4 billion users globally⁹.

Hence, the biggest obstacle going forward remains the issue of data in motion, meaning how to move it from secure storage to end-devices safely. “It’s that messaging link between the enterprise and the consumer where there’s a huge risk because it’s that transport, once it leaves your secure spot and tries to get down to a consumer’s device, where we lose control,” says Mr Naismith. “We know the consumer doesn’t have all that security, and we know bad actors can actually intercept data and that’s where I think we’ve seen the importance of end-to-end encryption come to light.”

8 SCS, <https://www.solarium.gov/>

9 Statista, Most popular global mobile messenger apps as of October 2020, based on number of monthly active users <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>

A futuristic, glowing blue and yellow architectural rendering of a building with a large question mark in the foreground. The building is composed of various geometric shapes and is illuminated with bright blue and yellow lights. The background is a dark blue, almost black, with some faint, glowing lines and shapes, suggesting a digital or technological environment. The overall aesthetic is high-tech and modern.

“There will only be significant change if there is a significant event and the pandemic is proof of this”

*Mark Montgomery, executive director
at the CSC*

Tracking awareness across the board

The Cyberspace Solarium Commission (CSC) was created in 2019 to “develop a consensus on a strategic approach to defending the US in cyberspace against cyber attacks of significant consequences” and works to reshape the data ecosystem, in part by raising awareness on people, processes and technology standards.

“If we continue the usual debate then we will have improved incrementally,” says Mark Montgomery, executive director at the CSC. “There will only be significant change if there is a significant event and the pandemic is proof of this,” he says—predicting we’ll be more ready for another pandemic 3-5 years from now because of the current crisis. The same should be true for cybersecurity.

According to the survey conducted for this report, awareness has greatly increased with regard to data protection. Roughly nine in ten (91%) say their own understanding has improved in the past three years, with this sentiment proved strongest in Brazil, India and Indonesia.

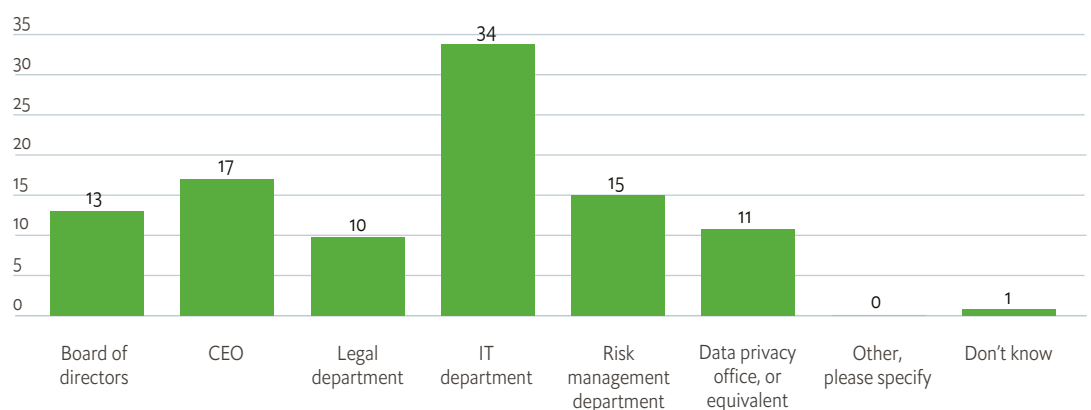
“I think there is an increasing awareness now,” Ms Bárcena agrees. “It’s very important to understand who is in charge of co-ordinating the various initiatives, as many of them are coming from different sectors that have different goals.”

Despite overall increasing awareness, however, some organisations may not be big enough to have their own

Figure 4. How are systems managed?

Who presently designs the data protection systems in your organisation and who manages the company’s data protection systems on an on-going basis?

Manages data protection systems (%)



Source: The Economist Intelligence Unit

internal cybersecurity function and chief cybersecurity officer (see Case study II). “Then you really do need to have a trusted source of expertise,” says Ms Price. “In Australia, we have seen a pretty significant proliferation of managed security services providers to be able to respond to that demand,” a long-standing trend in IT circles. For example, companies used to be reluctant to host their data in the cloud for fear of losing control until they realised that large and specialised providers offered better security than in-house hosting.

The covid-19 pandemic has likely exacerbated this as IT, compliance and risk-management departments work to meet the new challenge of keeping data

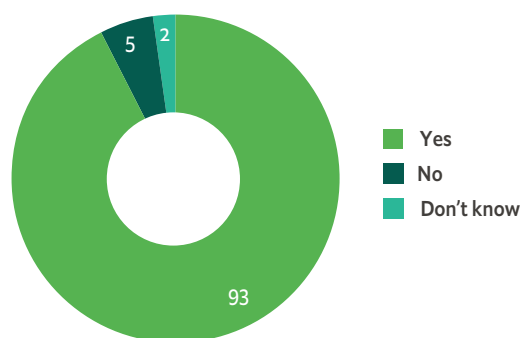
secure as more people work from home and, especially, as the shift coincides with previous trends of bring-your-own-device. Increased awareness has also led senior management to become more active: almost a third of survey respondents say the board of directors or CEO of their organisation are actively involved in managing data protection systems (13% and 17% respectively); respondents in India claimed the highest instance of a hands-on CEO.

“We have always had a concept of privacy without necessarily being compliant, but with the new data protection law under way [The Personal Data Protection Bill, 2019 (PDPB)], CEO awareness and involvement is increasing,” explains Rahul Matthan, a

Figure 5. Keeping tabs on security

Does your organisation track the time and resources in developing, testing and securing data protection software? Select one.

(%)



Source: The Economist Intelligence Unit

10 <https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217>

partner at Trilegal, an India-based law firm. “Europe has a long history of data protection compliance regulation and just had to harmonise it, whereas India is starting from zero, and therefore CEOs need to be hands on.”

It wasn't until 2017 that the Indian Supreme Court held that the Indian Constitution included a fundamental right to privacy and data protection started to garner more attention.¹⁰ “We were a little late to the game,” says Mr Matthan. “But it's increasingly important and awareness levels are becoming very high, especially as Indian corporations are connected to the global economy.”

This reinforces the point that regulations in and of themselves may not be the driver behind corporate profit motives but raise awareness among consumers and high-level executives. “There is more consumer awareness now, as there is a constant stream of discussions about privacy, which didn't exist five to six years ago in every household and that is likely why corporations are responding to this,” says Mr Matthan.

“It's not just a back-room discussion any more, it's a boardroom-level discussion,” explains Mr Naismith about the view from down under. “And once that starts happening, that's because it has a bottom-line impact, and once that happens the investments will be put in and the results will improve.”

Increased awareness leads to a spending boost. Almost all organisations surveyed (93%) report keeping track of time and resources in developing, testing and securing data protection software, including encryption (see Case study I).

“Tracking them is always a bit late,” suggests Mr Naismith. “Protection requires you to actually stay on top of new threats and how they're presenting, and obviously the way we do that is a combination of internal security expertise and partnering with external providers,” he explains, echoing Ms Price's sentiment that there is a growing ecosystem of security firms working together to share intelligence. “It is like a war and it's a cyber war. The changes of the attack vectors are so frequent now that you need tools that can respond and alter in real-time and look for those threats in real-time.”

Case study II: A concern to both David and Goliath

Many regulations are designed for big business, and as a result can have a dramatic impact on smaller or even medium-sized companies, which often lack the budgets or staffing to manage their implications. Small, innovative companies that deal with sensitive personal information can find this issue particularly challenging.

In the Economist Intelligence Unit survey, executives were asked about the primary business challenges their organisations face with data protection regulation. Sorting responses into two groups—those with annual revenue between US\$100m and US\$1bn versus those above US\$1bn—uncovers differences. Limits on data mining on potential customers (24% vs 19%) and burden of compliance with internal policies (27% vs 21%) are particular challenges at smaller companies.

Large entities have established or enhanced corporate processes regarding internal company data policies to a far greater extent (37%) than smaller organisations (27%). The same is true for established or enhanced corporate processes regarding compliance with national data regulations (43% at big firms vs 32% at small ones).

“A lot of organisations, particularly at the larger end of the spectrum in terms of global reach—but also how many employees they have—are starting to get the sense that data protection is something that they need

to focus on,” says Michelle Price, CEO at AustCyber, which has developed tools and resources to track cybersecurity progress across different dimensions.¹¹ “There is, of course, a good chance of organisations even at the big end of town falling short [in this area],” she continues. “But at the smaller end of town, there are some who really don’t have any kind of consciousness about why they should be looking after data in a way that ensures privacy and also security.”

Small and weak links

Despite efforts among large corporations to shore up cybersecurity policies—and by extension data protection—they often rely on smaller entities as part of their value chain. Attackers know this and exploit the weakest link. According to another recent survey, more than 80% of companies have experienced a data breach due to third-party vulnerability.¹²

Survey takers from US\$1bn+ organisations in our study are more likely to agree that encryption is a core business requirement in the country where they are located (90% vs 83% for smaller firms) and that data policy regarding access to data is a core business requirement (93% vs 86%). “You can see a whole set of quite small firms in the supply chain of major organisations, and the small firm doesn’t have the wherewithal to bear the liability,” says Andrew Stott, former CIO in the UK Government.

¹¹ AustCyber: <https://www.austcyber.com/tools-and-resources>


¹² ZDNet, Cybersecurity: Your supply chain is now your weakest link, <https://www.zdnet.com/article/cybersecurity-your-supply-chain-is-now-your-weakest-link/>

“The strategy of many companies is based on the collection of market data and to have information on consumer preferences because that allows businesses to produce goods and services [demanded] by the market,” explains Alicia Bárcena, executive secretary of the Economic Commission for Latin America and the Caribbean. “I think even the small and medium-sized enterprises [SMEs] are starting to understand there is a growing need; and there is an awareness that there’s a need for increasing data protection and regulation.”

The increase in awareness has captured the attention of senior management more among small enterprises (annual revenue of US\$100m to US\$1bn), where 32% of respondents say that the board of directors or the CEO is actively involved in designing data-protection systems; only 26% of large enterprises (over US\$1bn in annual revenue) say the same. Survey takers at small companies are also slightly more likely to say that the board of directors or the CEO is actively involved in managing systems (31% vs 29%).

One reason may be that larger enterprises designate data protection responsibilities throughout operations to a greater extent. “You often see data protection under the CIO’s remit, as opposed to other business units having responsibilities and performance requirements around how they undertake the protection of the data that they’re generating and the data that they hold,” says Ms Price. This trend also seemingly separates smaller and larger enterprises as they tackle organisational structure as part of shoring up their data protection policies.

With the development of new and emerging solutions at competitive costs, the discrepancies between small and large enterprises may diminish over time. “SMEs and consumers have access to ubiquitous encryption services, often for free, but they may not even realise it,” says Nigel Cory, associate director at the Information Technology and Innovation Foundation. “Any firm of any size can take advantage of such data protection and it can be applied across the enterprise.”



“SMEs and consumers have access to ubiquitous encryption services, often for free, but they may not even realise it”

*Nigel Cory, associate director
at the Information Technology
and Innovation Foundation*

Surprising motivations as a driver towards data protection

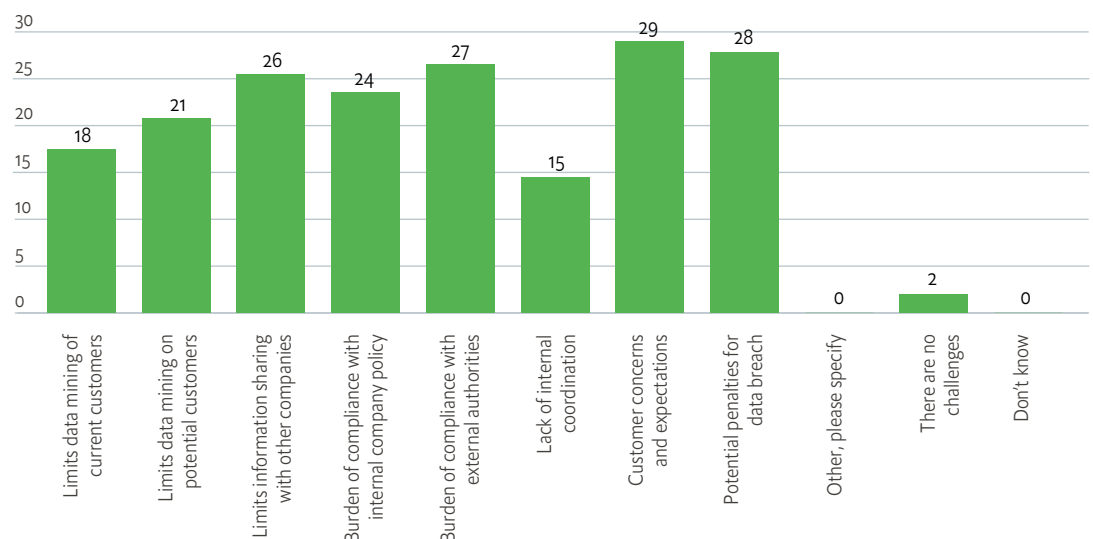
The GDPR has highlighted the issue of data protection, not only in Europe but also globally—and other regions have followed suit, such as the US state of California with its Consumer Privacy Act (see Case study III). “I think those sorts of fines and the publicity that comes with it, and particularly publicity in the financial community, have really raised the profile of data protection in the corporations,” says Mr Stott. “There’s financial penalties, but there’s also when they have to write to each of their customers and offer them credit fraud protection and to make formal public disclosures.”

Customer perception and satisfaction are major motivations for companies. Potential penalties for data breaches (28%) and the burden of compliance with external authorities (27%) rated highly as drivers for data protection in the survey. However, these factors still fell slightly behind customer concerns and expectations (29%), which was broadly true across the countries tested but appeared strongest in Australia and Mexico, whereas regulatory concerns rated slightly higher in the US. Protecting data of current customers, potential customers and meeting their concerns and expectations

Figure 6. Consumer concerns comparatively ahead

In your opinion, what are the primary business challenges with data protection regulation in the country where you are located? Please select up to two.

(%)



Source: The Economist Intelligence Unit

for data protection are the top three aims at organisations globally with minimal variance across markets.

“The starting point is obviously that compliance part is there and it’s growing,” says Mr Naismith. “But really, I think it is the customers really starting to understand the challenges of keeping their data secure, and have probably seen more than they’ve ever seen by those data breach notifications that it is challenging for even the most sophisticated business to keep data secure.”

The trust factor

In order to protect their data, consumers are starting to realise they have to make smart choices about who they do business with. “I think that it’s a growing thing; the customer’s going to drive an understanding of an increase in the demands on the companies they deal with, to secure their data in more and more ways as the risks continue to go up,” says Mr Naismith, whose business uses end-to-end encryption to provide that security (see Case study I). The focus on customer and customer experience is really driving behaviour now,” adds Ms Price.

Consequently, trust in organisations is emerging as an important competitive advantage to build and maintain customer relationships, rather than compliance with external regulations. As a case in point, the Digital Trust Report 2020 from AustCyber highlights the issues relating to remote work and education, as well as supply chains and service delivery.¹³ “It really does play a really big role into whether or not you

are undertaking data protection practices because you have to or because you see that if you can demonstrate that you do it effectively, it will grow your business opportunities or it will embed trust if you’re a public institution,” explains Ms Price.

In a global consumer study from PwC, 85% of respondents agreed with the statement: “I wish there were more companies I could trust with my data;” according to the report: “If consumers haven’t switched businesses yet, it’s not because privacy doesn’t matter. It’s because they feel that they have no choice.”¹⁴ The implication is that trust in a company’s data handling can be a competitive advantage.

The dependency on digital technologies during the pandemic has further highlighted trust issues. “I think there’s more and more examples that consumers are seeing where trusted organisations are struggling or being taken offline for considerable periods of time.” says Mr Naismith. “And I think they can’t ignore that; it’s in their field of vision very much now. And I think consumers are certainly seeing it and are asking the questions about, what are you doing to prevent it?”

Ms Bárcena concurs, adding: “I think the lack of trust is something that we do really need to deal with regarding, of course, the adequate protection of sensitive and private information, especially during the pandemic but also in a post covid-19 world. The authorities should be able to ensure that once the health emergency is over, sensitive information that is no longer needed or critical should be destroyed.”

¹³ AustCyber, Australia’s Digital Trust Report 2020, <https://www.austcyber.com/resource/digitaltrustreport2020>

¹⁴ PwC, Consumer Intelligence Series, Trusted Tech Survey, 2020, <https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/trusted-tech.html>

Case study III: Regulatory approaches

“Any data protection regulation can be a burden [to enterprises] and the question is whether they are reasonable,” says Eduardo Araral, associate professor at the Lee Kuan Yew School of Public Policy in Singapore. He suggests the appropriate answer is a balance between the need for government regulations and industry self-regulation. “The government sometimes doesn’t know what to regulate,” he says. “Because technology moves faster than regulations and governments are always trying to fix problems from yesterday and they don’t want to overregulate too much to stifle innovation.”

Different markets are taking various approaches to data protection, including where government policy making lacks proper consultation with business and those that have open consultations. This can result in a contrast between the regulation created and the challenges that come with it for companies, commerce and, indeed, governments themselves. A global map from DLA Piper, a global law firm, illustrates that they range from “heavy” regulations in the EU (due to the General Data Protection Regulation) to “limited” in large parts of Asia and Africa. In some cases, online protection is non-existent.¹⁵

Mr Araral, who is a principal investigator of the ABCD (AI, blockchain, cloud and data)

programme at the Lee Kuan Yew School of Public Policy, suggests that there is a second-mover advantage with regard to establishing data protection regulations in this area. “Let other jurisdictions make the first move, and learn from their mistakes.” The Singaporean government has often been at the forefront of regulatory sandboxes, which are real-time experiments to test new regulations before approval. In 2016, for example, the city-state famously became the hotbed for approving driverless vehicles.¹⁶

Input needed

There is also a case to be made for bringing in the views of various stakeholders beyond government. “It should be written in regulations that government should consult stakeholders,” says Mr Araral, although he emphasises that the key difference between countries in this regard will also depend on quality, resources and frequency of such a process. “Sometimes it just ticks a box,” laments Mr Araral. “The transparency of the consultation process is important; does the government pay attention and respond to comments?”

Open government data and e-participation initiatives at the national level to support inclusive decision-making with stakeholders have therefore proliferated around the

¹⁵ DLA Piper, Compare data protection laws around the world, <https://www.dlapiperdataprotection.com/>

¹⁶ EDB Singapore, World’s first driverless taxi system comes to Singapore, <https://www.edb.gov.sg/en/news-and-events/insights/innovation/world-s-first-driverless-taxi-system-comes-to-singapore.html>

world. The Open Knowledge Foundation, a non-profit, tracks efforts in this area through its Open Data Index, which includes national laws and draft legislation.¹⁷ Another example is the UN's global E-Government Development Index report, covering all 193 member states.¹⁸

"Governments have to use e-consultation and e-participation to raise awareness about data protection and to update regulation," explains Alicia Bárcena, executive secretary of the Economic Commission for Latin America and the Caribbean (ECLAC). "Access to information is one of the main goals of ECLAC, and we have been not only [been] talking about data governance and data protection strategy, but also how we have to move into open government and open data strategies." To promote such efforts, ECLAC has established an intergovernmental body that will tackle such issues as they relate to the digital economy, as well as relevant stakeholders. This latter category includes the governments themselves, which are in charge of digital strategies, and the private sector that operates in the region's digital sector.

This approach is also evident in India, where a process to implement a new law on data privacy is currently ongoing. After the release of an initial white paper, there were public comments and consultations.¹⁹ Right from the beginning, the process encouraged

everyone to submit suggestions," says Rahul Matthan, a partner at Trilegal, an India-based law firm. "When it goes before parliament, they will invite experts [to comment], which is part of the legislative process."

After the law is passed, Mr Matthan suggests the biggest challenge will be enforcement. "Europe just had to upgrade its enforcement; in India, we have to start from the beginning," he says. The country's Data Protection Authority will have their hands full to ensure that corporations are compliant. "It is only then that we will see development in this area," summarises Mr Matthan.

Corporate response

"I think some of the concern about data sharing for the public good can be tackled by being more transparent about the sharing and about what the benefits are, and about having independent ethics boards considering that," says Andrew Stott, former CIO in the UK Government. "Whereas, at the moment, it tends to be very binary. Either it's in the law or it isn't, and if it's law then it just happens, and no one is really accountable for whether it's worth doing or not."

From a corporate perspective, 89% of survey takers say their organisation tries to have an adaptive approach to data protection ecosystems with regard to current or potential new regulations. The

¹⁷ Global Open Data Index: <https://index.okfn.org/>

¹⁸ UN E-Participation Index: <https://publicadministration.un.org/egovkb/en-us/About/Overview/E-Participation-Index>

¹⁹ Digital India, Data Protection in India, <https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf>

most commonly implemented measures that entities say they deploy in response to regulations include enhanced spending on cybersecurity-related technical measures (40%), established or enhanced corporate processes regarding compliance with national data regulations (39%), and established or enhanced corporate processes regarding internal company data policies (33%).

“Existing laws are always a constraint,” says Mr Araral. “Is Bitcoin a commodity or

currency or something else?” Regulations sometimes offer answers that run contrary to use cases.

In addition, he raises issues of how governments perceive the importance of technologies in terms of innovation, creating jobs and raising revenue as important points of the regulatory equation, in addition to competitive market structures. “Consultations are important because new technologies can disrupt industries in a good or a bad way,” summarises Mr Araral.





“Despite constant and numerous reports highlighting the risks of cyber threats over the past decades, there has been very little progress with regard to cybersecurity”

*Mark Montgomery, executive director,
Cyberspace Solarium Commission*

Conclusion

“When organisations start their digital development journey they often don’t necessarily understand what types of data they hold,” adds Ms Price. “They might think that they only have to protect data when it comes to, for example, customers as opposed to also protecting the data of their employees and the data that they generate in the normal course of their business.” However, she predicts in the future, there will be greater recognition and that public-private partnerships can help to achieve those goals.

“Despite constant and numerous reports highlighting the risks of cyber threats over the past decades, there has been very little progress with regard to cybersecurity,” laments Mr Montgomery. “The risk drivers are increasing exponentially while risk mitigation is only increasing incrementally.” In addition to password enhancements and VPN solutions, Mr Montgomery suggests the possibility of establishing a national cybersecurity authority to certify devices against commonly accepted security standards.

Mr Naismith says investments should increase “right across the chain from the consumer, right up to the practitioner and back-end to government. Because if all those three work together I’m confident that the capability, the need for it—and the people’s understanding of the need for it—will all be improved in three to five years’ time. But I’m pretty confident that we’re starting to see the consumer will drive cyber to be a critical factor, and we’re starting to see it at the boardroom level; this not just a back-room discussion any more.”

Regulatory approaches to data protection vary greatly across the world, as does the approach towards these, with some countries employing high-quality and transparent e-participation consultations with key stakeholders while others have non-existent efforts. But data flows across borders as easily as water or air, and is becoming as vital a resource in both business and government. Discrepancies in data protection are apparent in the different approaches taken by small and large organisations, the latter of which is increasingly dependent on their smaller counterparts to improve in order to secure the value and supply chains of a larger eco-system. A more harmonised approach, across businesses and borders, could be a tide to lift all ships.

To achieve better cybersecurity across the board, organisations are turning to technical tools, such as VPNs, cloud services and end-to-end encryption. But at the end of the day, greater data protection for the benefit of socio-economic progress boils down to its lowest common denominator: people.

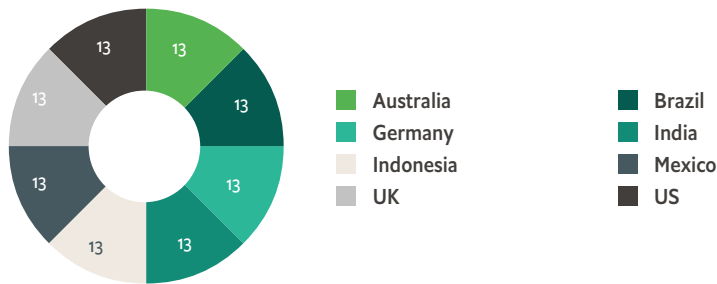
“I think the education of the end-user is really the biggest challenge for all of us,” says Mr Naismith. “If you can educate them and have the best tools and have the expertise in-house with a good backup externally of those skills, you can do a good job to protect the interests in the data you’ve got.”

Key takeaways

- 1. Greater data protection can lead to corporate opportunities:** companies say that customer expectations are more important than external compliance, indicating that there may be competitive advantages to tackling the issue properly. Experts cited in this report also highlight competitive advantages associated with reputations for strong data protection.
- 2. Cyber threats are on the rise:** attacks were already increasing before the pandemic but have reached new levels since as people work from home and use remote digital tools. Companies need to ensure secure communication channels and technologies such as VPNs, firewalls and end-to-end encryption are widely available and often low cost. Companies that fail to use them put both valuable data and trade reputations at risk.
- 3. Data can be different:** some data that organisations hold or share are more sensitive than others. By identifying the most sensitive information, organisations can focus on efficacy in data protection. At the same time, regulations forcing organisations to keep or discard certain data risks being a burden to smaller entities when rules target immaterial data or complex solutions.
- 4. Awareness has increased but more is needed:** top leadership generally understand the challenges ahead but obstacles remain, as people at all levels of the organisation, as well as customers and users, need to be educated on the importance of data protection. As long as there are risks to data, there are corresponding risks to the economic activity associated with it.
- 5. Data protection is akin to bank security:** consumers and citizens share valuable pieces of their life through the data they exchange with private and public organisations—and they expect those transactions to be as secure as money in the bank.

Appendix

Figure 7. In which country are you personally located? Select one.
(%)



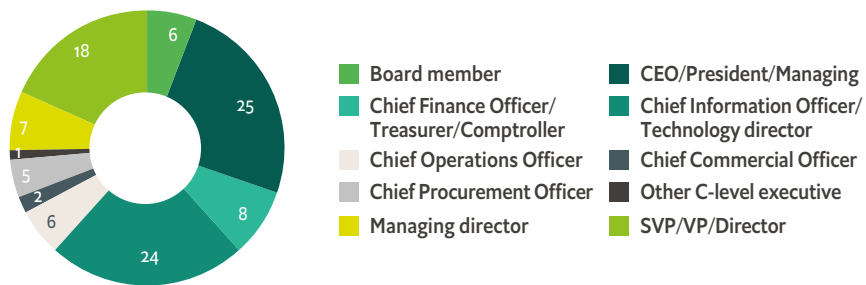
Source: The Economist Intelligence Unit

Figure 8. What are your organisation's global annual revenues in US dollars? Select one.
(%)



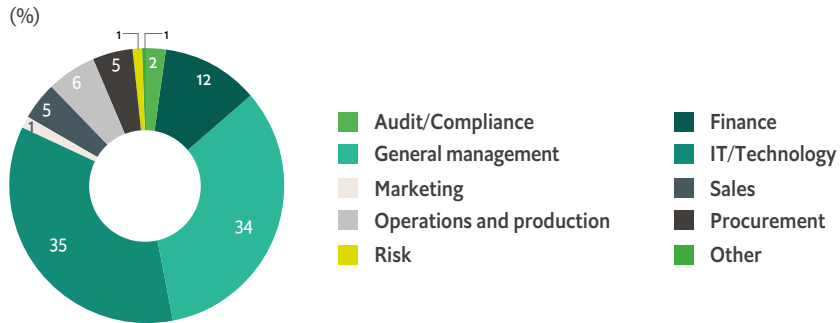
Source: The Economist Intelligence Unit

Figure 9. Which of the following best describes your title? Select one.
(%)



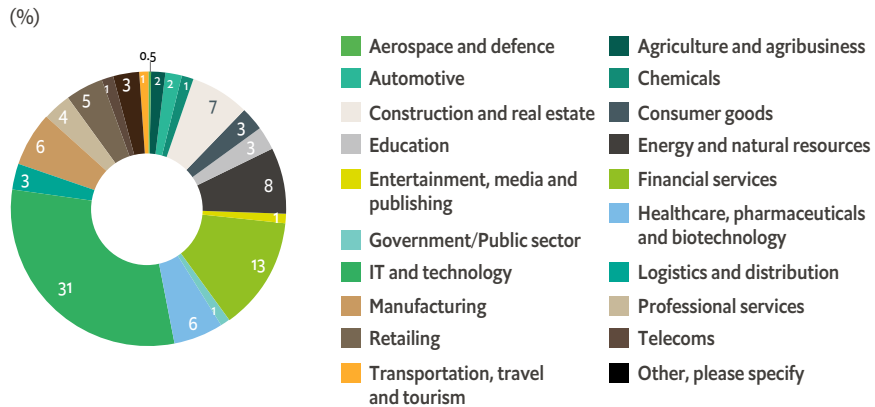
Source: The Economist Intelligence Unit

Figure 10. What is your main functional role? Select one.



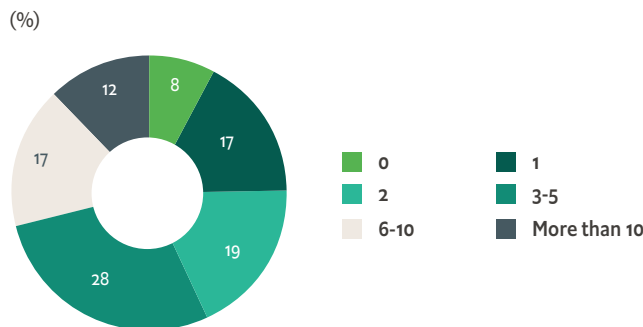
Source: The Economist Intelligence Unit

Figure 11. What is your primary industry? Select one.



Source: The Economist Intelligence Unit

Figure 12. How many countries does your organisation have operations in other than its home country? Select one.



Source: The Economist Intelligence Unit

While every effort has been taken to verify the accuracy of this information, The Economist Intelligence Unit Ltd. cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report. The findings and views expressed in the report do not necessarily reflect the views of the sponsor.

