Cyber security

Is your safety net strong enough?

mazars

Contents

Foreword

Cyber security: a delicate balancing act

Cyber threats are all around us. This is not paranoia, it's an unfortunate reality: every day brings new hacks, new data leaks, new embarrassment -and new costs, both financial and commercial. Nobody is spared. The attacks target companies large and small, as well as public-sector institutions and individuals. Collectively, we are getting better at preventing and detecting cyber break-ins and limiting their damage, thanks in part to technological solutions, but also because of greater awareness of the dangers of phishing and other classic hacking techniques. Yet no system is fool proof. The technological advances that can protect us also provide cyber criminals with more advanced tools including artificial intelligence that can keep them several steps ahead of the organisations they target.

Given that context, this report takes as its starting point the inevitability of being attacked. Cyber security is no longer a question of if, but when. That may amount to a mindset shift for many business leaders, but we believe it's an important one to make. In our view, cold-eyed realism is the best cyber defence strategy, as it will inform each of the five key operational aspects that need to be in place to safeguard company data. These five pillars are: identification, prevention, detection, response and recovery.

A litmus test for organisational resilience

A survey we conducted of more than 1,000 executives worldwide last December for our annual C-suite barometer emphasised how cyber security is now a major preoccupation among corporate leaders. More than half of the respondents told us that cyber risks have increased in the past year, and more than one-third are bracing for data breaches in the next 12 months. Yet the same survey showed that top management has a level of confidence in their own company's ability to withstand attacks that may seem surprising, perhaps even paradoxical. Do they know something their own IT departments don't? Probably not. Yet these findings suggest that cyber security has now become a delicate balancing act for many businesses, akin to a tightrope walk: yes, it's perilous, but the important thing is to build a strong safety net that can cushion any eventual fall.

Many tools that can help identify, prevent and detect cyber breaches are now readily available. CEOs can put numbers for board updates around spending as well as examples that illustrate their purported readiness. Response and recovery after an attack are much harder, given that every breach can be different. Yet how a company or a public-sector institution reacts to cyberattacks is an essential test of strategy and leadership. Waiting until a crisis hits before crafting an effective response plan is like trying to hang the safety net as you stumble. And the ability of an organisation to bounce back from a cyber meltdown can be hard to gauge before it is tested in real life.

In that sense, cyber security is a revealing indicator of organisational health. If the skills you need to deal with cyber threats are not isolated to the IT or communications teams but permeate your whole organisation—and if your response to a breach is well planned and well executed—the likelihood is that you are healthier and more resilient as a whole. Finding your feet and keeping your balance in cyber security makes for good business overall.

Robert Kastenschmidt
Partner and Head of Consulting, Mazars

Executive summary

Business leaders everywhere are bracing for cyberattacks but remain confident they can withstand them.

More than half of business leaders surveyed in our annual C-suite barometer see an increase in cyber threats over the past year, and 35 percent expect a significant data breach in their own company in the coming year. The concern is global, although most pronounced in large companies with more than $1 billion in annual revenue. Nonetheless, most companies seem confident of their ability to cope with attacks: globally, 68% of business leaders see their company's data as being "completely protected." In the United States, that figure rises as high as 80%.

Financial losses are the biggest perceived risk.

More than half of the business leaders we surveyed put financial losses at the top of the list of the biggest data protection risks, followed by compliance risk, (44%). Just one third cited concerns about reputation and business continuity. The levels of concern and confidence range from industry to industry, with finance, technology and consumer businesses the most confident—potentially because they are the most exposed given their handling of often-sensitive consumer data.

Cyber security goes far beyond compliance. Crisis scenarios need to be tested, retested and continuously improved.

Effective cyber defence rests on five pillars: identification, prevention, detection, response and recovery.

Each has an important technological component, but equally each has a critical human component. Knowing your own system vulnerabilities and being able to detect unusual patterns is a starting point for both prevention and detection. Tech solutions can include segmentation of computer networks to put extra layers of security around the most sensitive data and extensive offline backups, but everyone from top management to part-time staff needs to undergo frequent training and reminders of the risks. A detailed and well-tested communications plan is essential for an effective response, both for internal use and to reach out to customers, suppliers, regulators and anyone in your data ecosystem. Business continuity plans need to have been painstakingly elaborated and extensively tested so they can be adopted seamlessly by the entire organisation.

Shifting mindsets to prepare for the worst is the best defence.

Cyber security is a fast-evolving field, with attackers now heavily armed (including with AI) and often two steps ahead of the organisations in their sights. Technological vigilance combined with ongoing education efforts and permanent war-gaming of scenarios can ward off some of the trouble. Regulation is growing; increasingly, companies in many sectors have an obligation to report on their cyber readiness—and notify about breaches. But cyber security goes far beyond compliance. Crisis scenarios need to be tested, retested and continuously improved. Accepting that data breaches will happen and having robust plans for handling them provides the best assurance that the response will be swift, recovery effective and the costs limited.

Chapter 1

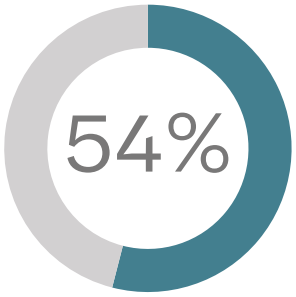
Getting real about rising cyber risk

Business leaders are worried about growing cyber threats, with more than one in three bracing for a significant attack in the next 12 months.

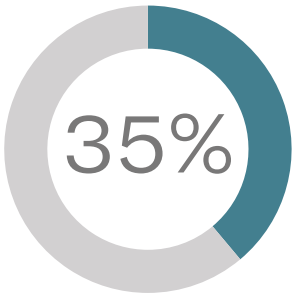
Getting real about rising cyber risk

Cyber threats are real, dangerous and becoming more acute. That realisation is now widespread among business leaders. Our C-suite barometer showed that more than half of the respondents believe cyber threats to their organisations have increased over the past twelve months—and 35 percent expect a significant data breach over the next year.

These overall numbers mask significant differences by company size and location. Large companies with more than $1 billion in annual revenue are the most worried: two-thirds of them see rising threats, compared to just under half of companies in the $1 million to $100 million range. And the risk awareness is highest in both the United States and Europe, with more than 60% seeing rising dangers.



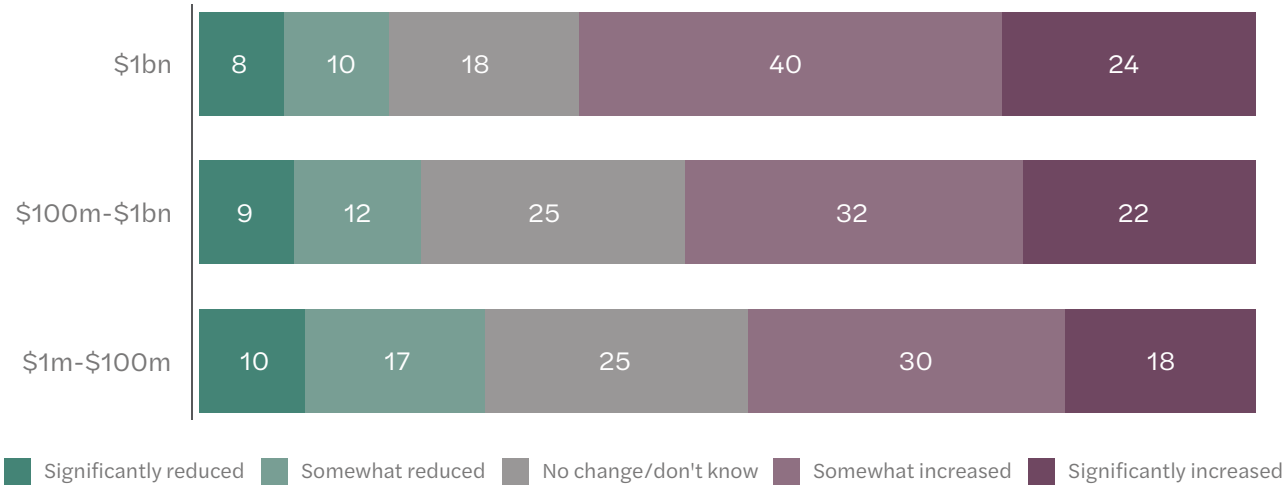
Over half of respondents believe the cyber security risk to their organisation has increased over the past 12 months.



More than a third think a significant data breach in the next 12 months is likely.

Change in cyber security risk

Percent of respondents by revenue band



Q: How has the cyber security risk to your organisation changed over the past 12 months?
$1m-100m, n=432; $100m-$1bn, n=350; $1bn+, n=348

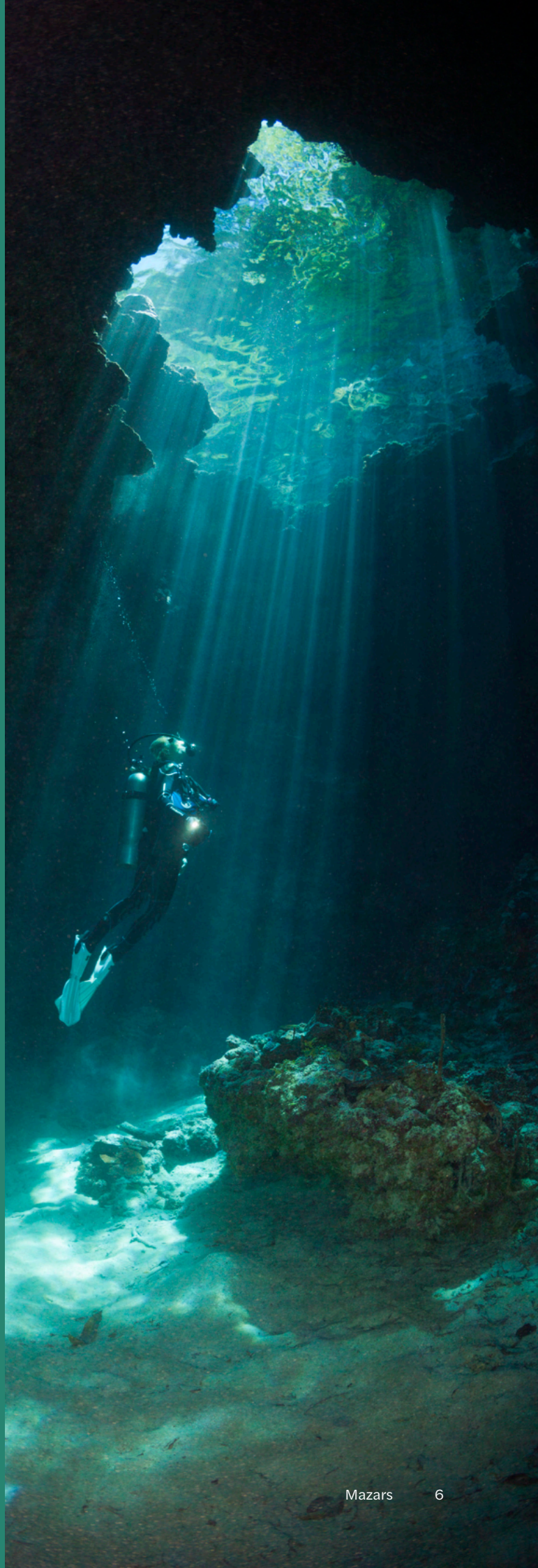
Getting real about rising cyber risk
Small companies, big threats

Just because you are a small company doesn't mean your risks of cyberattacks are less important than they are for big companies. That's not how cyber threats work. The criminals who attack your IT system don't discriminate—they probe everyone for vulnerabilities, regardless of size. And in some ways, small businesses are more at risk. They tend to have fewer staff with cyber security capabilities to help protect their systems. And they may lack the rigorous internal controls to identify and detect threats that many larger organisations have in place.

The nature of the destabilisation can be different for smaller companies, however. Ransomware attacks—which lock users out of a system until money is paid—tend to focus on larger corporations or institutions, including in the public sector. Likewise, denial of service (DoS) attacks, which flood targets with traffic or trigger a crash with an information overload, tend to be aimed at bigger players. Nonetheless, classic phishing and CEO fraud, or "whale phishing," which consists of a hacker impersonating a senior executive in the hope of persuading an employee or contractor to divulge valuable information via email, are common to all companies, small and large.

In some ways, small businesses are more at risk, as they have fewer staff with cyber security capabilities and may lack the internal controls to identify and detect threats.

Digital technologies, and especially digital platforms such as those operated by Amazon, Facebook and others, have enabled small companies to extend their reach around the world. These platforms can provide stronger cyber protection for firms on their platforms than many companies can manage to put in place on their own. But they certainly don't guarantee immunity. For all companies, the most vulnerable IT you have is the system you use to connect to the outside world. And in a world that revolves around relevance, timeliness to market, and innovation, small companies need to strike a difficult balance: how to upgrade and change their IT systems to keep pace with marketing requirements without needlessly creating new vulnerabilities.



Getting real about rising cyber risk
Small companies, big threats

What, then, can smaller companies do to protect themselves given their size constraints? Their possibilities are intrinsically more limited, because small businesses have fewer resources than large ones, both in terms of money and cyber expertise. That makes it paramount for smaller firms to focus on the strongest but also the simplest possible measures. Three stand out:

First, be old-fashioned: make a very good backup of your data with an air gap. In other words, store a full copy of your key data offline, somewhere safe, so that you can retrieve it in the case of a debilitating attack.

Second, segment data into sub-sectors to prevent one intrusion into your system contaminating all your data. Segmentation is not an expensive IT system fix, but it's a strong one—and highly relevant for small businesses.

Finally, stay informed and adaptable. Some small companies think they can put a cyber security system in place and then stop worrying. That's a misguided approach: all companies need to stay alert. Organising communications with IT providers and stakeholders when you or they have an incident is a must. And it's essential to stay informed about new cyber threats and risks.

In the world of cyber security, it's not impossible to protect yourself if you're small. But it takes a lot of careful footwork.

Jan Matto
Partner, Mazars

Chapter 2

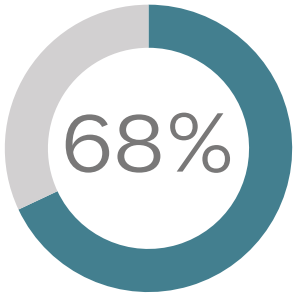
Bring it on: gauging readiness for cyber security

Despite their concern about cyber risks, most companies express confidence about their ability to protect themselves in the event of an attack.

Gauging readiness for cyber security

For C-suite executives worldwide, cyber risk largely translates into fear of financial risk. More than half of the business leaders we surveyed put financial losses at the top of the list of the biggest data protection risks, followed by compliance risk, (44%). Just one third cited concerns about reputation and business continuity.

At the same time, confidence about being able to withstand cyberattacks is high, with more than two-thirds of business leaders — 68% — telling us that they feel their organisation's data is "completely protected." A geographical cut of the survey results shows that confidence is highest in the United States, where 80% of respondents feel their data is completely protected.



Over two-thirds are confident their data is completely protected. A further 29% say their data is partially protected.

Biggest cyber security and data protection risks

Percent of respondents

Q: Which TWO of the following are the BIGGEST risks to your organisation regarding cyber security and data protection?
Total, n=1130

Gauging readiness for cyber security
Keeping the lights on: public-sector cyber readiness

The cyber dangers that lurk in the shadows for private-sector companies are no less of a threat to national and local government and other public sector organisations—and in some ways more so. The data these organisations hold is often intensely private and confidential, ranging from social security details and tax filings to education information and health and criminal justice records. In extreme cases, national security can be compromised, if key infrastructure such as power stations or even defence installations are attacked. Put bluntly, when it comes to public-sector risks, you are only ever one major incident away from knocking out the lights.

Highly publicised cyber breaches in local or national organisations in many countries in recent years have raised awareness about the risks that public-sector institutions face. One particular challenge is "ransomware"— a type of malware that encrypts files on a device or network, rendering them unusable. The perpetrators then demand ransom in exchange for decryption, often threatening to sell or leak data or authentication information if the ransom is not paid. To pay or not to pay is an impossible juggling act for the affected organisation: how would the public react to the idea of rewarding criminals with taxpayers' money?

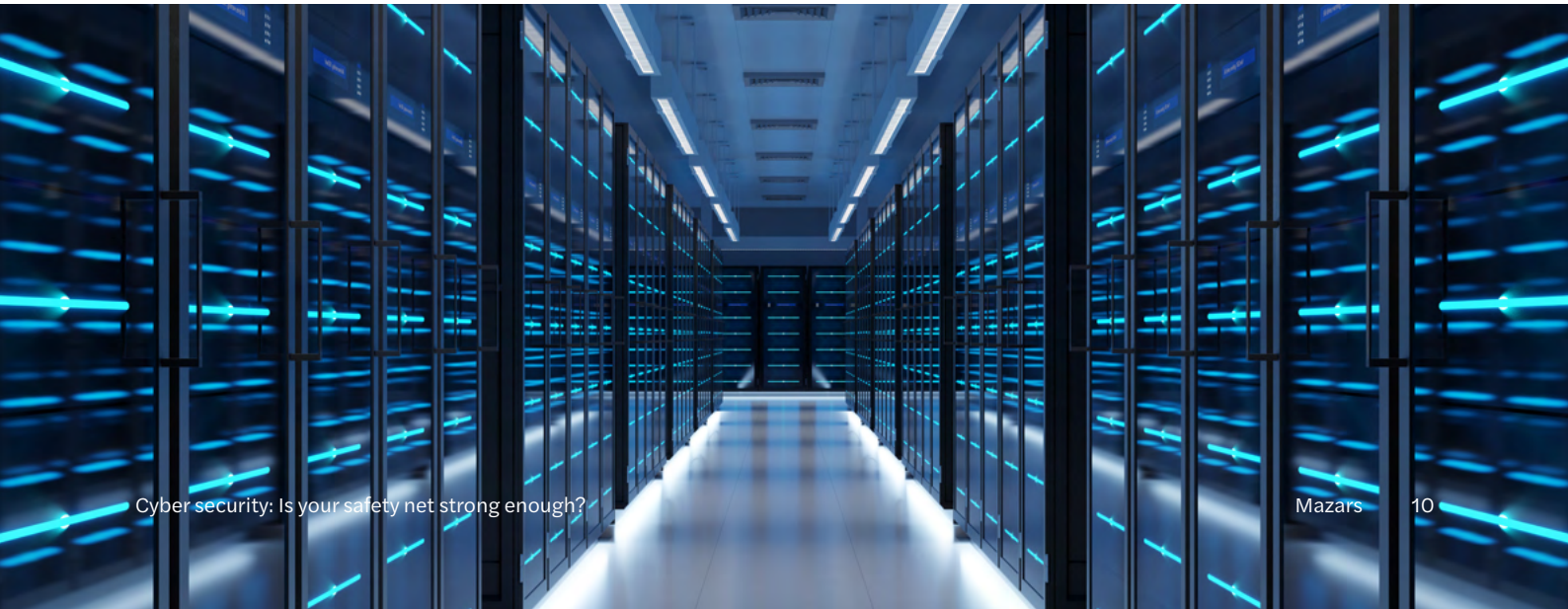
To defend themselves, public-sector organisations need to strengthen the same five pillars that the private sector also needs to shore up, namely identification, detection, prevention, response and recovery. Yet the public sector faces some particular challenges in doing so.

First, the systems themselves can be highly vulnerable. For many public-sector organisations, IT systems are a patchwork of old and new, and legacy systems are the most vulnerable to ransomware and other attacks. At the same time, these organisations tend not to have the funding to upgrade everything to the most recent technology.

A second disadvantage is that even those public-sector organisations most conscious of the risks and seeking to build stronger defences can have a hard time recruiting the cyber experts they need to put their aspirations into practice. Cyber specialists have a hefty market value everywhere, often well beyond the reach of public budgets. And even if an organisation does recruit or train competent people, they are often poached.

Much can and is being done with careful use of resources. National cyber organisations share best practice and more. In the United Kingdom, for example, the National Cyber Security Centre provides "exercise-in-a-box" cyber security toolkits and many other resources to help public-sector organisations prepare. Senior civil service management is now acutely aware of cyber risk, and doing more to assess vulnerabilities, test systems, and bring in external help where useful to improve defences. Awareness training for all staff has moved into a higher gear. In some countries, instant response planning is far advanced, and disaster recovery and business continuity plans are in place—at least on paper. Yet as the ongoing cyber breaches on public institutions worldwide continue to demonstrate, enough is never enough. Keeping those lights on remains a question of nonstop heightened vigilance, more resources, more training—and never-ending cycles of testing.

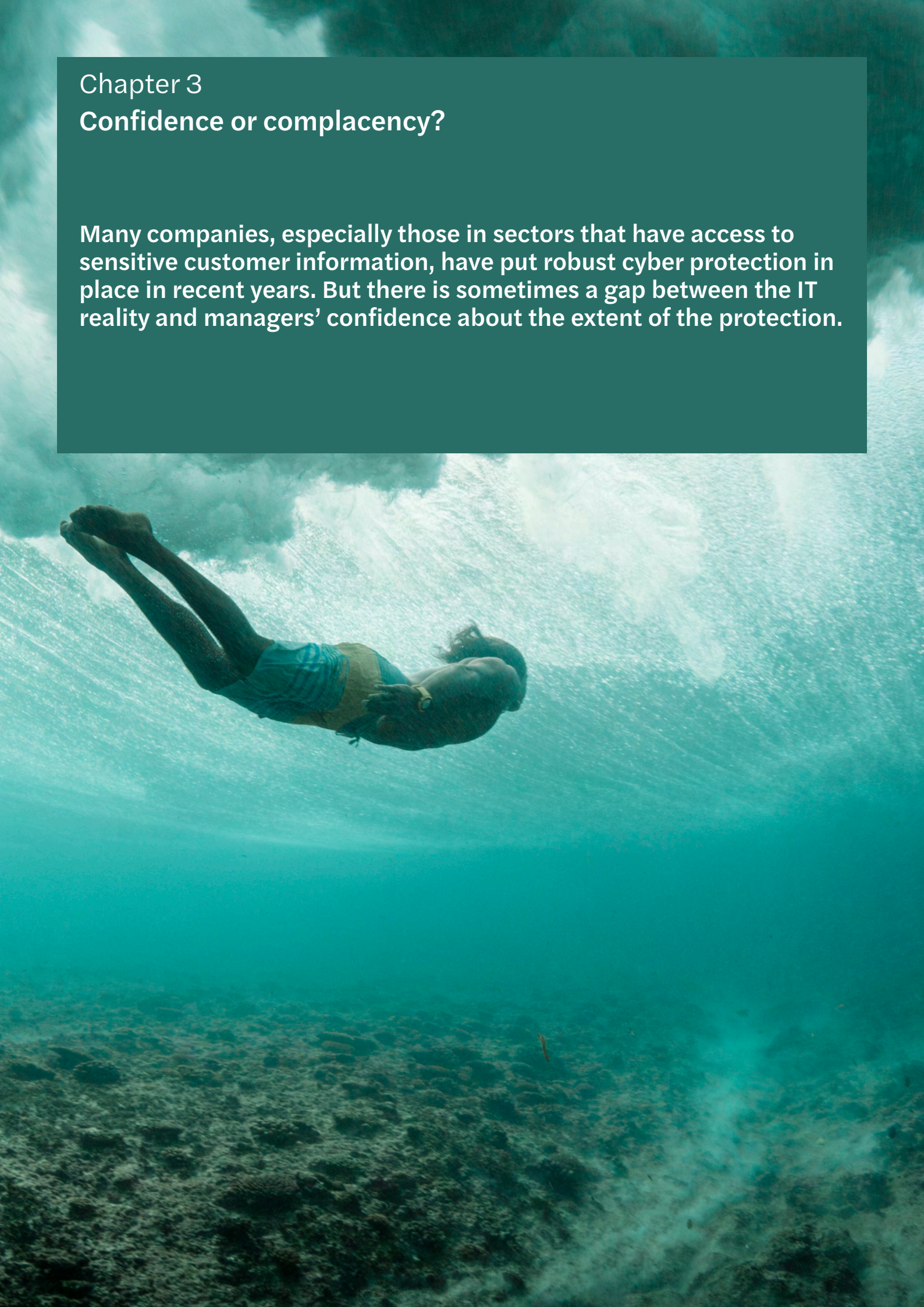
Anton Yunussov
Cyber security expert, Mazars



Chapter 3

Confidence or complacency?

Many companies, especially those in sectors that have access to sensitive customer information, have put robust cyber protection in place in recent years. But there is sometimes a gap between the IT reality and managers' confidence about the extent of the protection.



Confidence or complacency?

How to explain the apparent disconnect in the C-suite between the rising fear of cyber threats and the seemingly solid confidence among business leaders that their companies are well protected? We noticed a similar disconnect in a survey about data that we conducted last year: four in every five executives in charge of data governance said their company was more data mature than their competitors. At the same time, many of those companies simply didn't meet the best practices underpinning data maturity, particularly regarding data quality, an essential ingredient for digital prowess.

The day-to-day reality in IT departments is becoming ever more complex and fraught with risk.

It is possible that a parallel universe is taking shape in companies: while top managers make governance plans in the belief that they can or have achieved a high level of security compliance, the day-to-day reality in IT departments is becoming ever more complex and fraught with risk. Technology and the Covid-19 pandemic help explain the latter state of affairs: if the office mantra back in 2019 was "bring your own device," today—in part because of the trend of working from home—that has changed to "bring your own cloud."

At the same time, a growing number of companies—especially in the most exposed sectors such as banking and retail—have accumulated a deep understanding of both the risks and the organisation-wide response and recovery strategies that are needed to deal effectively with cyber threats. To that extent, best practices are emerging that inform the takeaways of this report.

Confidence or complacency?
Retailers: careful confidence after years of experience

"When you handle private data from clients including credit card numbers you have to be pretty sure about yourself. And retailers are taking cyber security really seriously—they have been doing so for years. That is why they seem confident.

Cyber risk in retail increased during the pandemic because there was such a big surge in e-commerce. At the same time, the importance and intensity of the care retailers take with data also increased. All big retailers now have cyber security specialists in-house and their investment in security accelerated in the past two to three years. So, even as the risks increase, the way they deal with them has improved.

What's important is having a comprehensive plan. It's always a shock when you are attacked, but it should not be something that paralyses you, because you prepared for it.

You need to be ready not just from a tech perspective. You need a Plan B for business continuity. And you need a great communications plan, especially if client data is compromised, since that can jeopardise your image. If it ever happens, you need the right words. You need to be as transparent as possible.

That's true for the sector as a whole, but there are differences. Sometimes it's a matter of scale, and sometimes a question of generation. If you're a digital native, all your systems have been built to be secure, and can scale securely. It's quite different if you are a classic retailer and need to enter the digital world.

My takeaway is that you can never tell, so get ready. This is a sector at risk all the time."

Isabelle Massa
Partner, Mazars

Chapter 4

Not if, but when: five pillars of defence

A robust defence against cyber attacks depends on your ability to identify, prevent, and then detect attacks. Post-attack response and recovery need to be carefully planned and extensively tested.

Not if, but when
Five pillars of defence

Smart defence against cyber threats has five pillars: identification, prevention, detection, response and recovery. Each of these pillars contributes to the overall balance of a company's cyber security, helping them manage risk by organising information, enabling risk management decisions, addressing threats, learning from previous activities—and getting more resilient as a result. Each of the pillars has an important technological component, but equally each has a critical human component. The IT tech reality and the human factors go hand-in-hand. Both require patience, training, investment and extensive testing.

Pillar 1: Identification

Develop the organisational understanding that will enable you to manage the cyber security risks to systems, assets, data and capabilities.

A critical first step for a company is to know yourself. Much of the heavy lifting here needs to be done by the IT team: identifying and mapping all the sources of data, the degree of sensitivity around these data, and all the potential system vulnerabilities that could expose them. The internal map is just a start: it needs to be complemented by a detailed understanding of external sources of potential contagion, from vendors and other stakeholders throughout the entire supply chain.

Beyond having the appropriate IT infrastructure, the mapping will require human expertise. Do you have the right people in your IT team to carry it out? And what sort of information about daily risks and threats should be transmitted to management? These are the core questions that every company needs to answer.

Pillar 2: Prevention

Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

Multiple technical solutions are readily available to help protect IT systems and ensure they keep working normally even in the face of attacks. These solutions can include segmentation strategies which consist of dividing computer networks into sub-sections to prevent system contagion. The most important data can be ring-fenced as part of a segmentation strategy.

Raising human awareness of the daily risks is a no less essential aspect that can be achieved through education programmes and regular "phishing" and other in-house testing. Multi-factor authentication for users is a valuable tool that enables companies to double-down on user fraud and, at the same time, improve employee cyber hygiene.

Not if, but when
Five pillars of defence

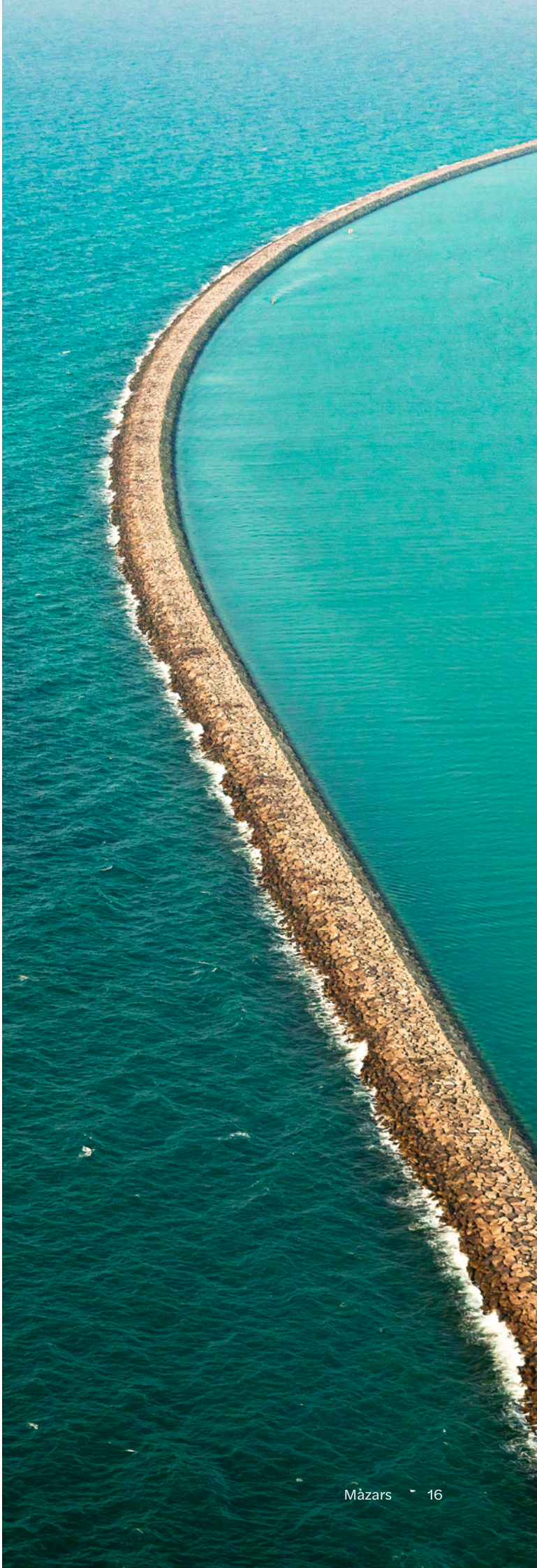
Pillar 3: Detection

Develop and implement appropriate activities to identify when a cybersecurity breach has occurred.

Cyber security audits can provide useful external perspectives on the effectiveness of system safeguards. Imperatives include understanding your company's potential exposure, having the tools to monitor network activity; and being able to detect abnormalities in real time and escalate where needed.

It requires more than IT staff to be involved in these efforts: well-trained managers at all levels are needed, to be able to spot issues and know whom to alert.

Cyber security audits can provide useful external perspectives on the effectiveness of system safeguards.



Not if, but when
Five pillars of defence

Pillar 4: Response

Develop and implement appropriate actions in the event of a detected cyber security breach.

Once an intrusion is detected, the technical response to isolate and neutralise it needs to be extremely rapid. An effective segmentation strategy will limit the damage by protecting the most essential data from contamination. Already at this first stage, understanding which data and systems have been compromised is an imperative that will inform the next steps.

Staunching the IT damage is inevitably the initial focus, but many other steps need to follow—in quick, and carefully planned, succession. Communication is key: business leaders need to reach out to management and staff, to clients, to suppliers and others in their data ecosystem, and—increasingly—to regulators. Indeed, rapidly evolving regulation on both sides of the Atlantic is requiring companies in a range of sectors not just to report cyber breaches but to show the extent of their cyber safety net and allow it to be tested. Given the way networks lie at the heart of our increasingly digital economy, that's not surprising: one cyber breach is never an isolated event but can quickly spread to others. Nobody flies solo in the digital world: a single trapeze artist who loses his or her grip can knock everyone on the team off balance.

Pillar 5: Recovery

Develop and implement the appropriate actions that can allow a return to normal after a cyber security breach.

In some ways, recovery is the hardest to plan and test in advance, since so much depends on the extent of the cyber breach and the damage it causes, to data, to customers and to reputations. Yet it is arguably also the most important: being able to resume business as usual is mission critical. Here too, technology offers some solutions. These include offline backup systems that can be quickly activated to restore normal IT functioning. Many other parts of a business need to coalesce around a tried and tested recovery plan. Business continuity is the watchword: what will it take to regain your balance on the high wire if a cyberattack temporarily knocks you off it? Business continuity plans will differ from sector to sector and company to company—and they can only function well if they have been carefully tested and retested well in advance, not just from a systems perspective but also from a human one. Managers will need to be able to switch to Plan B without so much as a hiccup. And increasingly, regulators are demanding that you prove you can survive cyberattacks and keep operating.

Cyber security regulation: a rapidly evolving field

Cyber security is not just a company-by-company issue. Increasingly it is subject to regulation, both national and international, covering issues that range from risk management to mandatory reporting of cyber incidents. As cyber risks grow, that regulation is evolving. Below we explore the key new pieces of legislation on both sides of the Atlantic.

EU: NIS2 Directive

The EU's first Network and Information Security (NIS) Directive was adopted in 2016. It focused on strengthening national cybersecurity capabilities, establishing cross-border collaboration, and putting in place national supervision of cybersecurity in critical sectors such as energy, transport, water, health, digital infrastructure and the financial sector. In 2021, the European Commission proposed replacing it with an updated version aimed at responding to growing threats. NIS2 addresses the security of supply chains and seeks to streamline reporting obligations and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU.

EU: Digital Operational Resilience Act (DORA)

This new regulation, which takes effect in EU member states in 2022, amounts to a detailed and comprehensive framework for banks and other financial institutions aimed at improving their cyber security. Critically, it also covers risk management of the ICT service providers with whom these financial institutions work. These vendors will be included in DORA's remit, as will both large and small financial firms. The wide-ranging regulation covers alternative investment firms, crypto-asset service providers, crowdfunding service providers and other entities that may not have been previously covered by financial-market regulation, alongside more traditional firms such as credit institutions, payment institutions and electronic money institutions. As a result, it will mean a heightened role for supervisory agencies, who will need to raise their own cyber awareness. The EU Commission first proposed this regulation in 2019. It has in the meantime undergone several rounds of consultation. The idea was to fill a void— an absence of EU-wide rules about digital operational resilience that had led to the proliferation of national regulatory initiatives. These national rules were at times inconsistent or duplicative and brought with them additional administrative and compliance costs.

US: Strengthening American Cybersecurity Act

On March 15, 2022, President Biden signed this Act into law. Using language from other bills, the Act requires critical infrastructure operators to report "substantial cyber incidents" to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and report ransomware payment within 24 hours. The Bill has several other provisions to strengthen cyber security including requiring all federal agencies to report substantial cyber incidents to CISA, effectively making this agency the lead government organisation for helping critical infrastructure operators respond to and recover from major network breaches.

Not if, but when
The human factor: a key vulnerability

“Education and awareness are an absolute must. In the end, cyber security is mostly about the human factor. It is not ethical to give humans badly protected systems, but humans need to understand what the risks are.

IT staff need sufficient cybersecurity capabilities, as many risks can stem from poor programming. You need to understand how to develop a mature system. But end users must also understand the risks and how to avoid them.

You need to understand what is in the data that you share with other parties, and that they share with you.

By now, everyone knows about passwords and the importance of not using obvious ones or reusing the same password for multiple work and home applications. But you also need to understand what is in the data that you share with other parties—and that they share with you.

There are a lot of things you can do to strengthen the safeguards. We often run phishing exercises and report on who falls for them. This makes people aware, but it needs to be accompanied by basic training for all employees. How do I spot a false email? How do I recognise that someone is using my credentials? This is still a work in progress in most companies. There’s greater awareness, but we’re not there yet.”

Jan Matto
Partner, Mazars

Chapter 5

Strengthening the cyber safety net

Improving your organisation's cyber security goes well beyond technical readiness. Surviving attacks and thriving in the face of them requires mindset and behavioural shifts.

Key takeaways

Cyber threats are here to stay—and they will get worse. That is the sober reality of C-suite sentiment, as reflected in our annual barometer. Business leaders have no choice but to live with that reality and deal with it as best they can. Many are confident they can withstand significant attacks, but why tempt fate?

Everyone needs a cyber safety net, and the stronger the better. This final section contains six takeaways for surviving and thriving in a cyber-scary world. They are tenets designed to spur action, with relevance not just for business leaders and IT teams but for all employees.

Shift your mindset

Prepare for the worst. Don't be overconfident or get too comfortable with the idea of the risk you're up against. If and when it strikes, it can and likely will surprise you by its virulence. Vigilance is the watchword. You need to constantly be on edge, alert to changing techniques, new vulnerabilities and evolving market conditions—and threats.

Know your systems, your data applications and their vulnerabilities

In many companies there are two realities: an IT reality, and a management assessment of that IT reality. The former, the IT reality, is about operational sophistication. How good is the programming? How safe are those new printers you've just connected or that new-fangled marketing software you integrated? The latter, the management reality, is too often about compliance: do we have a process for dealing with a breach? There's a need to close that knowledge gap, with better communication and greater understanding of the dual realities – on both sides.

Focus on external risk

Don't forget to include your supply chain exposure in your risk assessment. It can easily be the cause of contagion. How carefully do vendors manage their systems, especially if you've outsourced any part of yours to them? Third-party risk quickly becomes your risk in the event of a breach.

Learn, teach and educate

Don't underestimate the importance of the human factor as a primary cause of cyber crisis. One staff member clicking on one innocent-looking link in a moment of forgetfulness can have cascading and sometimes devastating consequences. Cyber security needs to be a compulsory all-company learning programme—and one that is a constant work in progress.

Test, test and retest

Your crisis management plan is only as good as the last time you took it for a trial run. As cyber threats grow and evolve, you need to finetune responses to a range of scenarios to ensure that everyone in the company—not just IT and communications—knows what to do to put in place the smoothest possible recovery plans in what are certain to be very trying conditions.

This is not just a compliance exercise

Yes, regulators are becoming more involved. Even so, it's essential to see cyber security for what it truly is: not just a compliance issue, but a common concern, a shared risk for individuals, companies and societies more broadly. We can all infect one another through inadvertent errors, but we can also protect one another through conscious choices, especially when it comes to full disclosure after an attack. Put bluntly, in a world where there is no cyber security, there is no business. So, effective response and recovery are not just a matter for individual companies, they concern society as a whole.

Methodology

The Mazars C-suite barometer was designed and conducted by GQR Research, in collaboration with Mazars. The data was gathered via an online survey between 24 September 2021 and 25 October 2021. The total sample is N=1,130, with 1096 sourced from online panels and 34 invited via email directly from Mazars.

Job role		Industry		Annual revenue (USD)	
CEO, Chairman, Board	706	Financial Services	219	$1m-$100m	432
Other C-suite executive	423	Technology & Telecoms	178	$100m - $1bn	350
		Retail & Consumer Products	149	$1bn+	348
		Automotive & Manufacturing	166		

Region	Country	Sample		Region	Country	Sample	
Africa & Middle East	Egypt	20	135	North America	Canada	53	108
	Kenya	20			United States of America	55	
	Morocco	20		Latin America	Argentina	10	171
	Nigeria	20			Brazil	25	
	South Africa	35			Chile	29	
	United Arab Emirates	20			Colombia	30	
Asia-Pacific	Australia	23	198		Mexico	72	
	China	20			Uruguay	5	
	Hong Kong	20		Europe	France	50	354
	Indonesia	20			Germany	60	
	Japan	20			Ireland	15	
	Malaysia	15			Italy	53	
	Philippines	20			Netherlands	51	
	Singapore	20			Spain	50	
	South Korea	20			Switzerland	22	
	Vietnam	20			United Kingdom	50	
Central & Eastern Europe	Austria	9	164		Turkey	3	
	Poland	36		**Total**	**39 countries**	**1,130**	
	Romania	48					
	Russia	43					
	Slovakia	12					
	Ukraine	16					

Contacts

Robert Kastenschmidt
Partner and Head of Consulting, Mazars
Robert.Kastenschmidt@mazarsusa.com

Jan Matto
Partner, Mazars
Jan.Matto@mazars.nl

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of more than 44,000 professionals – 28,000+ in Mazars' integrated partnership and 16,000+ via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*Where permitted under applicable country laws

mazars