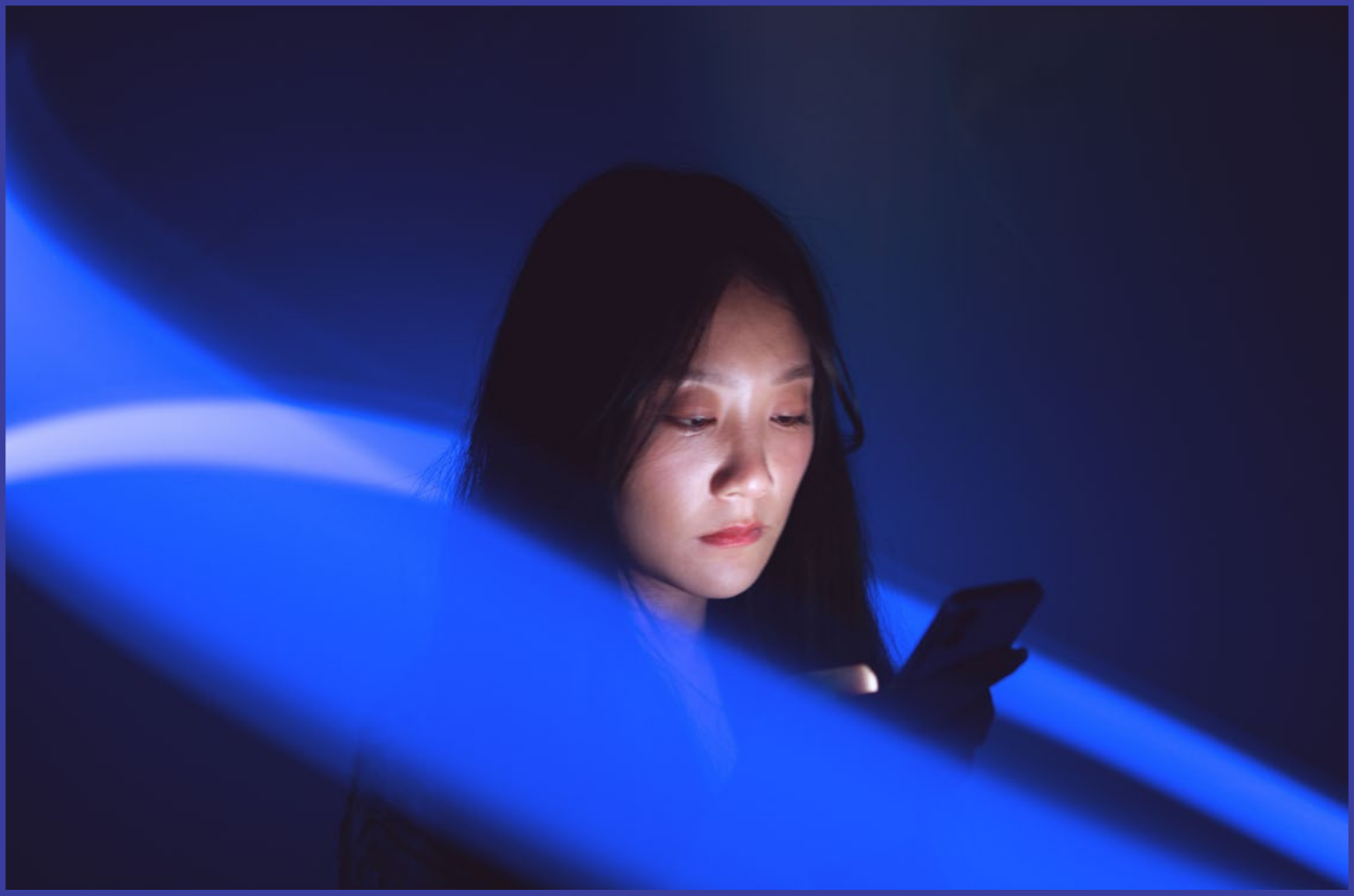


Future-proofing cyber security in an increasingly digital world

mazars

Your challenges

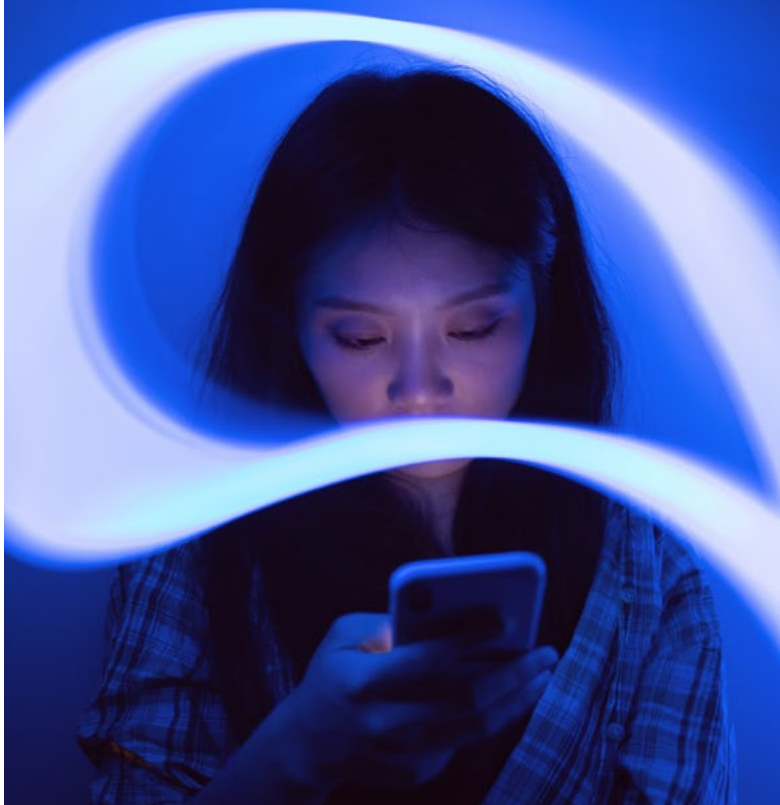
In a world that has become reliant on digital technology, most organisations' current cyber security strategies are no longer enough to combat threats.

Future-proofing cyber security means complying with a plethora of new threats, legislation, conducting assurance reviews, accepting the complexity of the IT reality and preparing the human factor – and developing and fortifying it so it continues to mitigate current and future risks.

Every minute, every day, someone, somewhere in the world is the victim of a cyber attack or data breach. Everyone is a target – from large corporations and government institutions to small businesses and individuals. The scale of threat is escalating and demands our immediate attention and action. This urgency is not just a reaction to growing hazards, but also a moral duty towards safeguarding our economy and society.

"Cyber security is not a luxury, it's a public interest obligation"

Jan Matto
Global Lead, Cyber Security and Data Protection, Mazars



Why act now?

Business leaders brace for cyber attacks

Our recently released C-suite barometer confirms the seriousness of the danger. Over half of the 800+ global business leaders surveyed saw an increase in cyber threats over the past year. More than a third expect a significant data breach in their own company in the coming year.

Despite their concerns, most executives are confident of their ability to protect themselves in the event of an attack. Two-thirds say their data is "completely protected" and around 30% say it is "partially protected".

But there is a growing disconnect between perceived and actual cyber risk. According to another Mazars report, Cyber security: is your safety net strong enough?, while top managers make governance plans in the belief they can achieve – or have already achieved – a high level of security compliance, the day-to-day reality in IT departments is becoming ever more complex and fraught with risk.

Cybercrime is expensive

Cybercrime is expected to cost a staggering $8 trillion globally in 2023[1]. That's double the size of the economies of Japan and Germany, and only smaller than the U.S. and China.

Besides the financial costs, cyber security attacks also cause reputational damage and loss of customer trust. When you have a cyber breach, how you react and then communicate with clients is vital to maintaining your brand and customer base.

It is critical for organisations to protect themselves from ransomware attacks and hackers, and also protect their IT systems, otherwise they will be a danger to others.

1 https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

"Every year the number of zero day attacks breaks the record set the prior year. With AI, we expect to see the number of zero day attacks grow exponentially."

Paul Truitt
Principal and National Risk Consulting Leader, Mazars USA

Digital evolution

The digital landscape is constantly developing, and as firms accelerate the adoption of emerging technologies such as generative artificial intelligence (AI), big data and the Internet of Things (IoT), the corresponding cyber risks escalate as well.

Everyone and everything with an internet provider (IP) address constitutes part of the 'tech surface' (digital presence). Each IP address that is visible is exposed to cyber attacks. Just as the internet is 'always on', so too are cyber criminals, capitalising on vulnerabilities and exploiting any weak points in our interconnected world.

While the fast pace of technological innovation has made our lives easier, it has also given would-be attackers more arsenal at their disposal. Of particular concern is the weaponisation of generative AI, making it simpler for criminals to launch sophisticated attacks on organisations.

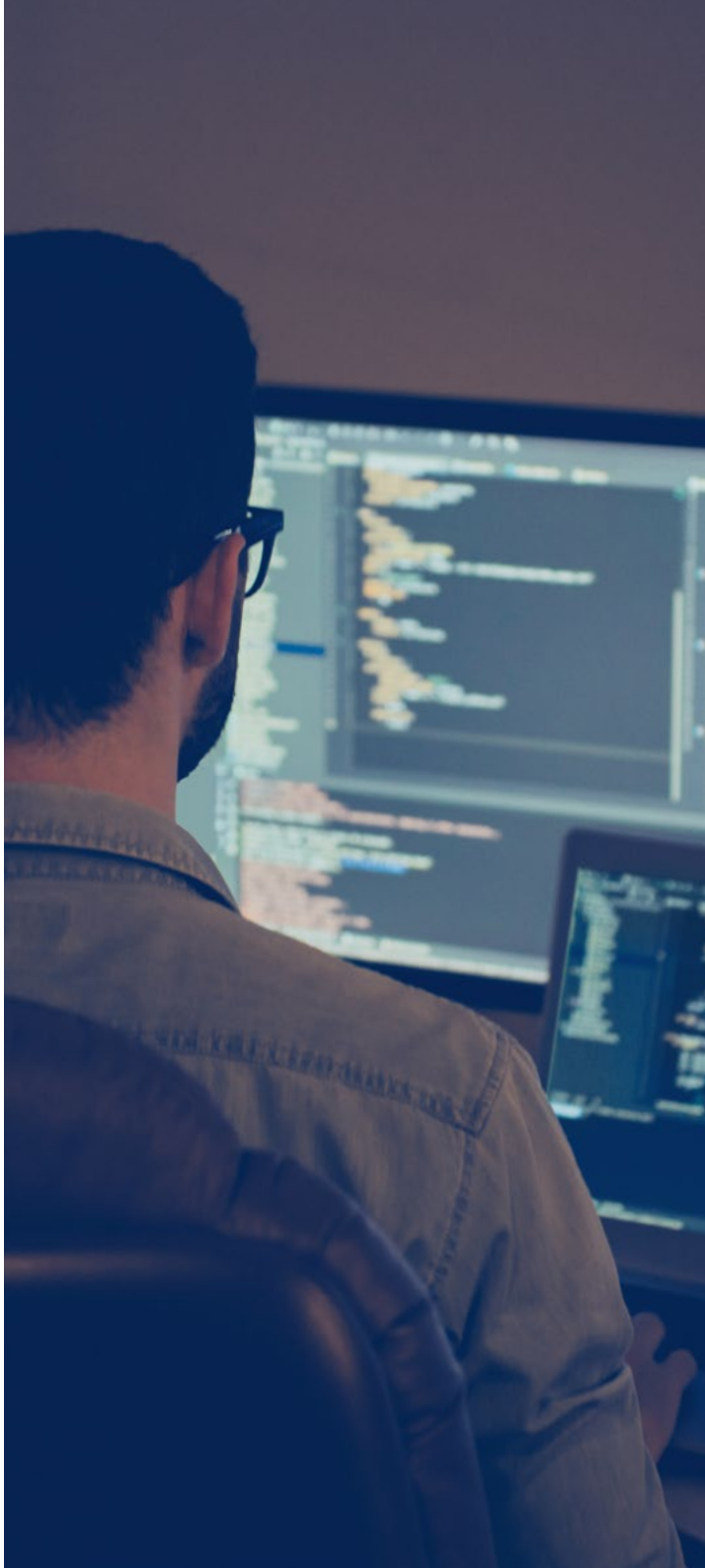
These new developments – coupled with the internet always being on – amplify the need for more comprehensive cyber security legislation.

“Identifying, securing and controlling data storage locations is extremely challenging, particularly when organisations must comply with data protection legislation whilst also facing increasingly sophisticated cyber attacks.”

Omar Chaabouni
COO, Mazars Cyber Security Center of Excellence

Data is everywhere

Data is now everywhere. It resides in many forms and locations that span from on-premises assets (such as workstations, laptops, servers and databases) to cloud platforms extending to user personal devices (smartphones and tablets). At the same time, data is much more accessible via VPN or internet access. Despite the benefits coming from increased data accessibility, organisations also become more exposed to cyber attacks.



Which cyber regulations are important?

Governments are introducing new legislation to mitigate the effects of cyber attacks and related systemic risks, partly because of its ease and ubquitousness, but mainly because of the 'contagion' effect it can have on the economy – the clients of clients – and society at large.

All these regulations aim to:

- **Standardise** cyber security measures across industries and regions
- **Increase** accountability, transparency and sharing knowledge
- **Limit** cyber attacks' impact and spread in an interconnected world
- **Establish** strict reporting/alerting protocols to quickly and effectively deal with risks
- **Encourage** the use of up-to-date technology and practices to protect against cyber threats
- **Incentivise** organisations to adopt better cyber security practices by imposing severe penalties for non-compliance

"No matter how well an organisation believes its data is protected there is always the risk of a breach, so businesses need to be ready."

Jan Matto
Global Lead, Cyber Security and Data Protection, Mazars

The most significant rules, both in Europe and the US, include:

EU EU NIS 2 for cyber resilience

- The EU's first Network and Information Security (NIS) Directive was adopted in 2016. It focused on strengthening national cyber security capabilities, establishing cross-border collaboration, and putting in place national supervision of cyber security in critical sectors such as energy, transport, water, health, digital infrastructure and financial services.
- In 2021, the European Commission proposed replacing it with an updated version. NIS2 addresses the security of supply chains and introduces more stringent supervisory measures and stricter enforcement requirements.
- Expected to be implemented by October 2024.

EU Digital Operational Resilience Act (DORA)

- DORA aims to standardise the approach to managing and mitigating cyber security risk among all types of financial sector entities and their IT providers.
- Alongside more traditional firms, it also covers entities that may not have been previously covered by financial market regulation including alternative investment firms, crypto-asset service providers and crowdfunding service providers.
- First proposed in 2019, this new regulation takes effect in EU member states in 2025.

EU Digital Markets Act (DMA) and Digital Services Act (DSA)

- Both legislative proposals put forward by the European Commission that came into force in November 2022.
- DSA aims to create new rules regarding the responsibilities of digital services to address the risk faced by their users and to protect their rights.
- DMA aims to ensure fair and open digital markets, particularly relating to large tech companies known as "gatekeepers." Both acts address issues of security, transparency, and data privacy.

EU General Data Protection Regulation (GDPR)

- A regulation on data protection and privacy in the European Union and the European Economic Area which has been in force since May 2018.
- It also makes provision for the transfer of personal data outside these regions.
- GDPR gives control of personal data back to consumers, mandates strict rules for reporting breaches, and imposes heavy fines for non-compliance. It requires organisations to implement adequate data protection safeguards.

EU SWIFT Customer Security Programme (CSP)

- Launched in 2016 as a response to multiple cyber attacks targeting SWIFT users' environments.
- It has been designed to help SWIFT users secure their local SWIFT environments and their access to the SWIFT Messaging Services.
- It requires SWIFT users to comply with Customer Security Controls Framework (CSCF) and to attest their compliance level annually.
- Since 2021, SWIFT requires from SWIFT users to perform an independent assessment against SWIFT CSCF.

“Ensuring compliance is increasingly challenging, not only because of the annual tightening of the SWIFT CSCF standard, but also due to the adverse effects of non-compliance on stakeholders’ trust and business operations.”

Wadi Mseddi
Lead Partner, Mazars Cyber Security Center of Excellence

US Strengthening American Cybersecurity Act

- President Joe Biden signed this Act into law in March 2022.
- It 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, which ensures a coordinated approach in responding to and recovering from major network breaches.

US Payment Card Industry Data Security Standard (PCI DSS)

- Initially created in 2004 to increase controls around cardholder data to reduce credit card fraud.
- It is a proprietary information security standard for all organisations that handle credit cards from the major card schemes.
- The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council.
- The latest update, Version 4.0 was published in March 2022.

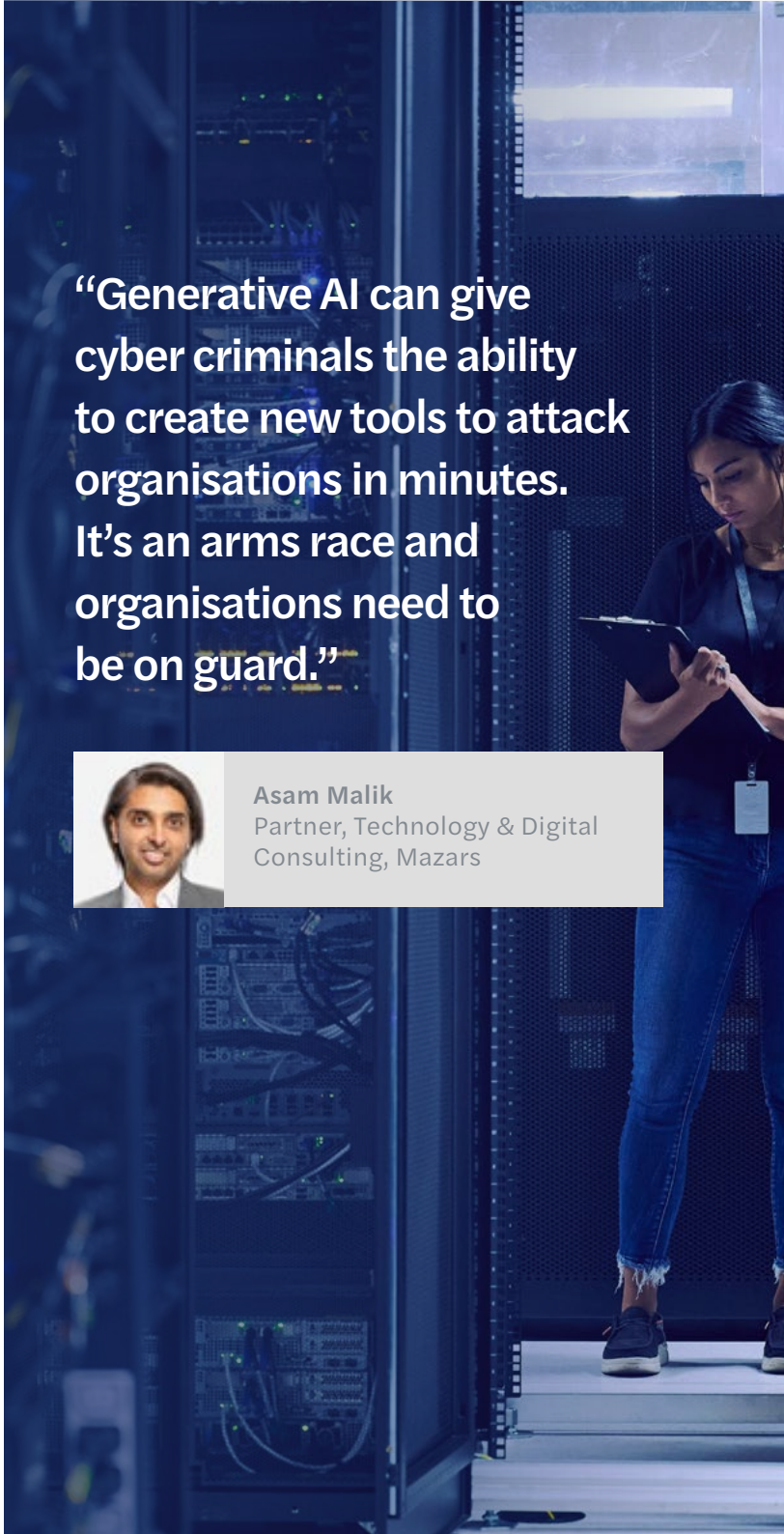
US SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companie

- Most public companies will be required to include an incident disclosure on their Form 8-K filed with annual reports for fiscal years ending on or after 15 December 2023.
- New regulations require disclosure on Form 10-K of any material weaknesses of a company's process to assess, identify and manage material risks.

Mandatory internal and external audits and assessments

Under most of these proposed laws, some form of cyber security audits will become more frequent, which will help organisations identify not only their vulnerabilities but also offer measures to enhance their security. The growing demand for cyber security audits further necessitates the need for professional service firms specialising in cyber security risk assessment and assurance. We predict the market for cyber security audits and assessments will be as big as financial audits in the future. These developments require a change in the approach of audits and assessments, deploying capable multi-disciplinairy teams, the use of a variety of digital cybersecurity tools and servces, 24/7 use of monitoring and detection tools and development of internal and external reporting standards.

However, it is important to understand that while legislation and regulation can provide guidelines and set minimum standards, the ultimate driver of strong cyber security measures will be market forces. As cyber security becomes a fundamental requirement to operate in a digitalised economy, it will influence business decisions, much like environmental, social and governance (ESG) legislation.



“Generative AI can give cyber criminals the ability to create new tools to attack organisations in minutes. It’s an arms race and organisations need to be on guard.”

Asam Malik
Partner, Technology & Digital Consulting, Mazars

What should companies do?

Firms now need to adopt a proactive approach towards cyber security: to navigate the regulatory landscape and avoid any knock-on effects of a potential breach. This involves shifting from responding to threats after they occur to anticipating and mitigating them in advance.

Our report Cyber security: is your safety net strong enough? identified five pillars for defence against cyber threats. Each has an important technological component, accompanied by an equally critical human component. Both elements require patience, training, investment and extensive testing.

Pillar 1 Identification

- Identify and map all sources of data, degree of sensitivity of data, and potential system vulnerabilities that could expose them.
- Perform risk analysis taking into account all stakeholders, including the ecosystem of the organisation.
- Understand 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.

Pillar 2 Prevention

- Apply multiple technical solutions such as segmentation strategies to help protect IT systems and ensure they keep working normally even in the face of attacks.
- Raise human awareness through education programmes and regular "phishing", and other in-house testing.
- Use multi-factor authentication for users to double-down on fraud and, at the same time, improve employee cyber 'hygiene'.

Pillar 3 Detection

- Cyber security audits provide useful external perspectives on the effectiveness of system safeguards.
- Get help from experts to implement threat detection and monitoring services to identify attacks and quickly take action.
- Understand your company's potential exposure, have the tools to monitor network activity; and detect abnormalities in real time to escalate where needed.
- Besides IT staff, you need well-trained managers at all levels, to spot issues and know whom to alert.

Pillar 4 Response

- Once an intrusion is detected, the technical response to isolate and neutralise it needs to be 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.
- Communication is key: business leaders need to contact management and staff, to clients, to suppliers and others in their data ecosystem, and - increasingly - to regulators.

Pillar 5 Recovery

- Resuming business as usual is mission critical.
- Technology solutions include offline back-up systems that can be quickly activated to restore normal IT functioning. This is not only focusing on data but the recovery the whole configuration.
- Many other parts of a business need to coalesce around a recovery plan that has been carefully tested and retested well in advance – not only from a systems perspective but also from a human one.

“Being cyber-ready isn’t just about surviving the battle; it’s about losing a battle and not losing the war.”

Jan Matto,
Global Lead, Cyber Security and Data Protection, Mazars

Cyber security isn’t a choice, it’s essential. The urgency to act now, amid the advancing regulatory landscape and the growing necessity for companies to adopt a proactive approach towards cyber security, form the basis for a digital society that is safe, secure and resilient.

Contacts

Jan Matto
Global Leader, Cybersecurity & Data Protection Services
+31 88 277 13 99
Jan.Matto@mazars.nl

Wadi Mseddi
Partner, Mazars Cybersecurity Center of Excellence
+216 71 96 34 74
wadi.mseddi@mazars.com

Frederic Malagoli
Partner, Cybersecurity, Mazars, France
+33 6 58 60 30 83
frederic.malagoli@mazars.fr

Asam Malik
Partner, Technology & Digital Consulting
+44 (0) 20 7063 4000
asam.malik@mazars.co.uk

Paul Truitt
Principal, Cybersecurity Practice Leader
+1 215 913 9968
Paul.Truitt@mazarsusa.com

www.mazars.com

mazars