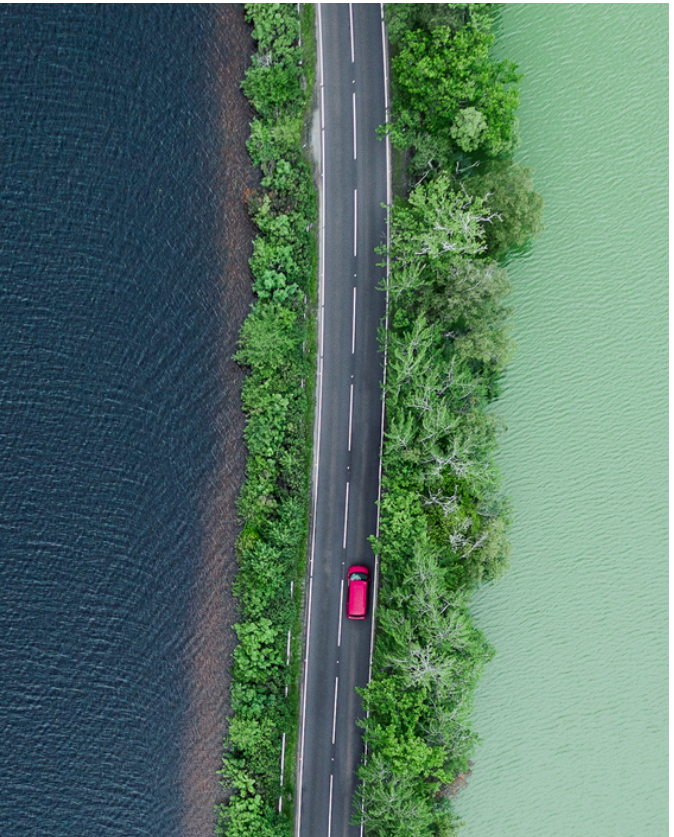
Marsh

Why the cybersecurity gap between SMEs and large organisations matters

Contents



Foreword

From the Federation of European Risk Management (FERMA)

When we saw the findings in this report regarding the cybersecurity gap between small and medium-sized businesses (SMEs) and large organisations and the impact this might have on our society, we were both surprised and excited. Surprised by the current situation regarding the implementation of cyber controls, and excited about the potential for improvement. Some of the data points make for stark reading. For example, incident plan testing is only conducted by 40% of SMEs versus 61% of large companies. This gap is notable and needs addressing. The Federation of European Risk Management (FERMA) is delighted to provide a foreword to this report, *Why the cybersecurity gap between SMEs and large organisations matters*, on behalf of the risk management community. Cyber risk is a strategic priority, now and over the longer term. Indeed, in FERMA's *Global risk manager survey report 2024*, a panel of more than 1,000 respondents ranked cyberattacks as the top risk and data breaches as the fifth.

FERMA has a long-standing cooperation with Marsh on the topic of cyber risk. In 2018, European industry bodies, including FERMA, collaborated with Marsh to produce the report, *Preparing for cyber insurance*, to help organisations understand cyber risk and assess their potential need for cyber insurance. In 2023, FERMA and Marsh were key contributors to a joint-industry report, *Cyber insurance dialogue: How Europe can lead the way to cyber resilience,* which called for greater collaboration on cyber risk and addressed the unique challenges confronting SMEs. Marsh's report reinforces the need to understand the nuances of the cyber threats facing SMEs. Against a background of multifaceted and metamorphosing cyber risks, it is important to focus on organisations' risk strategies because prevention of cyberattacks pays off.

This report will be of particular interest to risk managers, who play a crucial part in cyber hygiene.

Cyber insurance plays a vital role in enhancing cyber hygiene in organisations that are not large enough to have a dedicated risk management function. The report sheds light on the level of preparedness of SMEs and mid-cap organisations. Risk managers of large organisations should bear this in mind when evaluating the interdependencies within their supply chains.

The report also offers valuable insights for policymakers, particularly by providing key data points on the of-the-moment topic of cyber incident reporting. It is vital that policies in this area take account of the dynamic and evolving nature of cyber risk, as well as the potential impact of legislation and regulation on the competitiveness of European companies.

As the nature of this threat evolves, it is imperative that policy remains relevant and effective. FERMA, in its capacity as an advocacy body representing the risk management community, intends to use the data in this report in talks with decision-makers in Brussels.

About FERMA

The Federation of European Risk Management Associations (FERMA) brings together 23 national risk management associations from 22 European countries.

FERMA represents the interests of more than 5,600 risk and insurance managers in Europe that are active in a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. Find out more at: FERMA.

Introduction

According to the *Global Risks Report 2024*, published by the World Economic Forum (WEF) in collaboration with Marsh McLennan, nearly 40% of experts surveyed considered cyberattacks to be a paramount risk with the potential to trigger a material crisis in the near future. This placed cyberattacks within the top five risks in the current risk landscape.

SMEs can have lower cyber resilience than large organisations, a disparity that could have significant implications for society. To mitigate the potential impacts of a cyber event, SMEs need to become more resilient. This can be achieved by raising awareness, providing education, and offering support for the implementation of robust cybersecurity measures.

Governments, industry associations, and large organisations can play a role by offering SMEs resources, guidance, and collaboration opportunities to help them enhance their cyber resilience. Strengthening the cybersecurity posture of SMEs will help build a more secure and resilient society.

A collaborative approach is essential to align the risk appetite of the insurance market with the coverage requirements of corporate insurance buyers. Ultimately, solutions must reflect the interests of both insurers and buyers to create a balanced market. A strong presence of SMEs in the cyber insurance market is imperative to achieving this goal.

Earlier research from Marsh and FERMA published in the *Cyber insurance dialogue: How Europe can lead the way to cyber resilience* — involving the (re)insurance, insurance broking, and risk management communities — identified key cybersecurity controls and explained the rationale for implementing them.

More recently, Marsh and Zurich Insurance Group in *Closing the cyber risk protection gap* called for establishing partnerships to help reduce the cyber risk protection gap. They highlighted the cyber insurance market's strong growth in recent years, and a projection that the market will more than double by 2027.

Still, a substantial cyber risk protection gap persists. Demand from organisations seeking to transfer their cyber risk is growing, though unevenly. Additionally, there remains a worrying trend of SMEs being uninsured or underinsured.

In this report, we look at the cyber resilience gap between SMEs, mid-cap, and large organisations. We define SMEs as organisations with annual revenues lower than €51 million, mid-cap organisations as those with annual revenues of between €51 million and €250 million, and large organisations as those with annual revenues exceeding €250 million.

Using data from Marsh's Cyber Self-Assessment — which evaluates an organisation's cyber risks and streamlines the process of applying for cyber insurance — the analysis consists of two parts:

- A comparison of the cyber resilience gap of SMEs, mid-cap organisations, and large organisations.
- A comparison of the cyber resilience gap across the same segments by industry.

We analysed Marsh data across 12 cyber control categories, comparing their implementation rates among the three revenue bands. We also examined the differences in implementation rates of controls among different segments.

Key findings

Organisations that purchased cyber insurance improved their cyber resilience. This improvement is likely due, at least in part, to the increased requirements set by insurers in order for organisations to qualify for cyber insurance or to renew their policies.

We also found:

Large organisations exhibit a higher rate of cybersecurity controls implementation than mid-caps and SMEs.

- 91% of large organisations versus 75% of SMEs require multi-factor authentication for remote login to the corporate network.
- 72% of large organisations versus 55% of SMEs require multi-factor authentication and encrypted channels for administrator accounts.
- 76% of large organisations versus 61% of SMEs tag external emails to alert employees that the email originated from outside the company.

There is a need for improved implementation of incident response plans across the board.

- 61% of large organisations and 40% of SMEs test their incident response plans.

Financial institutions demonstrate a higher adoption rate of controls than other industries.

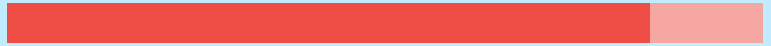
- Cybersecurity training is mandatory for employees of 85% of finance SMEs versus 58% of manufacturing SMEs.

There is still room for improvement, as cyberattacks evolve. Organisations must improve their cybersecurity controls to remain resilient.

75% **of SMEs** require multi-factor authentication for remote login to the corporate network.

55% **of SMEs** require multi-factor authentication and encrypted channels for administrator accounts.

61% **of SMEs** tag external emails to alert employees that the email originated from outside the company.



85% Cybersecurity training is mandatory for employees of 85% of finance versus **58% of manufacturing SMEs**.

Source: *Marsh*

The impact of SMEs on society's cyber resilience

There is no doubt that SMEs play an important role in society. Therefore, their lack of cyber resilience can have serious consequences — not only for their own organisations, but also for their supply chains.

Examples of the potential impacts of cyber incidents within SMEs include:

1. **Economic impact:** SMEs are fundamental to driving economic growth and job creation. However, insufficient cyber resilience can increase their vulnerability to cyberattacks, potentially resulting in financial losses, business disruptions, and even bankruptcy. This vulnerability can have a ripple effect on the economy, leading to job losses, reduced productivity, and diminished overall economic stability.

2. **Supply chain disruptions**: SMEs often form an integral part of the supply chain, providing goods and services to large companies. If an SMB falls victim to a cyberattack, it can become a weak link in the chain, potentially compromising the security of large organisations. This can lead to supply chain disruptions, delays in product delivery, and increased costs, affecting not only the SMB, but also the large companies and consumers that rely on their products or services.

3. **Data breaches and privacy concerns:** SMEs manage sensitive customer data, including personal information, financial records, and intellectual property. A lack of cyber resilience increases the risk of data breaches, exposing individuals to identity theft, fraud, and other cybercrimes. This erodes trust in businesses and can have lasting consequences for individuals and society as a whole.

4. **National security risks:** SMEs may have access to critical infrastructure or sensitive information that, if compromised, could pose a threat to national security. For example, an SMB involved in the defence or energy sectors may hold valuable intellectual property or have connections to government agencies. A lack of cyber resilience in such companies can make them attractive targets for cyber espionage or sabotage, potentially undermining national security.

5. **Social disruption:** Cyberattacks on SMEs can disrupt essential services and impact the daily lives of individuals. For instance, an attack on a healthcare provider or a utility company can result in the loss of access to vital services, affecting public health and safety. This can create social unrest and undermine public trust in institutions.

Large organisations outpace SMEs in cyber control implementation, especially for incident response management

To assess the potential gap in cyber resilience between SMEs and large organisations, we examined the controls that insurers typically consider essential hygiene factors that all organisations should implement, regardless of their size or complexity (see Figure 1).

Generally, we observed fewer controls implemented in SMEs and mid-cap organisations compared to large organisations.

The only control in which SMEs outperform large organisations is the area of conducting backups for critical information. A potential explanation for this could be that SMEs more often use a cloud service provider.

All organisations, irrespective of revenue size, have a high score of implementations regarding this control ranging from 89% to 90%.

01| Implementation of essential cyber security controls based on revenue

Question	Option	SMEs	Mid-caps	Large organisations
Multi-factor authentication for all remote login access to the corporate network. (For example, virtual private network (VPN), remote desktop protocol, or other secure remote access.)		75%	79%	91%
Multi-factor authentication and encrypted channels for all administrative account access, irrespective of user's location.		55%	63%	72%
Organisation deploys vulnerability patches.	Minimum response quarterly.	93%	95%	96%
Cybersecurity training is mandatory for all employees.	Minimum response annually.	76%	72%	86%
Backups are made of critical information (including business continuity and disaster recovery plans).	Minimum response weekly.	91%	89%	90%
Incident response programme encompasses.	Processes/procedures for performing incident classification, prioritisation, handling, reporting, and recovery.	63%	65%	85%
Incident response programme encompasses:	Plan testing or exercise requirements.	40%	33%	61%
Incident response programme encompasses.	Plan review and update schedule.	42%	41%	60%
The organisation operates the following IT and information/cybersecurity tools and capabilities:	Endpoint detection and response (EDR) solutions.	54%	62%	82%
The organisation operates the following information technology (IT) and Information/Cybersecurity tools and capabilities.	Advanced endpoint security.	56%	67%	75%
Formal firewall policy is deny all by default and permit by exception to ensure only explicitly approved incoming/outgoing traffic is permitted.		83%	90%	93%
External emails are tagged to alert employees that the email originated from outside the organisation.		61%	66%	76%

Source: *Marsh Cyber Self-Assessment*

How effective are SMEs in responding to cyber incidents?

We have observed a significant difference in the implementation of incident response management plans between SMEs and large organisations. Historically, most organisations focused their cybersecurity efforts on prevention rather than resilience. But knowing how to respond to an incident is just as important as preventing one, especially in today's risk environment where complete security is impossible to achieve.

To mitigate the impact of an incident and prevent it from becoming a crisis, many organisations have enhanced their incident response capabilities. However, it is evident that SMEs and mid-cap organisations are still lagging in this area.

The importance of incident management is underscored by its significant role in regulations such as the NIS 2 Directive, Digital Operational Resilience Act (DORA), and the Cyber Resilience Act.

For example, incident response management is an important aspect for organisations under the NIS 2 Directive, which aims to bolster cybersecurity across the EU. This management ensures compliance with regulatory requirements, helping organisations avoid penalties and maintain operational continuity.

A robust incident response plan enables proactive risk mitigation by identifying vulnerabilities and implementing preventive measures. Quick and effective responses to security incidents minimise their impact on operations, data integrity, and reputation. Furthermore, they foster better communication and coordination among internal teams and external partners, essential for effective incident handling and reporting.

Post-incident analysis is a key component, enabling organisations to learn from past events and continuously improve their preparedness. This not only builds public trust but also aligns with established cybersecurity frameworks, enhancing overall cybersecurity posture.

By structuring incident response management, organisations can allocate resources efficiently, ensuring that the right personnel and tools are available when needed. In essence, effective incident response management is crucial for meeting NIS 2 requirements, protecting critical infrastructure, and ensuring the resilience of essential services in an increasingly complex cyber landscape.

SMEs are a vital link in the supply chain

SMEs are at the heart of the European economy. According to the EU's *Annual report on European SMEs (2022/2023)*, SMEs make up over 99% of businesses in the EU and are considered the backbone of the financial system. Therefore, the inability of SMEs to handle a cyber incident due to inadequate or missing incident response measures can have serious supply chain repercussions. If one supplier is unable to deliver products to the next stage of the supply chain, production could come to a standstill, impacting many more companies and consumers than just the one company experiencing the cyber incident.

SMEs may struggle with the implementation of an incident response plan due to reasons including:

- SMEs often have a less mature risk management function. They may lack resources, budget, and expertise needed to develop effective incident management strategies.
- SMEs depend more heavily than large companies on information and communication technology (ICT) service providers. These providers may lack sufficient incident response capabilities and may not communicate this concern to their clients. Consequently, in the event of an incident, SMEs may not have access to the best experts available, leading to greater impacts and losses.
- SMEs have only recently become subject to cyber regulation and the establishment of incident management was not mandatory. However, new regulations, such as NIS 2, will impact SMEs directly and indirectly. Companies governed by NIS 2 are likely to scrutinise their supply chains more closely and demand greater cyber resilience from their SMB partners.

Implementation of cyber controls across industries based on revenue

To assess the extent of cyber control implementation across diverse industries and organisations with differing revenue levels, we analysed four industry segments (see Figure 2):

1. Manufacturing
2. Retail and wholesale trade
3. Financial institutions
4. Professional services

Across the board, we observed again that large organisations implement all cyber controls — except for the backup of critical information — more extensively.

We also saw that financial institutions lead in the implementation of controls, followed by professional services (see Figure 2). For financial institutions, this is unsurprising, as they are highly regulated and are, therefore, expected to have a greater awareness of cyber risk compared to less regulated sectors.

However, in this segment, we see a significant contrast between large organisations and SMEs, with the implementation of cyber incident management particularly lacking among SMEs.

02| Financial institutions lead in control implementation, followed by professional services

Question	Option	Manufacturing			Retail/wholesale trade			Financial services			Professional services		
		SMEs	Mid-caps	Large org.	SMEs	Mid-caps	Large org.	SMEs	Mid-caps	Large org.	SMEs	Mid-caps	Large org.
Multi-factor authentication for all remote login access to the corporate network. (For example, virtual private network (VPN), remote desktop protocol, or other secure remote access.)		69%	77%	89%	65%	68%	88%	85%	76%	95%	76%	94%	95%
Multi-factor authentication and encrypted channels for all administrative account access, irrespective of user's location.		41%	58%	69%	54%	54%	64%	64%	75%	82%	57%	73%	81%
Organisation deploys vulnerability patches.	Minimum response quarterly.	95%	94%	96%	**80%**	**93%**	**98%**	**100%**	**100%**	**97%**	**92%**	**95%**	**94%**
Cybersecurity training is mandatory for all employees.	Minimum response annually.	58%	63%	86%	80%	71%	80%	85%	90%	93%	80%	79%	90%
Backups are made of critical information (including business continuity and disaster recovery plans).	Minimum response weekly	97%	85%	88%	85%	93%	86%	90%	100%	94%	92%	88%	95%
Incident response programme encompasses.	Processes/procedures for performing incident classification, prioritisation, handling, reporting, and recovery.	50%	59%	78%	63%	57%	83%	70%	80%	98%	65%	71%	90%
Incident response programme encompasses.	Plan testing or exercise requirements.	22%	29%	53%	40%	32%	48%	50%	60%	86%	43%	26%	71%
Incident response programme encompasses.	Plan review and update schedule.	22%	38%	51%	43%	50%	50%	54%	55%	82%	43%	31%	71%
The organisation operates the following IT and information/cybersecurity tools and capabilities:	Endpoint detection and response (EDR) solutions.	39%	65%	79%	50%	59%	78%	71%	65%	91%	54%	58%	91%
The organisation operates the following information technology (IT) and information/cybersecurity tools and capabilities.	Advanced endpoint security.	63%	76%	70%	38%	59%	76%	62%	65%	83%	56%	61%	77%
Formal firewall policy is deny-all by default and permit by exception to ensure only explicitly approved incoming/outgoing traffic is permitted.		83%	88%	95%	71%	85%	89%	89%	100%	96%	84%	91%	90%
External emails are tagged to alert employees that the email originated from outside the organisation.		45%	69%	85%	71%	64%	66%	62%	50%	72%	68%	73%	80%

Source: *Marsh Cyber Self-Assessment*

Overall, the manufacturing sector had the lowest implementation scores.

This is especially concerning given that bad actors often target manufacturing organisations due to their low tolerance for downtime and relatively low level of cyber maturity compared to other industries. At the same time, their dependence on IT and OT (operational technology) infrastructure may increase the likelihood that they will opt to pay a ransom demand if they believe the purchase of a decryption key will allow the fastest recovery of systems and resumption of operations.

Despite these challenges, there is a growing recognition among manufacturing leaders of the need to future-proof their operations. Analysis carried out by Marsh on the National Institute of Standards and Technology (NIST) scores of manufacturers and other organisations across Europe showed many manufacturers have enhanced their abilities to detect and protect against cyberattacks. However, manufacturers generally have been less attentive to what should be done when bad actors infiltrate the ICT network. This trend, and the functions of the NIST framework, are discussed in more detail in Marsh's *The changing face of cyber claims in Europe 2024* report.

In summary, although organisations in Europe have made progress in implementing cyber controls, there is more work to be done.

Collective initiatives

To mitigate the societal impacts of cyber incidents, it is essential to promote cyber resilience across the value chain, particularly for SMEs that may not have sufficient resources to dedicate to cyber risk management. The following actions would contribute to this goal.

1. Education and support for SMEs:
Increasing awareness of cyber risks, providing education, and offering support for the implementation of effective cybersecurity measures can strengthen SMB's cyber resilience. The insurance market already plays a vital role, as organisations that have obtained cyber insurance have usually substantially improved their cyber resilience. This improvement is driven not only by the eligibility standards set by insurers, but also by the guidance provided by risk advisers, who assess organisations' cybersecurity posture and help them execute necessary improvements. SMEs can collaborate with brokers and risk managers of large enterprises, leveraging their expertise as a source of inspiration and guidance for best practices.

2. Public policy initiatives:
Investigations by public bodies into the cyber risk management practices and cyber insurance purchasing of SMEs can be highly beneficial. For example, many involved with cybersecurity are awaiting the release of results from a European Insurance and Occupational Pensions Authority (EIOPA) survey on SMB access to cyber coverage as many EU policymakers remain largely uninformed about cyber exposures.

Government bodies actively developing cybersecurity guidance include:

• *Cyber essentials from the National Cyber Security Centre (NCSC)* is an effective government-backed scheme designed to help organisations of all sizes protect themselves against a wide range of common cyberattacks.

• The five basic principles of safe digital entrepreneurship established by The Netherlands government to help entrepreneurs implement rudimentary security measures. By adhering to these principles, entrepreneurs can enhance their resilience against cyber risks that may disrupt business operations.

As the *Cyber insurance dialogue: How Europe can lead the way to cyber resilience* report puts forward, a set of minimum cyber risk standards, applicable to the size and activity of an organisation, is needed to boost awareness, identification, and prevention of threats.

These standards need to be appropriate for SMEs and consider the size and industry sector of the organisation. Regulators, policymakers, industry bodies, and the (re) insurance industry can play a significant role in developing baseline controls that align with the cyber insurance market.

3. Support for SMEs to attain regulatory compliance:
We have seen an increase in governmental and regulatory attention to cyber risk, as demonstrated by the EU digital strategy.

Such measures should help ensure that cyber risk management will continue to evolve from an information and communications technology (ICT) subject to include more C-suite discussions. Relevant regulations include the Digital Operational Resilience Act (DORA), which aims to strengthen the IT security of financial entities; *NIS 2 Directive*, aimed at increasing the resilience of organisations' networks and information systems; and the Artificial Intelligence (AI Act), with a goal to increase resilience in organisations' networks and information systems.

However, many SMEs continue to struggle to comply with such regulations and/or integrate their principles into daily operations. Many could benefit from the expertise of experienced brokers and risk managers used by large organisations.

The cyber insurance protection gap

The cyber insurance landscape for small and medium-sized enterprises (SMEs) in Europe has experienced challenges that have led to low insurance penetration rates. As cyber threats continue to evolve in sophistication and frequency, the necessity for comprehensive insurance coverage has become increasingly critical. However, many SMEs encountered barriers (outlined below) that impeded their ability to obtain adequate cyber insurance resulting in a substantial coverage gap. The following table outlines the primary causes of the low cyber insurance penetration rate and potential solutions to improve the insurance landscape for SMEs in Europe. With the recent softening of insurance rates, a growing understanding of the unique challenges faced by this segment, and innovative solutions emerging from the market, there is a promising opportunity to address these challenges. Ultimately, enhancing cyber insurance coverage and increasing the penetration rate for SMEs will contribute to building a more resilient economy.

Causes

- **Affordability issues:** Cyber insurance premiums have risen significantly in recent years due to a hard market, making coverage less affordable for small and medium-sized businesses. However, as insurers' appetite and capital increase, along with the improved security measures implemented by organisations, the cyber insurance market is softening, leading to lower premiums.
- **Accessibility challenges:** Historically, limited cybersecurity measures within SMEs have led to a reduced willingness from insurers to offer coverage.
- **Insufficient cyber risk awareness:** A general lack of understanding about cyber risks and cyber risk insurance contributes to the existing gap.erception of complexity: Cyber coverage and the procurement process is viewed as "complicated," deterring organisations from seeking coverage.
- **Perception of complexity:** Cyber coverage and the procurement process is viewed as "complicated," deterring organisations from seeking coverage.

Consequences

- **Low cyber insurance penetration rates:** A substantial number of organisations remain uninsured, with the insurance penetration rate for SMEs in Europe hovering around 15%.
- **Underinsurance:** Many organisations do not have adequate coverage or sufficient limits to tackle their cyber risks.
- **Lack of awareness of cyber insurance benefits:** Organisations often do not recognise the full range of benefits that cyber insurance policies can provide, including comprehensive prevention and assistance services.
- **Lack of awareness regarding coverage scope:** This results in low utilisation of available coverage options.

Solutions

- **Standardisation and simplification of the procurement process:** Streamlining the steps involved in obtaining cyber insurance will make it more accessible for SMEs.
- **Clear and broad policy language:** Insurance policies should utilise straightforward language to enhance understanding, ensuring that coverage is comprehensive and transparent.
- **Increased awareness training:** Enhanced campaigns and training programmes are necessary to improve understanding of cyber risks and the advantages of insurance coverage.
- **Prevention and assistance services:** Tailored services should be created to help SMEs effectively mitigate cyber risks.
- **Incentivising policyholders to improve cyber security posture:** Insurers should collaborate with clients by incentivising the implementation of security measures throughout their engagement.
- **Establishing public-private partnerships:** Collaboration for data sharing, training, and incentives aimed at enhancing security measures and awareness initiatives should be promoted.

Conclusion

It is clear that there is a gap in the implementation of security controls between SMEs, mid-cap organisations, and large organisations. Given the potential impact that cyber incidents can have on supply chains — and, consequently, on society — it is imperative to close this gap.

Regulators, policymakers, and the cyber (re) insurance market can play a significant role in doing so. By bolstering the cybersecurity posture of SMEs, we can collectively create a more secure and resilient society.

We invite all parties involved to engage in open and transparent discussions on this important topic.

Why Marsh?

Marsh remains committed to helping to quantify your cyber risk exposures with scenario-based loss modelling, benchmarking of potential cyber event losses and costs, consideration of the effectiveness of cybersecurity controls from a financial perspective, assessment of the economic efficiency of multiple cyber insurance programme structures, and help concerning management of your claims, should one arise.

We invest in our brokers and claims handlers and our bespoke Cyber Incident Management (CIM), which provides guidance in navigating cyber incidents. Marsh continuously learns from our clients' needs and questions, as well as from the claims we manage, to support organisations in enhancing their cyber resiliency.

Marsh's Cyber Practice provides organisations with experienced risk advice when managing their exposures.

- In-house, technical, and incident response practitioners to help clients before, during, and after cyber events.
- The incident management experience that comes from handling over 1,000 cyber and technology claims annually.
- Digital innovations to augment cyber response programmes.

If you have questions about any of the issues discussed in this report, please reach out to your Marsh representative.

About Marsh

Marsh, a business of Marsh McLennan (NYSE: MMC), is the world's top insurance broker and risk advisor. Marsh McLennan is a global leader in risk, strategy and people, advising clients in 130 countries across four businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. With annual revenue of $23 billion and more than 85,000 colleagues, Marsh McLennan helps build the confidence to thrive through the power of perspective. For more information, visit marsh.com, or follow on LinkedIn and X.