2024

EMEA Cybersecurity Report

NUMATA™

TABLE OF CONTENTS

> **Organisations need a strategic, adaptive, and multifaceted approach to cybersecurity that encompasses risk assessment, resource allocation, employee education, incident response planning, regulatory compliance, external collaboration, and a pervasive security culture. These elements form the foundation for a robust and resilient cybersecurity posture in the face of an evolving threat landscape.**
>
> -John O Mahony, Senior Cybersecurity Product Specialist at Kaseya

INTRODUCTION

Welcome to Numata's EMEA Cybersecurity Report for 2024.

This report aims to provide small- to medium-sized enterprises with a practical and valuable resource for gaining essential knowledge and insights required to manage cyber risk effectively. Excellent resources are available today, but many focus on the market's enterprise segment. Enterprise-sized organisations have enterprise-sized teams, budgets, and tools, making their insights and advice challenging to translate into an SME context.

By analysing trends and events of 2023, along with insights from key industry experts, you'll get a first-hand look into real-life encounters and perspectives on the security landscape. In addition, we delve into other critical aspects, including prevalent cyber threats, incident trends, the relationship between IT and cybersecurity strategies, and the nuances of cyber resilience geared specifically toward SMEs.

Our independent report adopts a vendor-agnostic approach to ensure we focus strictly on education and awareness rather than positioning vendors in a way that highlights the necessity of their products.

We hope you'll find value in our report and, of course, from the input of the best cybersecurity professionals worldwide.

Jakobus Koorts
Chief Executive Officer
Numata

REPORT CONTRIBUTORS

Chris Loehr

Solis | CTO and Executive Vice President

Chris is the EVP and CTO of Solis, where he leads Incident Response teams. He has over 25 years of leadership experience in cybersecurity and IT for the financial industry, and is an expert on various regulations and standards. He has held senior roles at IBC Bank and USAA, where he improved cybersecurity and IT capabilities.

In addition, Chris is a founding member of the CyberSecurity Think Tank and serves on several advisory boards and committees. He is a frequent speaker and guest on cybersecurity topics, even assisting NIST in reviewing their guidelines for managed services providers.

Chris believes that cybersecurity is a key business risk that must be respected. He has helped thousands of organisations recover from cyberattacks and advocates for strong and responsible cybersecurity practices.

Paul Delahunty

Stryve | Chief Security Officer

Paul is the Chief Security Officer at Stryve Secure, a multi-cloud and cybersecurity company based in Ireland. He is a certified CISSP and a prominent information security expert, recognised as the Security Leader of the Year 2023 by CIO and IT Leaders. He has a diverse background in engineering, start-ups, regulatory and compliance, information security and audit.

Before joining Stryve Secure, Paul worked for companies such as Ericsson, moQom, ThorsNet, and Hostelworld. He is also a founding Southeast Cyber Ireland committee member and holds an ICTTF membership.

Paul is a frequent speaker and guest on cybersecurity topics and events, and a regular contributor to the media. He is passionate about building a cybersecurity community and educating organisations on cybersecurity risks.

Jason Scanlon

Numata | Chief Information Security Officer

Jason is a seasoned IT professional with 20+ years of experience in consultancy and computer services, focusing on managed IT services. As a certified CISO with the EC Council, he's deeply invested in cybersecurity. He actively contributes to ITAG (West Chapter of Cyber Ireland), speaking at events like the global CISO Ensemble, and participating in the Cyber Ireland CISO Forum and ESCO, representing the EU. Jason's expertise spans strategic IT road mapping, network infrastructure design, systems troubleshooting, and network administration.

John O Mahony

Kaseya | Cybersecurity Solution Specialist

As EMEA Senior Cybersecurity Product Specialist at Kaseya, John oversees the security products within the suite. He has over 10 years of experience in the cloud, network, and information security field, working for companies such as AT&T Cybersecurity. He has also collaborated with internal IT teams, MSPs, MSSPs, and channel partners across EMEA and APAC regions, helping them optimise cybersecurity tools and services.

Wilmore Chininga

Island Networks | Infrastructure and cybersecurity consultant

Wilmore is an infrastructure and cybersecurity consultant passionate about helping organisations transform their digital environments to meet today's needs while preparing for the challenges of tomorrow. Although he has over 12 years of experience in the IT industry, Wilmore also brings a diverse skillset from his previous career as an architect, allowing him to deliver solutions that have stoodthe test of time.

Additionally, his experience with data centre infrastructure and cloud solutions gives him unique insights into the cybersecurity landscape. With an MSc in Cybersecurity and various industry certifications, Wilmore delivers solutions that would benefit any organisation.

Dr. Manuel Corregedor

Telspace Africa | Chief Executive Officer

Dr. Manuel, CEO of Telspace Africa, is a leading figure in information security, offering elite offensive security services like red teaming and penetration testing. With a deep passion for IT, his expertise spans both technical and managerial aspects. He holds significant academic credentials from the University of Johannesburg, including a BSc, BSc Honours, MSc focusing on Information Security, and a PhD in Computer Science with a specialisation in Information Security. His commitment to the field is further highlighted by his numerous certifications in information security, demonstrating his dedication to excellence.

Matthew Visser

Moore Infinity | Director

Matthew leads the Advisory team at Moore Infinity that provides strategic, financial and operational solutions to a diverse global client base. Their client base includes private equity funds, real estate investment trusts, private companies and listed corporations. Matthew has extensive experience in corporate finance, financial reporting, risk management and major projects advisory across geographies and sectors.

Wojtek Wierzcki

Sygnia | Head of Systems and Development

Wojtek brings a wealth of experience as both an Enterprise Infrastructure and Solutions Architect, combining technical expertise with strategic business insights to deliver secure, scalable, and resilient solutions that align seamlessly with enterprise objectives. He merges technical proficiency with commercial insight, ensuring the delivery of solutions that are not only service-oriented but also strategically aligned. Excelling in business and system analysis, due diligence, and technical evaluations, Wojtek's skill set spans traditional, cloud, and cybersecurity architecture, while ensuring compliance with regulatory and security frameworks.

UNDERSTANDING CYBER TARGETS: SECTORS AT RISK

Cybersecurity is a vital component of the digital economy and society, especially for SMEs that represent 99% of all businesses in the EU (ENISA, n.d.). SMEs not only drive innovation but also fuel economic growth, underscoring the critical need for robust cybersecurity measures within this segment. At Numata, we recognise the diverse spectrum encompassed by the term 'SME,' where classification often hinges on the number of employees. Typically, small businesses are defined as those with fewer than 100 employees, while mid-size enterprises encompass organisations with 100 to 999 employees. Understanding these distinctions is pivotal in tailoring cybersecurity strategies that effectively address the unique challenges faced by SMEs across the spectrum.

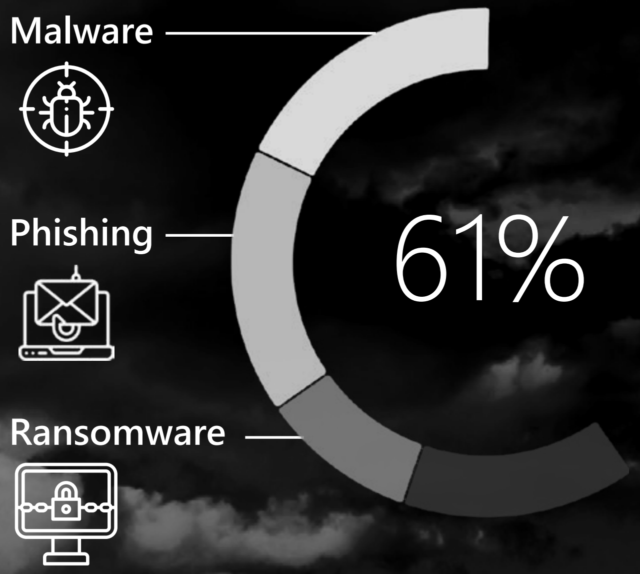
Key insights into industries most affected by breaches

In collaboration with a diverse panel of industry experts, Numata conducted a survey delving into the evolving landscape of cyber threats, examining changes, common incidents, and the industries most impacted. These responses, along with research reports, shed light on the strategies organisations implement to bolster their cyber resilience in the face of an ever-shifting digital threat landscape.

Cyber threat frequency and sophistication have escalated in recent years, with attackers targeting various sectors. According to survey responses, sectors providing human talent and technical services have been most targeted, including financial entities, healthcare providers, and manufacturing industries.

“Hackers tend to go for the weakest link simply because it’s easier. Businesses at risk usually lack effective cybersecurity protection and recovery plans,” says Paul Delahunty, Chief Information Security Officer at Stryve Secure.

A survey (StrongDM, n.d.) revealed that 61% of SMEs in the EMEA region were the target of a cyberattack in 2021. The most common types of cyberattacks aimed at SMEs were malware (18%), phishing (17%), and ransomware (10%). These attacks can have severe impacts. For example, 50% of SMEs reported it took 24 hours or longer to recover from an attack.



One of the main challenges for SMEs is the lack of awareness, particularly regarding their specific cyber risks, as well as resources to implement effective cybersecurity measures against these risks. Many SMEs don't have a dedicated cybersecurity budget, staff, or policy. Additionally, SMEs frequently collect and store sensitive customer data, such as credit card information, which could be compromised in the event of an attack.

In fact, 87% of SMEs have customer data that could be breached, and 27% have no cybersecurity protection to combat these breaches.

Another challenge is the increasing sophistication and frequency of cyberattacks, especially from state-sponsored actors and organised crime groups. These attackers often target the most vulnerable and valuable assets, including intellectual property, trade secrets, and customer data. In particular, CEOs and CFOs of SMEs are the most targeted by cybercriminals (Forbes, n.d.) as they have access to the most critical information and decision-making power. Adding to this complexity, the barrier to entry for cybercriminals has significantly decreased due to readily available tools and technologies that require minimal technical skill or capability. Criminals are now able to launch relatively sophisticated attacks with limited skills and experience. This democratisation of cybercrime tools is further exacerbated by models such as Phishing-as-a-Service and Malware-as-a-Service, making cybercrime more scalable and accessible.

> **"Cybersecurity is an essential part of modern business. You don't need to know how to do it yourself, but it does need to be done, and there are plenty of organisations out there who can help without costing an arm and a leg. Remember, security is not a destination; it's a journey**
>
> -Paul Delahunty, CISO at Stryve Secure

Are SMEs at greater risk?

Reasons why cybercriminals target SMEs:

Low-hanging fruit: SMEs have lower budgets than large enterprises, which doesn't enable them to have all the defence mechanisms in place. SMEs have different maturity levels and don't always have access to mature cybersecurity levels.

Valuable data: Although all businesses have valuable databases, some SMEs don't deem their data valuable enough to invest in high-level cybersecurity systems.

Supply chain vulnerability: They may be electronically connected to the IT systems of larger and more secure organisations, and cybercriminals may exploit this to infiltrate these networks through weaker security.

Collateral damage: They may be affected by large-scale cyberattacks that have nothing to do with them, but exploit common vulnerabilities or software they use.

Cyberattacks are a serious and growing threat to all organisations, regardless of size, sector, or location. However, many SMEs are often more vulnerable and less prepared than others.

That's why it's critical to understand your cyber risk profile, implement effective and affordable cybersecurity solutions, and seek guidance and support to enhance your cybersecurity resilience.

As Paul suggests, "Do the basics right. If you do this, you will protect yourself from the vast majority of attacks."

> **SMEs are the best targets for threat actors. If a threat actor attacks them, SMEs typically feel the most helpless and victimised. As a result, they are willing to do anything to remediate the situation. If more SMEs knew this and could actively experience what other SMEs have, their willingness to improve cybersecurity would change for the better.**
>
> - Chris Loehr, CTO at Solis.

IDENTIFYING COMMON CYBER INCIDENTS SMES FACE

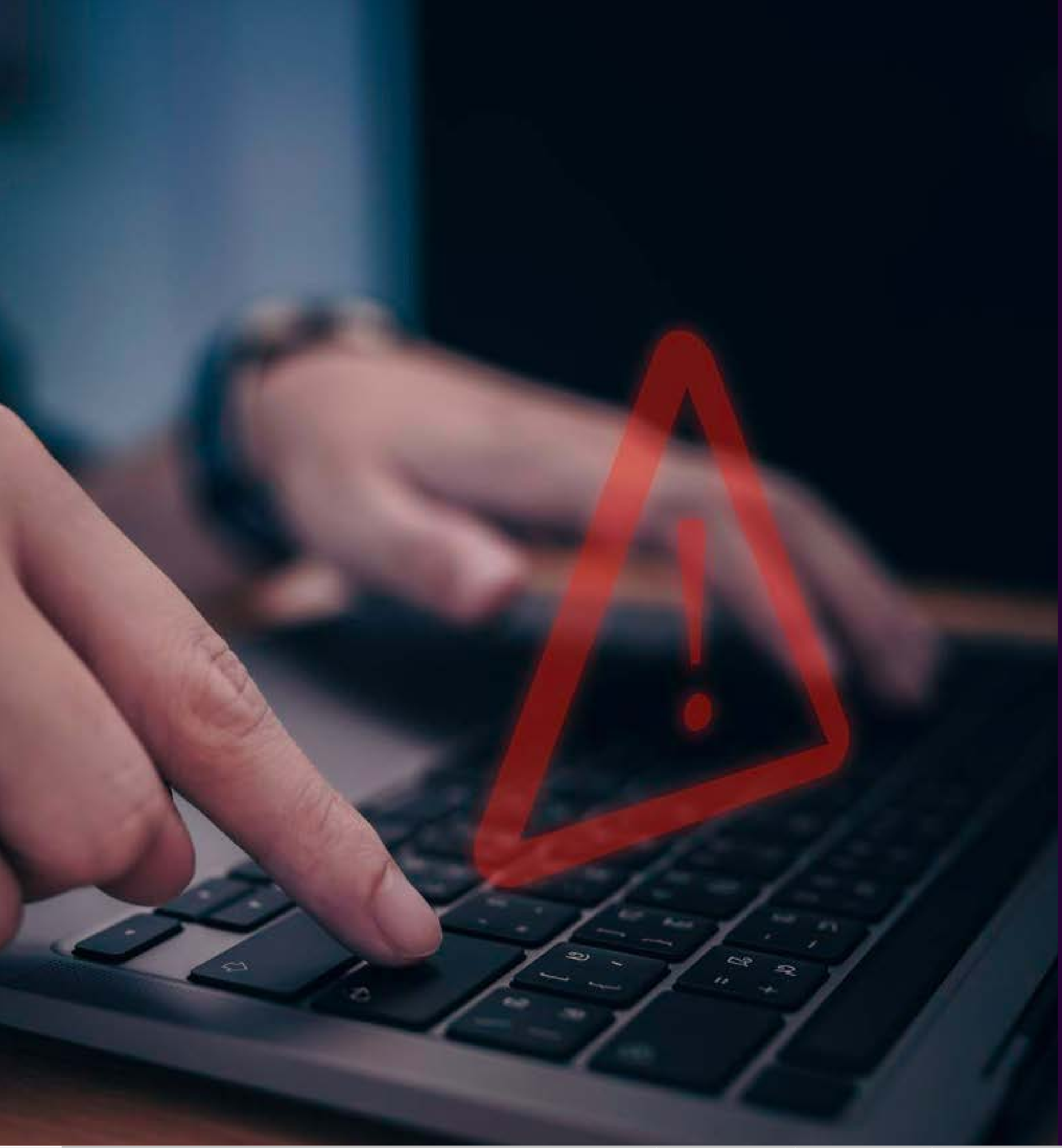
Cybersecurity is rapidly evolving, with new threats and vulnerabilities constantly emerging. While the nature of cyber incidents has shifted over time, certain types of attacks remain prevalent, posing even more risk to SMEs.

“According to ENISA, the top five SME cybersecurity incidents are phishing attacks, web-based attacks, general malware, malicious insiders, and denial of service. Any of these attacks have the potential to threaten business continuity, especially for SMEs with limited resources to withstand a prolonged attack,” says Paul Delahunty.

Phishing, for example, lures users into opening malicious emails or uses business email compromise (BEC) to hijack executives’ and financial employees’ email accounts into redirecting funds to fraudulent bank accounts, as well as accessing confidential information from the compromised mailboxes.

Most common cyber incidents

A cyber incident comprises any event compromising data integrity, confidentiality, or availability. These can range from malicious attacks by hackers, insiders, or state-sponsored actors to accidental incidents caused by human error or natural disasters. Repercussions of cyber incidents include financial loss, reputational damage, legal liability, and national security risks.



The most common types of cyberattacks include:

Distributed denial-of-service (DDoS): Flooding a website or server with a large amount of traffic, causing it to slow down or crash.

Insider threats: These attacks originate from within the organisation, either by a current or former employee, contractor, or partner. They could be motivated by financial gain, revenge, or espionage to leak sensitive information or sabotage the network infrastructure.

Domain Name System (DNS) spoofing: Modifying the DNS records of a website, redirecting users to a fake or malicious site.

Phishing and social engineering: Tricking or manipulating the victim into revealing information, clicking on malicious links, or downloading malicious attachments. Phishing and social engineering can be used to launch ransomware, data theft, identity based, or other types of attacks.

Person-in-the-middle (PiTM) / Man-in-the-middle (MiTM): Intercepting the communication between two parties, altering or stealing the data.

Ransomware: Encrypting the victim's files and/or stealing confidential data and demanding a ransom for the decryption key.

LINK BETWEEN IT & CYBERSECURITY STRATEGIES

There's a notable difference between an IT strategy and a cybersecurity strategy. An IT strategy defines how IT resources and capabilities support your company's mission, vision, and goals, whereas a cybersecurity strategy outlines the objectives, principles, and actions that ensure the security and resilience of your IT systems and data.

The two are interdependent and mutually reinforcing and should be integrated and coordinated to achieve optimal outcomes for your business.

CEO of Telspace Africa, Manuel Corregedor, stresses the importance of seeing them as two independent entities that need to be aligned, "I think the biggest problem is that most SMEs see cybersecurity as part of IT, but they are typically not aligned, especially when it comes to supporting business. Unfortunately, much like insurance, information security is perceived as a grudge purchase; something that doesn't add value or takes budget away from other business areas."

Misconceptions related to cybersecurity

Paul Delahunty believes too many SMEs regard the IT strategy as the cybersecurity strategy, saying, "While they absolutely need to be aligned – as they feed into each other and, in reality, all strategies within an organisation need to be aligned – they are separate strategies. Cybersecurity is not IT, and IT is not cybersecurity."

According to other survey responses, many business leaders still believe cybersecurity is:

- Too expensive
- Fearmongering
- Too burdensome for employees
- Introducing "bureaucracy" to time-efficient and cost-effective business processes
- Only necessary for larger businesses, under the misconception that cybercriminals won't target smaller businesses.

The importance of aligning IT and cybersecurity strategy:

Reduces complexity and costs

Contrary to misconception, there are many affordable ways for SMEs to integrate cybersecurity into their IT strategy. As cyber threats evolve, so do security measures, and modern technology is paving the way to make high-level solutions more accessible to SMEs.

It also avoids duplication, inconsistency, and inefficiency.

Overall, incorporating security into the design and development of IT systems and processes simplifies operations while lowering IT ownership and maintenance costs.

Enhances performance and productivity

By ensuring IT systems and services are secure, reliable, and available, you can improve your operational efficiency and efficacy, boosting customer satisfaction, loyalty, and, ultimately, your brand reputation.

More importantly, it significantly reduces the likelihood of a breach, directly affecting downtime and productivity.

Mitigates risks and impacts

Although breaches can still occur with cybersecurity measures in place, the chances are much lower than not having it at all. In fact, IBM's Cost of a Data Breach report (IBM, n.d.) states that businesses using threat intelligence identified breaches 28 days faster.

Furthermore, it may also help you comply with regulatory requirements and industry standards.

Interlacing key strategies company-wide

IT and cybersecurity strategies aren't merely technical and operational; they're business plans supporting your business's value creation and delivery. Wojtek Wierzycki emphasises that SMEs must recognise the distinct foundational requirements of IT and cybersecurity strategies, saying, "While both leverage technological components, a cybersecurity strategy is anchored in addressing cyber risks, be they standard or unique to the organisation. Conversely, an IT strategy is predominantly tailored to align the business strategy.

To a degree, I believe the appreciation and distinction of the two is more important than the alignment."

In essence, IT and cybersecurity strategies have everything to do with the business strategy. This is especially critical for organisations relying heavily on their IT infrastructure for smooth daily operations.

Wilmore Chininga, CISO of Island Networks, suggests working closely with the teams responsible for IT and business strategy. "These three teams should work together and develop a cybersecurity strategy to ensure alignment and, ultimately, successful strategy implementation," he says.

> **While both leverage technological components, a cybersecurity strategy is anchored in addressing cyber risks, be they standard or unique to the organisation. Conversely, an IT strategy is predominantly tailored to align the business strategy.**
>
> **To a degree, I believe the appreciation and distinction of the two is more important than the alignment.**
>
> -Wojtek Wierzycki, CISO and Head of Systems and Development at Sygnia

How to align cybersecurity and IT strategies

Start at the top: C-suite executives and board members should communicate cybersecurity's impact and value and how it supports the business's strategic objectives and priorities.

Focus on business outcomes: Don't worry about the technical details at first. Instead, use a plan that helps you make your cybersecurity strong, flexible, and fast. Your cybersecurity plan should match your business plan and deal with the problems and benefits of IT and cybersecurity.

Quantify and qualify risks and benefits: Use metrics and indicators to measure and demonstrate the performance and effectiveness of your cybersecurity solutions and how they contribute to business outcomes, such as innovation, efficiency, and compliance.

Foster a cybersecurity culture and awareness: Educate and train employees and customers about cybersecurity policies, standards, and guidelines, and how they can collaborate and contribute to the security and resilience of your IT infrastructure and services.

Aligning cybersecurity and IT strategies is vital for leveraging the benefits and mitigating the risks associated with technology. These two strategies aim to protect data and systems, ensure IT infrastructure security, and align with your business's broader goals and objectives.

To achieve this alignment, consider a holistic and collaborative approach to communicating cybersecurity's business impact, outcomes, risks, and benefits.

> **One way or another, cybersecurity will cost something to an organisation. It's better to put the cost towards protecting the business and helping it grow than paying for recovery and restoring business assets. The latter can never bring back business reputation.**
>
> -Wilmore Chininga, CISO at Island Networks

THE DIFFERENCE BETWEEN CYBER RESILIENCE FOR LARGE ENTERPRISES VERSUS SMALL BUSINESSES

> **There is no comparison. Smaller organisations can learn from doing the basics, like staff training and installing basic anti-virus software, encryption technology, and firewalls.**
>
> -Matthew Visser, Director at Moore Infinity

As a business leader, you want to ensure your organisation can withstand, recover from, and adapt to cyber threats. After all, they aren't going away any time soon. But cyber resilience isn't just about preventing cyberattacks but about minimising the impact and restoring operations as quickly as possible.

Fact of the matter is, cyber resilience is critical for any organisation that relies on digital systems and data, regardless of its size or sector.

However, these strategies may differ between large enterprises and SMEs, depending on your resources, capabilities, and needs.

Paul Delahunty believes that, although larger organisations have more resources for cyber resilience, SMEs should still prioritise it. "Larger organisations have more resources, both in finance and people. However, while SMEs can't compete on resources, they can take cybersecurity and resilience just as seriously. Most large businesses have security and resilience as a standing item at the board level. There is no reason SMEs cannot do the same," he says.

Matthew Visser, Director at Moore Infinity, doesn't think there is a difference between the two, saying, "There is no comparison. Smaller organisations can learn from doing the basics, like staff training and installing basic anti-virus software, encryption technology, and firewalls."

Key differences in cyber resilience measures

Cyber resilience measures, like security teams, tools, policies, and procedures, are essential for organisations of any size. However, the nature of implementation and the challenges faced can differ significantly between large enterprises and SMEs. Large enterprises often benefit from greater resources and expertise, yet they must navigate more complex and diverse IT environments. In contrast, while SMEs may contend with limitations in resources and expertise, it is important to acknowledge that their smaller scale can result in fewer assets requiring protection. This aspect potentially reduces their exposure and risks compared to larger counterparts.

Main challenges and risks SMEs face include:

Awareness and skills gap: SMEs need to know more about cyber threats and how to prevent them while upskilling themselves to manage and maintain their security measures.

Compliance and governance issues: It’s critical for SMEs to follow data and privacy laws and regulations, develop clear policies and procedures, and monitor and improve their cyber resilience.

Support and collaboration: Large enterprises often have more support from stakeholders who are just as serious about cybersecurity as they are. SMEs should tap into external help and cooperation from their customers, suppliers, partners, and regulators to improve their cybersecurity resilience measures and reduce costs and risks.

> **It is easy to get intimidated by regulations, but once you digest the regulations and accept them as part of your everyday requirements, it gets a lot easier.**
>
> -Chris Loehr, CTO at Solis

What SMEs can learn from large enterprises

A paper published on “Building SMEs’ resilience in times of uncertainty: the role of big data analytics capability and co-innovation”, (Ciasullo, 2022) analysed 192 big-data SMEs in Europe and found that only 28.6% are equipped to adapt to changing and uncertain environments.

In Wilmore Chininga’s experience, big companies recognise the importance of implementing cybersecurity measures because they have seen and experienced the financial and reputational costs caused by these incidents.

“The lack of proper cybersecurity strategies often prevents the SME from growing into a larger organisation. It’s a double-edged sword; treating cybersecurity as a hurdle to your growth results in it becoming a hurdle that prevents it from growing.”

Despite the differences in budget and resources, SMEs can learn key lessons from large enterprises. Paul Delahunty suggests:

» Developing a cybersecurity culture from the top down

» Providing training and awareness to employees

» Conducting backups and testing them

» Developing an incident response plan and practising it

» Securing access to systems

» Securing devices and networks

» Improving physical security

» Managing your third parties

“

SMEs should learn from larger organisations and implement cybersecurity from the very start, as it can get too costly to implement after it has evolved from an SME to a larger business.

The lack of proper cybersecurity strategies often becomes a hurdle preventing the SME from growing into a larger organisation. It’s a double-edged sword; treating cybersecurity as a hurdle to your growth results in it becoming a hurdle that prevents it from growing.

- Wilmore Chininga, Infrastructure and cybersecurity consultant at Island Networks

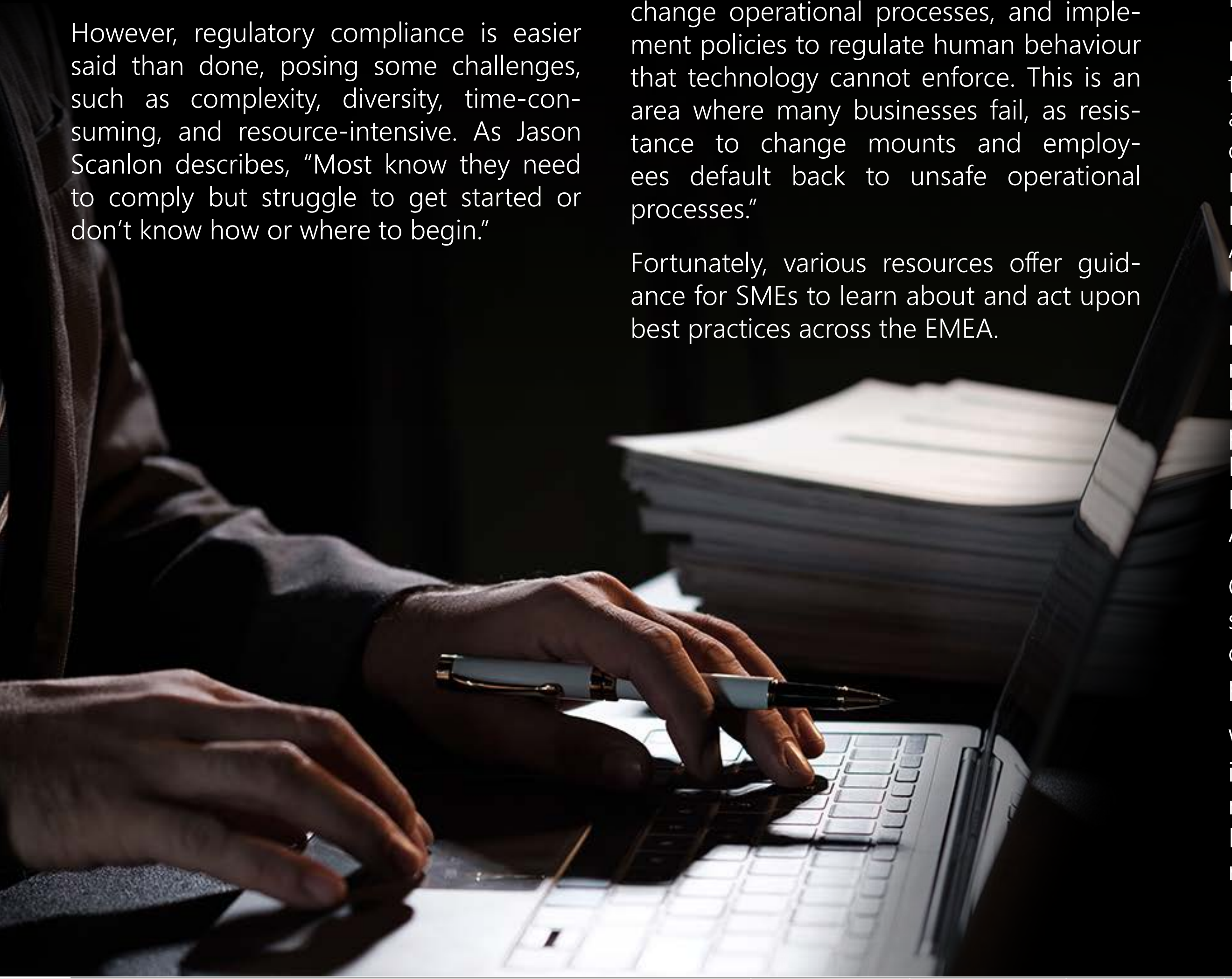
The role of regulatory compliance in building resilience

Regulatory compliance plays a vital role in building cybersecurity resilience. It can help you protect your assets, operations, and stakeholders from cyber threats while ensuring you achieve your business goals.

However, regulatory compliance is easier said than done, posing some challenges, such as complexity, diversity, time-consuming, and resource-intensive. As Jason Scanlon describes, "Most know they need to comply but struggle to get started or don't know how or where to begin."

Wilmore Chininga believes the most significant compliance challenge SMEs face is resistance to change. He explains, "To achieve regulatory compliance, an organisation has to raise its security baseline, change operational processes, and implement policies to regulate human behaviour that technology cannot enforce. This is an area where many businesses fail, as resistance to change mounts and employees default back to unsafe operational processes."

Fortunately, various resources offer guidance for SMEs to learn about and act upon best practices across the EMEA.



These include:

Cybersecurity frameworks: Recommendations and best practices that help businesses implement and improve their cybersecurity measures. Although they aren't mandatory, they can help SMEs align with industry standards and comply with legal obligations. Examples include the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the Center for Internet Security® Critical Security Controls (CIS Controls).

Data privacy laws: Legal mandates that regulate how organisations collect, process, store, and share personal data. These laws aim to protect the rights and interests of data subjects and impose obligations and responsibilities on data controllers and processors. Examples include the General Data Protection Regulation (GDPR) in Europe, the Protection of Personal Information Act (POPIA) in South Africa, and the Personal Data Protection Law (PDPL) in the Middle East.

Regulatory compliance: The process of adhering to the laws and regulations that apply to a specific industry or activity. This ensures businesses operate legally, ethically, and safely while avoiding fines, penalties, or legal actions. Examples include the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act (SOX).

Cyber resilience is vital for your business, regardless of size and sector. Not only does it help you withstand and recover from cyber threats, but it also helps you to adapt and evolve to modern practices.

While large enterprises may have more resources and expertise to invest in these measures, you can still learn from them and implement effective processes – even with limited staff and budgets. In addition, regulatory compliance also has a hand in building resilience.

PREDICTIONS FOR THE YEAR AHEAD

Cybersecurity is a dynamic and evolving domain requiring constant vigilance and adaptation. As we look ahead to 2024, we can expect to see more challenges and opportunities for businesses in the EMEA region. However, by understanding and anticipating future trends and threats, we can prepare and protect ourselves and our digital assets and build a safer and more resilient digital society.

The tactics we saw in 2023 will remain relevant in 2024. The tried, tested, and trusted approaches are still the best defence against known cyberattack tactics. And although it's too early to tell, DORA, NIS v2, and the newer NIST CSF v2 will hopefully impact the cybersecurity landscape. At the same time, there will be a greater focus on governance. One significant challenge that will only grow bigger over time is the evolution of cyber threats and artificial intelligence (AI). Paul Delahunty explains, "Phishing is more complex and harder to spot, and ransomware continues to evolve. However, AI is the most notable development for SMEs. It's still unclear how this will develop over the coming months and years, but AI can potentially make the landscape a lot more threatening."

In fact, according to John O Mahony, EMEA regions are experiencing the highest number of cyber incidents this year than ever before, stressing that the issue continues to rise.

Wojtek Wierzycki believes the evolution of threats within EMEA region largely mirrors global trends, saying:

> **Threat actors appear to have adopted a more indiscriminate approach, casting the net much wider regardless of the target. The ascendancy of ransomware and ransomware-as-a-service accentuates this shift and the emergence of layered ransomware strategies. This is not just encryption but rather threatening to release information.**
>
> -Wojtek Wierzycki, CISO and Head of Systems and Development at Sygnia

Forecasting the cybersecurity landscape for 2024

Artificial intelligence (AI) and machine learning (ML)

AI and ML are transforming the cybersecurity landscape for attackers and defenders. Although it can enhance cybersecurity capabilities and efficiency through detection, response, and automation, it also enables attackers to create more sophisticated and stealthier cyberattacks using AI to generate malware, evade detection, and impersonate targets.

According to Google Cloud's Cybersecurity Forecast 2024 (Cloud, n.d.) attackers will likely incorporate AI into their operations, while defenders will use it to strengthen detection and response. The report also predicts that AI will be used to create more realistic and convincing phishing and social engineering campaigns while automating zero-day vulnerability exploits.

To combat this, Chris Loehr suggests educating yourself and your staff: "This does not mean attending extremely technical courses, but interacting with peer organisations and experts who can educate you on cybersecurity in business risk terms."

Weaponised deepfake technology and phishing attacks

Check Point's Cybersecurity Predictions for 2024 (Point, 2023) predicts that weaponised deepfake technology and phishing attacks will increase and pose serious threats to both businesses and individuals. This attack involves using AI and ML to manipulate or generate audio, video, or image content that looks realistic and convincing but is unauthentic.

Although it can be used for various purposes, including entertainment, education, and research, cybercriminals can create fake news, propaganda, and blackmail.

Deepfake technology can also enhance the effectiveness and credibility of phishing and social engineering attacks, such as impersonating targets or their contacts and tricking them into revealing their credentials or transferring money.

Check Point's report also foresees that deepfake technology will create more convincing and personalised phishing campaigns using voice cloning, face swapping, and video synthesis.

Supply chain and critical infrastructure attacks

These attacks are becoming more prevalent and disruptive because attackers tend to target weak links and dependencies in the digital ecosystem. Supply chain attacks involve compromising trusted software and hardware vendors or service providers. During critical infrastructure attacks, cybercriminals disrupt the essential services and systems supporting society and the economy.

Defending against targeted attacks in 2024

As the cybersecurity landscape evolves, businesses must remain vigilant and adapt to new threats. AI and ML are revolutionising the field, enhancing cybersecurity measures while also empowering attackers with tools for crafting more advanced attacks.

Wojtek Wierzycki aptly summarises the evolving landscape: “While cybersecurity awareness is undeniably crucial in countering widespread attacks like phishing, it is often inadequate against targeted or persistent threats. The evolving landscape and widespread integration of AI will only magnify this, and AI-driven preventative technologies will be indispensable in mitigating such threats.”

Organisations must prioritise cybersecurity awareness and invest in preventative measures to safeguard their digital assets and build a safer and more resilient digital society.

PRACTICAL STEPS: WHAT'S NEXT?

1 Training

Implement regular cybersecurity awareness training

2 Frameworks

Start implementing an accessible framework like the CIS Controls then tailor your approach to fit your SME's needs. These can later align with broader frameworks such as NIST CSF.

3 Regulate

Review all legislative and regulatory compliance requirements relevant to your business.

4 Assess

Evaluate your current state against your chosen framework to understand your security posture. Then, create a roadmap for moving from the current to the future state, where all relevant controls are effectively implemented. Update it regularly as you progress in the journey.

5 Implement

Based on the findings from your assessment, implement the necessary people, process, and technology controls to mitigate any identified risks.

6 Monitor

Continuously monitor the effectiveness of your implemented controls. Annually re-assess measures (at a minimum).

CONCLUSION

As we navigate the cybersecurity ecosystem, it's critical to understand the common sectors and incidents posing the greatest threats to organisations across EMEA. By recognising these patterns, you can proactively implement robust cybersecurity strategies aligning with your IT infrastructure and adapt to the unique challenges facing SMEs and enterprises.

Looking ahead to 2024, it's crucial to stay cautious against emerging threats and embrace innovative solutions to safeguard your valuable assets in the digital era.

REFERENCES

(ENISA), T. E. (n.d.). SME Cybersecurity. Retrieved from enisa.europa.eu: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity

Ciasullo, M. M. (2022, March 11). Building SMEs' resilience in times of uncertainty: the role of big data analytics capability and co-innovation. Transforming Goverment: People, Process and Policy, 16(2). Retrieved from https://www.emerald.com/insight/content/doi/10.1108/TG-07-2021-0120/full/html

CIO. (n.d.). State of the CIO 2022 Focus turns to IT fundamentals. Retrieved from CIO.com: https://www.cio.com/article/306384/state-of-the-cio-2022-focus-turns-to-it-fundamentals.html

Cloud, G. (n.d.). Cloud Google. Retrieved from Cybersecurity Forecast 2024: https://cloud.google.com/resources/security/cybersecurity-forecast

Cost of a Data Breach Report. (n.d.). Retrieved from IBM: https://www.ibm.com/reports/data-breach

Cyber Framework. (n.d.). Retrieved from NIST: https://www.nist.gov/cyberframework/framework

Forbes. (n.d.). Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report. Retrieved from Forbes.com: https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=4a8624b452ae

Into the Cyber Abyss: Check Point's Riveting 2024 Predictions Reveal a Storm of AI, Hacktivism, and Weaponized Deepfakes. (n.d.). Retrieved from Check Point: https://blog.checkpoint.com/artificial-intelligence/into-the-cyber-abyss-check-points-riveting-2024-predictions-reveal-a-storm-of-ai-hacktivism-and-weaponized-deepfakes/#:~:text=Check%20Point%27s%2-0cybersecurity%20predictions%20for,deepfake%20technology%2

StrongDM. (n.d.). 35 Alarming Small Business Cybersecurity Statistics for 2024. Retrieved from strongdm.com: https://www.strongdm.com/blog/small-business-cyber-security-statistics#small-business-cybersecurity-overview

ABOUT NUMATA

Numata is a leading global business technology services and solutions provider for SMEs, with offices in the United Kingdom, Ireland and South Africa. As Business Technology Strategists for SMEs, we are passionate about positioning business and technology to enable SMEs to thrive. Our motivation has remained consistent since Numata was formed in 2004: to give SMEs access to world-class technology strategy, advice and services to solve business problems, manage technology risk, and ensure employees are supported, protected, and productive – wherever they are.

From a seamless switching process to endless support, our mission is to help your business become more scalable, agile, secure, and competitive.

Get in touch today!

numata.co
UK: +44 20 3890 5455
SA:+27 87 2310 311
IE: +353 1 223 2296
Email: info@numata.co

NUMATA™