FUNDAMENTALS OF THE FUTURE

HLB CYBERSECURITY REPORT 2024

HLB

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

CONTENTS

INTRODUCTION	3
DATA HIGHLIGHTS	4
FOCUSING ON THE FUNDAMENTALS	5
DEVELOPING CYBER RESILIENCE IN REAL-TIME	6
MANAGING CYBERSECURITY RISKS FROM THIRD-PARTY VENDORS	7
CASE STUDY: FROM ASSESSMENT TO DEPLOYMENT WITH BRICKWORKS	9
THE DUAL ROLE OF AI	10
THE VITAL NATURE OF PROTECTING YOUR DATA	12
TRANSFORMING FROM REACTIVE TO PROACTIVE CYBERSECURITY	14
CYBER FUNDAMENTALS OF THE FUTURE: ASSESS YOUR READINESS	16
HOW HLB CAN HELP	17
RESEARCH METHODOLOGY	18
ACKNOWLEDGMENTS	18

INTRODUCTION

In a world increasingly shaped by digital transformation, understanding the ever-evolving landscape of cybersecurity is crucial for business leaders and decision-makers. Emerging cyber threats call for more proactive measures within organisations to combat risks before incident. In the wake of a series of major outages throughout 2024, bolstering cybersecurity defences remains a strategic imperative for business as professionals face an increasing number of sophisticated attacks.

In September 2024, we surveyed over 600 senior IT professionals via an online questionnaire about the main cybersecurity threats of today, their progress in implementing cyber strategies and the dual role of AI. The fifth edition of HLB's cybersecurity report provides a snapshot of the current cyber-threat landscape and highlights the key actions leaders have taken since 2020 to become more cyber-resilient.

DATA HIGHLIGHTS

86%

expressed heightened concern over threats related to cybersecurity

64%

of those surveyed consider cybersecurity a major strategic priority

24%

of organisations run ongoing cybersecurity awareness training programs

FOCUSING ON THE FUNDAMENTALS

In an era where cybersecurity threats grow increasingly sophisticated, the importance of fundamental practices cannot be overstated. Since 2020, HLB International has been measuring global businesses' cyber readiness. Our latest insights reveal that many organisations face mounting pressures from cyber-attacks, with 39% reporting an increase over the past year. Yet, despite these threats, some organisations still overlook basic security measures, leaving themselves vulnerable to breaches.

Cyber hygiene is a key foundational aspect that can dramatically impact an organisation's security. Simple practices such as keeping software up to date, enforcing strong password policies, and using multi-factor authentication are essential. Yet, these measures are sometimes neglected in favour of more advanced, but not necessarily more effective, solutions.

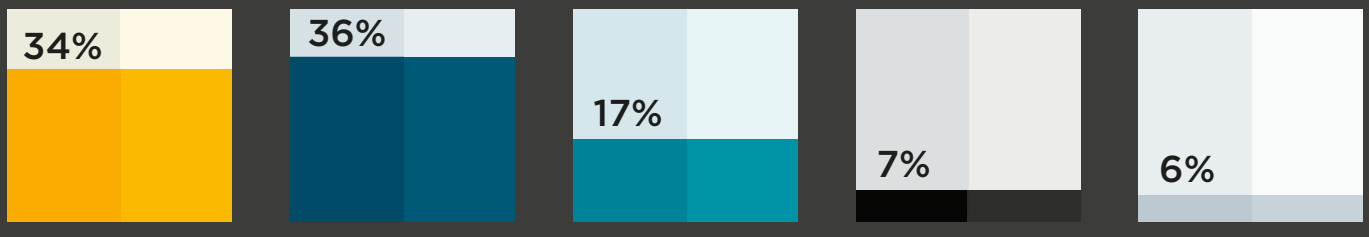
In 2024, 47% of our respondents identified email exploitation as a major threat, one which is evolving with the rapid developments of AI. Business leaders must prioritise the implementation of robust firewall rules and train employees to detect phishing attempts effectively. Despite 62% claiming that cybersecurity is a top priority, a concerning 30% of businesses only engage in staff audits annually or post-incident, illustrating a gap in proactive security measures.

"Our data demonstrates heightened concern over cybersecurity threats, and with good reason—92% have observed ongoing cyberattacks, and 38% report that these threats are escalating. Alarmingly though, while most businesses are conducting some form of cybersecurity training, for many this isn't happening frequently enough. It's crucial that training becomes a monthly practice, particularly as email exploitation remains a primary risk."

Jim Bourke | Technology and Advisory Services Leader, HLB Global

FIG.1: CURRENT LEVEL OF CYBER CONCERN

What is your current level of concern regarding cybersecurity threats to your company?



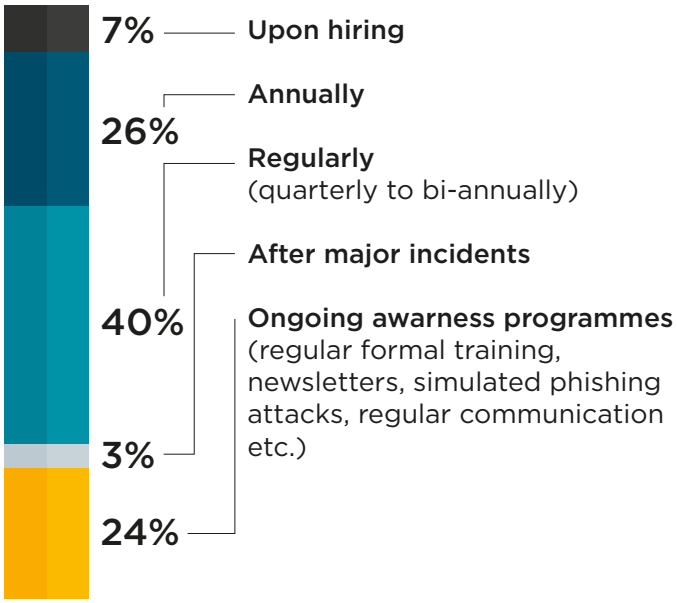
Investment in continuous employee awareness and training programmes is crucial. Organisations can significantly reduce their vulnerability by equipping staff with the knowledge to recognise and respond to potential threats. “We must consider that new employees are more vulnerable to attacks due to their lack of awareness.” Says Gustavo Solis, CEO at HLB Mexico.

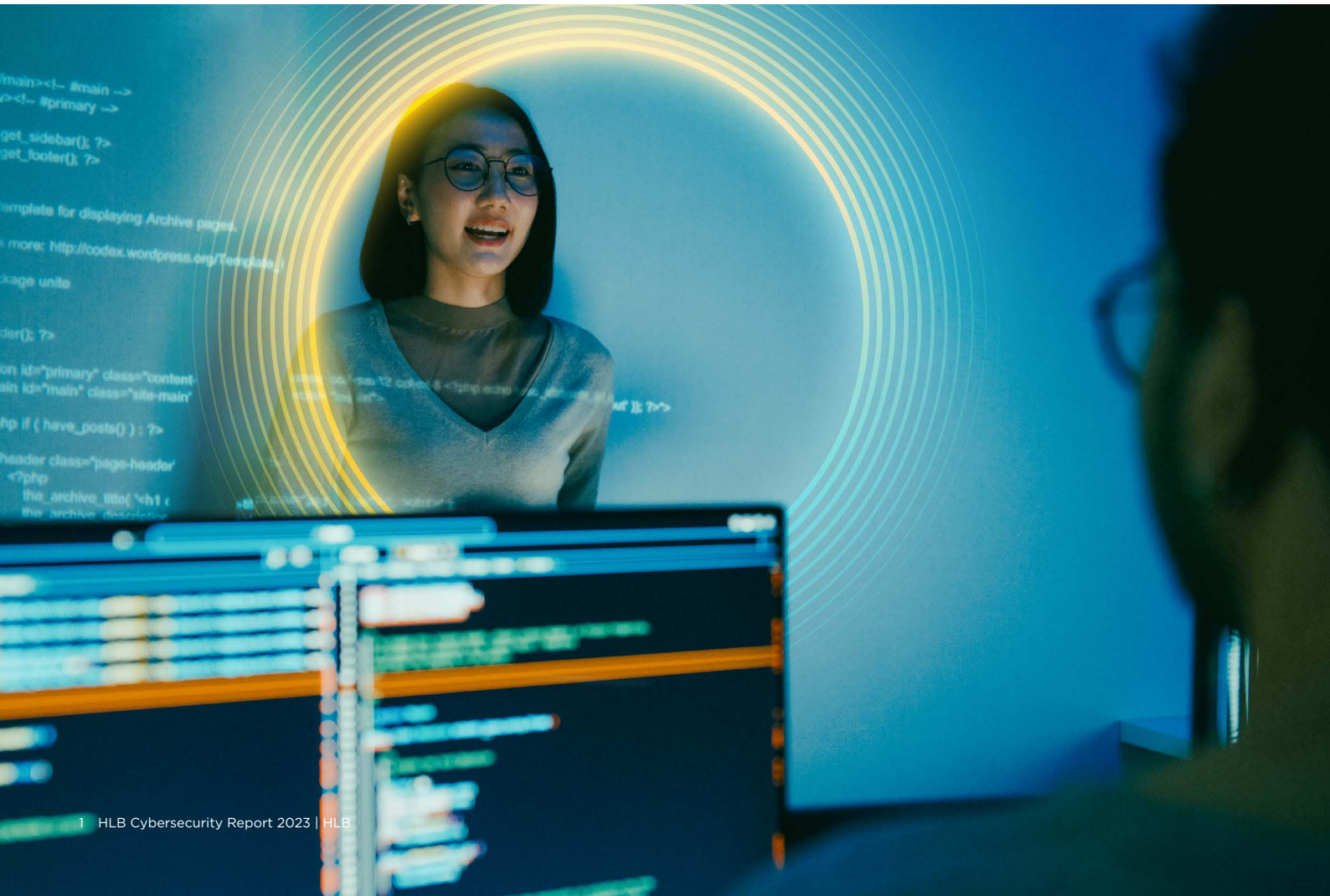
“Some of the major current cyber concerns are related to the human factor, for example social engineering, making cybersecurity training upon hiring alongside ongoing awareness programs an imperative.”

Organisations running ongoing awareness programmes increased four percentage points from last year’s HLB Cybersecurity Report[1] to 24%, indicating that the message for firms to adopt a more rigorous approach to cyber training is having an impact. This positive trend reflects the increased levels of importance business leaders are assigning to cybersecurity; by creating a culture of constant awareness, organisations are better positioned to face modern cyber threats.

FIG.2: CURRENT INVESTMENT LEVEL IN CYBERSECURITY TRAINING

How often does your company invest in cybersecurity training?





1 HLB Cybersecurity Report 2023 | HLB

DEVELOPING CYBER RESILIENCE IN REAL-TIME

Businesses face the reality of an increasing number of cyber threats that can have a major effect on operations and data security. Given the 71% rise in cyberattacks using stolen credentials[2], there's a clear need for organisations to develop and maintain their cyber resilience.

Cyber resilience refers to an organisation's ability to prepare for, respond to, and recover from cyberattacks, ensuring minimal disruption to operations and safeguarding data integrity. Our data reveals that an impressive 76% of organisations are confident in their ability to recover from cyberattacks quickly.

"There is still room for improvement; most companies know the risks and are taking cybersecurity seriously but could do more in terms of setting up stronger preventative measures from the outset, not waiting until the impact of cyber threats materialise to take action."

Pablo Kaplan | Managing Partner, HLB Argentina

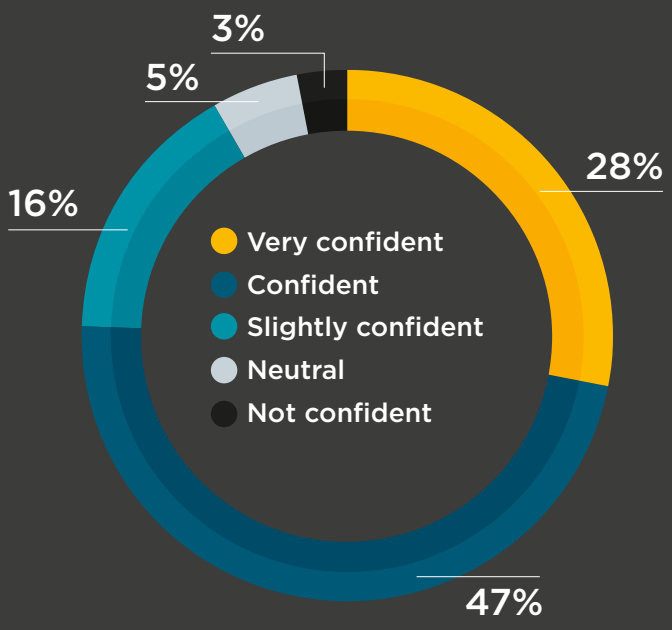
A crucial component of cyber resilience is the implementation of comprehensive and proactive strategies – such as e-learning, workshops and simulations – rather than relying on ad-hoc measures. This involves regular cybersecurity training, which 40% of organisations conduct quarterly or bi-annually, as well as maintaining up-to-date incident response plans, which according to our survey four in five companies already have in place.

Organisations must also adapt to the evolving threat landscape by integrating advanced technologies such as AI, while ensuring robust security and governance controls are in place.

With data theft and leaks accounting for a further 32% of incidents[3], a multifaceted approach to cybersecurity is essential.

FIG.3: CONFIDENCE IN RECOVERY FROM A CYBERATTACK

How confident are you in your company's ability to recover quickly from a cyberattack?



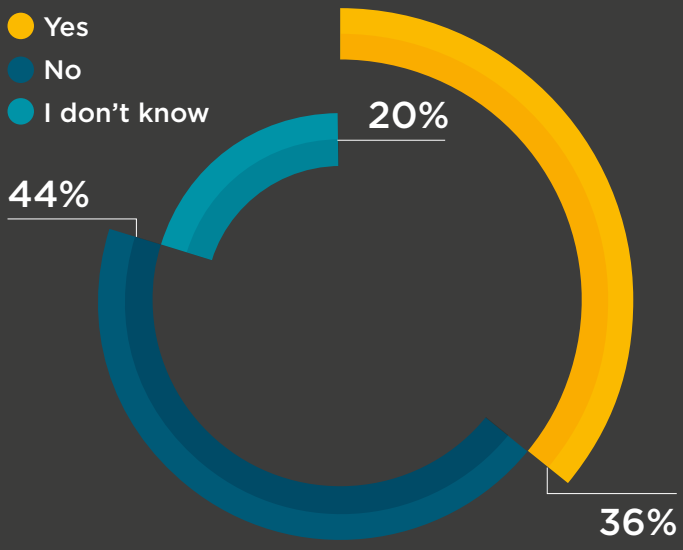
MANAGING CYBERSECURITY RISKS FROM THIRD-PARTY VENDORS

As the pace of technological developments continues to quicken, reliance on third-party vendors as essential hyper-focused experts is increasing, yet they can pose significant cybersecurity risks and misalignments in strategy if supplier research, selection and onboarding efforts are not managed correctly throughout.

Our survey reveals that 37% of organisations experienced a breach through a third-party vendor in the past year, while concerningly a further 20% are uncertain about their vendors' security status, emphasising the critical need for strong third-party risk management strategies.

FIG.4: THIRD-PARTY VENDORS AFFECTED BY BREACH IN 2024

Has one of your third-party vendors been affected by a cyber breach or security incident over the last 12 months?



Organisations increasingly rely on smaller vendors who may lack robust security measures, making them attractive targets for cybercriminals. These worries are well-founded, given the estimated $10.5 trillion cost of cyberattacks globally last year.[4]

"This (third-party vendor risk) is an often-overlooked area and is frequently associated with email exploitation and other attack vectors, leading to potentially critical impacts to business operations and reputations." adds Gareth Rees, Regional Executive at The Missing Link.

To mitigate these risks, businesses must implement comprehensive vendor management frameworks. Key steps include:

1. **Due Diligence:** Conduct thorough due diligence before onboarding any vendor, ensuring they meet your security standards. Evaluate their security posture through audits and assessments.

2. **Contractual Obligations:** Embed cybersecurity requirements in vendor contracts, mandating compliance with relevant regulations such as GDPR or NIS2. This ensures accountability and encourages vendors to maintain adequate security measures.

3. **Continuous Monitoring:** Implement continuous monitoring practices to assess vendors' security health over time. Automated tools can aid in detecting potential vulnerabilities and ensuring timely interventions.

4. **Incident Response Plans:** Develop and regularly update incident response plans that account for third-party risks. This equips organisations to respond swiftly and effectively in case of a breach.

4 The 10 Biggest Cyber Security Trends In 2024 Everyone Must Be Ready For Now (forbes.com)

CASE STUDY:

BRICKWORKS
BUILDING PRODUCTS

FROM ASSESSMENT TO DEPLOYMENT WITH BRICKWORKS

Brickworks Building Products is one of the world's largest and most diverse building material manufacturers, boasting over 90 years of experience. The company encompasses 17 brands, 45 manufacturing plants, over 2,000 products, and employs 2,500 staff worldwide.

Recognising the growing complexity of its business and the increasing number of suppliers, partners, and customers, Brickworks understood the necessity of enhancing its email security and cybersecurity awareness training. To achieve this, they partnered with The Missing Link, a company renowned for its innovative cybersecurity solutions and current HLB firm.

The Missing Link conducted a thorough assessment of Brickworks' current and future needs, connecting them with best-in-class providers. This collaboration resulted in the successful deployment of advanced email security solutions, significantly increasing protection from email and domain fraud, including business email compromise. With these solutions, Brickworks can now detect and stop both inbound and outbound email spoofing attacks and go beyond DMARC to expose fraud risks posed by their suppliers.

Brickworks' cybersecurity awareness training is also regularly reassessed, ensuring it remains effective and relevant. Real-world phishing simulations are utilised to train employees and identify risky users. By integrating data from Brickworks' email security solutions, they can pinpoint highly targeted personnel, providing them with specialised, focused training.

This comprehensive approach not only enhances Brickworks' cybersecurity posture but also offers governance committees and auditors tangible evidence of the company's commitment to cybersecurity.

THE DUAL ROLE OF AI

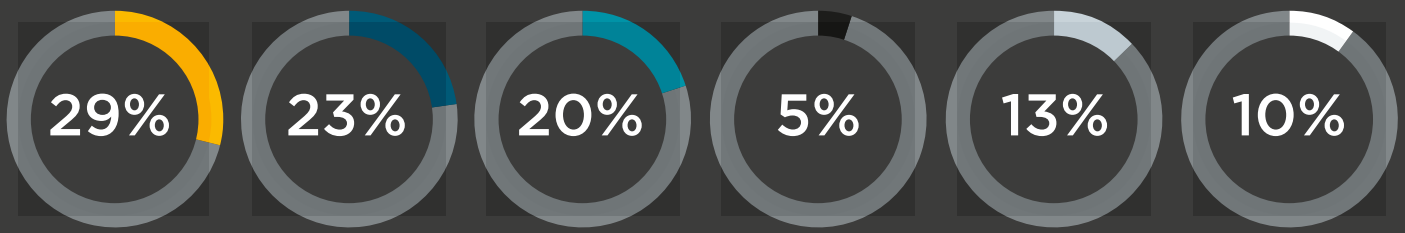
Artificial Intelligence (AI) stands as both a formidable ally and an unpredictable adversary. For IT professionals, cybersecurity experts and business leaders alike, understanding the role of AI is crucial for future-proofing their organisations.

AI is undeniably a powerful tool in enhancing cybersecurity measures. Its ability to quickly analyse vast datasets enables organisations to detect and respond to threats with unprecedented speed and accuracy. 29% of organisations surveyed have implemented additional security and governance controls when leveraging AI. These controls are designed to safeguard data integrity and protect against breaches, significantly strengthening defence frameworks.

However, AI's prowess is a double-edged sword. The same capabilities that enhance security can also be exploited by cybercriminals, leading to AI-driven attacks that are faster and more sophisticated than traditional methods. Alarmingly, we see that 28% of organisations either currently use or plan to use AI without proper controls in place, creating vulnerabilities that can easily be exploited.

FIG. 5: MAPPING ORGANISATION'S CURRENT USAGE AND PLANNED USAGE OF AI

Is your organisation currently leveraging, or planning to leverage within the next 12 months, transformative technology such as AI? If so, have you implemented, or will you be implementing, additional security and governance controls?



29%	23%	20%	5%	13%	10%
Yes, we are currently leveraging AI and have implemented additional security and governance controls	Yes, we are currently leveraging AI, but have not yet implemented additional security and governance controls	We plan to leverage AI within the next 12 months and will implement additional security and governance controls	We plan to leverage AI within the next 12 months, but have not yet implemented additional security and governance controls	We do not have any plans to leverage AI within the next 12 months	Not sure

The consequences of neglecting AI governance are severe. The potential for AI to be weaponised is heightened by its scalability and autonomous operations, posing a significant threat to data security. 29% have reported more severe consequences from cyber-attacks in the last 12 months, underscoring the urgency for comprehensive AI governance.

To mitigate these risks, firms should prioritise the development and implementation of robust AI governance frameworks, including establishing controls and oversight mechanisms to ensure the technology is used ethically and securely.

Companies should invest in regular audits and risk assessments, identifying potential vulnerabilities before they can be exploited by cyber criminals. Organisations must also focus on integrating AI with existing cybersecurity measures to detect and prevent AI-driven attacks more effectively.

By embedding this culture of accountability and proactive governance, firms can effectively harness the power of AI while minimising risks and protecting their data & systems from sophisticated and highly impactful attacks.

THE VITAL NATURE OF PROTECTING YOUR DATA

Safeguarding data through durable mechanisms such as encryption and data classification is not just advisable – it's vital. The growing sophistication of cyber threats has made data exfiltration a prevalent risk, capable of inflicting severe reputational damage to companies.

Encryption remains a pivotal tool, transforming sensitive information into indecipherable code that can only be unlocked by authorised parties, therefore providing a formidable barrier against unauthorised access. Data classification is another critical component, enabling organisations to identify and categorise data based on its sensitivity and value.

"With many new measures, frameworks and other ley legislations emerging from regulatory bodies globally, the need for clear organisational governance with regards to data protection and cybersecurity compliance has never been greater."

Mark Butler | Managing Partner, HLB Ireland

Regulatory compliance further accentuates the importance of data protection. The General Data Protection Regulation (GDPR), among other emerging regulations such as NIS2 and CMMC, has elevated the accountability of Chief Information Security Officers (CISOs) and executives, enforcing stringent data protection standards and imposing hefty penalties for non-compliance. The World Economic Forum (WEF) Cybersecurity Outlook 2024 reiterates this, highlighting the role of effective regulations in enhancing cyber resilience.[5]

FIG.6: HOW ORGANISATIONS COMPLY WITH CURRENT REGULATIONS

How does your organisation comply with current cybersecurity regulations relevant to your industry (e.g. GDPR, NIS2, DORA, CMMC)?

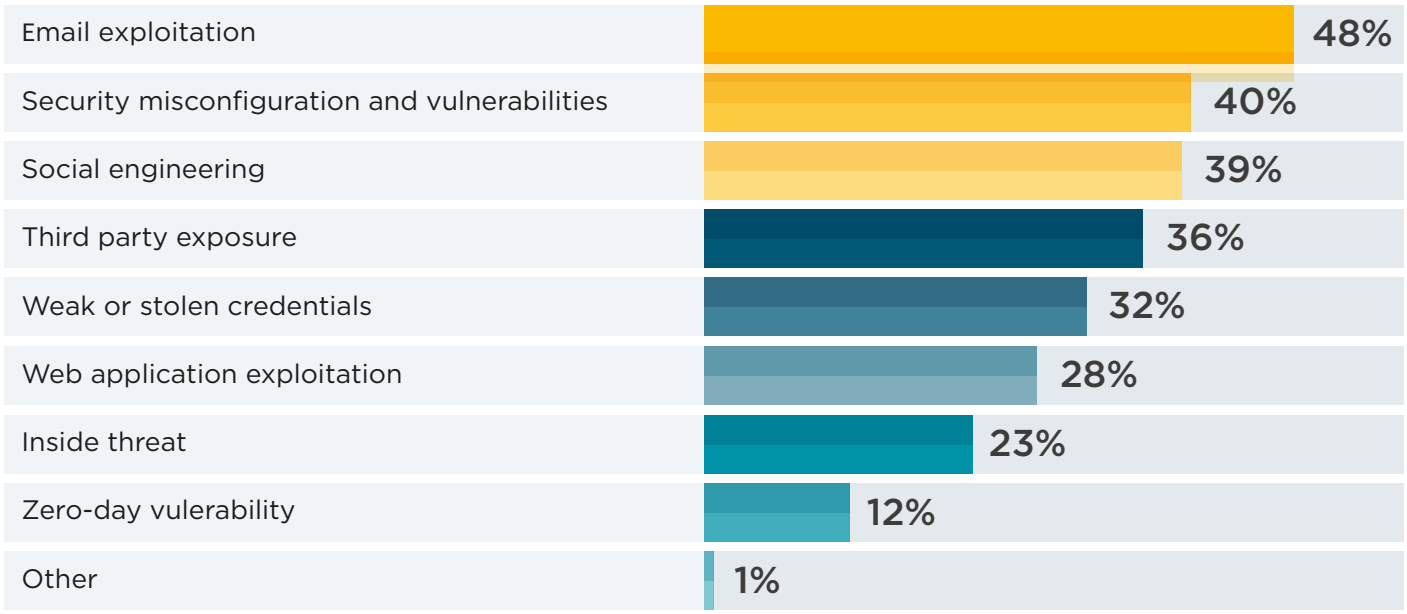
44%	**28%**	**13%**	**4%**
We have a dedicated team responsible for ensuring full compliance with all relevant regulations	We have implemented automated tools and systems to manage and monitor compliance	We have basic measures in place but are working towards full compliance	We are currently not compliant with the relevant cybersecurity regulations
5%	**2%**	**0%**	**4%**
We conduct regular audits and assessments to ensure compliance with cybersecurity regulations	We rely on external consultants or third-party services to maintain compliance	We are aware of the regulations but have not yet fully implemented compliance measures	We are not sure what cybersecurity regulations are applicable to our company

5 Global Cybersecurity Outlook 2024 | World Economic Forum (weforum.org)

By prioritising the protection of high-risk data, companies can allocate resources more efficiently and respond swiftly to potential threats. An impressive 44% of organisations now have a dedicated team in place, responsible for ensuring full compliance with relevant regulations, while a further 28% conduct regular audits and assessments.

Continuing on this path is critical to minimising certain key cyber threats, such as security misconfigurations (identified by 40% as one of the most prevalent risks in 2024) and weak or stolen credentials (identified by 32%).

FIG.7: WHICH CYBER THREATS DO YOU FEEL YOUR ORGANISATION IS MOST AT RISK FROM



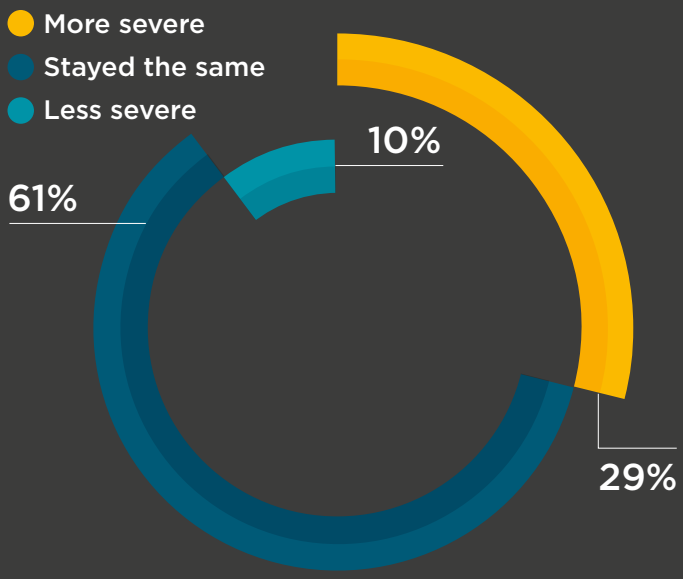
TRANSFORMING FROM REACTIVE TO PROACTIVE CYBERSECURITY

The shift to proactive cybersecurity measures is essential. 97% of companies acknowledged the necessity to increase their cybersecurity budgets in 2024[6], reflecting a collective awareness of the growing digital threats.

While 39% of organisations reported an increase in cyber-attacks over the past 12 months, 61% stated that the severity of these attacks stayed the same. This relative stability indicates that many organisations possess the foundational resilience required to withstand immediate threats. However, true security isn't about surviving attacks; it's about anticipating and preventing them.

FIG.8: CONSEQUENCES OF CYBER-ATTACKS OVER THE PAST 12 MONTHS

Have the consequences of cyber-attacks against your organisation been more severe, less severe, or stayed the same over the past 12 months?



A proactive approach entails identifying potential vulnerabilities before they are exploited, a practice that can significantly reduce the likelihood of severe consequences.

80% of organisations already have a defined incident response plan in place, with an additional 12% in the process designing one. This preparedness indicates a solid foundation upon which to build proactive strategies. By integrating risk-based vulnerability management, IT professionals can prioritise threats based on their potential impact, allowing for resources to be allocated in a more focused fashion. Meanwhile, attack surface management provides a comprehensive overview of all potential entry points, enabling organisations to fortify weak spots before they are targeted.

The transition to proactive security is supported by our data, which reveals that 63% of organisations have already prioritised cybersecurity within their strategic discussions. This commitment shows a broader trend towards not just reacting to incidents, but anticipating and neutralising threats before they materialise.

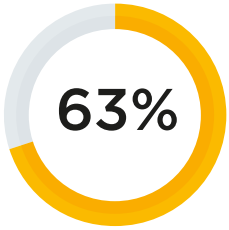
"Whilst many businesses prioritise cybersecurity within their strategic framework, and a significant portion believe they possess the technical, human, and financial resources to combat these challenges, a lower number have confidence in a swift recovery post-attack. This discrepancy highlights the need for organisations to continually reassess their readiness, especially as AI developments accelerate globally."

Jim Bourke | Technology and Advisory Leader, HLB Global

Moving towards proactive security is a strategic need. By adopting forward-thinking strategies, organisations can not only defend against current threats but also position themselves as leaders in cybersecurity resilience. This proactive stance will ultimately empower businesses to stay ahead in the cyber race, preserving both data and reputation.

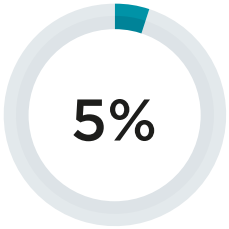
TO WHAT EXTENT IS CYBERSECURITY AN ORGANISATIONAL PRIORITY

To what extent is cybersecurity a priority in your organisation's overall strategy.

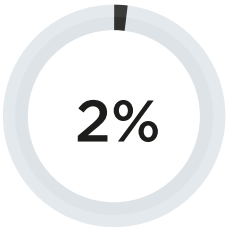


It is a top priorty with regular discussions

It is important but discussed occasionally



It is addressed only when issues arise



It is not a significant focus

CYBER FUNDAMENTALS OF THE FUTURE: ASSESS YOUR READINESS

In an era where cybersecurity threats evolve at an unprecedented pace, businesses must continually adapt their strategies to stay ahead. Understanding, implementing and future-proofing the fundamentals of cybersecurity is crucial to safeguarding organisational assets.

There are a number of recommendations we can derive from our data:

By focusing on these fundamental areas of cyber defence, organisations can remain resilient against future threats. When business leaders understand the cyber landscape and encourage methods of continuous assessment and adaptation, organisations can create an environment where security is embedded into every facet of the business.

HOW HLB CAN HELP

Cybersecurity is a lifecycle process, requiring ongoing diligence and investment. Training and technology isn't a one-time investment, nor enough to ensure ongoing resilience. The best cybersecurity programmes focus on achieving long-term impacts.

HLB's cybersecurity professionals can help you prioritise risks, assess your systems, and implement necessary changes to safeguard your organisation. Reach out to us today.

OUR SERVICES

CYBER RISKS CONSULTING

- STANDARDS COMPLIANCE GAP ANALYSIS
- RISK ASSESSMENT
- SECURITY MATURITY ASSESSMENT
- CYBERSECURITY STRATEGY

SOC AS A SERVICE

- MONITORING OF SECURITY EVENTS
- INCIDENT RESPONSE
- COMPUTER FORENSICS
- THREAT HUNTING

CYBERDRILLS

- ASSESSMENT OF INCIDENT RESPONSE

CAPABILITIES

- ASSESSMENT OF CYBER RESILIENCE
- NATIONAL CYBERDRILLS

TECHNICAL SECURITY ASSESSMENTS

- VULNERABILITY ASSESSMENT
- PENETRATION TESTING
- SOURCE CODE REVIEW
- RED TEAM EXERCISES

MANAGED SECURITY

- INTERNAL AUDITS
- THREAT INTELLIGENCE
- TECHNOLOGY MANAGEMENT & SUPPORT
- SECURITY AWARENESS

RESEARCH METHODOLOGY

In September 2024, HLB collected over 600 survey responses from Global IT leaders from a range of industry backgrounds. Responses were collected via an online survey tool. In addition, case study email exchanges have been conducted to collect data from external subject matter experts.

Note that not all figures in this report sum up to 100% as a result of rounding percentages, excluding neutral responses or when respondents could choose more than one answer.

ACKNOWLEDGMENTS

Abu Bakkar
Jim Bourke
Mark Butler
Rita Carolan
Martin Ellis
Toby Henness
Pablo Kaplan
Edward Keck Jr
Yusuf Malik
Gareth Rees
Michael Rooney
Gustavo Solis
Amy Spillard
Nicola Verespejova
Susannah Waters

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

HLB International Limited, registered in England & Wales No. 02181222, registered office: Lynton House 7-12, Tavistock Square, London, WC1H 9LT.