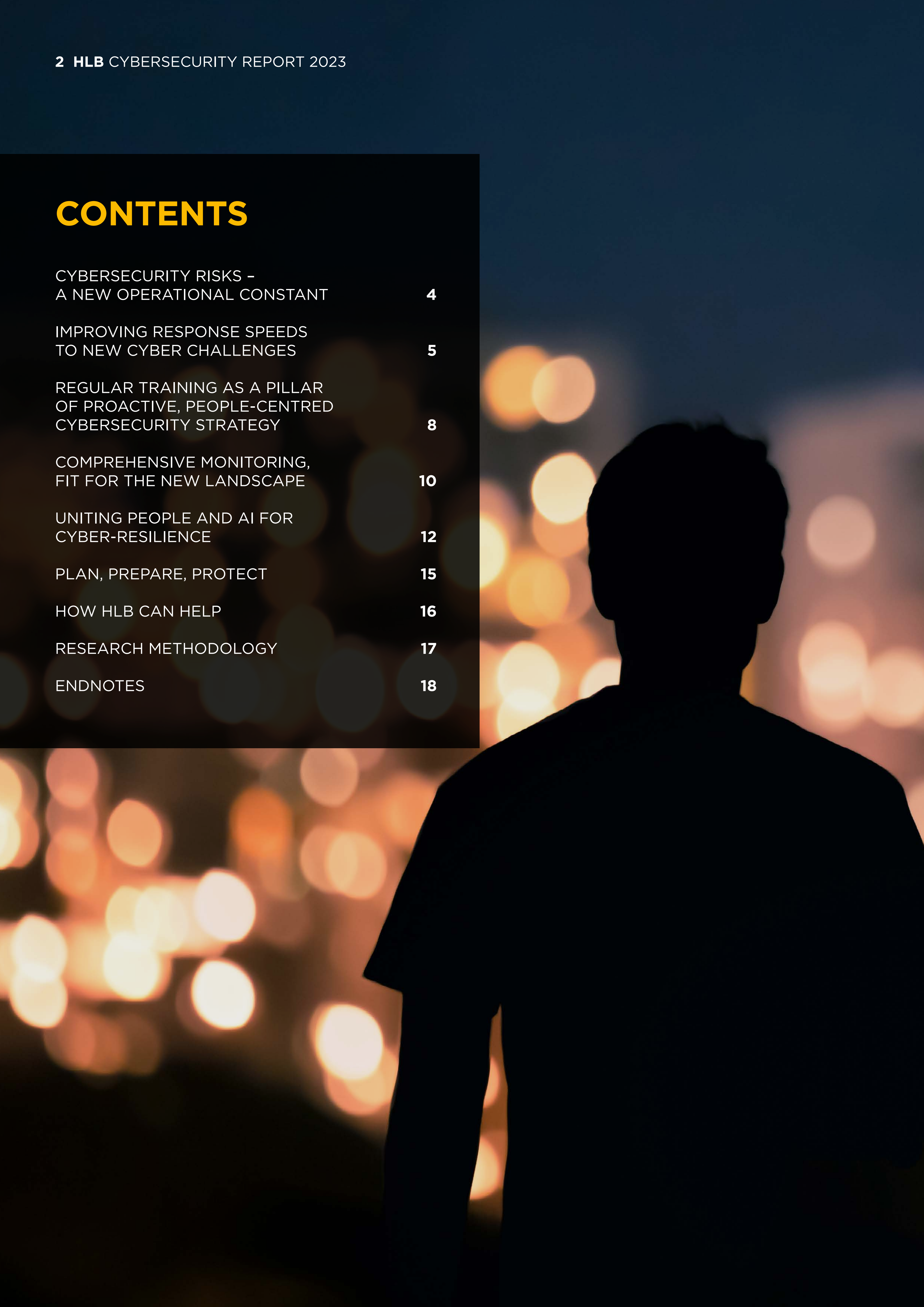
UNITING PEOPLE AND AI: THE FUTURE OF CYBER RESILIENCE

HLB CYBERSECURITY REPORT 2023

HLB
THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

www.hlb.global

TOGETHER WE MAKE IT HAPPEN



CONTENTS

Although IT leaders have already taken proactive steps to secure remote workers and implement better protection against persisting cyber threats, new challenges are on the horizon. The frequency, velocity, and sophistication of cyber-attacks continue to increase as organisations and their cyber adversaries embrace artificial intelligence (AI) technologies.

In August 2023, we surveyed 750 senior IT professionals via an online questionnaire about their progress in implementing better security measures and preparing for novel threats. The fourth 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 cyber-resilient.

CYBERSECURITY RISKS – A NEW OPERATIONAL CONSTANT

In cybersecurity, we're never "fighting the last war". Since 2020, HLB has been measuring global businesses' exposure to cyber threats. Although IT leaders have made significant progress in improving their security posture, there's still more work left to do.

In 2023, 50% of business leaders saw an increase in cyber-attacks, with another 35% saying the attack levels stayed the same as last year. That's 3 percentage points higher than in 2021, when 47% of business leaders reported an increase[1], although a slight cool-down compared to 2020, when 53% saw a spike in the number of cyber-attacks.

Cyber-attack frequency and sophistication continue to increase proportionally to organisations' digitisation efforts. Companies worldwide now face 1248 attacks per week[2] — and every organisation is a target. Since the start of the year, threat actors have successfully targeted public institutions (Metropolitan Police in the UK, French unemployment agency Pôle emploi, Indonesian Immigration Directorate General) and private businesses alike: US telecom companies, T-Mobile and AT&T; Australian Latitude Financial, Singapore-based retailer Cortina Holdings among others.

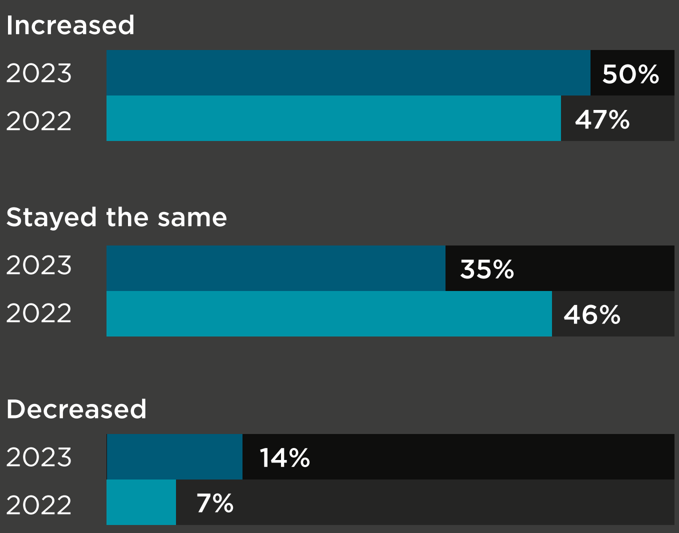
"A robust cybersecurity strategy includes three core principles: ongoing monitoring by experts who are fully up to date with the ever-changing threat landscape, the ability to respond to issues immediately to mitigate losses, and the establishment of comprehensive training and awareness programmes."

Mark Butler, Managing Partner, HLB Ireland

Democratisation of malicious software, the rapid pace of digital transformation, ongoing geopolitical conflicts, and economic uncertainty have created the perfect environment for perpetual cyber-threat upgrowth. In fact, 62% of leaders expect cybersecurity risks to become even more prominent in the five-year perspective, according to the 2023 global HLB survey of business leaders[3].

Cyber risk exposure is persistent. To ensure long-term protection, companies need to concentrate on the three pillars of cyber-resilience: rapid response, regular training and comprehensive monitoring.

FIG.1: CYBER-ATTACKS STILL ON THE RISE



IMPROVING RESPONSE SPEEDS TO NEW CYBER CHALLENGES

REMOTE AND HYBRID WORK AS MAIN CATALYSTS FOR CYBER-TRANSFORMATION

Cybersecurity has been the focal point of attention for business leaders since the transition to remote work began. From video conferencing apps to unprotected cloud storage locations, there have been few avenues cyber-criminals have not tried exploiting.

Although 57% of IT leaders admit to not having been initially prepared for the challenges of remote work, 88% managed to execute effective changes in their cybersecurity strategies and protocols in response to the pandemic[4]. From providing employees with access to virtual private networks (VPNs) and secure cloud data exchange tools to initiating regular cyber training, IT leaders mustered significant change in a short time.

By 2021, 44% of IT leaders said to have changed the tech infrastructure to be a zero-trust architecture, with another 44% indicating they have adopted some technology to support the new hybrid workforce.[5] In addition, leaders concentrated on promoting stronger cybersecurity awareness through regular training sessions. Over 57% of IT leaders we spoke to in 2021 implemented a “no exception” policy for the cybereducation of their staff[6].

In 2023, cybersecurity investments are bringing tangible dividends. 64% said that they see the positive impacts in the form of easier implementation of their cybersecurity education strategy, higher overall awareness, and decreased risks.

“Although the attack volume has increased, so did the overall cyber awareness levels. Thanks to remote work, employees now understand more about security and feel more empowered.”

Anurag Sharma, Partner and Market leader, System and Process Assurance services, Withum.

FIG.2: MAJORITY OF IT PROFESSIONALS THINK THAT REMOTE WORKING HAS HAD A POSITIVE IMPACT ON BUSINESSES

How do you feel the new world of remote working has impacted your cybersecurity intelligence/education strategy and overall employee awareness?

10%	26%	64%
No impact	**Negative impact** Increased risks, harder to implement our cybersecurity education strategy, awareness has decreased	**Positive impact** Decreased risks, easier to implement our cybersecurity education strategy, awareness has increased

RAISING CYBERSECURITY MATURITY LEVELS

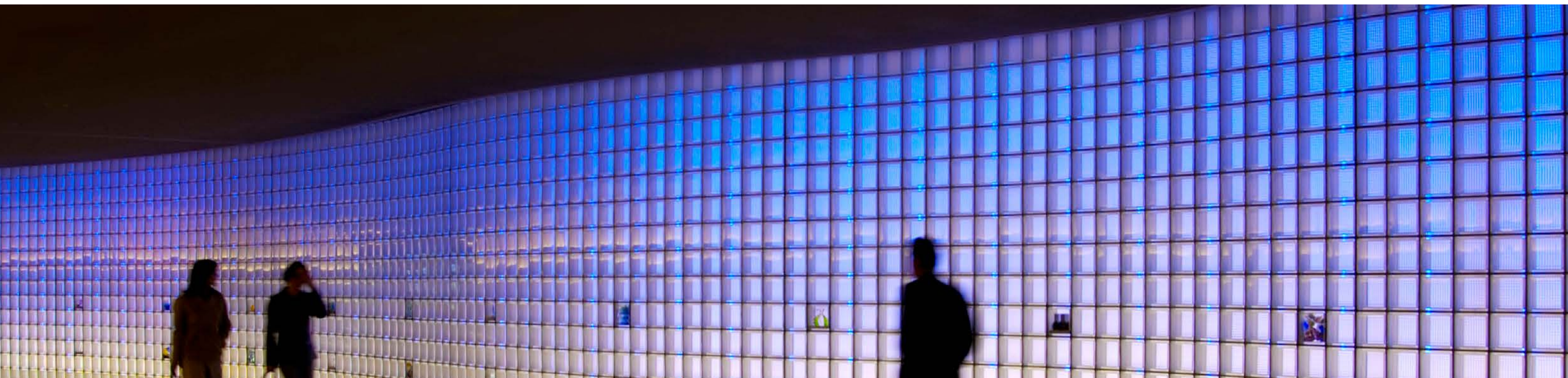
The majority of leaders have positively rated their progress with cybersecurity. However, a quarter of organisations also saw the negative impacts of remote work on security, citing increased risks and challenges in implementing the right educational strategy.

A growing IT estate and a hybrid workforce require new processes and technology for cybersecurity management. To jump-start a new cybersecurity programme, initiate an audit of your current environment — an area where HLB professionals can help.

Many of the cloud-based digital workplace solutions come with built-in security controls and automated policy enforcement. Ensure that all recommended configurations are enacted. Evaluate your current security policies to understand whether they suit a hybrid operating model. Look into new IT security vendors, which offer ongoing threat monitoring solutions and data-driven recommendations for security posture improvement.

"In addition to the awareness campaigns, some security measures have been reinforced by companies to protect remote points, such as VPNs, antivirus software, and next-generation firewalls (NGFWs)", says Gustavo Solis, CEO, Cynthus. By combining employee training with targeted improvements in security technology, organisations can proactively mitigate threats, rather than reactively deal with the consequences of an attack.

"In addition to the awareness campaigns, some security measures have been reinforced by companies to protect remote points, such as VPNs, antivirus software, and next-generation firewalls (NGFWs)."
Gustavo Solis, CEO, Cynthus



CASE STUDY:

Fane Valley
Growing Better Together

FANE VALLEY USED REMOTE WORK AS AN OPPORTUNITY FOR CYBER-TRANSFORMATIONS

Fane Valley is one of Ireland's most progressive agricultural and food processing businesses. Being in the manufacturing and retail sector, the company faces unique industry compliance demands and must maintain high cybersecurity levels.

To establish a new cyber-security programme, Fane Valley opted for an audit first. "Our first step was to understand where the business was vulnerable, as given the scale of our business, we wanted to ensure we dealt with the most significant potential risks first", says spokesperson. The investigation helped the company set benchmarks for measuring its security posture and prioritise the most pressing security gaps, which could be then addressed in a structured manner.

> "We firmly believe in making cybersecurity a collective responsibility, encompassing everyone in our organisation — from leadership to the frontline employees. It has become part of the way we do things, and our team is a cornerstone of our defence."

This shift to remote work spurred a holistic revamp of their cybersecurity framework, with robust password policies, added user verification measures and anti-phishing training being implemented, alongside other tools and policies.

"We firmly believe in making cybersecurity a collective responsibility, encompassing everyone in our organisation — from leadership to the frontline employees. It has become part of the way we do things, and our team is a cornerstone of our defence," says company spokesperson.

For sustained protection, Fane Valley opted for a "Cyber-as-a-Service" offering, with an experienced team monitoring their IT estate, addressing potential vulnerabilities, and ensuring industry best practices implementation. This approach has allowed Fane Valley to achieve comprehensive, scalable protection, adapted to the changes in the team size, operational practices, and threat landscape.

REGULAR TRAINING AS A PILLAR OF PROACTIVE, PEOPLE-CENTRED CYBERSECURITY STRATEGY

CYBERSECURITY AND AWARENESS TRAINING IS NON-NEGOTIABLE

Ongoing digitisation efforts resulted in a larger IT portfolio and complex data landscape. Terabytes of information digitally change hands in a matter of seconds. Yet, data-driven operations come at the cost of heightened security risks, especially when your people don't fully comprehend their roles in the security processes.

As the adage goes, 'A chain is only as strong as its weakest link.' In this case, that link often happens to be an unwitting employee," says Mark Butler. A weak email password, a click to an unknown link, or a document uploaded to a non-secure storage location can be a lever for a cyber-criminal.

Last year, 95% of IT leaders agreed that changing human behaviour was the greatest barrier to a more secure cyber defence[7]. Indeed, the human factor can increase cybersecurity risks. Everyone makes mistakes, especially when working remotely. Penalizing people for security mistakes, however, will only result in further concealment, and workarounds, making cyber professionals' jobs even more difficult.

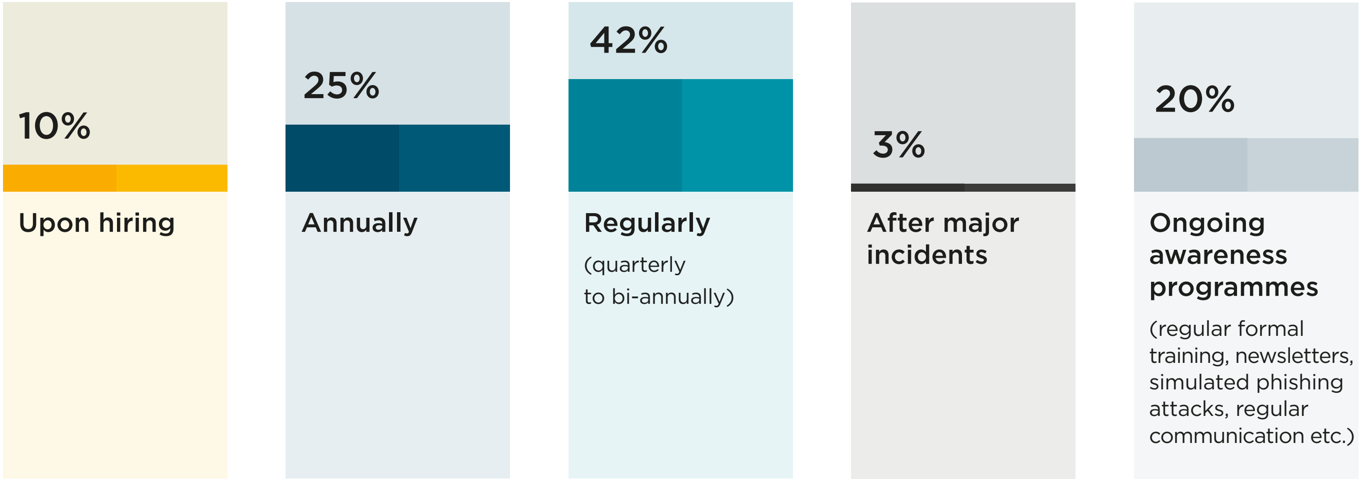
To cultivate a culture of high-security accountability, IT leaders should look into changing some of the core human behaviours through regular education and proactive coaching. Admirably, 87% of companies have some form of cyber training in place after hiring. However, only 18% have ongoing awareness programmes in place, which assume regular formal training, simulated phishing attacks, and regular communication. The majority of respondents (42%) invest in cyber-training quarterly or bi-annually and 25% – only once per year.

Jim Bourke, HLB Global Advisory Leader insists on a more regular occurrence. "I would recommend doing cyber training monthly and at a minimum quarterly". Regularity helps employees retain and update knowledge to keep up with the pace of evolving threats.

"I would recommend doing cyber training monthly and at a minimum quarterly."
Jim Bourke, HLB Global Advisory Leader

FIG.3: REGULAR INVESTING IN CYBERSECURITY TRAINING IS NOW THE NORM

How often does your company invest in cybersecurity training?



BUILDING AN EFFECTIVE CYBERSECURITY TRAINING PROGRAMME

Good cybersecurity training should be geared at emphasising the role of shared accountability, collaborative effort, and ongoing behaviour correction with the understanding of the importance of cybersecurity sitting at the heart of it.

“The quality of cybersecurity training is as important as its frequency. Tick-box security awareness drills don’t bring impactful results. Oftentimes, training programmes are designed in a way, where a user clicks a training spoof email and gets redirected to a training link, which they are forced to go through”, says Abu Bakkar, HLB Chief Innovation Officer. According to Bakkar, such training may have questionable long-term efficiency and doesn’t fully prepare users for emerging threats.

Quality cyber-training is aimed at changing the users’ perception and understanding of technology and the risks it carries, coupled with gentle nudges for improving their behaviours. Regular usage of strong passwords, secure data sharing, and timely risk reporting — such cornerstone actions create a strong culture of security. And, therefore, should be part of the regular drills.

When evaluating a new cyber-training programme, ask the following questions: Does it focus on behaviour correction? Is it adapted to your industry and type of operations? Does it account for newly emerged risks such as generative AI? “Companies should be continually evaluating the quality of their cybersecurity training programmes. Just to make sure that we’re keeping up with the pace that technology is advancing”, notes Jim Bourke.

By empowering teams with the knowledge and skills, organisations can substantially diminish the risks of breaches and data compromises. Investments made in cybersecurity education manifest as a long-term commitment to bolstering an organisation’s resilience and overall success.

> “The quality of cybersecurity training is as important as its frequency. Tick-box security awareness drills don’t bring impactful results. Oftentimes, training programmes are designed in a way, where a user clicks a training spoof email and gets redirected to a training link, which they are forced to go through.”
>
> Abu Bakkar, HLB Chief Innovation Officer

COMPREHENSIVE MONITORING, FIT FOR THE NEW LANDSCAPE

AI AS AN EMERGING THREAT ACTOR

Artificial intelligence (AI) has been making steady inroads into the company's operations, with 50% of leaders seeing AI as the most important technology to their businesses over the next 5 years[8]. However, when falling into the wrong hands, AI can also pose new security risks.

To carry out malicious activity, cyber-criminals are now using different artificial intelligence technologies such as machine learning, deep learning, large language learning models (LLMs), and generative adversarial networks (GANs). DeepFakes, AI-generated spear phishing emails, and autonomous, self-evolving botnets are just a few examples of the novel threats causing global concerns.

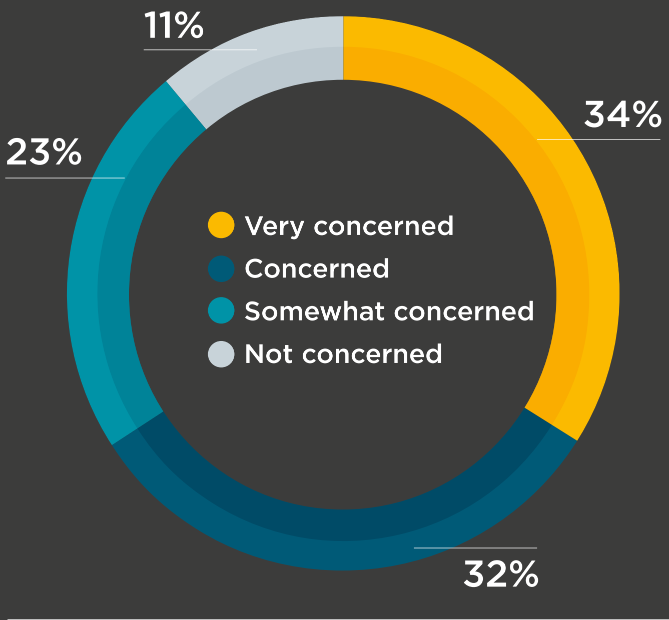
Despite the perceived novelty, AI attacks often borrow the underlying attack mechanics of traditional threats. "It still can be social engineering, for example.", explains Abu Bakkar. "But it's done with a new level of personalisation, scale, and speed".

Generative AI systems like ChatGPT can be effectively trained on public data, produced by your employees, to precisely mimic the tone of voice of the company's CEO in a phishing email. Or used to create bogus customer personas in baiting attacks. Recognising whether something is fake or real became harder because of AI.

Understandably, 89% of leaders are concerned with the current pace of technological innovation, particularly in generative AI, and the potential increase in cyber-related risk, of which 34% are very concerned.

FIG.4: IT PROFESSIONALS WORRY ABOUT THE CURRENT PACE OF TECH INNOVATIONS AND THE POTENTIAL INCREASE IN CYBER RISKS

To what extent are you concerned with the current pace of technological innovation, particularly in generative AI, and the potential increase in cyber related risk?



AI SOLUTIONS ALSO REQUIRE PROTECTION

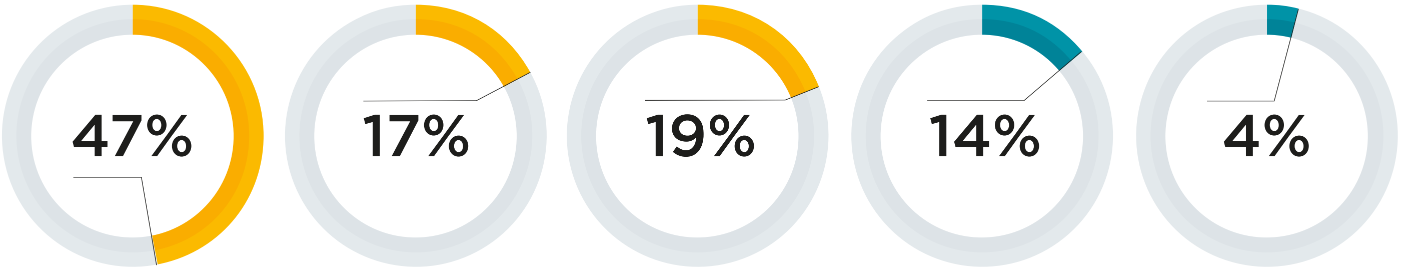
Collectively, we trust more and more decisions to AI — from lending request approvals to energy grid controls. Although rare at present, AI-targeted attacks can soon have visible real-world consequences in the form of disrupted road operations, fraudulent financing activity, or malfunctioning conveyor lines.

Poorly designed and operated AI systems can produce biased results, expose private data, or even deny service to legitimate users. Open-source generative AI models, used by employees, can also store private or sensitive corporate data that could breach privacy regulations. Google's AI Red Team also recently presented a set of tactics, techniques and procedures (TTPs), aimed at AI systems: Data poisoning, training data extraction, prompt injections, backdoor intrusion, adversarial attacks, and exfiltration[9]. Businesses designing and/or adopting AI solutions will need to adapt their cybersecurity processes to account for these new attack vectors.

At present, however, most organisations admit to not being fully prepared for AI threats. Over 50% of companies don't have sufficient deference strategies against AI attacks despite being concerned about their proliferation. The better news is that AI is a tool each side can use to their advantage.

FIG. 5: AI RELATED ATTACKS POSE A THREAT BUT IT PROFESSIONALS ARE READY FOR DEFENCE

Is your company concerned about AI-driven attacks and do you have corresponding defence strategies employed to counteract them?



We are concerned about AI-related attacks and we have corresponding defence strategies

We are concerned about AI-related attacks but we do not have corresponding defence strategies

We are concerned about AI-related attacks, we do not have corresponding defence strategies but we are currently investigating options

We are not concerned about AI-related attacks but we do have corresponding defence strategies

We are not concerned about AI-related attacks and we do not have corresponding defence strategies

UNITING PEOPLE AND AI FOR CYBER-RESILIENCE

AI not only empowers more sophisticated attacks but also helps cyber professionals and regular employees alike establish better defence mechanisms. By combining human intelligence with AI systems' large-scale data processing capabilities, businesses can stay one step ahead of attackers.

Cybersecurity is a data problem. Security analysts have to comb through a lot of security signals to understand their threat exposure. However, specialised staff is in short supply. Cyber-security talent shortages are a number of challenges for implementing better cyber-mitigation practices according to HLB's 2022 survey[10]. Machine learning solutions can act as a force multiplier, allowing human talent to capture, analyse, and act upon more data.

Although AI in cybersecurity is fairly new, it has already proven its efficacy. Intelligent algorithms can automatically scan through the entire technical estate to identify possible vulnerabilities, alert to anomalies, and proactively hunt threats. Supervised machine-learning algorithms can classify malignant email attacks with 98% accuracy[11]. A deep learning algorithm showcased 99.9% accuracy rates for network instruction detection[12].

Among the survey respondents, 100% are aware of the new AI-enabled security solutions, but only 30% have implemented at least one AI-enabled security tool in their environment. Another 36% are actively exploring such solutions.

Vendors like NVIDIA, IBM, and Microsoft among others have already released AI-powered cyber-security solutions for threat detection, endpoint security management, and IT infrastructure monitoring. Such platforms enable cyber professionals to maintain full visibility into the corporate environments, concentrate their attention on meaningful security signals, and respond faster to potential cyber threats.

47% of IT professionals are concerned about AI-related attacks and have implemented corresponding defence strategies.

FIG.6: LESS THAN A THIRD OF IT PROFESSIONALS HAVE IMPLEMENTED AI-ENABLED SECURITY TOOLS IN THEIR DEFENCE STRATEGY

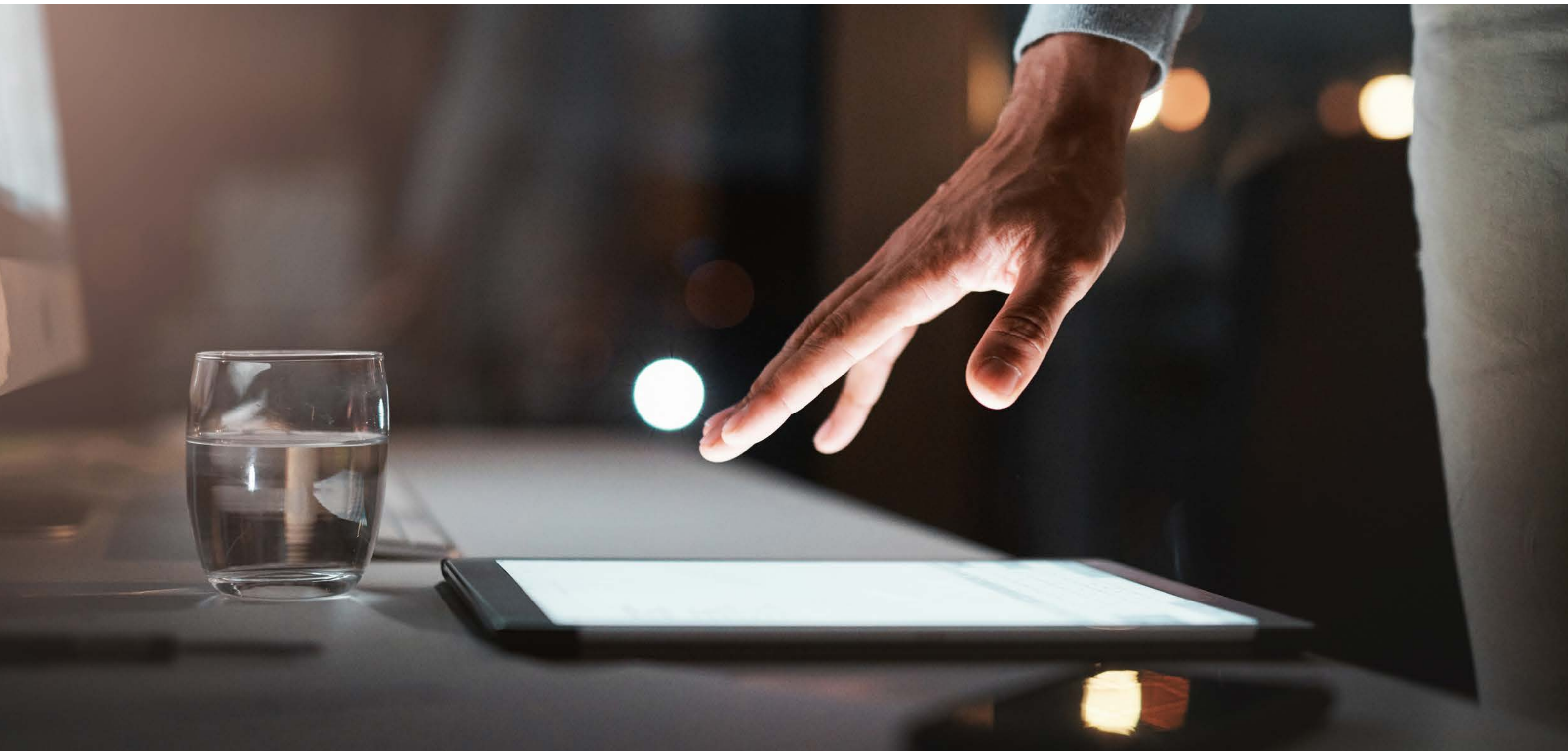
Is your company exploring use of any AI-enabled security tool as part of your overall defence strategy?

34%	36%	30%
We are aware of a variety of AI-enabled security tools in the market, however, we have not explored the option of deploying them in our environment	**We are actively exploring** AI-enabled security tools to deploy, however, we have not implemented any tool yet	**We have implemented** at least one AI-enabled security tool in our environment

Generative AI can also improve the user experience of cyber-security solutions, making them more accessible to senior and junior professionals alike. In March 2023, Microsoft released a Security Co-Pilot — an intelligent conversational assistant security professionals can use to fine-tune their defences. The assistant is trained on Microsoft's unique global threat intelligence and more than 65 trillion daily signals. Security Co-Pilot suggests improvements in system configurations, highlights inconsistencies in policies, and helps investigate cyber incidents alongside human analysts.

That said, it's important to not place unquestionable trust in AI. "We are happy to welcome advances in technology to protect us from our own careless or reckless behaviour and be 'off the hook,' since we can transfer the blame from human to AI error. To be sure, this is not a happy outcome for businesses, so the need to educate, alert, train, and manage human behaviour remains as important as ever, if not more so", says Dr Tomas Chamorro-Premuzic, Professor of Business Psychology at both University College London and Columbia University[13].

Organisations can achieve the best security outcomes by combining technological innovations with ongoing investments in people and processes.



CASE STUDY:

matillion

MATILLION RACES AHEAD TO ESTABLISH SECURITY AGAINST AI-DRIVEN THREATS

Matillion is The Data Productivity Cloud, enabling global businesses to design, deploy, and operate data solutions - making data business-ready faster. Trusted by the world's most progressive data-driven companies and Fortune 500 enterprises, Matillion must maintain exceptional standards of cybersecurity.

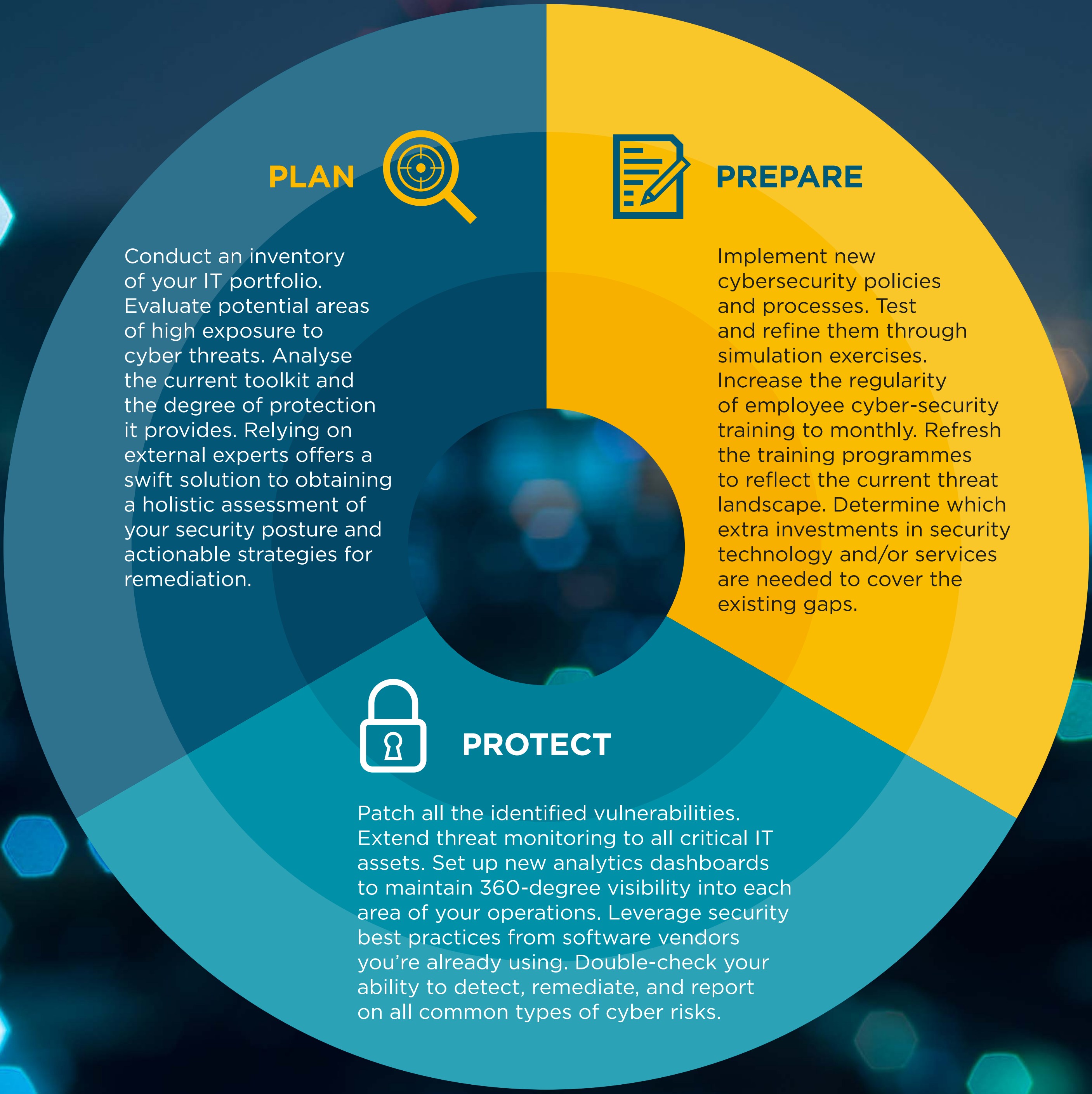
> "We've seen an uptick in quality phishing campaigns and know that malware is being generated through AI. AI lowers the barrier to entry and speeds up the skills of an attacker or adversary exponentially."
>
> Graeme Park, Chief Information Security Officer (CISO) Matillion

The team already leverages AI in the current security tooling and its team used generative AI to assist with building new security scripts at a faster pace. On the people front, Matillion runs continuous awareness programmes, based on short sharp videos. "These videos offer an engaging Netflix style series about security, covering topics such as DeepFakes and AI threats. In addition, we have regular communication from the security team to the wider business to explain near misses and other events of significance to keep security on top of the minds of our team", says Graeme Park.

PLAN, PREPARE, PROTECT

Developing a robust cyber-defence isn't a one-time affair – it's an ongoing exercise that evolves alongside the threat environment and your technology portfolio. Processes and solutions once deemed state-of-the-art lose efficacy over time. Regular commitment to auditing, optimising, and modernising corporate cybersecurity defence mechanisms is essential for long-term resilience.

There are three steps organisations can take to create a positive lifecycle of cyber-transformations:



PLAN

Conduct an inventory of your IT portfolio. Evaluate potential areas of high exposure to cyber threats. Analyse the current toolkit and the degree of protection it provides. Relying on external experts offers a swift solution to obtaining a holistic assessment of your security posture and actionable strategies for remediation.

PREPARE

Implement new cybersecurity policies and processes. Test and refine them through simulation exercises. Increase the regularity of employee cyber-security training to monthly. Refresh the training programmes to reflect the current threat landscape. Determine which extra investments in security technology and/or services are needed to cover the existing gaps.

PROTECT

Patch all the identified vulnerabilities. Extend threat monitoring to all critical IT assets. Set up new analytics dashboards to maintain 360-degree visibility into each area of your operations. Leverage security best practices from software vendors you're already using. Double-check your ability to detect, remediate, and report on all common types of cyber risks.

HOW HLB CAN HELP

Cybersecurity is a lifecycle process, recruiting ongoing diligence. Investing in new training and technology once isn't enough to ensure ongoing resilience. The best cybersecurity programmes focus on achieving long-term impacts: Better visibility into the operated environments, proactive threat mitigation, and outcome-driven employee training. HLB's cybersecurity professionals help organisations holistically evaluate their security posture and prioritise investments in the right areas, across the people-processes-technology axes. Reach out to us for an initial audit.

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

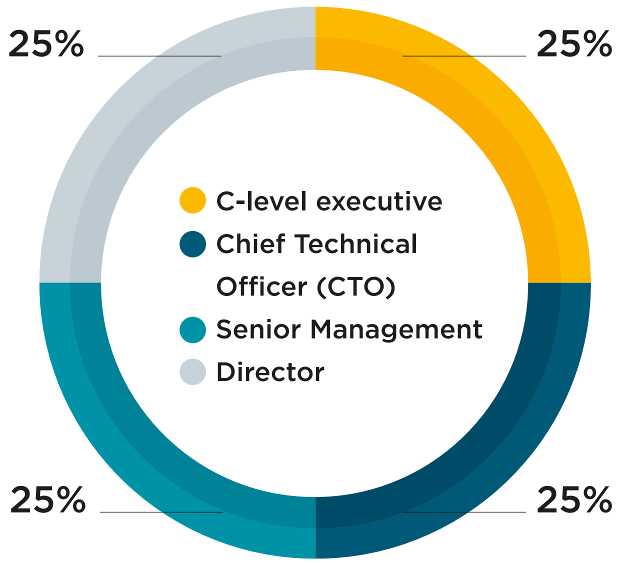
SECURITY AWARENESS

RESEARCH METHODOLOGY

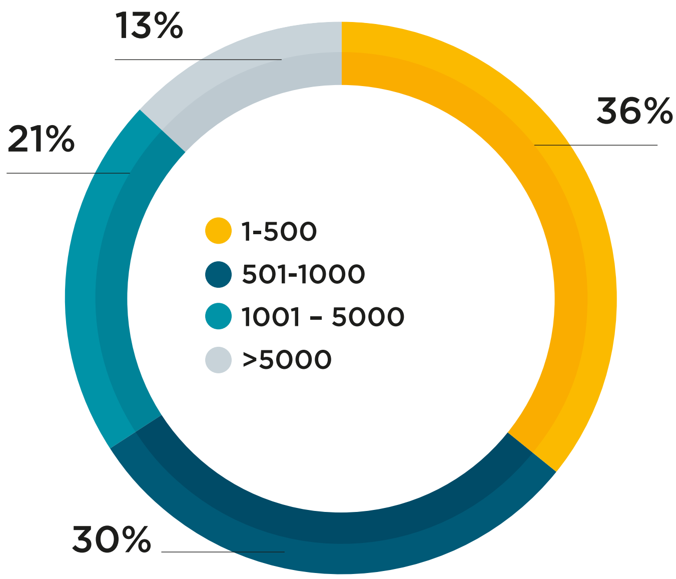
In August 2023, HLB collected 750 survey responses from IT leaders across four countries and a range of industry backgrounds. Responses were collected via an online survey tool. In addition, two case study email exchanges have been conducted to collect data from external subject matter experts.

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.

Respondents by title of employees



Company Size by the number of employees



ENDNOTES

1. HLB International, 2023. HLB Cybersecurity Report 2022: Hidden Risks in Cyber-Defence Laying a Foundation for Effective Cybersecurity Risk Mitigation

2. Check Point Software, 2023. 2023 Cyber Security Report

3. HLB International, 2023. HLB Survey of Business Leaders 2023: Leading Through a Perfect Storm

4. HLB International, 2023. HLB Cybersecurity Report 2020: Navigating the cyber-risk landscape in the age of remote working

5. HLB International, 2023. HLB Cybersecurity Report 2021: Addressing the cyber-risk landscape in the age of hybrid work

6. HLB International, 2023. HLB Cybersecurity Report 2021: Addressing the cyber-risk landscape in the age of hybrid work

7. HLB International, 2023. HLB Cybersecurity Report 2022: Hidden Risks in Cyber-Defence Laying a Foundation for Effective Cybersecurity Risk Mitigation

8. HLB International, 2023. HLB Survey of Business Leaders 2023: Leading Through a Perfect Storm

9. Google 2023. Why Red Teams Play a Central Role in Helping Organizations Secure AI Systems

10. HLB International, 2023. HLB Cybersecurity Report 2022: Hidden Risks in Cyber-Defence Laying a Foundation for Effective Cybersecurity Risk Mitigation

11. MDPI 2023. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model

12. IEEE Access 2023. A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection

13. HBR 2023. Human Error Drives Most Cyber Incidents. Could AI Help?

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

HLB THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

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

HLB International Limited is an English company limited by guarantee which co-ordinates the international activities of the HLB International network. HLB International is a global network of independent advisory and accounting firms, each of which is a separate and independent legal entity and as such has no liability for the acts and omissions of any other member. In no event will HLB International Limited be liable for the acts and/or omissions of any member of the HLB International network.