HIDDEN RISKS IN CYBER-DEFENCE: LAYING A FOUNDATION FOR EFFECTIVE CYBERSECURITY RISK MITIGATION

HLB CYBERSECURITY REPORT 2022

HLB THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

CONTENTS

CEOs worldwide face a broad and complex risk environment. Challenges appear at every turn, from supply chain disruptions to talent shortages. The rising costs of inflation and energy reverberate across operations as geopolitical tensions mount, like the war in Ukraine.

However, another threat is happening in real-time, and it's far less visible than other issues: Cyber-attacks. Indeed, 47% of respondents to our 2022 cybersecurity survey cited an increase in attacks against their organisations in the past twelve months. Yet, only 22% are fully prepared for an incident. Part of the problem lies in the sheer number and types of cyber-attacks. But, barriers to mitigating risks also impact readiness.

In September 2022, we surveyed 753 senior IT professionals via an online questionnaire about the challenges they face in today's cyber-risk landscape. In this report, we cover the top cybersecurity threats and offer recommendations for navigating them successfully. This report also contains a framework to help you enhance your security practices and ready your business for an attack.

THE INVISIBLE THREAT

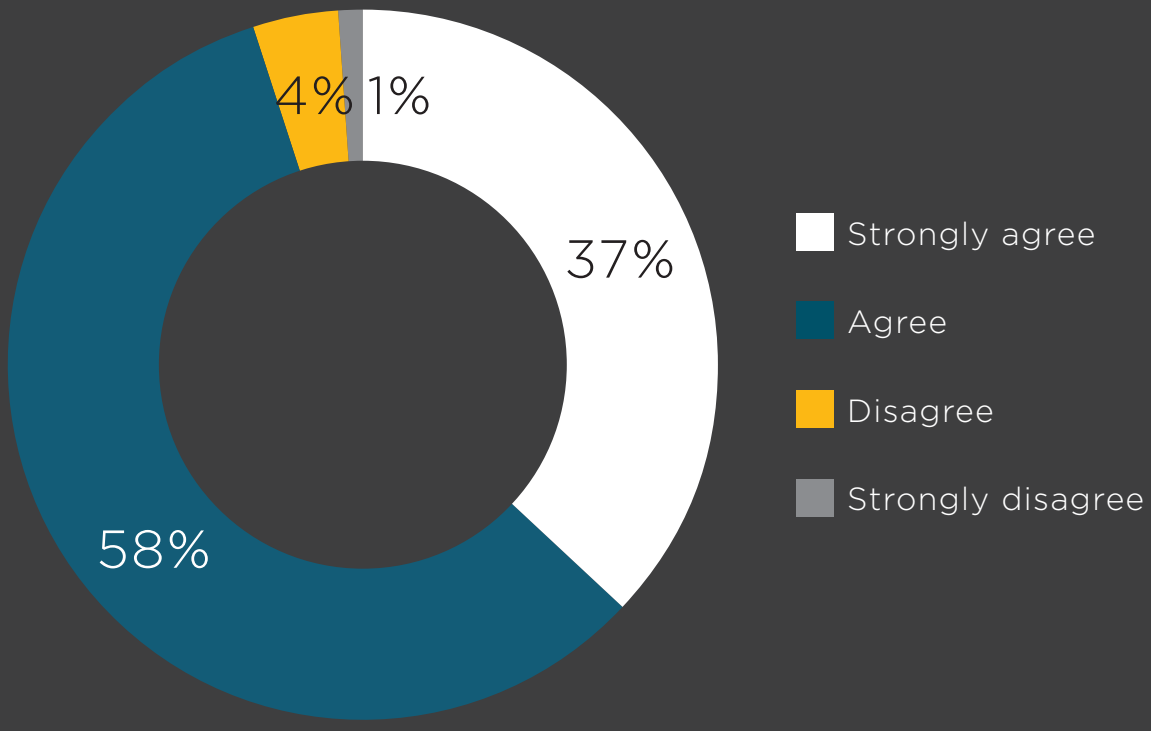
Work occurs in the cloud over networks where hundreds or thousands of devices connect.

The expanding attack surface and increasingly sophisticated cyber-attacks make it challenging to protect assets and infrastructure. Cybersecurity and password tools provide protection, but hidden weaknesses lurk in your network, software or hardware. Moreover, human error remains a constant threat.

The technology leaders we surveyed almost unanimously agree that changing human behaviour is the most significant barrier to better cybersecurity. Accordingly, most concerns and data breaches are linked to human mistakes or conduct.

FIG. 1: HUMAN BEHAVIOUR POSES THE GREATEST SECURITY CHALLENGE

To what extent do you agree or disagree that changing human behaviour is the greatest barrier to a more secure cyber defence?



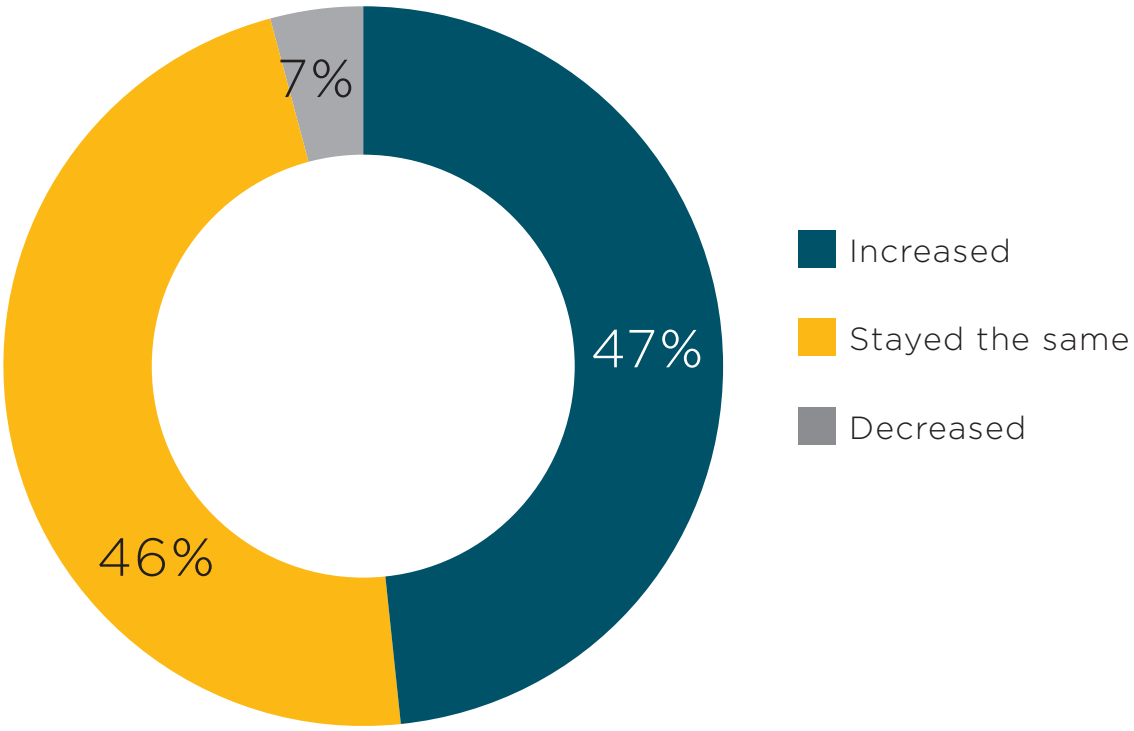
Senior information technology professionals experienced higher numbers of cyber-attacks during 2020 and 2021. As a result, 81% of respondents to HLB's 2021 Cybersecurity survey[1] altered their security strategies and protocols. But the scrutiny diminished slightly as new, formidable challenges arose. The obstacles to securing diverse environments left businesses vulnerable.

Indeed, only 7% of respondents to HLB's 2022 cybersecurity survey saw cyber-attacks decrease over the past twelve months. The incoming threats had sweeping consequences, affecting operations across the board. Business activities were disrupted, and employee productivity dropped. As leaders deployed IT resources to remedy the situation, they faced the loss of intellectual property and corporate data. Those severely impacted reported regulatory fines and legal issues.

It's time to shed light on cybersecurity and increasing visibility into your risks is an essential first step. Understanding the main challenges and how to resolve them helps your organisation move from a reactive approach to a proactive strategy.

FIG. 2: CYBER-ATTACKS STILL ON THE RISE

Have the number of cyber-attacks against your organisation increased, decreased or stayed the same in the past 12 months?

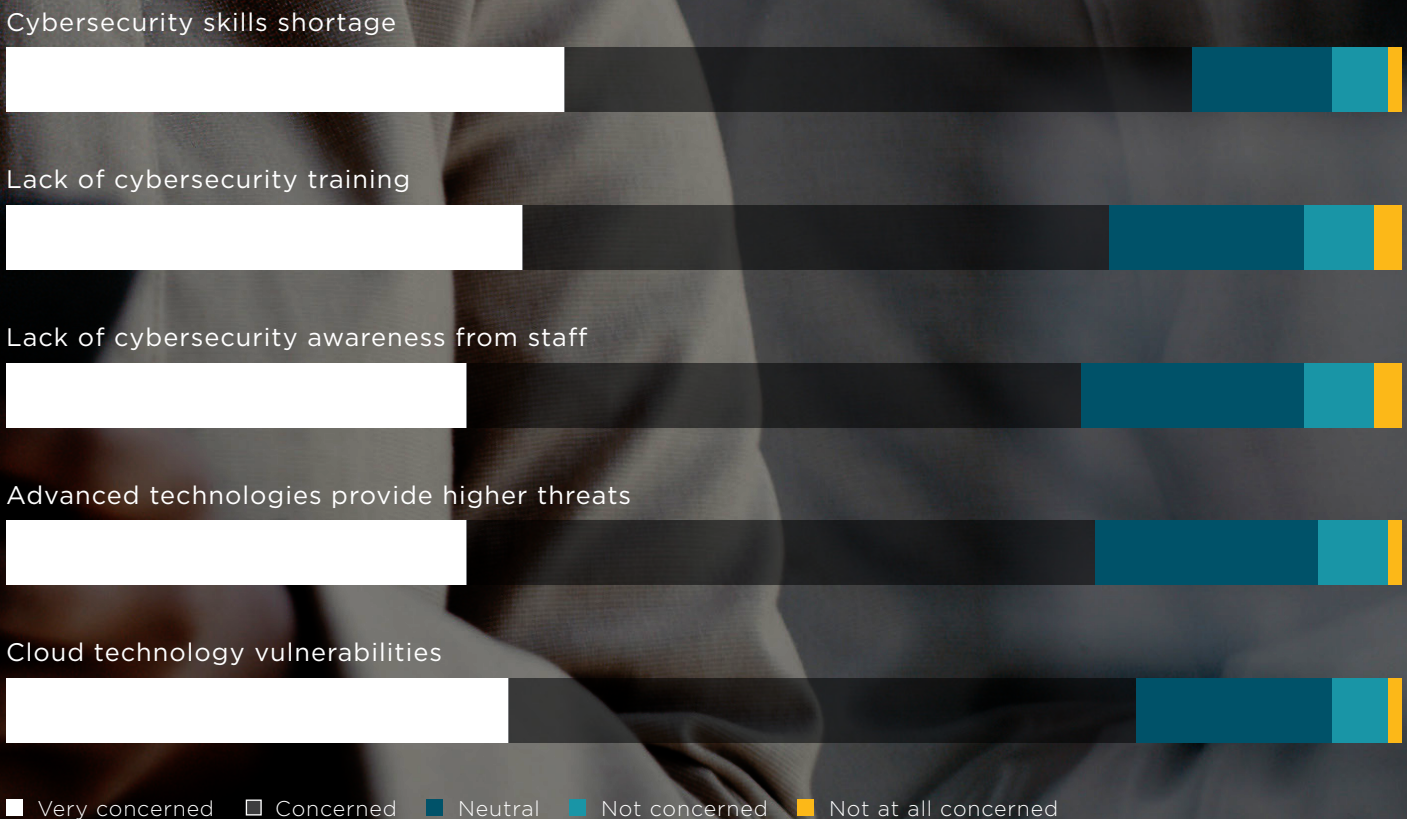


TOP 5 CYBERSECURITY CONCERNS

Technology professionals are well aware of the increase in cyber-attacks and are actively working to mitigate them. But several challenges impede progress. Here's how to break down the barriers preventing practical cybersecurity management.

FIG. 3: CYBERSECURITY SKILLS SHORTAGE IS THE TOP CONCERN

To what extent are you concerned about the following challenges in order to mitigate cyber-risk?



ONGOING CYBERSECURITY SKILLS SHORTAGE

In 2021, 2.7 million cybersecurity positions remained unfilled worldwide, according to ISC2[2]. The Information Systems Security Association International (ISSA)[3] reported that the multi-year shortage had affected more than half of organisations. Likewise, it's a top issue for HLB survey respondents, with 85% saying they are concerned or very concerned that a lack of talent is a cybersecurity risk.

The cybersecurity skills crisis is due, in part, to rapid technological advancements. In cybersecurity, the game of prevention and detection changes every 24 hours. Many security professionals aim for 40 hours of training annually, at a minimum. Yet, ISSA found that 21% of those surveyed failed to achieve this goal.

There is also a high demand for people with data security backgrounds, including security analysis and investigations, application security and cloud computing security. As positions go unfilled, cybersecurity staff experience burnout and heavier workloads, potentially leading to increased staff turnover.

Solution

A holistic approach to professional development and worker retention

Start with an investment in your current and future workforce, focusing on recruitment, retention and training. This multi-level approach uses a continuous learning environment to attract and keep employees while helping IT teams fine-tune their talents. Indeed, nearly half of IT professionals lacking yearly training said it was due to their employers not contributing to the cost. You can differentiate your business by highlighting your professional development programme.

It's also essential to align your human resources (HR) and cybersecurity goals. Almost one in three IT workers believe their organisation overlooks promising job candidates "because they don't understand the skills necessary to work in cybersecurity." The National Institute of Standards and Technology (NIST) provides resources for companies to assess, measure and develop cybersecurity teams. Use NIST's National Initiative for Cybersecurity Education (NICE) workforce framework to build a model that works for your business.

In the meantime, consider outsourcing to supplement your in-house team. After all, only 4% of respondents to a CISO buying trends survey[4] handle all cybersecurity tasks within their company. An outsourced CISO, training consultant and managed IT services can reduce the burden on your staff, allowing them to update their skills.

2

LACK OF EMPLOYEE TRAINING

Without an ongoing training programme, companies face severe cybersecurity vulnerabilities. HLB survey respondents acknowledge this, with 79% feeling concerned or very concerned about a lack of education affecting their security posture. The human factor is almost always involved when a data breach occurs. Half of CISO survey[5] respondents said that human error or inadequate training is the main reason for IT vulnerabilities.

Yet, only 50% of global CISOs surveyed by Proofpoint[6] expanded the frequency of employee cybersecurity training. And those that attempt to train workers still face issues. In fact, one in three HLB survey respondents said they try to educate staff but face non-compliance.

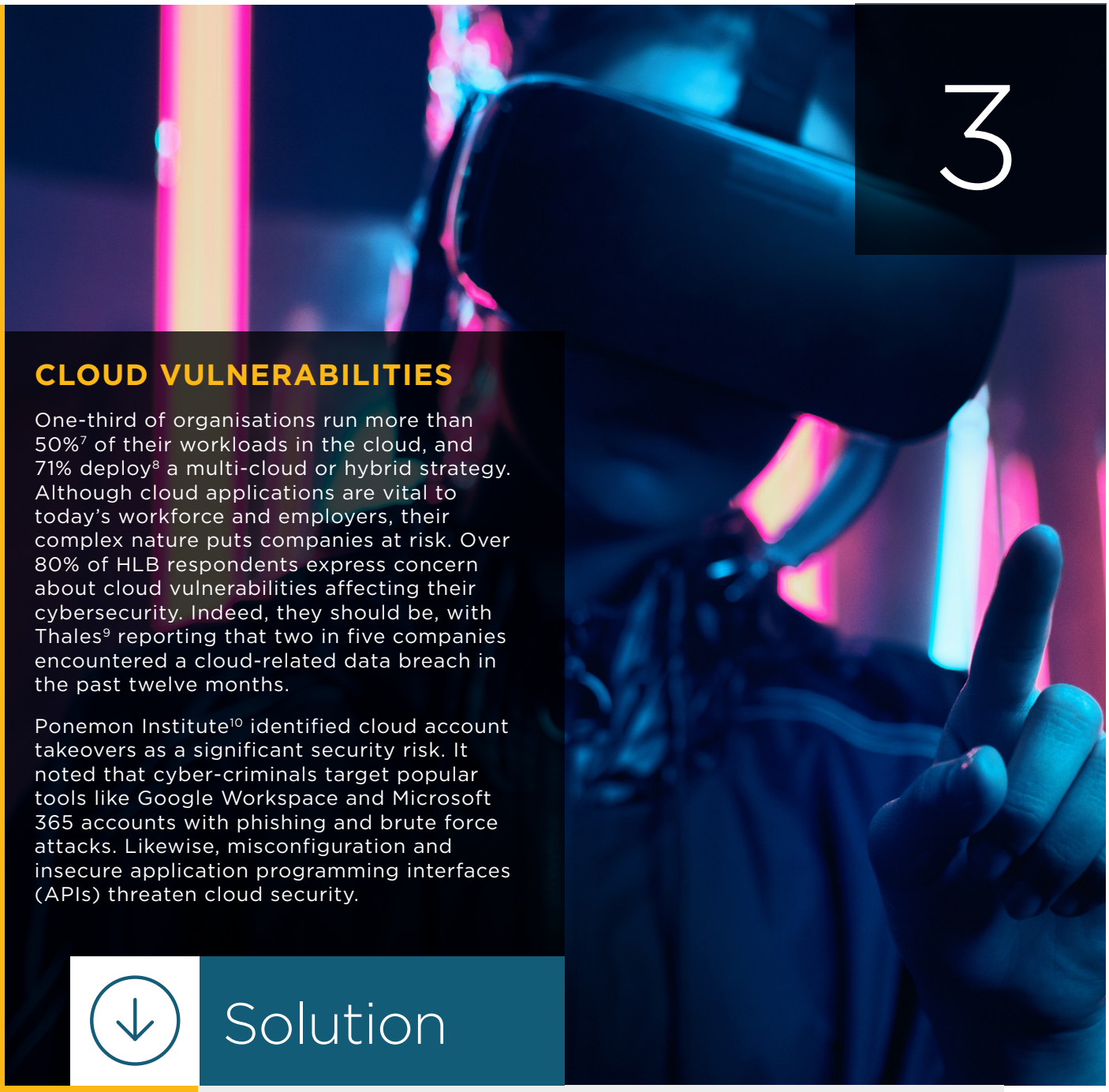
Solution

Enforce mandatory training with real-life drills

Many training objectives and activities look good on paper, helping companies meet compliance and cybersecurity goals. Yet, too often, training doesn't reflect real-life scenarios. A comprehensive programme with cyber simulations increases awareness while reducing risky behaviour. When combined with a security-first culture, you can empower employees to be guardians of security and privacy.

Aim to develop security-focused mindsets from day one of employment by providing staff with the right tools and information. Training should be mandatory for every individual, from the top down. Your team must understand that cybersecurity isn't just a knowledge workers' problem.

Use technology to gamify the experience, reward participation and allow staff to engage from their preferred devices. Random drills and simulations mimic real-life experiences, helping leaders find weaknesses and continually improve training efforts. Outsourcing training alleviates pressure on cybersecurity leaders and HR staff. It also ensures that your programmes have the latest information and resources.



3

CLOUD VULNERABILITIES

One-third of organisations run more than 50%[7] of their workloads in the cloud, and 71% deploy[8] a multi-cloud or hybrid strategy. Although cloud applications are vital to today's workforce and employers, their complex nature puts companies at risk. Over 80% of HLB respondents express concern about cloud vulnerabilities affecting their cybersecurity. Indeed, they should be, with Thales[9] reporting that two in five companies encountered a cloud-related data breach in the past twelve months.

Ponemon Institute[10] identified cloud account takeovers as a significant security risk. It noted that cyber-criminals target popular tools like Google Workspace and Microsoft 365 accounts with phishing and brute force attacks. Likewise, misconfiguration and insecure application programming interfaces (APIs) threaten cloud security.

Solution

Develop and maintain a robust cloud security posture

In many cloud deployments, security is an afterthought. Companies rely on third-party providers to secure the application but fail to take a security-first mindset with their strategy. Cybersecurity should be at the core of your cloud migration plan. One of the best ways to protect your hybrid or multi-cloud environment is by working with a cloud migration and cybersecurity professional. Risk management experts assess threats and make recommendations to ensure a seamless transition.

In addition, our HLB cybersecurity professionals can help implement best practices when migrating to the cloud. These approaches typically involve understanding compliance concerns and deploying policies and technologies to limit risk exposure. Other essential measures include adopting a security framework with clearly defined roles and accountability, increasing employee awareness and training staff.

LACK OF CYBERSECURITY AWARENESS FROM STAFF

Verizon's 2022 Data Breach Investigations Report (DBIR[11]) found that four in five data breaches involved human-related weaknesses. In 2021, bulk phishing attacks increased by 12%, and business email compromise (BEC) incidents rose by 18%. Accordingly, 77% of HLB survey respondents are concerned that a lack of awareness negatively impacts cybersecurity.

Your employee's personal choices and risk tolerance affect your organisation's security. Unfortunately, more than 30% of working adults consider emails with familiar logos safe, and 35% believe that all cloud-stored files are secure. Even with training, 42% reported taking a dangerous action such as clicking a malicious link or downloading malware. Additionally, over half of employees admit they allow family or friends to use employer-issued electronic devices, and 77% use them for personal purposes.

4

Solution

Embrace vigilance as a shared responsibility

Training can only get you so far. To increase awareness, companies must develop a culture with security at its core. In this model, everyone from the CEO to the entry-level worker participates in cyber-defence. As stewards of your organisation's cyber policies, employees feel they contribute to a greater purpose. For this approach to work, leaders must frequently communicate, sharing the latest threat intelligence and explaining the impact on individuals and the company as a whole.

It's also critical to acknowledge that cybersecurity skills are life skills, meaning personal habits affect workplace cybersecurity. Your awareness initiatives should help staff improve vigilance at home and in the workplace. Work with risk management specialists to identify vulnerabilities based on role or permission levels, and develop a strategy that considers current challenges and behaviours.

A personalised approach encourages mindfulness when performing everyday routines. Focus on policies and systems that work with employees, not against them. To this end, the right technologies should boost awareness without disrupting workflows and productivity.

5

INCREASED THREATS FROM ADOPTING NEW TECHNOLOGIES

Big data, artificial intelligence (AI), cloud infrastructure and the internet of things (IoT) fuel growth opportunities across industries. Yet, their application expands the attack surface and complicates governance. Hence, 78% of HLB respondents express concern about the impact of new technology on cybersecurity.

Cyber-criminals also weaponise the same technologies companies use to improve operations and protect networks. Threat actors leverage AI to design malware capable of imitating a secure system, which leads to undetectable ransomware attacks. Hijacked IoT devices assist with denial of service (DDoS) attacks and harvest sensor data.

These hidden threats cause significant harm. To avoid danger, organisations may complete an internal risk-benefit analysis. While beneficial, this process can be time-consuming and slow down or halt digital initiatives. A risk-averse mindset to new technologies can hinder growth and reduce a company's competitiveness in the rapidly changing marketplace.

Solution

Assess risks and prepare for attacks

Safeguard your critical assets and infrastructure by completing a risk assessment before adopting new technology. An independent evaluation lays the groundwork for a security-first strategy. It identifies key weaknesses and threats without bias, allowing leaders to make evidence-based decisions.

Also, consider requesting external audit results from technology partners before signing a contract or deploying new software or systems. Doing so establishes trust and increases visibility into third-party practices.

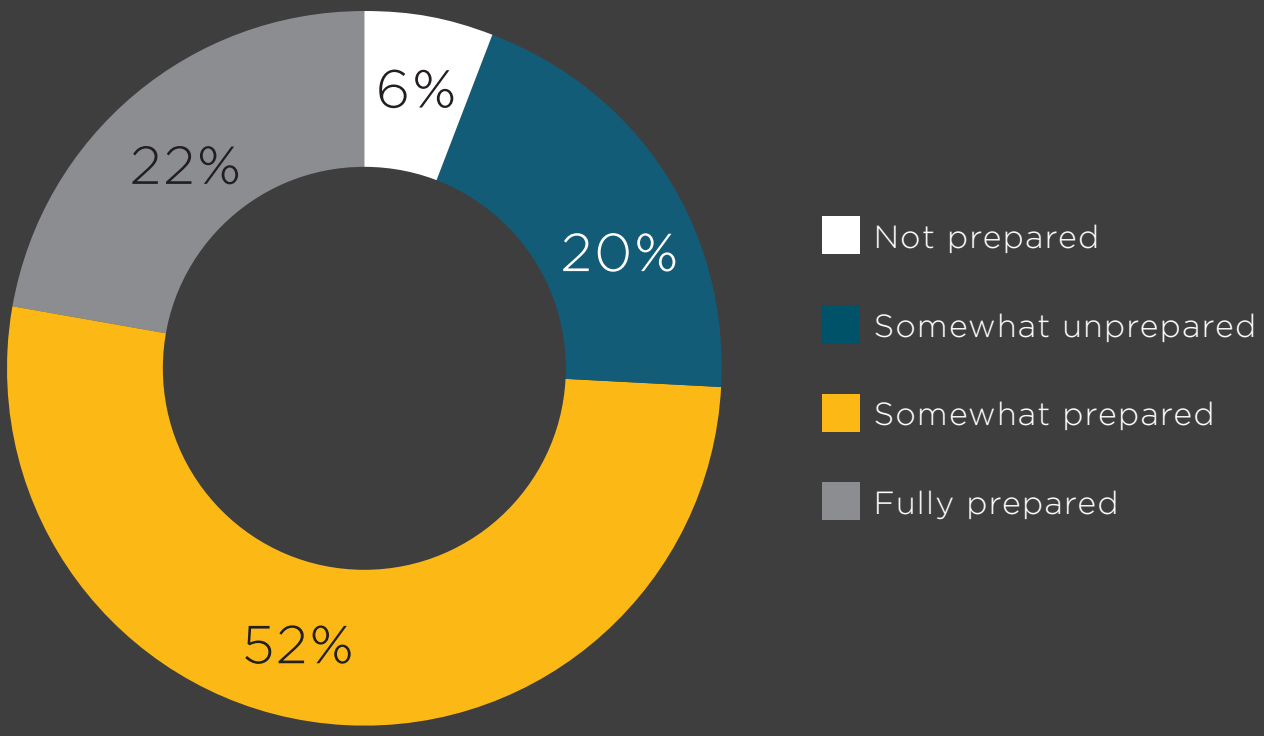
Even with these protections, your cyber-defence plan isn't foolproof. Leaders should plan for business continuity and disaster recovery to prevent stagnation from risk aversion. Work with a risk specialist to build a cohesive, actionable BCDR strategy that outlines solutions to data privacy and cybersecurity incidents. Outsourcing security audits and evaluations can reduce your internal staff and resource burden, allowing you to stay on track for your transformation goals.

ACHIEVING CYBERSECURITY MATURITY

An effective cybersecurity programme is an organisation's strongest defence. Yet maturity rates vary among companies. The majority of HLB survey respondents feel somewhat prepared to respond to a severe cyber-attack. Still, nearly 20% report being somewhat unprepared and 6% are not ready.

FIG. 4: LESS THAN A QUARTER OF ORGANISATIONS IS FULLY PREPARED FOR CYBER-ATTACKS

Where do you rank your organisation's level of readiness to respond to a severe cyber-attack?



Businesses with a low maturity level may have undersized teams with skill gaps, unpredictable processes and poor asset management. Medium cybersecurity maturity rates improve systems but lack consistent measurement and monitoring. Often mid-level firms have documented the best practices to ward off an attack and implemented security frameworks, such as ISO, SOC and NIST.

Yet, resources and capabilities remain a barrier to risk mitigation efforts. Low and mid-maturity companies may have trouble executing the strategy, running drills and performing penetration tests in-house. It's also difficult to attract cybersecurity talent and set aside resources for implementation and ongoing testing.

In contrast, higher maturity organisations have formalised policies in place. These establishments uniformly measure and monitor risks while focusing on cyber cost reduction and a positive return on investment (ROI). Also, leaders meet regularly with cyber professionals to evaluate the resiliency and strength of their security technology and processes.

Overall security programme improvements are among the top three outsourced cybersecurity services. In addition, organisations outsource technology integration and optimisation services along with 24/7 threat monitoring, detection, and response.

You can develop a pathway to cybersecurity maturity by following the framework of the National Institute of Standards and Technology (NIST). These guidelines and best practices help organise and improve your cybersecurity program.

UNDERSTANDING THE NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework[12] has three main elements: the core, implementation tiers and profiles. The Framework Core highlights preferred cybersecurity activities and outcomes. It guides companies toward the best ways to manage and reduce cybersecurity risks and complements your current cybersecurity and risk management system. The core consists of five pillars, and companies can choose activities and threats to address under each category.

At the implementation level, the framework helps leaders decide what level their cybersecurity programme requires. Companies can use the implementation tiers to spark internal conversations about risk appetite, budget and mission priority. Lastly, the framework profiles align your organisational requirements, goals, resources and risk appetite against your desired outcomes. Leaders use the profiles to find and prioritise opportunities to improve their cybersecurity.

NIST

CYBER SECURITY FRAMEWORK

1

Identify

AM: Asset Management
BE: Business Environment
GV: Governance
RA: Risk Assessment
RM: Risk Management Strategy

2

Protect

AC: Access Control
AT: Awareness Training
DS: Data Security
IP: Information Protection Processes and Procedures
PR: Protective Technology

3

Detect

AE: Anomolies and Events
CM: Security Continious Monitoring
DP: Detection Processes

4

Respond

RP: Response Planning
CO: Communications
AN: Analysis
MI: Mitigation
IM: Improvements

5

Recover

RP: Recovery Planning
IM: Improvements
CO: Communications

Identify

The first function of the NIST framework encourages companies to increase visibility under the premise that anticipating attacks is impossible when you don't fully understand your risks. Companies with low cybersecurity maturity can start by listing all software, data and equipment used. This should include on-premise and remote devices and applications.

Next, develop and share a company cybersecurity policy. Have discussions with leaders from various departments to clarify employee roles and responsibilities. The idea is to provide the right amount of access to data and programs without creating additional vulnerabilities. Remember to include anyone with access to sensitive data, such as vendors and contractors. Outline the steps you currently take to protect against an attack and how you minimise the damage if one occurs.

This procedure gives you a high-level view of how employees, systems and processes interact. Use this time to connect the dots showing how everything is interconnected. Superimpose your security measures over your usage diagram to discover activities and assets requiring more protection.

Protect

During the protect phase, the focus is on minimising the impact of an attack. It defines the security measures to defend mission-critical functions, systems and employees. Begin by reviewing the list of assets you identified in the first part of the framework. Prioritise them according to your business needs and level of cybersecurity maturity. This helps focus your cybersecurity efforts on the most important items first.

Layer security safeguards, such as:

- Restrict permissions for digital and physical assets.
- Provide awareness education and training.
- Implement processes for securing data and systems.
- Conduct necessary repairs and maintenance.
- Leverage protective technology solutions for cyber-resilience.

Detect

The detect function relates to how you catch and analyse anomalies and events. It requires processes and technologies to establish an environmental baseline, perform vulnerability scans and set alert thresholds. Companies must implement various controls, including continuous security monitoring and detection. Additionally, this phase requires regular testing.

Your organisation should understand the threats to operational continuity and the potential impact of security incidents. Leaders should be able to speak to the effectiveness of protective actions. Again, methods vary according to cybersecurity maturity level, business size, industry and more.

Ways to detect issues include:

- Use threat hunting, file integrity monitoring (FIM) and intrusion detection and prevention systems (IDS/IPS).
- Monitor all connected devices and software for unauthorised personnel access.
- Take note of abnormalities and investigate unusual network or employee activities using logs or third-party tools.
- Regularly stress test your cybersecurity system, including after implementing technology changes.

Respond

Nearly half of HLB respondents reported an increase in cyber-attacks. As a result, they experienced business disruptions and loss of data and intellectual property. However, more than half of small and mid-sized companies[13] don't have an incident response strategy.

The respond function of the NIST framework recommends that organisations develop a response plan. Your plan should outline the immediate steps to contain the attack and keep your business operational. Also, it must detail your investigation and elimination methods.

Your cybersecurity strategy will identify ways to collect and analyse incident data. This allows you to gain insights and use them to revise your plan. You also need a communication process to alert those involved, including employees, customers, vendors and, if necessary, the authorities. Remember to identify the human and financial resources required, and have a system for allocating resources as needed.

However, documenting your strategy is only part of the respond function. It's essential to test your plan regularly by running practice drills. Adjust it as needed and update your policies and training to ensure a smooth response to an attack.

Recover

The recovery period after a data breach or cyber-attack is risky for businesses. On average, companies experience 20 to 23 days of downtime after a ransomware attack. IBM[14] reported that the global average data breach cost reached an all-time high in 2021, and almost 50% of the expenses incur more than a year after the breach. Even after paying a ransom, only about 8% of victims recuperate all of their data.

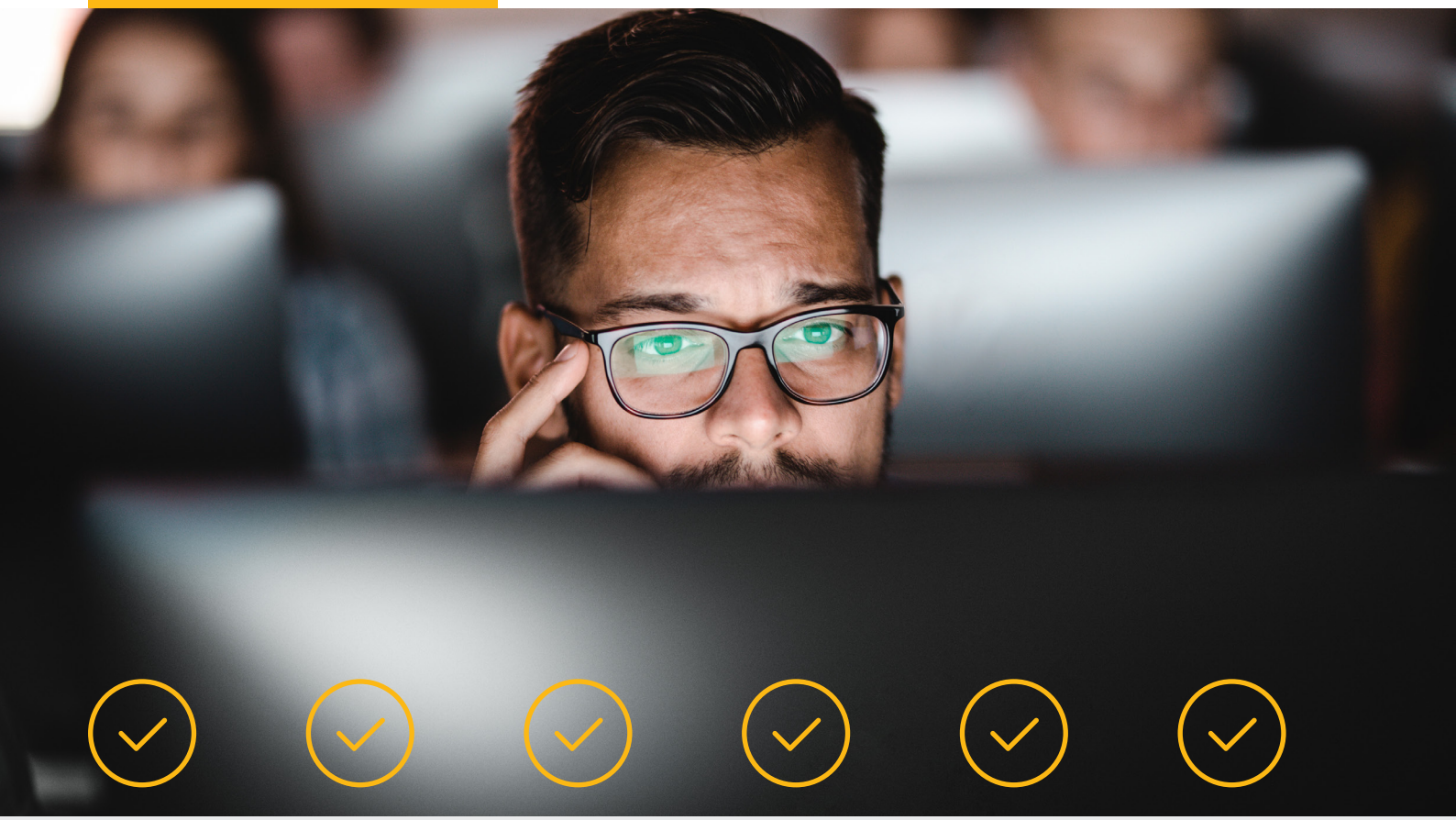
FIG. 5: THE COST OF CYBER-ATTACKS

What negative impact have security incidents had on your company?

HOW HLB CAN HELP

Invisible threats to your data privacy and cybersecurity hide in the shadows, waiting for one human error or unpatched weakness. Being somewhat prepared isn't enough to withstand the sophisticated attacks leveraged at businesses of any size. A robust security posture safeguards your organisation, and it begins with an accurate risk assessment. HLB's experienced cybersecurity professionals specialise in helping you understand, prioritise and harden vulnerabilities. Move the needle from somewhat to fully prepared by reaching out to us.

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

ENDNOTES

1 HLB International, 2021. HLB Cybersecurity Report 2021: Threat or opportunity: Addressing the cyber-risk landscape in the age of hybrid work

2 (ISC)2, 2021. (ISC)2 Cybersecurity Workforce Study 2021: A resilient cybersecurity profession charts the path forward

3 ISSA, 2021. Cybersecurity skills crisis continues for fifth year, perpetuated by lack of business investment

4,5 Nuspire, 2022. Nuspire Annual Study: Top 10 CISO buying trends of 2022

6 Proofpoint, 2022. 2022 voice of the CISO: Global insights into CISO challenges, expectations and priorities

7 Fortinet, 2021. Cloud security report

8 Thales, 2021. 2021 Thales Cloud Security Study – report

9 Ponemon Institute, 2021. The cost of cloud compromise and shadow IT

10 Verizon, 2022. 2022 Data breach investigations report

11 Proofpoint, 2022. 2022 State of the Phish: An in-depth exploration of user awareness vulnerability and resilience

12 NIST, 2022. Cybersecurity Framework

13 Connectwise, 2021. Vanson Bourne shares stats on the state of SMB cybersecurity in 2021 and how to prepare for attacks

14 IBM, 2022. Cost of a data breach report 2022

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

© 2022 HLB International Limited. All rights reserved.

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 HLB International Limited has no liability for the acts and omissions of any other member. HLB International Limited is registered in England No. 2181222 Limited by Guarantee, which co-ordinates the international activities of the HLB International network but does not provide, supervise or manage professional services to clients. Accordingly, HLB International Limited has no liability for the acts and omissions of any member of the HLB International network, and vice versa and expressly disclaims all warranties, including but not limited to fitness for particular purposes and warranties of satisfactory quality.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, HLB International does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

In no event will HLB International Limited be liable for the acts and/or omissions of any member of the HLB International network, or for any direct, special, incidental, or consequential damages (including, without limitation, damages for loss of business profits, business interruption, loss of business information or other pecuniary loss) arising directly or indirectly from the use of (or failure to use) or reliance on the content of this Website or any third party website, or from your use of any member's services and/or products. Any reference to a member's services or products should not be taken as an endorsement.

HLB refers to the HLB International network and/or one or more of its member firms, each of which is a separate legal entity.