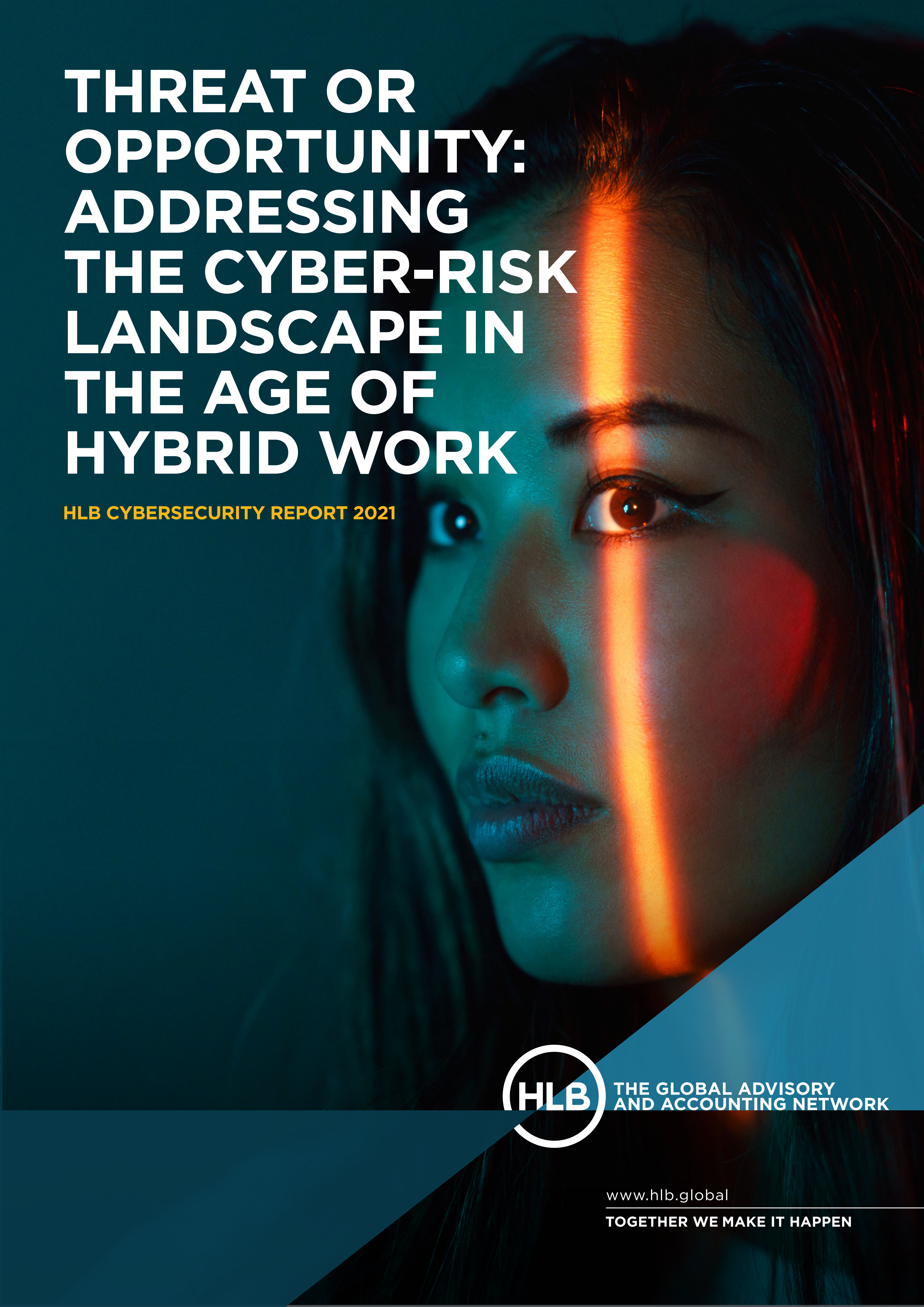


THREAT OR OPPORTUNITY: ADDRESSING THE CYBER-RISK LANDSCAPE IN THE AGE OF HYBRID WORK

HLB CYBERSECURITY REPORT 2021

HLB THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

As we emerge from lockdowns and government restrictions caused by COVID-19, more companies across the globe are adopting hybrid work models. In doing so, CTO’s and IT managers face heightened risks and vulnerabilities from cyber-attacks and data breaches.

In light of Cybersecurity Awareness Month 2021, we surveyed 136 IT professionals between August and September and interviewed HLB cybersecurity experts about today’s cyber-risk landscape, the lessons learned from lockdown and the road ahead for CTOs to protect against cyber-crime in the age of hybrid working.

CONTENTS

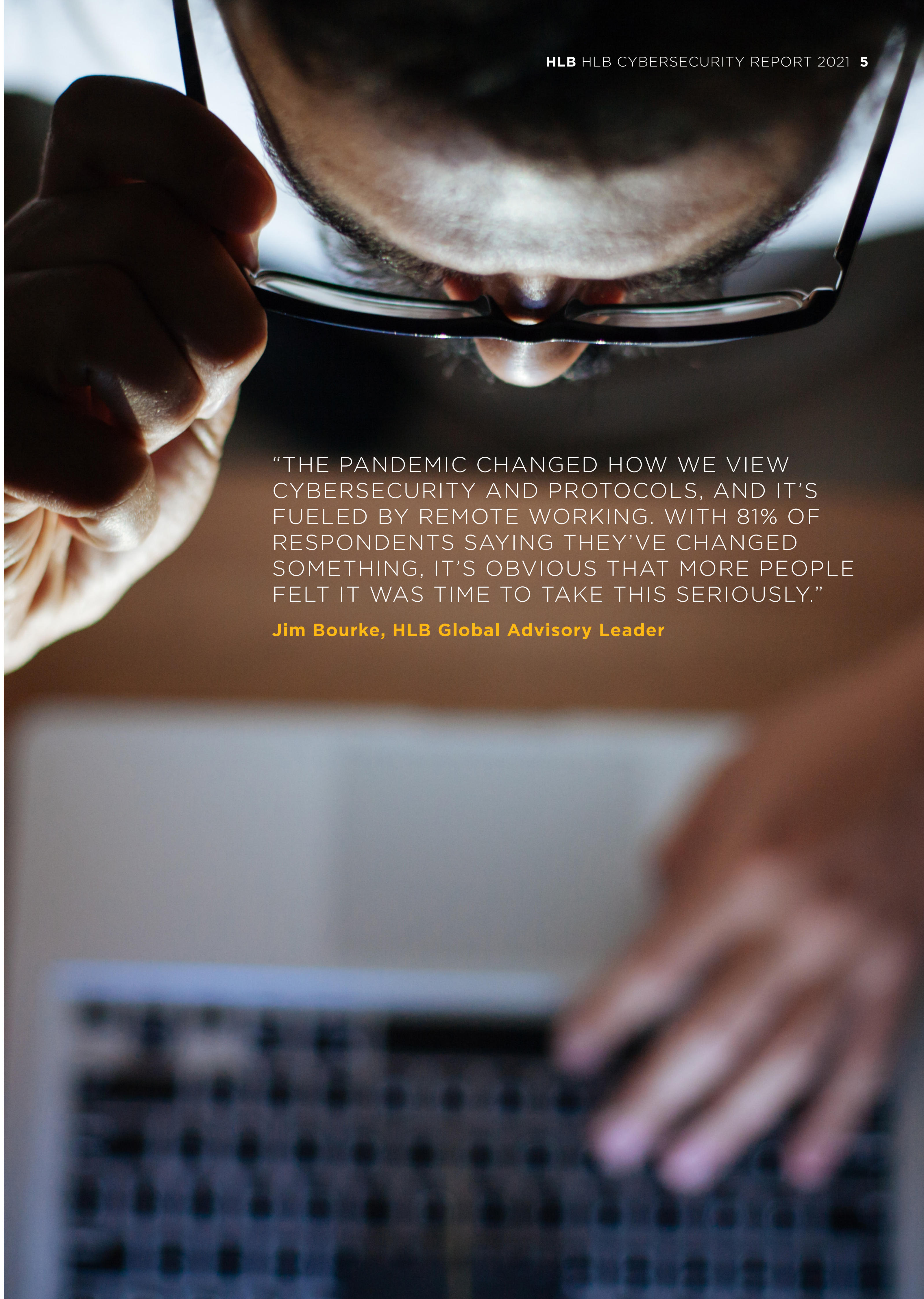
FROM BUSINESS CONTINUITY TO CYBERSECURITY: THEN AND NOW

In 2020, leaders focused on putting technologies in place and getting employees back to work, albeit remote. It required a shift to cloud computing while ensuring staff had high-speed internet connections and capable devices. While cybersecurity was important, the first step was implementing remote work successfully.

But, 53% of 2020 HLB survey[1] respondents said they were aware of unusual cyber-related activity and attacks since the start of the pandemic. Accordingly, their top priority for 2020 was to complete an internal risk assessment.

Since our 2020 survey, cyberattacks have increased, and organisations continue to face disruption from COVID-19. Workers have embraced a hybrid work model, while leaders moved from being reactive to being proactive. Instead of assessing and fixing security issues as they occur, the majority of CTOs responding to our 2021 HLB survey now prioritise developing an incident response plan.

[1] HLB International, 2021. HLB Cybersecurity Report 2020: Navigating the cyber-risk landscape in the age of remote working



> "THE PANDEMIC CHANGED HOW WE VIEW CYBERSECURITY AND PROTOCOLS, AND IT'S FUELED BY REMOTE WORKING. WITH 81% OF RESPONDENTS SAYING THEY'VE CHANGED SOMETHING, IT'S OBVIOUS THAT MORE PEOPLE FELT IT WAS TIME TO TAKE THIS SERIOUSLY."
>
> **Jim Bourke, HLB Global Advisory Leader**

CYBER-RISK MANAGEMENT: HYBRID WORKING IS THE FUTURE OF WORK

COVID-19 has broken through cultural and technological barriers that prevented remote work in the past, setting in motion a structural shift in where our work takes place. Respondents to our 2021 survey made changes to support hybrid workers, with 44% saying they feel well-prepared for hybrid working, and 44% being somewhat prepared.

According to McKinsey & Company[2], since 2019, the number of people wanting to work on-site declined by 25%, with around 30% likely to switch jobs if forced to return to fully on-site work.

In industries with highly skilled and highly educated workers, such as those in professional services, research[3] shows that 20% of the workforce could work remotely three to five days a week as effectively as they could if working from an office. Gartner noted “51% of all knowledge workers worldwide are expected to be working remotely, up from 27% of knowledge workers in 2019.”

CEOs recognise opportunities in a hybrid work model, from reducing their real estate costs to retaining employees. Pearl Meyer[4] observed that almost “40% of organisations reported increased productivity with nearly 50% reporting no change.”

By 2022, Gartner estimated that “31% of all workers worldwide will be remote (a mix of hybrid and fully remote).” This estimate varies by location, with remote workers accounting for 53% of the U.S. workforce, 52% of European and U.K. employees, 37% in Germany, 33% in France, 30% in India and 28% in China.

However, a hybrid workforce requires adaptive environments. Adaptive workspaces empower employees to work where and when they are most productive. Flexible environments provide well-designed and equipped on-site areas while ensuring work-from-home teams have the technology and tools to complete their work.

Organisations turn to the cloud to support a hybrid workforce. But adding remote endpoints and increasing reliance on online software poses a considerable cybersecurity risk. As we look ahead to the future of work, cybersecurity solutions play a prominent role in the success of the hybrid work model.

[2] McKinsey & Company, 2021. What employees are saying about the future of remote work
[3] Gartner, 2021. Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021
[4] Pearl Meyer, 2021. Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021

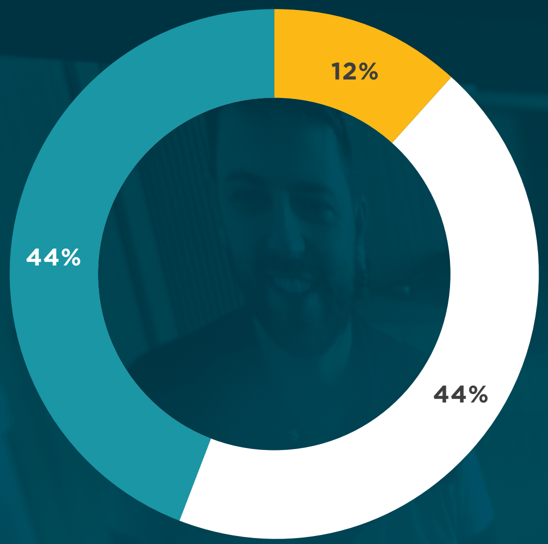


FIGURE 1: LEVELS OF READINESS FOR HYBRID WORKING MODEL

Q: TO WHAT EXTENT ARE YOUR IT INFRASTRUCTURE AND CYBERSECURITY PROTOCOLS PREPARED FOR HYBRID WORKING MODEL?

🟨 NOT AT ALL PREPARED. WE STILL HAVE OUR STAFF WORK FROM THE OFFICE AND WORK IN A CORPORATE PERIMETER SECURITY MODEL

⬜ SOMEWHAT PREPARED. WE ARE USING NEW TECHNOLOGY TO SUPPORT REMOTE AND OFFICE-BASED EMPLOYEES

🟦 WELL PREPARED. WE HAVE EMBRACED HYBRID WORKING AND CHANGED OUR TECHNOLOGY INFRASTRUCTURE TO BE A ZERO-TRUST ARCHITECTURE.

SECURITY ISSUES AND HYBRID WORKPLACES

In HLB Survey of Business Leaders 2021[5], we asked how concerned the C-suite were about the risks to their businesses from cybersecurity issues. Although 47% were concerned or very concerned, several other issues stood out further, such as COVID-19 consequences, economic and geopolitical instability and supply chain disruption.

While these matters are valid, the data shows us that cybersecurity should be a priority, especially for hybrid workplaces. According to McAfee[6], the number of “threats from external actors targeting cloud services increased 630%,” with most incidents stemming from stolen credentials. Likewise, cloud traffic from unmanaged devices doubled, suggesting a need for CTOs to control cloud access by device type.

Adding off-site endpoints requires more resources to monitor them. And it’s tougher to gain visibility into what your employees are doing and how they handle a potential security incident when they’re not in the office.

At the same time, third-party vendor safety measures affect organisations as well. Therefore, leaders must reassess technology partnerships to confirm their software providers are also prepared for a ransomware attack.

ADJUSTING CYBERSECURITY STRATEGIES AND PROTOCOLS

While companies want to retain talent by offering flexibility, they also need to protect their organisations from cyber threats. To do this, the overwhelming majority of 2021 HLB survey respondents said they’d altered their cybersecurity strategies and protocols, with 43% saying they’ve changed them somewhat and 39% have changed them drastically. Only 17% report no changes since the pandemic began.

These results are comparable to the 2020 survey, in which 88% said they changed their cybersecurity policies and plans. However, the number of respondents saying they changed them drastically increased by 14% in 2021.

Of those reporting drastic changes, 66% now oversee cybersecurity at a senior level. This is significant because historically, cybersecurity was seen as an IT role with less involvement from senior executives. But, research shows that a top-down approach is essential to cybersecurity. Bourke notes, “Awareness has now been elevated, and senior management is being held accountable, not just IT. Previously, legacy CEOs would rely on IT to keep them protected. Not any more.”

[5] HLB International, 2021. HLB Survey of Business Leaders 2021: Achieving the post-pandemic vision: leaner, greener and keener
[6] McAffee, 2021. Cloud Adoption and Risk Report

> “CYBERSECURITY NEEDS TO BE DONE AT A HIGHER LEVEL. IT NEEDS TO BE RUN AT THE SENIOR LEVEL. OTHERWISE, IT DOESN’T GET THE TRACTION IT NEEDS.”
>
> **Abu Bakkar, HLB Chief Innovation Officer**

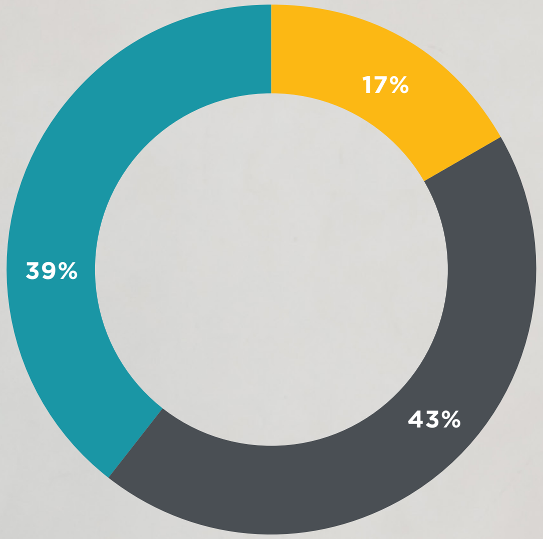


FIGURE 2: CYBERSECURITY STRATEGIES CHANGED IN RESPONSE TO COVID-19

Q: SINCE THE START OF THE PANDEMIC, TO WHAT DEGREE HAVE CYBERSECURITY STRATEGIES AND PROTOCOLS AT YOUR ORGANISATION CHANGED?

HLB’s Chief Innovation Officer Abu Bakkar adds, “Cybersecurity needs to be done at a higher level. It needs to be run at the senior level. Otherwise, it doesn’t get the traction it needs.” However, Bourke notes, “If it’s actioned at a senior level, what are they doing — especially if they don’t want to outsource their cybersecurity.” In other words, clarifying the roles of senior members and finding the disconnect between what the IT team does and what the CEO thinks they do is essential.

In addition, 28% of survey respondents reported implementing a framework. Typically, a framework includes business continuity and a disaster recovery plan. It requires support from executives, as it’s a vast undertaking involving changes to policies and procedures. Bakkar mentions that “implementing a framework sounds like a simple thing, but it is not. You need help and support because there are so many policies, procedures, and lots of things change.” HLB Digital partner Carlos Camacho adds, “It is not just a year, it is the mindset that makes the difference”.

In contrast, only 6% of drastic changes include outsourcing cybersecurity. The lower percentage may result from executives wanting to work with known partners and being wary about whom they bring into their cybersecurity process. For security providers and consultants, low market saturation may provide opportunities for future partnerships.

Of the 42% who said they made changes, 39% increased employee training, 36% increased their budget and 12% invested in a cyber resilience programme. According to Bourke, “More risk sits with the employees, so training programmes are important.” We also found that while 14% chose “other,” upon inspection of their written responses, they indicated that their changes were a combination of all three options.

HYBRID WORKING PREPAREDNESS

Last year, many survey respondents noted the importance of getting employees into remote working conditions, such as getting them the tools and resources needed to continue doing their job. Yet, many leaders didn’t realise how long their workforce would stay remote and weren’t looking for long-term solutions. Consequently, at the start of the pandemic investing in stricter cybersecurity protocols wasn’t a priority.

With work flowing more smoothly and with high-profile cyber-attacks in the news, leaders are now looking to adopt more robust security measures to protect their business.

EMPLOYEES ARE AT THE CORE OF CYBERSECURITY FOR YOUR ORGANISATION

Although organisations implement many security measures, ultimately, employees play one of the most significant roles. HLB Digital partner Carlos Morales said, “People understand that cybersecurity is not a computer issue. It’s a human issue.”

And far too often, it’s employees who are the weak link in cybersecurity. Bourke says, “A greater degree of cybersecurity incidents have originated from employees, and it drove the importance of developing an incident response plan.” The Verizon 2021 Data Breach Investigations Report[7] found that “85% of breaches involved a human element, and 61% of breaches involved credentials.” Moreover, “88% of UK data breaches caused by human error, not cyberattacks,” according to data obtained from UK’s Information Commissioner’s Office (ICO).

While tools can provide much-needed visibility into employee password practices, leaders must focus on team member training and awareness. Our survey found that 57% of respondents take employee education seriously and have a no-exceptions policy. In contrast, 33% of the IT professionals we surveyed state that they educate their staff, but they constantly deal with non-compliance. This underlies organisations’ great difficulty in getting employee compliance, especially when using the hybrid work model.

Since some of the biggest risks stem from employees, it’s important to understand the threats that come with hybrid workplaces. From there, leaders should take note of challenges to implement security measures and come up with solutions.

THREATS TO HYBRID ENVIRONMENTS

Social engineering and phishing scams result in security issues for companies. In some cases, a vendor email compromise (VEC) makes it difficult to ascertain fake email addresses. This often occurs from stolen or phished email credentials.

Increasingly, we see more business email compromises (BECs). These appear to come from an internal employee or manager and request confidential data or some invoice payment. Remote desktop intrusions often stem from misconfigurations. As noted in McAfee’s study, work-from-home devices add complexity to cybersecurity management. Organisations lacking endpoint visibility and control face greater cyber risks than those with a comprehensive endpoint protection plan.

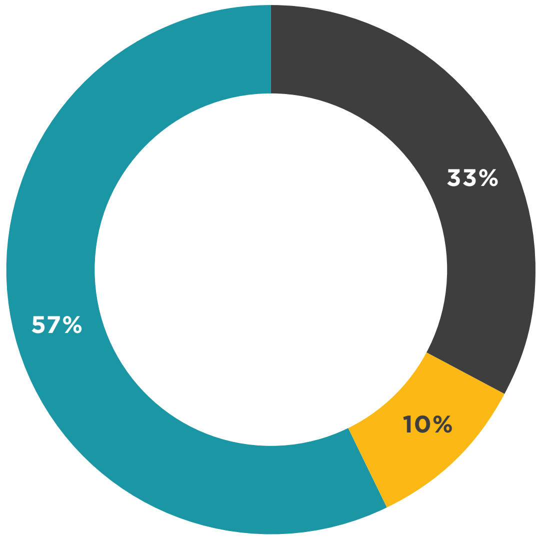


FIGURE 3: CYBERSECURITY EDUCATION FOR STAFF

Q: WHEN IT COMES TO CYBERSECURITY EDUCATION FOR OUR STAFF:

■ WE EDUCATE OUR STAFF, BUT WE ALWAYS ARE DEALING WITH NON-COMPLIANCE.

■ WE ENCOURAGE IT BUT DON’T ENFORCE IT

■ WE TAKE IT SERIOUSLY AND HAVE A NO EXCEPTIONS POLICY

COMMON BARRIERS TO EMPLOYEE SECURITY MEASURES

With one-third of CTOs and CIOs dealing with non-compliance, it’s vital to understand the root of the problem. There are many reasons why employees don’t follow cybersecurity protocols, including inconvenient or unclear processes. Additionally, non-IT staff may not be aware of the different threat types or understand the consequences of security failures. Although over 90% said they educate their staff, Bourke notes that “33% have non-compliance issues, highlighting why a no-exceptions policy is essential. It just takes one person to make a mistake.”

Hybrid employees may rely on wireless internet to work from anywhere, and if it’s a choice between not working or taking a risk with public wifi, it makes for a tricky situation. Morales says, “People are usually not aware that working remotely or working from anywhere could be a risk.”

On the other hand, hybrid workers may lack technology tools to complete their work securely, such as password managers, two-factor authenticators and virtual private networks (VPNs). If companies offer a bring your own device policy, there’s a higher chance that these devices are used for personal and professional tasks.

Lastly, employee education may be lacking. Employees can view the training as a task to complete, not a learning activity. Some may play the required videos on mute and breeze through the quiz with help from online search engines. Others may not understand the lengthy policy documents before they sign them.

In comparison, successful programmes are inclusive, user-friendly and ongoing. They come in different formats, and, like adaptive workplaces, cybersecurity training empowers staff to learn when and where they’re comfortable and in a manner that suits their skill and style.

SOLUTIONS FOR OVERCOMING CYBERSECURITY OBSTACLES

Carlos Camacho says, “That human element requires education, because education is the key to the change in the human pattern.” That’s why the best cybersecurity solutions look to build better habits by altering processes and increasing awareness. Furthermore, when asked to tell us what actions they’ve taken to protect their business, we received dozens of responses related to employee training, demonstrating that focusing on employees is crucial to combat cyber threats.

[7] Verizon, 2021. Data Breach Investigations Report

Like all cybersecurity measures, employee cyber hygiene relies on a three-pronged approach: people, technology and environment. People require educational training to spot fake phishing emails, such as mandatory online training programmes. Moreover, leadership must model the behaviour and keep lines of communication open to really drive home the importance of cybersecurity. Roughly one-quarter of respondents shifted to cybersecurity actioning at the senior level, suggesting that leaders recognise the importance of a top-down approach.

In written responses, those surveyed reported using various solutions to improve employee education, including intensive company-wide workshops, online instruction and third-party training services.

According to Bakkar, some firms "use a training company that provides training videos. And it doesn't matter if you're a partner or professional or staff, if you do not take those videos and watch them, then you don't have access to your laptop or to the network."

The work environment, regardless of location, must be secured. Remote-access VPNs are one solution. Giving just enough access permissions is another. Other CTOs told us they'd taken steps to prevent personal browsing and use content filtering and monitoring tools.

Technology also plays a role. For instance, two-factor or multi-factor authentication applications or enabling 2FA on existing tools can significantly reduce hacked accounts. Password management programmes make it easier to abide by your password policies. Using standard cybersecurity measures, such as firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS) and endpoint monitoring, also help protect your teams and business data. Furthermore, adopting policies and implementing the National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) frameworks are critical to reducing cyber risks.

According to Bakkar, some firms

"USE A TRAINING COMPANY THAT PROVIDES TRAINING VIDEOS. AND IT DOESN'T MATTER IF YOU'RE A PARTNER OR PROFESSIONAL OR STAFF, IF YOU DO NOT TAKE THOSE VIDEOS AND WATCH THEM, THEN YOU DON'T HAVE ACCESS TO YOUR LAPTOP OR TO THE NETWORK"

STRENGTHENING YOUR CYBER-RISK MANAGEMENT STRATEGY

As noted earlier, in 2020[8], most respondents told us their top priority was conducting an internal risk assessment. However, that objective dropped to number four in our 2021 survey. Instead, the leading strategic action is developing an incident response plan. For this year's survey, people have moved on from assessing risks and now want to figure out how to respond to them.

Although organisations differ in their approach to digital transformation, including timelines and objectives, employee education continues to rank number two on our priority list, which is the same as last year.

For CTOs deciding their next steps, the first place to start is conducting an internal risk assessment. From there, leaders should prioritise tactics to mitigate threats, educate employees and respond to incidents.

DEVELOP AN INCIDENT RESPONSE PLAN

Last year, business continuity plans focused on getting employees back to work. This year, 88% of executives are at least somewhat prepared for hybrid work. As a result, their top priority is designing an incident response plan. With the idea that a cyber attack is imminent, leaders look for ways to limit disruption using proactive monitoring and seamless responses if a breach occurs.

Bakkar remarks, "Business continuity is huge. You have to make sure your business is capable of being up and running as soon as possible after an incident. There's no way of 100% stopping a cyber attack. You can mitigate against most things, but if you have a good response plan, you know you are also mitigating with business continuity."

CYBERSECURITY TRAINING FOR WORKFORCE STRATEGIES

According to Camacho and Morales, people are both your strength and your weakness. Therefore, prevention and incident response depend, in part, on your employees. Our 2021 HLB cybersecurity survey found that 90% of respondents educate their employees. However, not all have successfully achieved employee compliance, suggesting there's a need to review current training programmes and address their weaknesses.

[8] HLB International, 2021. HLB Cybersecurity Report 2020: Navigating the cyber-risk landscape in the age of remote working

[9] HLB International, 2021. HLB Survey of Business Leaders 2021: Achieving the post-pandemic vision: leaner, greener and keener

57%

OF RESPONDENTS TAKE CYBERSECURITY EDUCATION FOR THEIR STAFF SERIOUSLY AND HAVE NO EXCEPTION POLICY.

According to Bourke, "57% take it seriously and say they don't tolerate exceptions, which is a good start. At HLB, we are the trusted advisor, and our clients trust us to look after their confidential data. As such, we take access to documents and information seriously. We don't want to run the risk of a potential compromise."

Cybersecurity policies should cover mobile and desktop devices, third-party application downloads, social media use and email security. Likewise, ongoing courses should review data protection rules and the consequences of failing to abide by cybersecurity protocols at the employee and corporate levels.

However, bombarding employees with reading material or lengthy videos is less helpful than interactive training models and simulations. Communication from leadership is also essential. Executives should update teams on the latest scams targeting their industry and job roles and talk about what they're doing at the senior level to protect employees and the organisation as a whole. Frequent conversations keep cybersecurity top of mind and, in doing so, increase employee awareness.

Lastly, employee training will only go so far unless backed by the resources workers require. To this end, CTOs may consider surveying teams to assess their understanding of cybersecurity measures and ask about their concerns. Employers should provide one-on-one support to help staff update or upgrade their home office and device security.

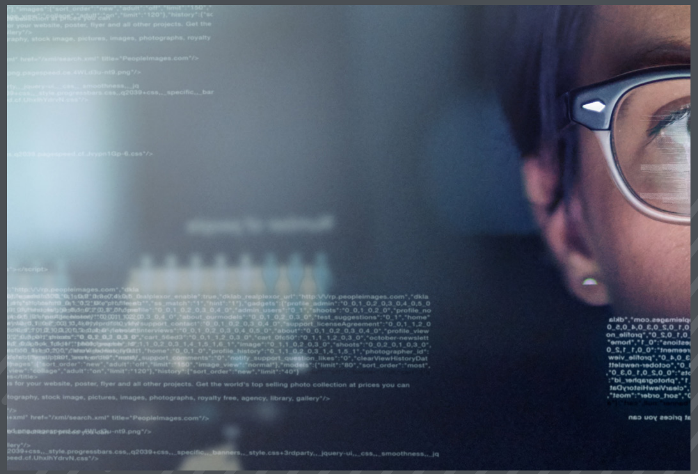
ANALYSIS OF CLOUD COMPUTING STRATEGIES

Respondents ranked reviewing cloud computing strategies third on our survey[9]. According to Gartner[10], "worldwide end-user spending on public cloud services will grow 23.1% in 2021." Gartner estimates that "at least 40% of all remote access usage will be served predominantly by zero-trust network access (ZTNA), up from less than 5% at the end of 2020." Although Gartner expects VPN usage to continue, they say, "ZTNA will become the primary replacement technology."

Bakkar notes, "To change to zero trust architecture is a huge, huge deal. You have to change processes, policies, hardware and systems. So, it's not a cheap or quick change. Shifting to ZTNA means nothing is trusted until you pass internal security processes, such as 2FA. Only when an end-user gains "trust" can they access networks and applications.

CONDUCT AN INTERNAL RISK ASSESSMENT

In 2020, more than half of survey respondents were aware of atypical cyber events, and 12% experienced a breach. However, many cybercrimes go unnoticed for months or years. It's nearly impossible to prioritise cybersecurity objectives and know where to put your budgeted funds without first completing an internal risk assessment.



Since the majority of respondents to this year's survey are taking immediate action to improve cybersecurity, there's a good chance they completed and are acting on an internal risk assessment. However, it's important to note that IT teams should complete threat assessments regularly. Some companies may prefer to outsource the evaluation to ensure it gets done correctly and promptly.

THIRD-PARTY (VENDOR) CYBERSECURITY RISK ASSESSMENT

Vendor assessments also ranked low on our 2020 survey, as leaders prioritise internal actions over what others are doing. Yet, last year major corporations including Marriott, P&N Bank and General Electric faced attacks after third-party vendor breaches. According to the Mastercard RiskRecon[11] report, leaders believe attacks on most of their vendors would result in a risk or severe impact on their organisation.

However, the report notes that 57% of respondents cited a lack of staff for struggling to keep up with managing third-party vendor risk. With tight budgets and labour shortages, completing assessments and monitoring vendor compliance is challenging. At the same time, there is an opportunity for assessment providers to assist latecomers with evaluations and planning.

FIGURE 4: DEVELOP AN INCIDENT RESPONSE PLAN IS NOW TOP PRIORITY

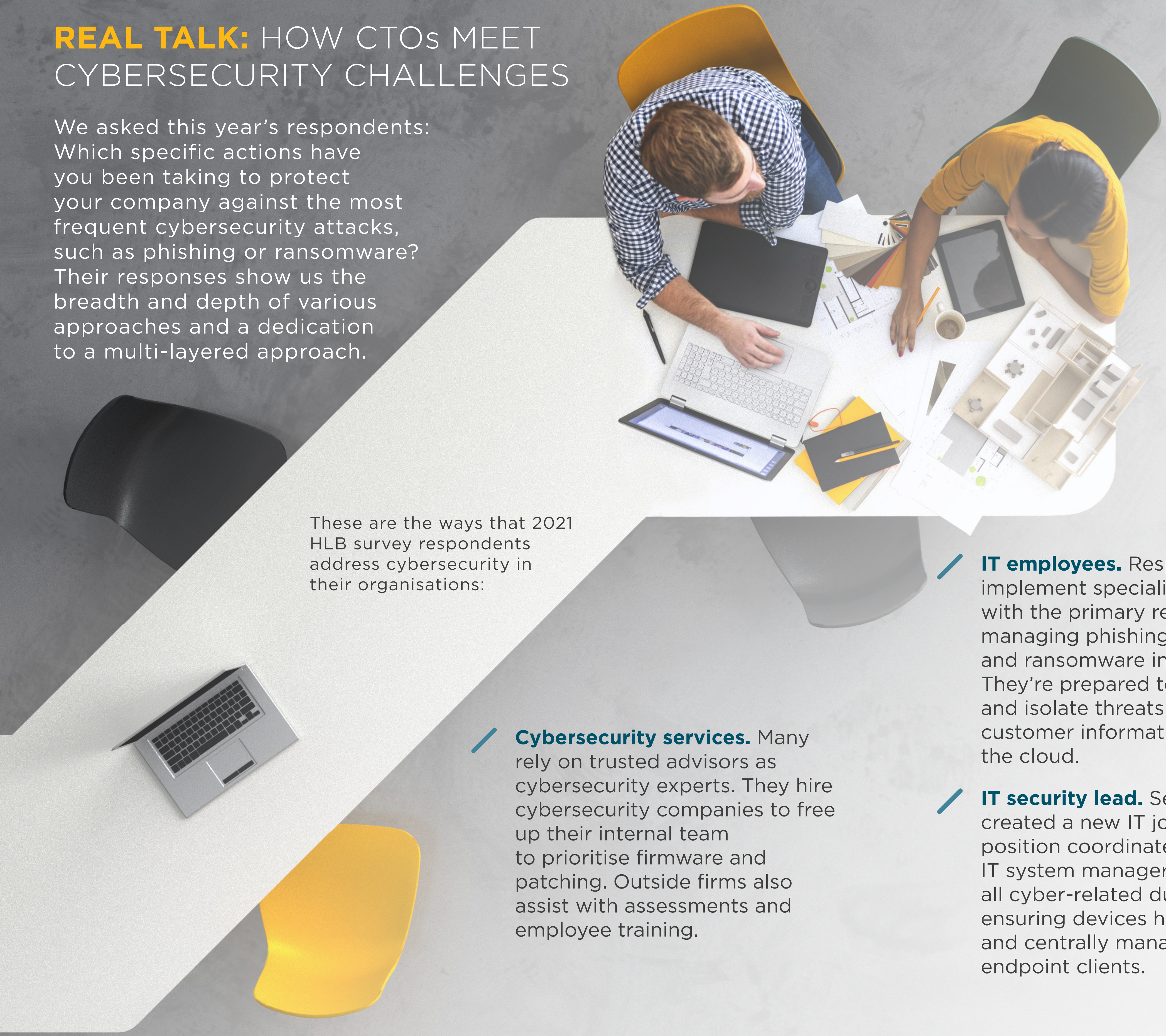
Q: PLEASE RANK THE FOLLOWING ACTIONS TO STRENGTHEN YOUR CYBERSECURITY IN ORDER OF PRIORITY:

RESPONDENTS RANKED THE ACTIONS IN THE FOLLOWING ORDER:

1. DEVELOP AN INCIDENT RESPONSE PLAN
2. CYBERSECURITY TRAINING FOR WORKFORCE STRATEGIES
3. ANALYSIS OF OUR CLOUD COMPUTING STRATEGIES
4. CONDUCT AN INTERNAL RISK ASSESSMENT
5. THIRD PARTY RISK ASSESSMENT

[10] Gartner, 2021. Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021

[11] Mastercard: Riskrecon, 2021. The State of Third-Party Risk Management



REAL TALK: HOW CTOs MEET CYBERSECURITY CHALLENGES

We asked this year's respondents: Which specific actions have you been taking to protect your company against the most frequent cybersecurity attacks, such as phishing or ransomware? Their responses show us the breadth and depth of various approaches and a dedication to a multi-layered approach.

These are the ways that 2021 HLB survey respondents address cybersecurity in their organisations:

- **Cybersecurity services.** Many rely on trusted advisors as cybersecurity experts. They hire cybersecurity companies to free up their internal team to prioritise firmware and patching. Outside firms also assist with assessments and employee training.

- **IT employees.** Respondents implement specialised teams with the primary responsibility of managing phishing and ransomware incidents. They're prepared to identify, track and isolate threats to protect customer information in the cloud.

- **IT security lead.** Several have created a new IT job role. This position coordinates with each IT system manager and oversees all cyber-related duties, including ensuring devices have current and centrally managed endpoint clients.

- **Analytics.** Respondents are also increasing their use of analytics and security event reporting. Monitoring and acting on the three tenets of information security (data confidentiality, integrity, and availability) are essential.

- **Cybersecurity tools.** CTOs deploy various tech tools to bolster cybersecurity efforts, such as using cloud services for disaster recovery, quarantining unknown emails, using account verification for email and encrypting data.

- **Policies and protocols.** Businesses adopt clear procedures for reporting and dealing with suspicious emails, protocols for file versioning and retention and maintain a rapid response recovery plan.

- **Employee education.** From mandated training for network access to company-wide workshops, respondents are focusing on increasing awareness and building good cyber hygiene habits.

CYBERSECURITY: OPPORTUNITY VERSUS THREAT

In this year's survey, we asked respondents if they saw cybersecurity as a threat or opportunity. 45% view it as an opportunity to offer advisory services versus 44.85% who see it as a threat that will consume organisational resources. Fewer than 10% of respondents don't expect drastic changes, whereas over 90% believe the threats will continue to grow at a rapid pace.

Bakkar notes, "I think that there has to be a risk to create an opportunity. If everything was perfect, there would be no opportunity." For the leaders, who are actioning cybersecurity at the senior level and have a framework in place, opportunities are vast.

At the same time, cybersecurity poses a threat. It's costly to implement changes, provide enough resources and prioritise cybersecurity. If these expenses take away from revenue-generating areas, leaders may worry about programme sustainability. Accordingly, respondents worry that the spike in threats is still to come

45%

VIEW IT AS AN OPPORTUNITY TO OFFER ADVISORY SERVICES

10%

OF RESPONDENTS DON'T EXPECT DRASTIC CHANGES

NEXT STEPS: SECURING THE FUTURE

Some organisations lead the industry by moving swiftly to adjust protocols and build frameworks. Others lag but seek out best practices and quick wins while moving towards secure hybrid workplaces. Finally, a minority of leaders have made minimal changes and continue to retain on-site staff secured within the corporate perimeter. In this case, industry, company size or geography may reduce the necessity for remote workers, cloud-based tools or off-site security measures.

However, the fact is that cyberattacks are increasing, regardless of the business size or industry. And sophisticated threat actors continually find new ways to gain access to business-critical data and programmes. While a piece-meal approach works as a temporary fix, a comprehensive cybersecurity strategy, actioned at the senior level, is vital for companies with a long-term hybrid workforce.

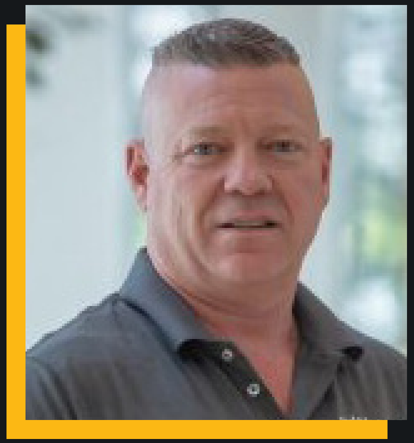
Moreover, one of the best things leaders can do is design employee awareness and education programmes, including campaigns to highlight specific threats and interactive modules focusing on forming good habits. As your company navigates the cyber-risk landscape, our trusted advisors can help. Reach out to us to learn how to take advantage of opportunities while mitigating threats.

GET IN TOUCH

Our cybersecurity experts are ready to help identify risks and secure your business in today's remote working environment. We operate across 159 countries wordwide. Get in touch:

ABU BAKKAR

Chief Innovation Officer
a.bakkar@hlb.global



JIM BOURKE

Global Advisory Leader
j.bourke@hlb.global

CARLOS CAMACHO

HLB Digital
c.camacho@hlbdigital.global

ALMERINDO GRAZIANO

HLB Digital
a.graziano@hlbdigital.global

CARLOS MORALES

HLB Digital
c.morales@hlbdigital.global

GUSTAVO SOLIS

HLB Digital
g.solis@hlbdigital.global

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

HLB THE GLOBAL ADVISORY AND ACCOUNTING 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 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.