HLB CYBERSECURITY REPORT 2020

NAVIGATING THE CYBER-RISK LANDSCAPE IN THE AGE OF REMOTE WORKING

HLB THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

CONTENTS

The COVID-19 pandemic forced many organisations across the globe to adopt remote working and digital processes with record speed. In doing so, CTOs and IT management faced increased vulnerabilities allowing for cyber-attacks and data breaches to take place.

Overnight, organisations went from controlled office environments to diverse home worksites. Continuing business, while securing multiple virtual environments, proved to be a challenge. But remote working is here to stay, so enterprises must adjust and overcome security hurdles.

In light of Cybersecurity Awareness Month 2020, we surveyed 76 IT professionals about their perceptions on information security and data protection in today's complex digital environment. We also spoke with 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 remote working.

IT PROFESSIONALS REPORT CYBERSECURITY CHANGES

Across the globe, companies shifted teams to remote work to reduce disruptions to business when governments announced lockdown measures to prevent the further spread of Coronavirus. While business continuity was the most immediate, and pressing concern, changes also had to reflect the unexpected cybersecurity challenges of virtual workforces.

The results of our HLB survey and expert analysis finds that as time went on, companies settled into remote work yet saw an increase in cyber threats, which led to changes to cybersecurity strategies and protocol for 88% of respondents. HLB's Chief Innovation Officer Abu Bakkar together with Global Advisory Leader Jim Bourke and HLB Digital partners Carlos Morales and Gustavo Adolfo share their experiences alongside responses from IT professionals.

BIGGEST CHALLENGES TO MAKING HOME OFFICES SECURE

From securing personal devices to giving access to virtual private networks (VPNs), CTOs scrambled to get remote workforces running. Initially, the most significant difficulties stemmed from individual home setups, such as:

Home WiFi access. With home WiFi, everything is completely open, and workers use different types of infrastructure, making it hard to standardise. Bourke remarks that organisations went from just a couple of offices to secure, to having as many different configurations to track as the business has employees, when they shifted to remote working from home, creating a massive hurdle.

58%

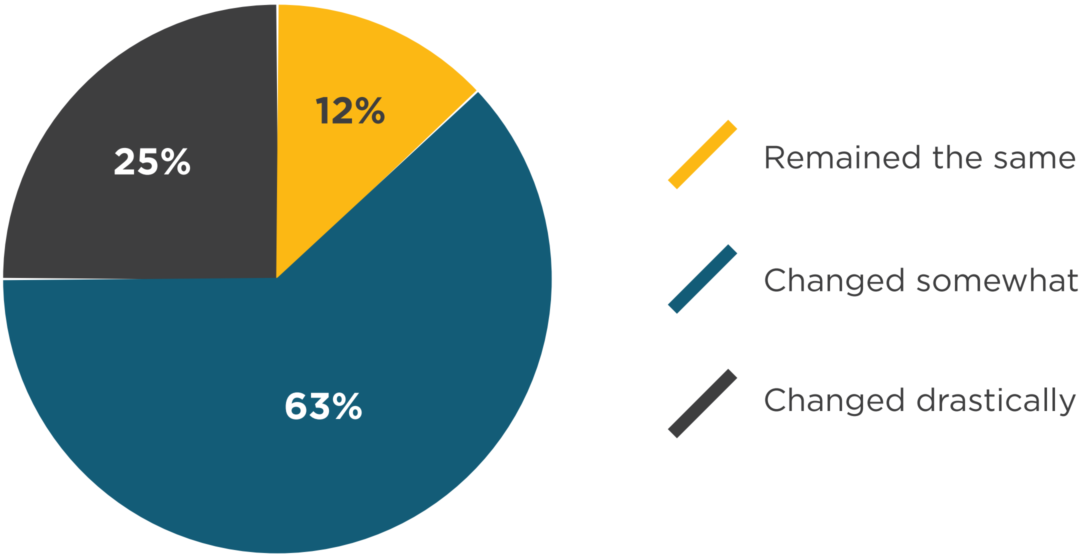
OF ORGANISATIONS WERE NOT PREPARED FOR A REMOTE WORKFORCE

VPN access. Virtual private networks provide safe connections. However, few companies offer access to all employees. Adolfo recognises that companies were using VPN, but it was not widely available for all employees. For example, in some cases only IT staff and people who needed to work remote regularly had VPN access. This was a challenge they had to overcome.

Performance. High-bandwidth video conferencing and various voice technologies strain home networks. Whereas some countries suffer from this more greatly than others, differences in regional infrastructure can affect remote working performance. While office buildings can work around these issues, it's harder when all of your staff are remote.

Figure 1: Cybersecurity strategies changed in response to COVID-19

Q: Since the start of the pandemic, would you say cybersecurity strategies and protocols at your organisation have...



CTOs AND CEOs IDENTIFY AND PRIORITISE URGENT CONCERNS

With any crisis, CEOs and CTOs must act fast. However, during the pandemic, it also required an immense amount of flexibility. According to Bourke, “The top concern, from day one, was access to data to ensure business continuity.”

It comes as no surprise that the first order of business for IT teams was to quickly implement solutions to support the availability of data to the remote workforce and maintain operations as smoothly as possible. But, as time went on, companies found ways to improve data access which shifted their focus to cybersecurity and data confidentiality.

And now, even though four out of five respondents say they’re comfortable with their level of security, they also mention that their top priority is to complete an internal risk assessment. This suggests that they’re confident in their company’s ability to identify and address issues. Still, they also recognise that remote working has altered initial risk assessments, and it is vital to reassess.

MAINTAINING BUSINESS CONTINUITY

Few companies can fully prepare for global locations to face similar challenges of being shut down or not having employees in the office. Bourke says, “Most companies lost that continuity. They were able to do most things, but they couldn’t do everything. And now, they don’t ever want to be in that position again.”

Once organisations shifted to virtual teams, CEOs expressed concerns over staff efficiencies. These trust issues led many to ask, “Can our employees be productive outside the office?" Early on during the pandemic, Morales received multiple client requests for information solutions about employee monitoring systems or monitoring services.

ADJUSTING TO REMOTE WORKING

Even for companies with some remote staff, suddenly having dozens, hundreds, or thousands of employees working from home creates disruption. Morales says, "What we've seen is that many businesses are finding out how to make working from home technology available. Most organisations had local servers at the office, and VPN solutions weren't as solid as they should be." The result was a rapid shift to SaaS solutions like Microsoft Office 365 or Google Drive to share information.

A positive that has come out of the rapid shift to remote working is that the digital adoption process within organisations has accelerated. Those previously sceptical about collaboration platforms and video calls to interact with others now had no choice but to adopt these technologies. Many have found them far more user-friendly and efficient than they thought and have changed their perceptive on them. The initial CEO mindset of worrying about efficiencies resolved, as remote workers demonstrated efficiency.

ADDRESSING OFF-SITE CYBER-RISKS

With a quarter of respondents saying they've had to make drastic changes to their cybersecurity strategies and protocols, many organisations looked for ways to transfer their organisational cybersecurity objectives into employees' homes. After all, the isolation of remote work makes organisations more vulnerable to cyber-attacks.

> "Many organisations were prepared for cybersecurity. But what they weren't prepared for was cybersecurity concerns in a remote work environment. Decision-makers didn't anticipate that their entire workforce would be working virtually. So now their mindsets shifted again to ask how can we protect our confidential and private data that all our employees need access to while working from home?"
>
> **JIM BOURKE**
> **GLOBAL ADVISORY LEADER**

CYBER-ATTACKS ON THE RISE IN 2020

From mobile security threats to unauthorised access to files, recent cyber-attacks shed light on an increasing problem. These online assaults may affect multiple networks and computers. It disables programs and steals data. Cyber-attacks may also use your remote workers' computers to launch additional attacks.

Cyber risks include reputational damage, financial loss, and disruption to business operations. The threats are widespread with our survey finding that:

- 53% of respondents were aware of unusual cyber-related activity and/or attacks since the start of the pandemic;
- 12% reported their organisation had been breached;
- yet, the remaining 35% responded they had not noticed a difference.

Unfortunately, without reassessing cyber-risk and adjusting protocols, its possible many organisations don't yet realise existing cloud computing threats and vulnerabilities. Bourke comments, "Knowing that 65% of organisations have been or may have been exposed during this period is scary! And out of the 35% who didn't notice a difference, how many of them may have missed a potential breach of data?"

WORKFORCE ISOLATION AND PHISHING ATTACKS

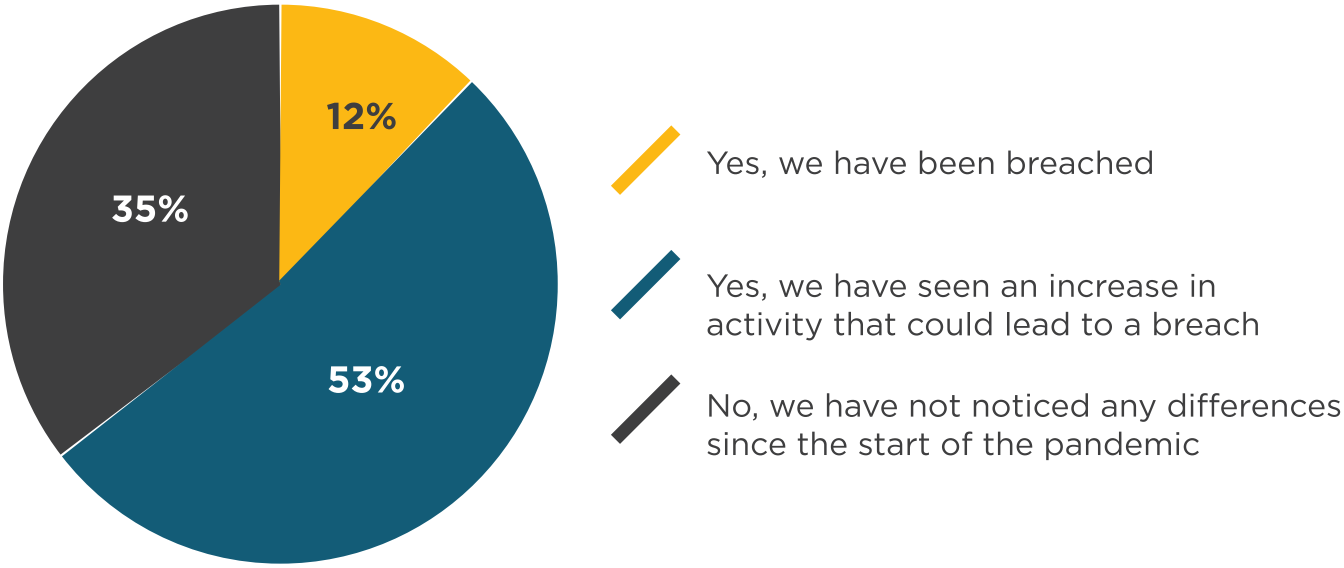
Our experts' overwhelming opinion is that phishing attacks are increasing, with a trend pointing to cyber-attacks involving employee login details to their virtual work platform being targeted. These primarily ask users for their logins on tools like Microsoft Office 365 or Dropbox.

According to Bakkar, social engineering is also rising. He says remote workers may be more vulnerable to phishing emails that get people to click on a link. This is especially true with employees who attend physical or virtual events and leave a digital footprint. Bakkar shared a recent instance when hackers followed their target, an event attendee, on social media to see what they were doing. Then they sent him an email seemingly from the event organisation with the message “here’s your invoice.” In this case, the target knew to double-check the request before paying the invoice. However, many newly remote workers may simply open the document or click on a payment link. The fact that so many of our processes have changed in a short period of time and have become less personal due to their remote and digital nature, it is easier to social engineer an attack.

Social isolation also plays a role here, as in an office environment, you’d ask a co-worker for their input or pop into the administrative assistant’s office to double check what you received is correct if you have a moment of doubt. But remote workers must make these small decisions on their own and often, the consequences can be disastrous.

Figure 2: Organisations notice increase in suspicious cyber activity

Q: Have you and/or staff members at your organisation noticed any unusual cyber-related activity and/or attacks since the start of the pandemic?



COMPANIES ARE OVERCOMING DATA PROTECTION HURDLES

With business continuity addressed, organisations turned to security. But there isn't a one-size-fits-all solution to this complex problem. Instead, professionals must assess a range of pressing issues then develop an approach that works outside of the office. When asked to rank five actions in order to strengthen cybersecurity in order of priority, respondents provided the following ranking. HLB experts provided commentary to each:

1. Conduct an internal security risk assessment:
Changing infrastructure to allow data availability makes businesses more exposed, which is why our respondents listed internal security risk assessments as a top priority.

2. Update cybersecurity training for workforce:
Attackers exploit vulnerabilities in software like Microsoft Office 365 and Zoom. As a result, training programmes and objectives need to be revised. Many organisations already rolled out additional cybersecurity training videos to meet new challenges as new ways of working were adopted.

3. Develop a cybersecurity incident response plan:
Many cybersecurity incident response plans relate directly to the corporate offices, not remote workplaces, which makes it essential for CEOs to reassess their reporting procedures and responses.

4. Revisit cloud computing strategies:
As organisations move through various stages of digital transformation, the three tenets of information security prove vital. To meet this challenge, executives must understand where data availability, confidentiality, and integrity fit into home offices.

5. Complete third-party cybersecurity risk assessments:
Although our respondents listed this low on their priority lists, our experts point out how security risks include our interactions with third-party vendors. Our interconnected supply chain means that what happens to your supplier can affect any number of your remote team members or the entire organisation.

"One of the positive side effects of the pandemic and rapid shift to remote working is that the adoption speed of digital processes and platforms by employees has accelerated. Where some people were slow to adjust to new, more digitised ways of working before, now they did not have a choice."

ABU BAKKAR
GLOBAL CHIEF INNOVATION OFFICER

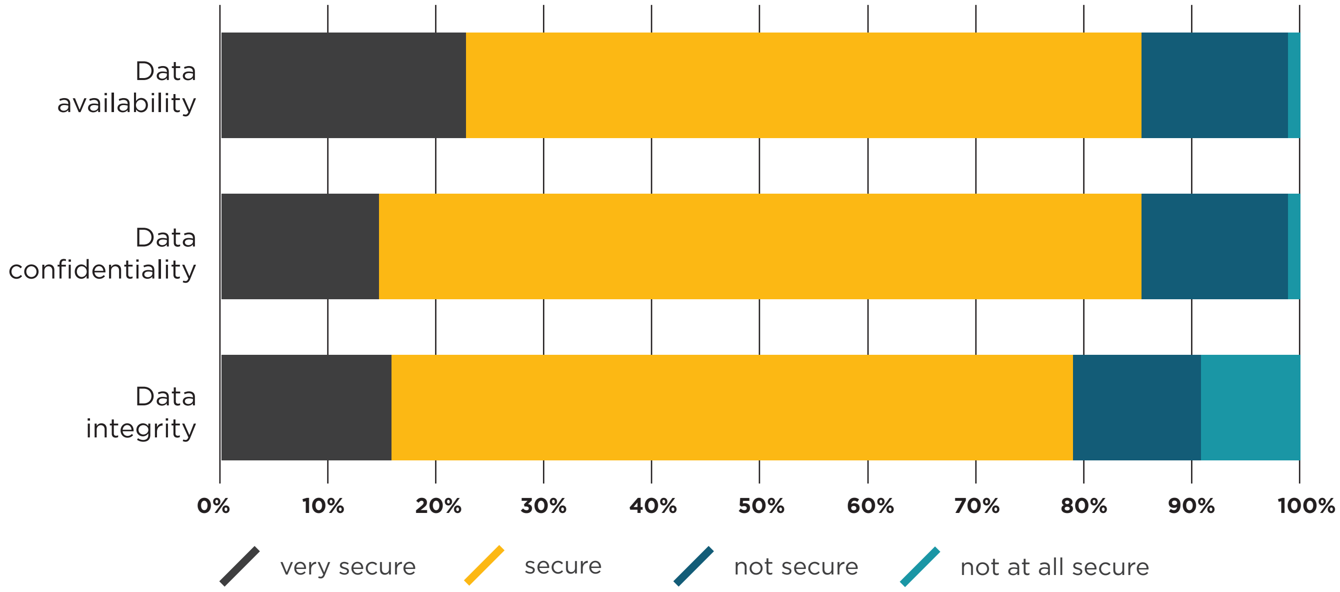
STRENGTHENING YOUR CYBER-RISK MANAGEMENT STRATEGY

When asked about the level of security across the three tenets of information security, one in five respondents doesn't believe their online systems are secure. In a regular work environment, it's simply unacceptable for anything less than 100% security. But with remote work, we're seeing 21% of respondents question their data integrity.

Bourke notes, "From a cybersecurity month perspective, it's worth noting that the question about data confidentiality should have been answered with 100% secure. We have rules and regulations, like GDPR, so we should be secure." Yet, some organisations have trouble managing data security as they would under normal circumstances and have not yet completely caught up.

Figure 3: One in five do not consider tenets of information security 100% secure

Q: How secure do you consider the following three tenets of information security at your organisation?



To manage cyber-risk, it's necessary to adapt the three tenets of information security to remote working environments:

Data confidentiality. The idea is to ensure information is only provided to those who are authorised to manage or view it. Measures are designed to protect against unauthorised disclosure of information. In an office environment this is easier to enforce whereas when users are working remotely it becomes increasingly complex and risky.

Data integrity. Stakeholders and employees at all levels must have confidence in the systems and data. Moreover, data integrity is a key component of meeting regulatory compliance standards. Ensuring the quality of the data you collect and keeping it up to date comes down to internal access and data management. The principle of integrity is designed to ensure that data can be trusted to be accurate and that it has not been inappropriately modified.

Data availability. The objective of availability is to ensure that data is available to be used when it is needed to make decisions. For remote working to work, your people need access to the data they need to do their job. It's as simple as that. But balancing availability with confidentiality and integrity requires strategic planning and infrastructure.

Every threat to security is not necessarily malicious. Major security breaches have been caused by well-intentioned users, which is why security training is essential. Access to data should be given to users on the principle of least privilege, which means that the level of access given to users should be confined to what they need to accomplish their duties.

LESSONS LEARNED FROM LOCKDOWN

When the pandemic hit, and many countries adopted lockdown measures to prevent COVID-19 from spreading, business leaders' priority was business continuity. However, the cyber-risk management lessons learned continue to build on the common themes of agility and resilience.

LESSON 1: Improve cybersecurity training and support

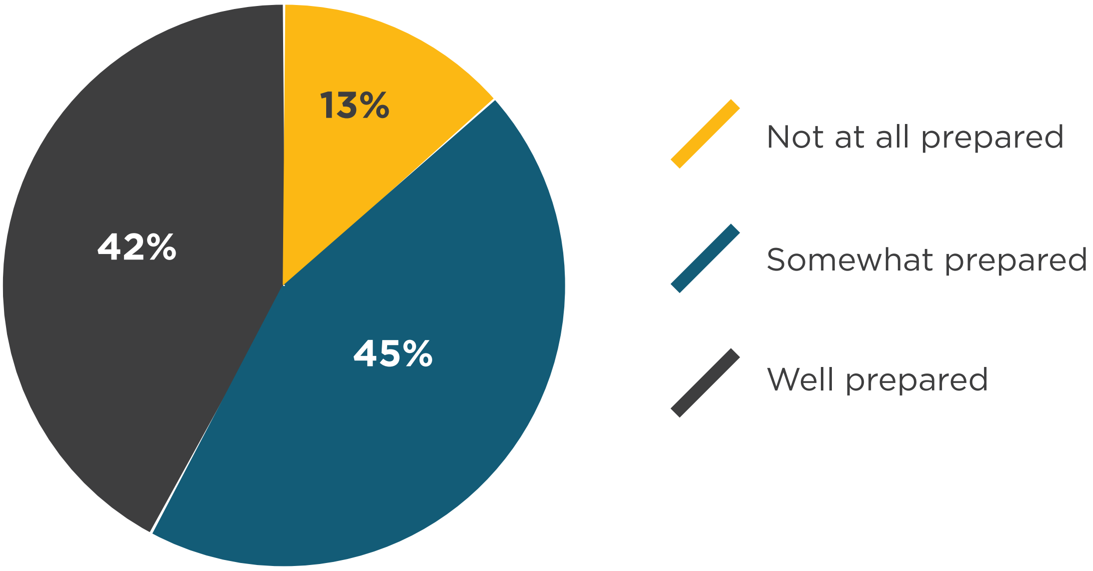
It takes a 360-degree approach to manage cyber threats. Workforce training ranked second in terms of priority as indicated by our respondents. Morales reports an increase in questions from business leaders about making and enforcing rules for remote offices. This is a tricky area, because "you can have an NDA for your employee, but you can't have an NDA for a life partner, cousin, or anyone else in the home." Keep in mind that people may unintentionally or without maleficent intent leak information. So, preventing leaks of confidential information can get complicated in remote environments.

However, increased awareness and training can combat this issue, along with addressing the heightened risk of phishing scams and other cyber-attacks. Adolfo says, "The isolation of people is a risk factor. You have secluded people, and they have to make decisions on their own." The fact that this makes them more vulnerable is something they might not be aware of and is something that needs to be addressed in security training fit for the current circumstances.

Moreover, Bakkar claims, "Your workforce is your most significant asset yet also your biggest liability. You can increase protective measures, but if your people are not trained, then they give access to the wrong people and open your organisation up to vulnerabilities." Combat this by assessing your support channels, surveying your employees and identifying ways to help them navigate remote work safely and securely.

Figure 4: Levels of readiness for lockdown varied

Q: To what extend were your IT infrastructure and cybersecurity protocols prepared for lockdown and remote working?



LESSON 2: Don't wait to prepare IT infrastructure and cybersecurity protocols

While 42% of IT professionals claim the IT infrastructure and cybersecurity protocols of their organisations were well prepared for operating the business remotely, the majority stated they were somewhat prepared (45%) or not at all prepared (13%) for lockdown. Bakkar says, "Everything happened in such a quick, short time. If your infrastructure is not set and ready, then you have issues with data confidentiality and figuring out who has access to what."

Infrastructure plays a crucial role in data confidentiality, so now that data is accessible in more places, professionals are under pressure to address their approach to cybersecurity and regulatory compliance standards while people remote work. According to Gartner[1], companies must invest "to protect the technologies that support their business outcomes. Understanding an organisation's most important outcomes, its most important processes, and its most important technology outcomes are the first step in putting a business context around cybersecurity."

[1] Gartner, 2020. *The Gartner Business Risk Model: A Framework for Integrating Risk and Performance*

LESSON 3: Think long-term relief not short-term solutions

Organisations did not anticipate the length of time the workforce would be working remotely for.
While data availability was the first concern, now as remote working looks like it's here to stay, data security needs to be strengthened. Bourke says, "CTOs may have been prepared for employees to work remotely, but they weren't ready for the cybersecurity concerns around employees working remotely for an extended period of time. They didn't anticipate cybersecurity concerns with a stretch of months or maybe a year or more."

Whether you believe remote working a temporary solution while the world combats a pandemic, or that it is here to stay for good, you need to start thinking long-term relief. Just as businesses are reviewing their office space leases and plan to scale down the amount of office space they use, so should CTOs plan for cybersecurity in a world where people will not return to a single controlled office environment.

LESSON 4: Regularly assess cloud computing threats and vulnerabilities

A recent study by Oracle[2] reports that two-thirds of senior executives say cloud native is integral to their firms' competitiveness. The way we are operating today and accessing data is different from the way we were working a year ago. Adolfo notices a considerable jump in requests for internal security assessments. "Everyone's focus is on internal security. The pandemic has given rise to this assessment; everyone wants to know if they're good. So when we go in and do these assessments, we're finding exposure in areas not anticipated before the pandemic."

While data availability was essential to business continuity, data confidentiality and data integrity have become more challenging to govern. It is likely circumstances will be ever changing and therefore advisable to conduct regular assessments of vulnerabilities. In particular as they relate to cloud computing.

[2] Oracle, 2020. *Cloud 2020: Cloud Accelerates with Urgency*

''We are all part of the business ecosystem. This means that we are very interrelated and depend on our suppliers. So when a supplier of ours is hit by a cyber-attack, it will affect us as well.''

GUSTAVO ADOLFO
PARTNER, HLB DIGITAL

LESSON 5: Addressing cyber risk is an organisation-wide exercise

As we've noted, a current top priority for IT professionals is doing an internal risk assessment. But don't limit conversations to only business leaders. It's essential to start a company-wide conversation about the three tenets of information security. Traditionally, digital transformations take a long time. But under the current circumstances, adoption of digital technology has been accelerated. To get everyone on board with your cybersecurity strategy, it's necessary first to get buy-in from decision-makers. Then empower them to get everyone else behind your program.

It is important to avoid reactive fear-based decision making. Often this is the result of asking staff and stakeholders the wrong questions leading to poor cybersecurity investments. The ultimate focus should be on addressing employee behaviour and helping them realise how they impact security as a whole.

KEY TAKE-AWAYS: CYBERSECURITY AND REMOTE WORKING

So what can your organisation do to promote cybersecurity awareness during the age of remote work? Our experts offer their top tips for managing your cyber risks while supporting your virtual workforce.

ACKNOWLEDGE THE RISKS

Carlos Morales suggests that an underlying issue in most cybersecurity concerns is that many companies don't realise their vulnerabilities. Business leaders focus on continuity and giving people access to the data they need to work. But it's essential to acknowledge that the current circumstances increase risk and may lead to a data breach or privacy concerns.

ASSESS YOUR ENTIRE CYBERSECURITY PROCESS

Jim Bourke recommends revisiting cybersecurity training for workforces. And if you haven't done a cybersecurity assessment in the last six months, then you need to do one immediately. Lastly, it's essential to re-examine your cyber risk within and outside of your organisation. For instance, you rely upon your vendors and your customers. Their security concerns become yours.

"The first step in tackling cyber-risks is acknowledging they exist, and they are a real thread to the business. And that is something that, at least in Central America, I don't think always is the recognised."

CARLOS MORALES
PARTNER, HLB DIGITAL

ANALYSE DIGITAL INTERACTIONS IN AND OUTSIDE OF YOUR COMPANY

Gustavo Adolfo agrees with Bourke and adds that risk assessments need to rely on data analysis to determine if rules have been broken or if unusual activity or abnormal parameters in business occurred. Because it's possible that respondents who reported no data breaches or changes in activity that could lead to a breach, simply haven't noticed them. Moreover, our business ecosystem and current events highlight the dependencies we have with vendors. These third-party companies are embedded in our supply chain or daily operations, making them more critical than in previous years. It can be possible for cyber criminals to find a way into your organisation via your vendors.

81% OF BUSINESS LEADERS ARE EXPLORING MORE FLEXIBLE WORKING ARRANGEMENTS[3]

BUILD CYBERSECURITY INTO YOUR BUSINESS STRATEGY

According to Abu Bakker, cybersecurity isn't just about protocols; it needs to be part of your overall business strategy. CEOs must work closely with their CTOs and IT consultants, and recognise the investment needed in this area. Organisations require the right technology, so cloud adoption is critical. But your teams must know how to use it, making training equally important. By combining all facets into your strategy, you'll present a consistent and comprehensive approach to cybersecurity.

3. HLB International, 2020. *HLB Survey of Business Leaders: The Execution Challenge for New Decade*

NEXT STEPS: IDENTIFY YOUR CYBERSECURITY RISKS AND COUNTERMEASURES

So are you one of the 53% of IT professionals who've noticed an increase in activity that could lead to a data breach? Or could it possibly have gone undetected in your organisation? As attacks continue to increase globally, executives must adjust operations to account for changes while finding innovative ways to build resilience into every aspect of a business. Take your next steps by:

- Start with a Cloud risk assessment checklist.
- Assess third-party vendor risks.
- Analyse data sets to see if any breaches already occurred.
- Identify the role your cybersecurity measures play in your business strategy.
- Develop cybersecurity training for remote workforces.

CONTACT US

Our cybersecurity experts are ready to help identify risks and secure your business in today's remote working environment. We operate across 158 countries wordwide. Get in touch:

Abu Bakkar
Global Chief Innovation Officer

a.bakkar@hlb.global

Jim Bourke
Global Advisory Leader

j.bourke@hlb.global

Gustavo Adolfo
Partner, HLB Digital

g.solis@hlbdigital.global

Almerindo Graziano
Partner, HLB Digital

a.graziano@hlbdigital.global

Carlos Morales
Partner, HLB Digital

c.morales@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.

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.