THOUGHT LEADERSHIP 01

Cybersecurity and the hybrid workplace

PRAXITY™
Empowering Business Globally

Cybercrime is easy these days

The explosion in 'anywhere' working, increasing reliance on cloud computing and evermore complex supply chain networks has left independent accounting firms and their clients more exposed than ever to the risk of a devastating cyberattack. In this special feature we examine the key threats and how to ramp up security to protect staff, networks and systems. We showcase best practice within Praxity Global Alliance and demonstrate how firms are working together to support each other and their clients.

Cybercrime is easy these days. External hackers can breach 93% of company network perimeters and gain access to local network resources. Even more alarming, internal hackers can easily gain full control of 100% of company infrastructure, according to research from security specialist Positive Technologies.

Cyberattacks are growing in number and scale. The most damaging can cost an organisation millions of dollars and seriously impact brand and reputation.

The onset of the pandemic saw a 300% increase in cybercrimes reported to the FBI's Internet Crime Complaint Centre, as both domestic and international hackers took advantage of increasing activities online. During this time, the rise in the 'anywhere workforce' has created a surge in sophisticated cyberattacks and material breaches.

In a report by cloud services provider VMware, 76% of global cybersecurity professionals say attacks increased due to employees working remotely. The number of attacks is rising sharply although not all of them are successful due to increased security protection. 2021 saw an average of 270 attacks per company globally, an increase of 31% on the previous year, according to IT firm Accenture, while IBM research shows the average cost of a data breach is $4.24m.

Analysts predict cybercrime costs will grow by 15 percent per year to reach $10.5 trillion USD by 2025, up from $3 trillion USD in 2015. These costs range from theft of intellectual property and financial data to post-attack disruption and damage to reputation. A significant chunk of cybercrime is likely to result from attacks on devices used outside a main office, or an attack on poorly protected cloud-based data.

The cost of inaction

£80 Million Fine

$575 Million Fine

The consequences of even a basic breach can be catastrophic, not only in terms of the breach itself but also the fallout if an organisation fails to take appropriate action to mitigate the risk.

In one of the biggest data breaches to date, hackers gained access to sensitive information held by Equifax, the U.S. based multinational consumer credit reporting agency. The breach affected 147 million people. After an investigation, Equifax Inc. agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories, which alleged that the credit reporting company had failed to take reasonable steps to secure its network.

Similarly, UK communications firm TalkTalk suffered huge damage to its reputation after failing to take simple steps to patch up a known vulnerability. TalkTalk suffered an SQL (structured query language) attack whereby computer code is used to hack databases and steal information.

In this case, attackers targeted legacy web pages operated by TalkTalk following a company acquisition. The hackers gained access to 160,000 customers' personal data, including bank account numbers and sort codes. An investigation by the Information Commissioner's Office (ICO) concluded TalkTalk should have known the legacy pages existed and that despite two previous attacks on the same vulnerable page, the company didn't take any action and its software was outdated.

Announcing a penalty of £400,000, Elizabeth Denham, Information Commissioner, said: "Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this because they have a duty under law, but they must also do this because they have a duty to their customers."

The attack on TalkTalk cost the organisation more than £80 million and resulted in the loss of 101,000 existing customers, according to Information Age. TalkTalk's former CEO Dido Harding subsequently vowed to be more transparent. Following the attack, Charles Bligh, former MD of TalkTalk Business, Technology said the company introduced substantial improvements. In monitoring, security and prevention. The business also underwent a cultural change to ensure board members ask the right questions and to improve the decision-making process.

Cases such as this are no longer the exception. Vulnerabilities can exist throughout an organisation, from remote workers using equipment such as cameras and printers through to cloud-based storage and external suppliers. Moreover, today's cybercriminals are not only targeting weak links to internal networks, they are launching coordinated attacks on entire supply chains.

Equifax

Talktalk

Key threats

At the most basic level, the threat of cybercrime can be as simple as an easy-to-hack password, unsafe link, or cleverly-worded email to induce individuals to reveal personal information (phishing).

Increasingly, the threat comes from software devised to disrupt, damage or gain unauthorised access to a company system (malware), often resulting in a hefty ransom demand (ransomware). In 2021, one in 61 organisations globally was being impacted by ransomware each week.

One of the biggest ransomware attacks to date occurred in the U.S. where hackers gained entry to Colonial Pipeline infrastructure by stealing a single password. The attack shut key conduits delivering fuel from Gulf Coast refineries to East Coast markets for days. This triggered a spike in gasoline prices, panic buying and localised fuel shortages. Colonial Pipeline later claimed it had paid the hackers nearly $5 million to regain access, according to Reuters.

The threat of ransomware and other attacks has dramatically increased as a result of the global shift in work patterns. The most vulnerable are remote workers, especially if using personal devices to access data while at home or on the move.

Employees working from home using public networks are a sitting target because their data is easily exposed. Insecure devices linked to laptops such as printers and cameras also present weak points.

In research by NCC Group, Which and the Global Cyber Alliance, thousands of hackers attacks were launched on smart home devices such as TVs and wireless printers. The 'honeypot' test resulted in 12,807 attacks in a single week, almost a fifth of which were attempts to log into a device with a weak default username and password. The most concerning issue was a connected camera with poor password protection, allowing hackers to gain access to the camera stream.

"If the connection isn't properly secured and encrypted, it creates an access point for attackers"

Jorge Rey, Chief Information Security Officer at Praxity member firm Kaufman Rossin in the U.S., says: "While working remotely, we're constantly sharing sensitive information over the internet. If the connection isn't properly secured and encrypted, it creates an access point for attackers and your data could be exposed."

"When employees use personal devices to conduct business, the organization has no oversight of those devices' setup, which may not include proper encryption or the latest version of an operating system. Critical security patches may not have been installed on employee laptops for more than six months."

Sharing documents on the 'cloud' can increase vulnerabilities. Chris Allen, IT Director at Praxity member firm Shorts, based in the UK, explains: "Users have adopted 2FA (dual-factor authentication) quite successfully, but sharing documents via our permitted cloud services gives issues with the propagation permissions and the associated data leakage, sprawl and oversharing."

There are also issues over the length of time data is shared and when clients and third parties invite users to connect to cloud services such as Dropbox. "Recordings of video conferences and screen sharing present a particular issue. Chris stresses the importance of ensuring that users check what data is on screen before sharing the screen and allowing third party recordings of such data. He also warns of the dangers of logging into Teams or Zoom on someone else's PC and not fully signing out, leaving data exposed.

Jorge says connecting to the cloud through third party applications is "the biggest challenge" facing businesses in the hybrid environment and creates a "high area of risk". The other main challenge is user access, Jorge states, adding:

"We see companies' data being compromised because stealing credentials has become easier for hackers."

As cybercrime becomes increasingly sophisticated, businesses large and small require much broader cybersecurity strategies in a bid to identify and sure up weak points in their operations, support supply chains, and keep disruption to a minimum in the event of a major attack.

Heightened risk

Given the increased threat across different environments, coupled with different security requirements in different industries and geographies, it is little surprise that cybersecurity and regulatory compliance are now regarded as the top two biggest concerns of corporate boards.

Indeed, over the past five years, the percentage of boards that consider cybersecurity a business risk has risen from 58% to 88%, according to Gartner.

Accounting firms are only too aware of the increased threat. A recent survey by Praxity reveals most accounting and IT/cybersecurity leaders believe a cyberattack is "very likely" or "extremely likely". In a sample of independent accounting firms across the world, the main concern is the threat of ransomware, followed by phishing/malware attacks and identity theft.

SMEs with poor cybersecurity controls are particularly at risk of an attack, either from a lone wolf or a criminal gang. There is a danger companies could be caught up in global cyber attacks, including attacks stemming from the Russia Ukraine conflict and other regional and global crises.

"Too many local businesses are unaware, unprepared and unprotected"

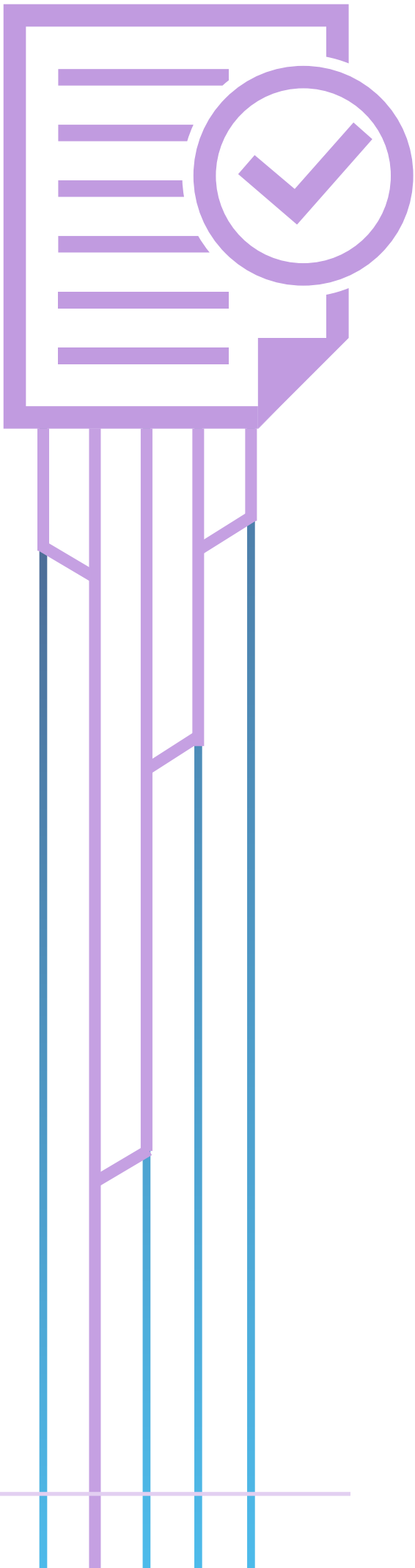
Adam Hack, Head of Security Operations at security specialist Nuago, says unsuspecting local businesses may be targeted by overseas-based criminal organisations looking for vulnerable targets beyond the geography of the current conflict.

In an article published by Australian Praxity member firm William Buck, Adam Hack says the threat level to SMEs has definitely risen during the Russian invasion of Ukraine, adding:

"Unfortunately, SMEs are often their own worst enemy when it comes to cyber security. Despite the heightened risk, it's worrying that too many local businesses are unaware, unprepared and unprotected."

This lack of protection is highlighted in a William Buck Survey of Business Expectations which found 42% of SMEs in South Australia did not have any formal risk management plan in place. William Buck Audit and Assurance Director Matthew King says the impacts of a cyber attack can be far-reaching. "It can cause significant financial, productivity and data loss as well as reputational damage," Matthew says. "Employees, customers and the whole supply chain can become compromised, which can have longer term consequences for your business."

Regulation & guidance



The cybersecurity challenge facing accounting firms and their clients is not helped by the fact regulation is often lacking and confusing to negotiate in different industries and geographies.

Businesses have to deal with various competing laws across different jurisdictions, such as retention period for data. Definitions vary regarding what constitutes a cybersecurity incident and when regulators and consumers need to be notified.

In an article calling for better and more consistent regulation, the World Economic Forum says "global cybersecurity and privacy regulations – while well-intentioned and seeking to contribute positively to the daily onslaught of emerging cyber threats – give limited consideration to harmonisation between countries", adding:

"The result, unfortunately, is discordant and confusing, like each section of an orchestra playing in a different key. This creates complex and costly processes for compliance obligations across industries and makes it difficult for new innovators to become cybersecure."

Accounting bodies are endeavouring to provide some clarity with guidance to help organisations demonstrate the effectiveness of their cybersecurity measures. The AICPA (American Institute of Certified Public Accountants) has developed a cybersecurity risk management reporting framework to help organisations as they provide relevant and useful information about the effectiveness of their cybersecurity risk management programs. The framework is a key component of a new System and Organization Controls (SOC) for cybersecurity engagement, through which a CPA reports on an organisations' enterprise-wide cybersecurity risk management program. The aim is "to help senior management, boards of directors, analysts, investors and business partners gain a better understanding of organisations' efforts".

Accounting bodies are also assisting with identifying the right insurance for cyber risks. The ICAEW (Institute of Chartered Accountants in England & Wales) says audit and accountancy firms are particularly vulnerable to attacks because of the type and volume of data they collect, process and hold. All audit firms, whatever their size or structure, need to factor cyber risks into their business risk protection strategies, the ICAEW says.

The hybrid factor

The cybersecurity issues facing accounting firms and their clients have been exacerbated with the explosion in remote and hybrid working. This global shift in work patterns has provided an open door for cybercriminals to infiltrate poorly protected systems, exposing individuals and businesses to embarrassing and potentially catastrophic cyberattacks.

In a report in Forbes, cybersecurity expert Gopi Sirineni, President & CEO of Axiado, says remote working exposed cracks to company networks in three main areas:

- **Employees active on networks outside normal hours, when in-person security monitors were not active.**
- **Employees accessing shared networks from multiple devices, including personal ones with less protection than company computer.**
- **Outsourcing jobs to lower-cost jurisdictions and providing contractors with access to databases.**

There appears to be a false sense of security in the hybrid environment. An IBM Work From Home study conducted in 2020 reveals that while 93% of those newly working from home were confident in their company's ability to keep personal identifiable information secure, 52% were using personal laptops for work, often with no new tools to secure it, and 45% hadn't received any new training.

The growth in flexible working has impacted virtually every industry sector, especially accounting and finance, where a large proportion of employees continue to work from home at least part of the week.

This trend – and the increased cybersecurity risk it poses – is highlighted in the Praxity survey. Of the independent accounting firms surveyed, all have adopted some form of hybrid model. At least 50% of employees work partly from home among those firms surveyed, and the majority of firms expect this percentage to rise.

"Working from home is no longer a choice but a new normal for our employees"

In Finland, workstation usage at the main Helsinki office of Praxity member firm Oy Tuokko is only 24%, demonstrating the ongoing impact of the pandemic but also changing employee preferences. Sanna Lehtikanga, Oy Tuokko's Administrative Specialist, Systems Support, says: "Hybrid working has become the new norm for our offices. Working from home is no longer a choice but a new normal for our employees."

For Praxity member firm Aronson in the U.S., the shift to 'anywhere' working during the pandemic has been dramatic. Previously, the firm had a central office in Maryland with tri-state coverage. Now, employees are spread across 25 states, all requiring high levels of protection to connect to data remotely.

Azunna Anyanwu, Chief Technology Officer and Director at Aronson's Technology Advisory unit, says the change in the way people work, which began long before the pandemic, resulted in a shift in the firm's protection model and mindset. He explains: "Everyone wants to connect to the office 'crown jewels'. When they work from home, they have to connect via a VPN (virtual private network) to get to those crown jewels.

Prior to the pandemic, we identified the end point as an area of risk and we invested in tools such as EDR (end point detection and response), multi-factor authentication and anti-virus software."

"Over the past two years, the typical enterprise has been turned inside out."

Being able to pivot in this way is critical. Peter Firstbrook, VP Analyst at global research consultancy Gartner, says: "Over the past two years, the typical enterprise has been turned inside out. As the new normal of hybrid work takes shape, all organizations will need an always-connected defensive posture and clarity on what business risks remote users elevate to remain secure."

The way forward is to develop a flexible cybersecurity strategy to provide greater levels of security across different environments and keep disruption to a minimum in the event of an attack.

Getting the basics right

The scale of the cybersecurity challenge facing business leaders and security chiefs cannot be underestimated. Those responsible for security typically need to address a broad range of issues including:

- **Securing business data remotely.**
- **Complying with data security regulations in different jurisdictions.**
- **Improving security for individuals working outside the main company office with, for example, encryption and new protocols.**
- **Reducing the burden on overstretched I.T departments.**
- **Training employees to be more aware of the threats.**

It can be difficult to know which cybersecurity measures to prioritise, especially when budgets and employee resources are stretched. This is evidenced in the Praxity survey which reveals the biggest cybersecurity challenge for independent accounting firms is keeping pace with evolving threats. This is followed by mitigating the strain on IT resources and securing data that can be accessed remotely. The survey reveals a similar picture for clients although encryption and multi-factor authentication is seen as a bigger challenge among clients than accounting firms, largely because many firms have already invested in this aspect of security.

Securing data accessed in the office and remotely should be the number one priority. The risk of employees working from home using public networks with restricted bandwidth can be mitigated with the use of VPNs which provide greater security by ensuring information is encrypted even when working remotely. Identity-first security is critical. Organisations need to adopt multi-factor authentication, where a user is required to provide two or more verification factors to gain access to an application, account, or VPN.

"The first step to protecting your business data is to ensure that everyone's wireless connection is properly encrypted"

Jorge Rey says: "The first step to protecting your business data is to ensure that everyone's wireless connection is properly encrypted. Instruct your teams to turn on full encryption from their wireless access point and set up strong passwords."

Tom Gardner, IT Manager at UK Praxity member firm Rouse Partners, points out: "Regardless of a hybrid setup, the users will always be the greatest point of vulnerability for any common IT environment and thus the biggest cybersecurity challenges usually revolve around authenticating them. This takes many forms, including guarding against user mistakes, preventing phishing attacks and social engineering. Yet security is always a trade-off versus convenience and finding the correct balance point will be unique for every business."

Tom adds: "Security methodologies are clearly moving away from very outdated user plus password-based authentication, to multi-factor authentication including biometrics and conditional access policies as standard. Combining this with Single Sign-On (SSO) based authentication for authorised apps, gives you an outcome instead of each user having a whole load of weak passwords to remember. You can instead ensure a very robust single-point authentication for your user, and automatically grant access to all the cloud-based applications they require from that one authenticated login. It's 'AVA' (Authentication, Security-policy Validation and Authorisation) all in one go. This hugely reduces administrative burden, user burden, provides a single-pane-of-glass for logging or diagnostics and creates a more seamless user experience too."

Ongoing employee training is essential. Security incidents are often caused by employee error and remote workers may not have the same level of IT assistance as their office-based colleagues. It is important employees are aware of security protocols and stick to them, wherever they work.

Shorts' Chris Allen says IT functions must be aware of services being connected while users need to understand the risks of accepting just any invitation to access a cloud service. He adds: "We will be working towards educating our users in sharing and collaborating. Making sure that files are only shared for limited time and are shared to the right person."

Many organisations have developed incident response plans with clear actions for employees in the event of a security breach. These plans need to evolve to reflect the fact different staff will be working in different locations on different days.

For Aronson employees, training is ongoing. Azunna Anyanwu explains: "Previously, we didn't have a formal training programme in place; we just a had a tool with various training courses linked to it. We then shifted to a micro-learning approach. For three weeks in a month, employees receive three-minute videos. In the fourth week, they do a quiz to validate what they have learnt."

The various models and tools to improve cybersecurity can be baffling, but there are a few basic steps every business should take. Jorge Rey recommends the following:

Communicate

Make sure everyone is aware of your remote work policy and cybersecurity best practices, and make your IT team easily accessible.

Secure your WIFI

Use proper encryption and strong passwords, and instruct employees to turn on full encryption from their wireless access point.

Secure cloud-based services

Make sure you have enabled paid-for document-sharing tools, not free versions, for added security.

Set up multi-factor authentication and encryption

Give an email address or a cell phone number for codes to be sent and enable notifications so you can see when someone has tried to access your data or to change your password.

Ensure operating systems are fully patched

Make employees aware that when notified of an upgrade, it is important to install it to enable automatic patching.

Reintegrate

Secure and automate part or all of the processes that were once done using pen and paper. Automation can mean that something is done the same way every time. Reducing or eliminating manual errors can lead to improved data security and increased efficiencies.

These measures should not be seen in isolation. They need to be woven together into cohesive strategy.

What should your cybersecurity strategy look like?

Every business will be at a different stage in its cybersecurity evolution but it is important to be aware of, and to know how to tackle, all of the potential vulnerabilities that the hybrid environment throws up.

Organisations large and small need to develop comprehensive and flexible cybersecurity strategies to increase protection and minimise risk across all environments, both in the office, in the cloud and remotely.

These strategies should include ways to improve identity-security and being able to configure, maintain and monitor identity infrastructure. Also, enabling secure data processing, sharing and transfer.

It is important to think of cybersecurity in terms of business risk, not just technology, and to ensure all architecture and environments are addressed.

At corporate board level, much of the current focus is on the recruitment of cyber specialists dedicated to specific areas of security, such as securing remote access, and making sure resources are in place to respond to threats to different aspects of the business at different times.

In a report examining latest security and risk trends, Gartner outlines how corporate boardrooms are responding to the hybrid working phenomenon and the increased threat of security breaches.

"flexible, agile, scalable and composable"

The Gartner report illustrates how cyber strategies are evolving to cover a broader range of vulnerabilities. These strategies must be "flexible, agile, scalable and composable" to reflect changing environments and threats.

The new focus for larger organisations is on creating a 'cybersecurity mesh' to deploy and extend security where it's most needed, overseen by cyber-savvy boards with dedicated committees. Businesses are also introducing privacy-enhancing computation techniques to protect data as it is being used.

Other areas of focus include managing machine identities with greater authentication and monitoring, rebooting cybersecurity policies to reflect the explosion in remote work, introducing breach and attack simulation with continuous testing and validation of security controls, and consolidating vendors to make security more efficient and integrated.

Best practice at Praxity

Few organisations are in a position to implement such a comprehensive strategy, at least not without significant support from independent specialists. However, it would be extremely risky, perhaps even dangerous, not to make continuous improvements to security, coupled with staff training, to protect against, and minimise the impact of, multiple attacks.

To find out what's happening on the ground, we asked Praxity member firms in the U.S., Australia, Canada, Brazil, the UK and Finland to list the cybersecurity measures they are adopting to reduce the risk of attack. Their main areas of focus include:

Education and Awareness Programmes

Monitoring, Record Retention and Antivirus Policies

Virtual Cloud Desktops

For all third-party workers.

Cloud Access Security Brokers (CASBs)

Security software used to enforce security policies through risk identification and regulation compliance whenever cloud-based data is accessed.

Data Encryption

EDR

To continuously monitor end-user devices to detect and respond to cyber threats like ransomware and malware.

Privileged Access Management (PAM)

Software to safeguard identities with special access or capabilities beyond regular users.

Creating Security Operation Centres (SOCs)

A centralized function to continuously monitor and improve security while preventing, detecting, analysing, and responding to cybersecurity incidents.

Identity and Access Management (IAM)

Security to manage digital identities and user access to data, systems, and resources. Controls on who can access what and where, using software such as Intune and Azure Active Directory.

Zero Trust Security

Incorporating strict identity verification for every person and device trying to access resources on a private network.

Different firms are implementing different measures depending on their current level of protection, expertise and employee awareness. However, the scale and breadth of response demonstrates accounting firms within the Alliance are taking the cyber threat extremely seriously.

At Shorts, the focus is on moving the security boundary to the cloud using the Azure and Defender tools, and educating users in sharing and collaborating. The firm has put in measures to protect its IP, with increased monitoring and auditing. It has introduced Domain Name System filtering to provide an extra layer in the fight against malware. This provides keyword blocks to unsavoury types of website. Controls have also been introduced on permitted access.

Shorts has also introduced a 'honeypot' tool, a network-attached system which provides a decoy to lure cyber attackers away from legitimate targets. The system detects, deflects and studies attempted hacks on dummy services with poor security.

"through good strategy and investing for the future we were well positioned"

For the majority of firms, the focus has been on ensuring secure remote access and protecting sensitive data, while also helping clients develop responses to the changing cybersecurity landscape.

Commenting on the strategy at Rouse Partners, Tom Gardner says: "We were in a fortunate position, having carried out significant upgrades to our remote work environment prior to the pandemic. This was driven by the need to develop a scalable, robust remote work environment for our audit team but also rolled out to the wider team, in anticipation of longer-term trends towards flexible and off-site working. So, through good strategy and investing for the future we were well positioned."

"Whilst we were in a strong position, we did find that some clients and contacts were not as lucky and were particularly impacted by the global rush to acquire remote working equipment (laptops, webcams, iPads etc). Thankfully we have strong partnerships with a good number of globally-leading suppliers and were able to step in to assist with equipment acquisitions and offer advice in certain cases. I think this shows the importance of building strong, long-lasting relationships with your suppliers."

Shorts has been advising clients on key threats and encouraging clients to collaborate using methods other than email, such as Teams channels and Citrix ShareFile. In some cases, Shorts IT team has been given access to clients' Microsoft Office 365 'estates' for review and help with security and filtering.

Other firms within Praxity have expanded their cybersecurity resources and technological capabilities to help clients adjust to new cyber threats. Brazilian member firm VBR has developed a joint venture with Israeli consultancy CyberTeam 360 to devise a range of "treatments" for companies of all sizes and at different stages of their cybersecurity journey, from evaluation of the current security status through to protection of data from advanced attacks.

This multi-layered approach features:

- **An evaluation tool to provide a quantitative estimate of a company's current remote access security status including VPNs, virtual desktops and apps, remote desktops and cloud access;**
- **An advanced 'Quick Cyber Security Assessment' tool to assess information security programme status including policy and standards, threat intelligence and vendor management; A treatment plan tailored to an organisation's specific cyber security needs;**
- **A virtual Chief Information Security Officer (vCISO) to manage cyber security on a customisable, scalable basis.**

"There is a bare minimum you need to be doing"

Similarly, Aronson set up a dedicated IT security consultancy focusing on key areas of cybersecurity including assessments, awareness training, and remediation. "There is a bare minimum you need to be doing," says Azunna Anyanwu, adding: "The problem, in many cases, is not so much funding, but having the right tools and organisations in place."
A growing area of client support for Aronson's Technology Advisory service is compliance, especially for public sector organisations and government contractors.

At Kaufman Rossin, the focus has switched from building the right cybersecurity infrastructure to securing the right configurations for hybrid work. "Two years ago, everyone was being hacked. We had to make tweaks to our infrastructure and re-evaluate the threats," Jorge Rey explains. In terms of advisory services, the US firm is helping clients with risk assessments, identifying where the risks are and making sure they have the right cloud software and reporting in place.

Sharing global expertise

Developing and evolving cybersecurity strategies to address different environments and architectures is an increasingly difficult task and almost impossible to achieve in isolation.

Accounting professionals around the world are therefore working closely together to support one another and share best practice. They are doing so by sharing expertise via the Praxity platform. The knowledge gained is being used internally and externally.

Tom Gardner explains: "Praxity has given me a forum to bounce ideas off my IT counterparts within other member firms and to share information about projects and useful tools. This was especially useful during the Covid-19 pandemic where I worked very closely with one of my Praxity contacts. It was valuable to know the person I was talking to was addressing similar challenges to me and we were able to support one another."

"In addition, many new tools we've adopted over the last 18 months have originated from recommendations made to my colleagues in the Praxity conference working groups. Looking forward, I understand that Praxity will be launching an IT Working Group at the forthcoming UK autumn conference. I think this is a really positive step forward and will further help us to communicate and collaborate, ensuring Praxity member firms are well positioned to navigate the ever-evolving IT landscape."

"I think we should always consider that there could be vulnerabilities across the supply chain, as information and data flows between environments outside our control, and thus aim to support and assist others we work with, to ensure their IT infrastructures are strong and robust."

"The more that we do, the more we can enhance our knowledge, understand what others are doing, and ultimately do things better"

Chris Allen says the ability to share experience and expertise using the Praxity platform "would better enable security amongst our peers and would help everyone". It would also provide "a great way to reduce the 'unknown unknowns' that are a great risk surface for all of us."

One way in which firms can share expertise in this way is through Praxity working groups. In the U.S, for example, accounting leaders meet regularly to discuss key issues including security challenges. Commenting on the benefits, Jorge Rey says: "The more that we do, the more we can enhance our knowledge, understand what others are doing, and ultimately do things better."

Cybersecurity was already a top priority for accounting firms and their clients before the pandemic. With the surge in hybrid and remote work, the threat of cybercrime has significantly increased, and so too has the potential consequences of a successful attack.

With so much at stake, it is imperative businesses of all sizes work towards comprehensive and robust cyber strategies that address all the potential weak points across all architecture and environments.

By sharing knowledge and expertise, accounting firms stand a better chance of minimising the risk not only to protect their employees, networks and systems, but also to protect their clients' businesses now and in future.

What is Praxity?
Praxity is a multi-award-winning alliance, the largest in the world, in 120 countries with 780 offices in strategic locations and access to over 65,000 business practitioners, accountants and tax experts who really know and understand the traits and risks that lie beyond local borders. Together they share their combined expertise and technical knowledge providing highly customised business solutions and deep regional understanding - driving outstanding results for clients worldwide.

Our member firms amplify competitive advantages, support unique and diverse cultures working to support clients ranging from small ambitious businesses to established global, listed organisations. Business issues don't stop at the border – the solutions shouldn't either.

Media Enquiries
Deborah Poulter, Head of Business Development, Praxity
01372 738190
dpoulter@praxity.com

PRAXITY™
Empowering Business Globally