CYBER SECURITY ROADMAP FOR 2022

DRIVING TECH FLUENCY IN A HYBRID WORKING WORLD

counterparts TECHNOLOGY

hp

intel CORE i7 intel CORE i9 intel CORE i5 intel CORE i3

FOREWORD

Organisations around the globe have faced unprecedented disruption since the start of the pandemic. As businesses shifted to hybrid work models almost overnight, new threats and attacks have emerged across every sector. In fact, 69% of APAC organisations have seen an increase of 25% or more cyber threats or alerts since the onset of COVID-19 .

The role of a robust cybersecurity strategy has never been more critical. But what should this strategy look like? We've identified 10 crucial security layers that businesses need to consider in the formation of a security strategy for the next year and onwards. The Cyber Security Roadmap for2022 is your route to a solidified cybersecurity strategy that looks to protect all your employees, customers, data, organisation and bottom-line.

> "Security has never been more imperative for the modern business. For clients, we strive to embed security across all systems and processes inside an organisation. For executives specifically, it's about bringing your organisation to a point of acceptable cyber risk. Risk will always be present, though it's about the actions and investments taken to reduce the overall risk."

Matt Wynn Jones on Cyber Security
Managing Director, Counterparts

1 ENDPOINT PROTECTION

With remote work now accepted as standard across many sectors, having a secure on-premise network is no longer sufficient to ensure protection of critical data. In addition to network security, careful consideration must be given to endpoint protection.

According to a 2020 report by the Ponemon Institute, 68% of organisations experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. The same report found that 68% of IT professionals found that the frequency of endpoint attacks had increased since the year prior .

Endpoint protection aims to mitigate these risks by using multiple detection techniques to investigate and remediate threats.

At Counterparts, we believe there are three key elements to endpoint protection – hardware and embedded technology, software and applications, and device management. When delivered in unison, these elements deliver a total endpoint protection strategy.

1. **Hardware and Embedded Technology**
2. **Software and Applications**
3. **Device Management**

By 2025, there will be 38.6 billion connected devices globally[3]

HARDWARE AND EMBEDDED TECHNOLOGY

Endpoints are a common entry point for malware and other malicious attacks as they offer an easy access point to breach a network . To combat the ever evolving risks of cyber-crime, vendors are introducing embedded technology tools that directly offset particular threats such as the HP EliteBook powered by 11th Gen Intel® Core™ processors. HP Sure View, for example, is an integrated privacy screen that protects employees against visual hacking while HP Sure Click protects your PC from websites and browser .pdf files that could potentially be infected with malware, ransomware or viruses. With more tools like HP Sure Run and HP Sure Recover that assist in protecting the devices functionality, they're great examples of embedded technology designed as the first line of defence to protect both the device and its contents.

91% of visual hacking attempts – physically spying on others' device screens – are successful[5]

SOFTWARE AND APPLICATIONS

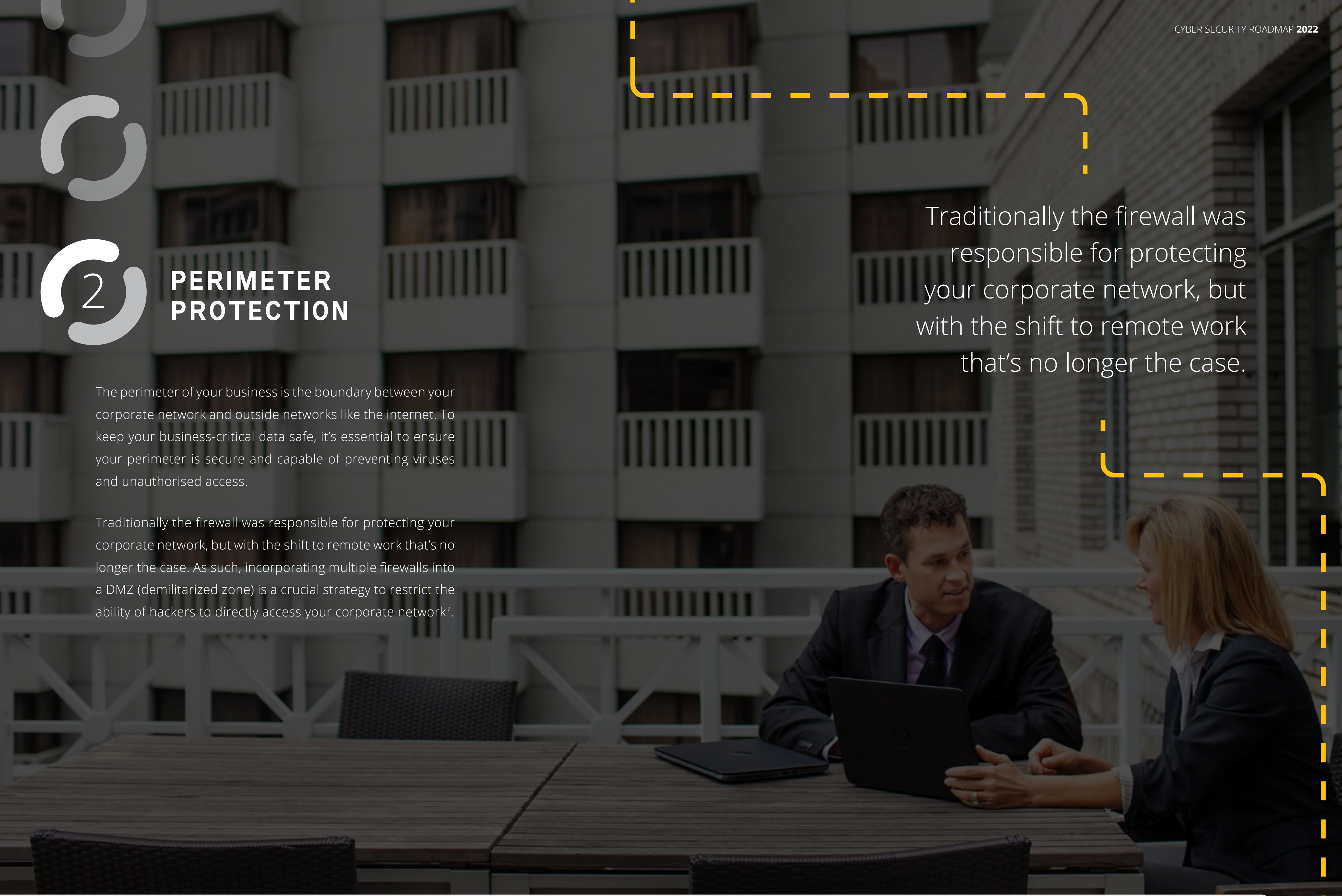
As cyber threats become increasingly more sophisticated, organisations should look to security software that can adapt, predict, and stay ahead of the latest attacks. Following best practice, it's important to leverage software that holds data protection capabilities including application control, disaster recovery, machine learning, and protection capabilities against spam, phishing and malware, as well as targeted attacks against your mail server, gateway or applications. Different software suites will suit different businesses – it's important to acknowledge this and identify what works best for your business.

DEVICE MANAGEMENT

End-user device management is a critical aspect to any security strategy. To properly protect all the endpoint devices in your business, they must be managed correctly. Such management includes:

- **Installing and updating operating systems**
- **Application updates and patches**
- **Managing user accounts**
- **Maintaining up-to-date security**
- **Monitoring lifecycle of devices**
- **Ability to remotely wipe if lost or compromised**
- **Safe disposal of device at end of lifecycle including hard disk**

By 2025 there will be more than 38 billion internet-connected devices installed globally3. That's more than four devices per person, and the importance of protecting them will only grow exponentially. Fortunately, management services like HP Device as a Service are stepping in to offer a complete, scalable device lifecycle management solution[6].



2 PERIMETER PROTECTION

The perimeter of your business is the boundary between your corporate network and outside networks like the internet. To keep your business-critical data safe, it's essential to ensure your perimeter is secure and capable of preventing viruses and unauthorised access.

Traditionally the firewall was responsible for protecting your corporate network, but with the shift to remote work that's no longer the case. As such, incorporating multiple firewalls into a DMZ (demilitarized zone) is a crucial strategy to restrict the ability of hackers to directly access your corporate network[7].

> Traditionally the firewall was responsible for protecting your corporate network, but with the shift to remote work that's no longer the case.

WHAT IS A DMZ?

A DMZ is a physical subnet that separates an internal local area network (LAN) from an untrusted network like the internet. A DMZ network can provide access to necessary internet services from the public internet in a secure way. You can use them to isolate and keep potential target systems separate from your internal network to avoid compromising it.

Many businesses have implemented a hybrid approach to leverage the convenience of the cloud alongside the flexibility of the data centre. According to Gartner, "hybrid, multi-cloud and edge environments are growing and setting the stage for new distributed cloud models". Indeed, global user spending on cloud services is expected exceed $480 billion in 2022[8].

While the cloud offers unmatchable agility, knowing how to use it securely is pivotal. Regardless of the structure you may be using, following these practices will help to maximise its security:

- **Employ the principle of least privilege**
- **Isolate the most critical infrastructure**
- **Encrypt data passing through the cloud**
- **Back up critical data on external storage devices**
- **Choose the right cloud security solution**

There are many cloud security solutions out there and choosing the right one should come down to the parameters of your environment, and which solution gives that environment the most protection.

3 PROACTIVE THREAT MONITORING

Any organisation is just one unidentified threat away from compromise. Proactive threat monitoring is focused on isolating potential threats to stop them before they become an issue; being proactive as opposed to reactive. In our increasingly interconnected world, digital alarms surround employees every day and, with every false alarm, your business gets one step closer to what we call 'alert fatigue', where alerts go ignored and one legitimate alarm slips through the cracks.

This approach means your business can gain a fully-managed, security analyst-delivered service that defends against zero-day (on the spot) attacks and advanced persistent threats, as well as identify any potential weak spots in your defences. Keep in mind of course, this is only one layer of the ten we have identified in an all-encompassing cyber strategy.

WHO'S OFFERING PTM

Leading providers such as HP leverage best-in-class security solutions to continuously protect your devices against complex threats. HP Wolf Security for Business, for example, includes a portfolio of security solutions that are built into the hardware to equip you with a secure foundation that puts protection first[10].

The evolving threat landscape is predicted to be the top factor impacting IT organisations over the next three to five years[9]

Global IoT spending will reach $1.1 trillion by 2023[9]

4 IOT

The Internet of Things (IoT) is another area focused on endpoint devices. Specifically, IoT is a system of interrelated computing devices, mechanical or digital machines that together have the ability to transfer data across a network with no human-to-human or human-to-computer interaction required – printers, fridges and lift management systems are just a handful of examples with IoT capabilities.

Increasingly, organisations across a variety of industries are leveraging IoT to operate more efficiently, enhance customer service and business value, and even improve business decision-making. This trend is reflected by the projection that IoT spending will increase from $749 billion in 2020 to $1.1 trillion by 2023[11].

In the same vein as your end-user devices, any device with an IP address is a potential security threat, and because IoT devices are so closely connected across your network, it only takes a hacker exploiting one vulnerability to potentially manipulate an entire network of data. It's therefore imperative that you regularly update all your devices and if you work with manufacturers that don't provide updates for their devices regularly, assess alternatives or else leave yourself vulnerable to attack and the risk of compromising business continuity.

5 END USER TESTING TRAINING

88% of malware is delivered by email into users' inboxes[12]

One of the biggest cyber risks to a business is its people. At Counterparts, we recruit programs that can administer "fake spam" and identify which staff members unknowingly respond to these test threats. Through a targeted and structured program, this group of users then undergoes training to improve their vigilance and awareness around malicious link clicking. Key warning signs can include:

- **You receive an email, text or phone call claiming to be from a bank, telecommunications provider or other business you regularly deal with, asking you to update or verify your details.**
- **The message does not address you by your proper name, and may contain typing errors and grammatical mistakes.**
- **The website address does not look like the address you usually use and it is requesting details the legitimate site would not normally ask for.**
- **You notice new icons on your computer screen, or your computer is not as fast as it normally is.**

We've seen across several programs that pre-testing normally identifies almost 30% of staff to be posing a risk, at the completion of the Counterparts delivered program that threat reduces to less than 2%. It needs to be highlighted that this is not an overnight fix. We operate 12 and 24 month programs and, on average, it takes approximately 6 months before we can start to identify a definitive reduction in staff behaviour. With the workforce becoming more and more flexible, focus is also given to the home life where many workers will send emails outside of business hours. Cybercrime doesn't wear a watch and as such, staff must learn to be vigilant at all times in all locations. After staff complete the program, we recommend revisiting the tests every 6 months or so to maintain awareness and minimise potential cyber risk.

6 EXECUTIVE PREPAREDNESS

According to the 2020 survey conducted by Cisco, 85% percent of business decision-makers globally said that cybersecurity is extremely important or more important than it was before the pandemic1. Yet many senior executives report not being informed or involved in data breach response planning.

This kind of disengagement can seriously hamper an organisation's ability to efficiently and effectively respond to a cybersecurity breach. Reputational risk is paramount when dealing with a cybersecurity breach and does require preparedness training and simulation.

Similar to our spam testing programs, we also run data breach simulation programs that prepare Board Members and Executive Teams via a structured non-technical approach to threat assessment. From a corporate standpoint, it's imperative to be forward thinking. We've identified three classification levels to a cybersecurity breach that should be adopted in executive preparedness plans:

1. **Classified in terms of yes, we have a breach but we don't know what it is**
2. **Classified in terms of yes, we have a breach and we know what it is**
3. **Classified in terms of yes, we have a breach and we know what it is and we know who's impacted**

For each level of classification there needs to be a response plan in place. For example, executives need to be aware of the relevant parties to contact and inform of the situation depending on the classification, press releases must be ready and the communications team aware of the necessary protocol. Legal obligations need to also be acknowledged and adhered to, and there must be "Plan B" if an entire system is compromised. How do you avoid downtime if your email servers go down? It's imperative that all of this is known and available to be rolled out swiftly in a crisis.

Much akin to a fire drill, our response management methodology includes assessment, training simulation and assistance with prepared statements and processes for all stakeholders, so when the time comes to react, it's like clockwork. Undertaking such training and simulation eliminates the risk of haphazard, frantic responses, which can potentially lead to irreversible damage to your business's reputation.

7 RISK ASSESSMENT MITIGATION

Penetration testing (often called "pen testing") is central to maintaining a secure IT environment. Pen testing attempts to exploit identified vulnerabilities to determine whether malicious activity or unauthorised access is possible. Essentially, it is designed to answer the question: "What is the real-world effectiveness of my existing security controls?"

So, who do you employ to undertake pen testing? We recommend soliciting the services of an objective third party. Hiring a third party eliminates the risk of complacency from a business perspective, and exaggeration from an integrator's. There are, however, some critical points you need to cover when evaluating which third party to employ, including five key areas you should assess before making a decision:

1 COMMUNICATION

Your provider should ensure you have a clear objective for the test, with a realistic scope outlined in a formal proposal.

2 TIMING

A clear timeline of when the test will be performed and how it can best avoid interrupting business functionality is critical.

3 NON-DISCLOSURE

Confidential information such as client data and personal details can come to light during a pen test so it's important your provider is willing to sign a non-disclosure agreement.

4 DOCUMENTED METHODOLOGY

Before commencing work your provider should be able to highlight their testing methodology through documentation that should use the Open Source Security Testing Methodology (OSSTMM) manual.

5 INSURANCE

You provider should have liability insurance that will cover the cost of an unforeseen data loss or business damaging incident during testing.

Once the pen tests have been completed, your provider should provide a report that will include, among other things, information about specific vulnerabilities, data that was accessed and the amount of time spent without any detection.

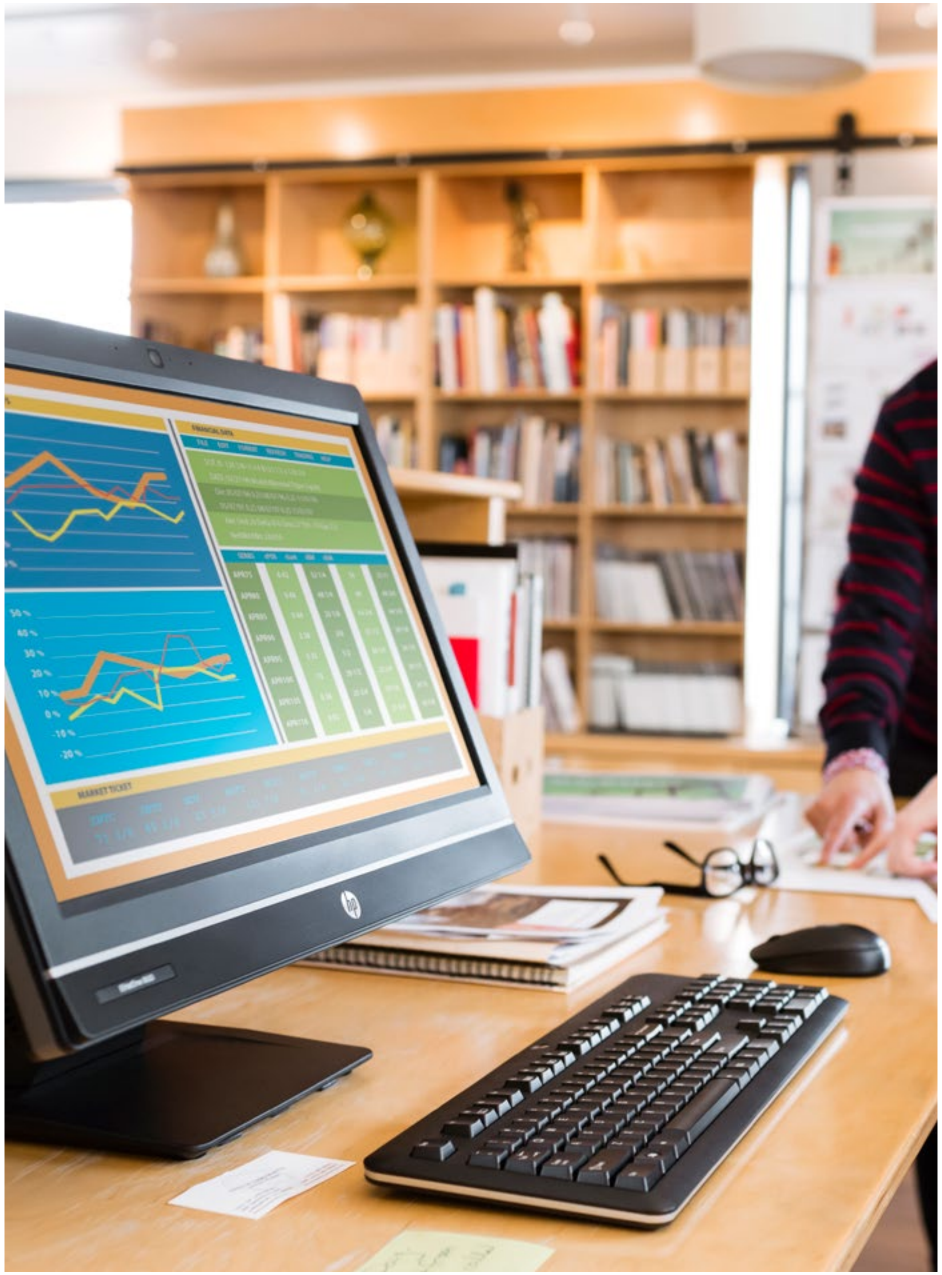
With this information, Counterparts can formulate a remediation plan that addresses the pen testing findings, ultimately boosting the confidence and strength you have in your virtual environment, and maintains your overall security strategy to keep business flowing.

8 INSURANCE LEGAL RECOMMENDATIONS

Cyber insurance policies and products are constantly evolving as both insurers and their clients keep up with the rapidly changing landscape. Consequently, you should proceed with caution when assessing which protection policy is the right fit for your organisation.

That said, you need some form of cyber insurance and it's important to be aware of the products on the market. Two such products are First Party Cyber Insurance and Third Party Cyber Insurance. First Party generally protects and reimburses your business directly after an attack as well as the ensuing fallout, while Third Party protects a business's customers and assists with issues that arise from litigation and legal expenses.

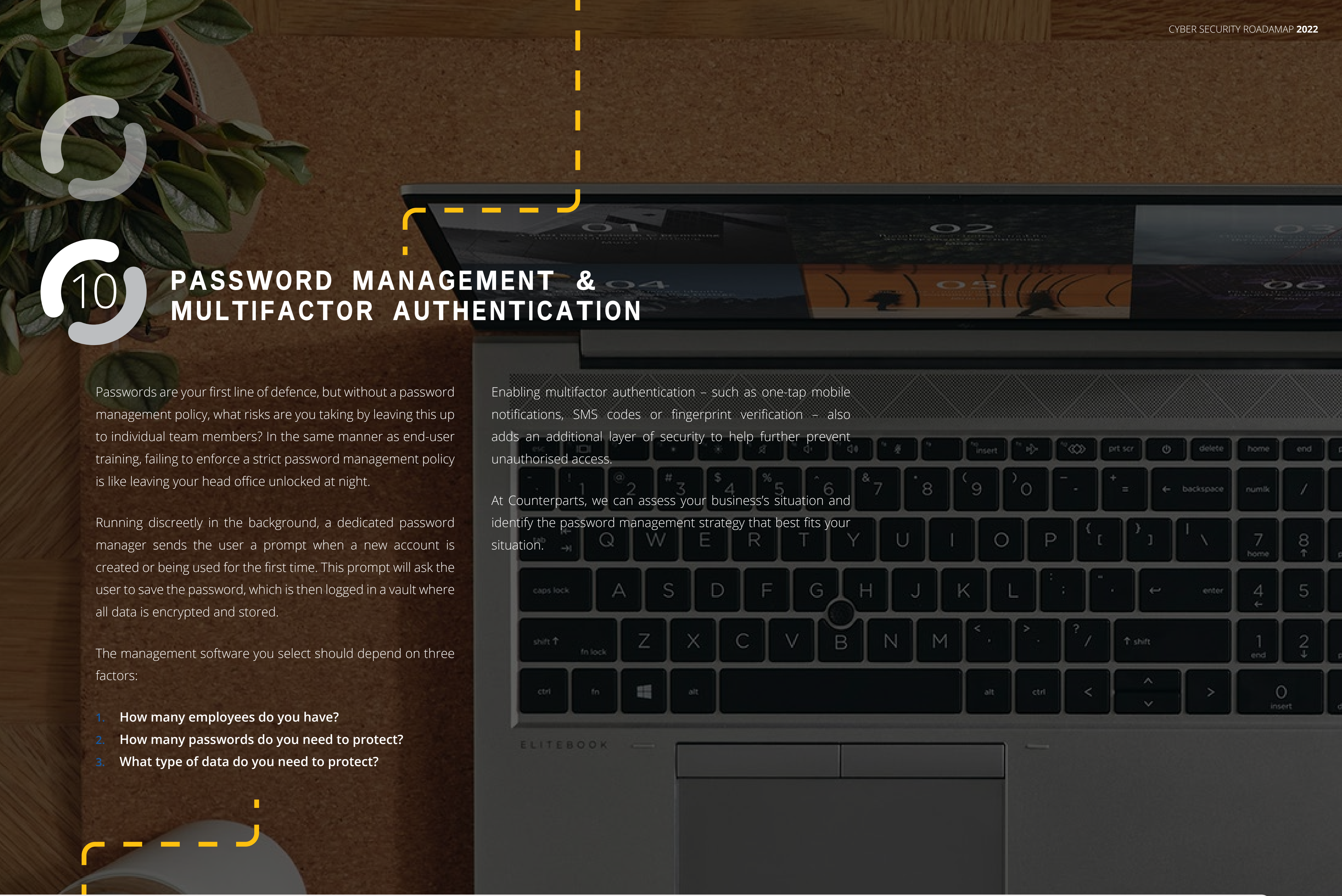
Counterparts has established relationships with insurance providers who can support you and advise on these specialist areas.



9 BUSINESS CONTINUITY & DISASTER RECOVERY (DR)

In the event that something does go wrong, what are you going to do to ensure business continuity? A business continuity plan, along with a solid, tested disaster recovery plan is crucial when disaster strikes.

Counterparts works with businesses across Australia to formulate business continuity and DR plans leveraging the latest technology from leading providers such as HP.



10 PASSWORD MANAGEMENT & MULTIFACTOR AUTHENTICATION

Passwords are your first line of defence, but without a password management policy, what risks are you taking by leaving this up to individual team members? In the same manner as end-user training, failing to enforce a strict password management policy is like leaving your head office unlocked at night.

Running discreetly in the background, a dedicated password manager sends the user a prompt when a new account is created or being used for the first time. This prompt will ask the user to save the password, which is then logged in a vault where all data is encrypted and stored.

The management software you select should depend on three factors:

1. **How many employees do you have?**
2. **How many passwords do you need to protect?**
3. **What type of data do you need to protect?**

Enabling multifactor authentication – such as one-tap mobile notifications, SMS codes or fingerprint verification – also adds an additional layer of security to help further prevent unauthorised access.

At Counterparts, we can assess your business's situation and identify the password management strategy that best fits your situation.

ARE YOU 2022 PREPARED?

How many layers of the ten does your organisation have in play? This is a good indicator of your security maturity and a window into just how much cyber risk you are handling. Understanding potential infiltration points is the first step. Creating an actionable plan to reduce overall cyber risk and stay protected is the next step.

Counterparts is a Sydney-based, national technology consultant with a high pedigree in solving complex technical problems that help keep businesses growth-oriented and secure. Our approach to security is business-led and technology enabled, through a lens unique to your organisation.

NEED HELP PUTTING THE TEN LAYERS TOGETHER?

For the modern organisation, cyber breaches are not a matter of 'if' but 'when'. Take the first step in protecting your staff, customers and organisation by reaching out to the Counterparts Cyber Team today.

GET IN TOUCH

REFERENCES

1. https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-remote-worker-solution/future-of-secure-remote-work-report.pdf

2. https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

3. https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

4. https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101

5. https://multimedia.3m.com/mws/media/1254232O/global-visual-hacking-experiment-study-summary.pdf

6. https://www.hp.com/au-en/services/daas.html

7. https://searchsecurity.techtarget.com/definition/DMZ

8. https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud

9. https://www.gartner.com/en/newsroom/press-releases/2020-09-15-gartner-survey-finds-the-evolving-threat-landscape-is-top-priority-for-security-and-risk-management-leaders

10. https://www.hp.com/au-en/security/pc-security.html

11. https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/

12 https://press.hp.com/us/en/press-releases/2021/29-percent-of-cyber-threats-previously-unknown-hp-research-finds.html

COUNTERPARTS TECHNOLOGY