CYBER SECURITY ROADMAP FOR 2020

DRIVING TECH FLUENCY IN THE BOARDROOM

counterparts TECHNOLOGY

FOREWORD

In the digital age where every connection is an opportunity, every connection can also pose a potential cyber risk. At Counterparts, we understand the fundamental role that security plays in a modern business. We've identified 10 crucial security layers that boardroom executives need to consider in the formation of an overall security strategy for the next year and onwards. The Cyber Security Roadmap for 2020 is your route to a solidified cyber security strategy that looks to protect all your employees, customers, data, organisation and bottom-line.

"Security is an integral piece 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

Having a secure network is paramount, but equal consideration must also be given to the endpoints that access your network. Defined by Gartner as "a solution that converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioural blocking) capabilities into a single and cohesive solution,"[1] endpoint protection is largely gaining traction due to the number of mobile devices such as laptops, smartphones and tablet PCs that are now in circulation.

At Counterparts, we believe there are 3 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**

"Globally, there were already 17.1 billion networked devices in 2016" [2]

At the touch of a button, HP SureView darkens your screen to those around you while you see your content clearly.

"Visual hacking entails physically spying on others' computer screens and desks" [5]

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[3]. To combat the ever evolving risks of cyber-crime, vendors are introducing embedded technology tools that directly offset particular threats. 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.

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[6]. 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. Vendors with strong capabilities in this space include Trend Micro, Sophos, Kaspersky and McAfee. Different software suites will suit different businesses and therefore 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 2020 there will be more than 24 billion internet-connected devices installed globally, that's 4 devices per person and protecting them will only grow exponentially in importance. Management tools like Microsoft Enterprise Mobility + Security (Microsoft EMS) and HP Touchpoint Manager are evidence of this importance.

"Incorporating multiple firewalls into a demilitarized zone is a strong means of restricting the ability of hackers to directly access your corporate network" [7]

6

2 PERIMETER PROTECTION

The perimeter of your business is the connection to an untrusted network like the internet. For your organisations data to remain safe, it's essential to ensure your perimeter is secure and capable of preventing viruses and unauthorised access. Traditionally, the firewall is responsible for protecting your corporate network, however the corporate network is no longer a place, but more so an environment where we work, often remotely. As such, incorporating multiple firewalls into a DMZ (demilitarized zone) is a strong means of restricting the ability of hackers to directly access your corporate network[7].

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[8].

Are you using cloud services? Most likely you are and you've implemented a hybrid approach to leverage the convenience of the cloud alongside the flexibility of the data centre. According to Gartner, by 2020, 90 per cent of organisations will have moved to hybrid cloud infrastructure. So knowing how to secure it correctly is imperative.

Regardless of the cloud structure you may be using, following these practices will help to maximize its security[10]:

- **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's 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

An organisation is one unidentified threat away from compromise. Proactive threat monitoring is focused on isolating potential threats in order 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[11], where the 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.

"With every false alarm your business gets one step closer to what we call alert fatigue..."

WHO'S OFFERING PTM

LMNTRIX's Adaptive Threat Response (ADR) is a tool that can offset the potential for alert fatigue; a validated and integrated threat detection and response architecture, it hunts down and eliminates the advanced and unknown threats that routinely bypass perimeter controls[12]. Adaptive Threat Response comprises advanced network and endpoint threat detection, deceptions everywhere (honey potting), analytics and real-time global threat intelligence technology accompanied by continuous monitoring as well as both internal and external threat hunting[13].

> " [A recent PWC report] predicts IoT investments by businesses to grow from $215B in 2015 to $832B in 2020" [16]

4 IOT & PRINT SECURITY

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[15]. This is reflected in a recent PWC report that predicts IoT investments by businesses to grow from $215B in 2015 to $832B in 2020[16], creating an exponentially increasing number of access points across an organisation.

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[17]. 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.

Print security is much more than simply securing your documents, special consideration must also be given to data-in-transit and endpoint devices on the network. Implementing technologies that prevent the unauthorised use of printers when documents are in queue greatly reduces the risk of confidential information being compromised. Such technologies include user and PIN authentication as well as smartcards[18], while printers that aren't patched and updated regularly pose all the same risks any other device does, so the security protocol you adopt for end-user devices and IoT must also apply here.

5 END USER TESTING & TRAINING

Often the biggest cyber risk to a business is its people. As an analogy, you may have the world's most expensive and elaborate security at your residential home, but if you forget to lock the front door when you leave it is essentially rendered useless. The same applies with your business's security strategy.

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[19]:

- **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.**

" Pre-testing normally identifies 30% of staff to be posing a risk"

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 BOARD/EXECUTIVE PREPAREDNESS & SIMULATION

In a survey conducted by the Ponemon Institute, 57% of IT professionals polled advised that their senior executives were not informed about or involved in data breach response planning. This kind of disengagement can seriously hamper an organisations ability to efficiently and effectively respond to a cybersecurity breach[20]. 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 3 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. In light of the new Australian Notifiable Data Breach Scheme, legal obligations need to also be acknowledged and adhered to, and what are your fall back options or "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") through identifying and remediating breaches is central to maintaining a secure IT environment. We often see organisations mistaking vulnerability assessments with penetration testing. Undertaking a vulnerability assessment will help you identify potential vulnerabilities within your overall environment, whereas pen testing goes a step further and attempts to exploit these identified vulnerabilities to determine whether malicious activity or unauthorised access is possible[21]. Pen testing is designed to answer the question; "What is the real-world effectiveness of my existing security controls against an active, human, skilled attacker?"[22]

So, who do you employ to undertake the pen testing? We always recommend soliciting the services of an objective, third party. Many security consulting companies and Big Four auditors have started offering pen testing services to their clients[23]. 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, and we've identified 5 key areas you should assess before making a decision[24].

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 time line 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

Goes without saying but your provider should have liability insurance that will cover the cost of an unforeseen data loss or business damaging incident during testing.

> "Hiring a third party eliminates the risk of complacency from a business perspective"

Typically, penetration testing consists of network pen testing and application security testing that also includes testing particular controls and processes around your networks and applications[25]. Once the tests have been completed, your provider will provide a report that will include among other things; specific vulnerabilities, data that was accessed and the amount of time spent without any detection[26]. With this information Counterparts can then 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. 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.

8 INSURANCE & LEGAL RECOMMENDATIONS

When it comes to IT security, insurance and legal matters must be treated with extra care. In many cases, cyber insurance policies and products are new and constantly evolving. Both insurers and their clients are very much still coming to grips with the cyber insurance domain, and as such you should proceed with caution when assessing which protection policy is the right fit for your organisation[27].

Although the context of specifics is still unclear, one thing is certain, you need some form of cyber insurance and you need to be aware of the policies on the market. Two such policies are First Party Cyber Insurance and Third Party Cyber Insurance. First Party 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[28].

Features of the two policies can be seen below[29]:

FIRST PARTY

- Assistance with direct losses caused by a cyber attack
- IT forensic costs
- Retrieval of data costs from a compromised system
- Cyber extortion expenses (including ransom payments)
- Credit monitoring costs

THIRD PARTY

- Unintentional breach of privacy
- Breach of confidential information including employees
- Intellectual property rights infringement
- Unintentional disclosure of personal or financial information

Cyber-crime is an ever-evolving and constantly moving threat, and we strongly advise against looking into cyber insurance post cyber-attack. Proactive as opposed to reactive speaks strongly in this layer and Counterparts has established relationships with expert legal and insurance companies who can support you and advise on these specialist areas.

9 BUSINESS CONTINUITY & DISASTER RECOVERY (DR)

In the instance 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. A good way to evaluate how important a DR plan is to your business is to forecast the loss of revenue and staff wages that your organisation would forfeit in the event of a disaster. An example of how to calculate such a loss can be seen opposite[30].

Disasters can come in many different forms, can become very costly in a short period of time, and contrary to the running theme of this roadmap, not all of them come in the form of a cyber-attack. Storms, fire, power outages and many other 'disasters' can result in 'business as usual' not being possible. In the event of a disaster occurring you need a structured plan in place that details the processes every stakeholder in your business must implement to resume business-critical functions swiftly, and without significant losses in revenues or business operations[33].

Counterparts work with many businesses across Australia to formulate business continuity and DR plans. Too often we see businesses out of action due to a power outage or their infrastructure is down, earlier this year an architecture firm suffered a flooded basement in their building which resulted in the main server being down for 8 days, 120 staff unable to work productively, you do the math. Develop a continuity and DR plan to ensure your workforce, from executives down, know exactly what to do in the case of a disaster or downtime.

Loss of revenue*
Employee costs^

HOURLY COST OF DOWNTIME

Cost of downtime
Amount of downtime

TOTAL COST TO BUSINESS

*__Loss of revenue per hour__ = (Revenue/business days in the year/business hours in the day)
^__Employee costs per hour__ = Number of employees down (hourly wage + overhead costs)

10 ENTERPRISE PASSWORD PROTECTION MANAGEMENT

Password protection has quickly become an essential layer to any digital security strategy and the use of enterprise password management software is the element driving it[34]. Everyone enters their information online, whether it's personal details or for business purposes, it all requires a password and even the average user can have dozens of accounts, from a business perspective this multiplies tenfold.

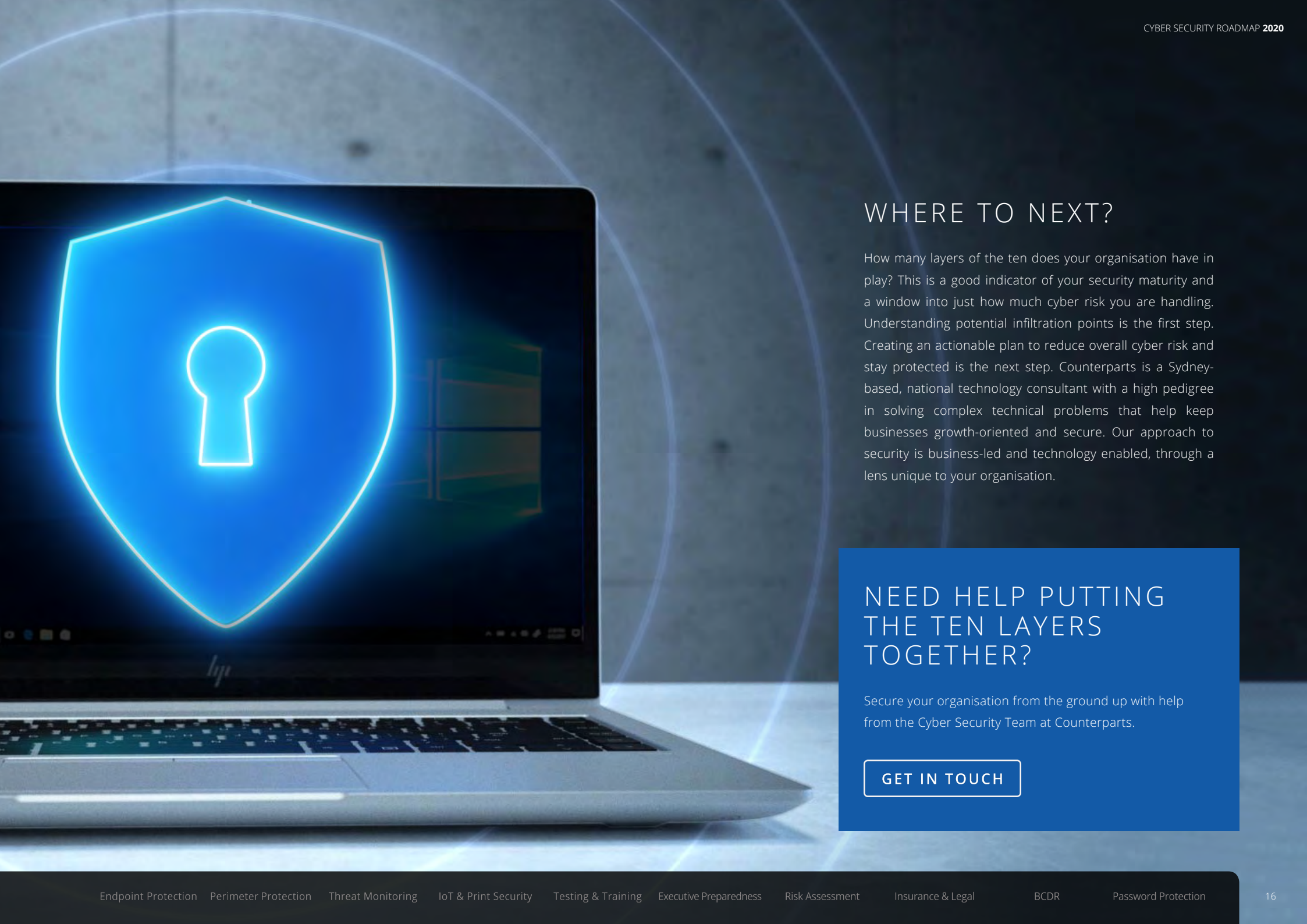
Passwords are your first line of defense and using separate passwords for each account is considered best practice, but without a password management policy, what risks are you taking by leaving this up to individual team members? In the same manner as end-user training, failing to enforce a strict password management policy is like leaving your head office unlocked at night[35]. The moment an employee has to record a password in an excel spreadsheet or on a notepad, it's time to introduce password management.

Running discreetly in the background, the 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 once entered, all data is encrypted and stored[36]. The management software you select will depend on three factors[37]:

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?**

Counterparts work with many vendors providing enterprise password management software. We can assess your business's situation and identify the management tool that best fits your situation, eliminating the risk of you remaining vulnerable, or potentially overpaying for software you don't necessarily need.

"Failing to enforce a strict password management policy is like leaving your head office unlocked at night"



WHERE TO NEXT?

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?

Secure your organisation from the ground up with help from the Cyber Security Team at Counterparts.

GET IN TOUCH

REFERENCES

[1]https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101
[2]https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_Device_Growth_Traffic_Profiles.pdf
[3]https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101
[4]http://www8.hp.com/us/en/solutions/computer-security.html
[5]https://www.infosecurity-magazine.com/news/visual-hacking-is-successful-91-of/
[6]https://www.trendmicro.com/en_au/business/products/user-protection.html
[7/8]https://searchsecurity.techtarget.com/definition/DMZ
[9/10]https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/key-strategies-for-securing-the-hybrid-cloud
[11]https://www.tripwire.com/state-of-security/security-data-protection/alert-fatigue-is-a-big-cybersecurity-problem/
[12/13]https://www.lmntrix.com/ATR
[14/15]https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[16]https://www.pwc.fr/fr/assets/files/pdf/2017/03/2017_ai_and_iot_v13b.pdf
[17]https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[18]https://www8.hp.com/au/en/solutions/business-solutions/printingsolutions/datasecurity.html?jumpid=in_r12012_au/en/ipg/hp_secure_print_overview/data-security-learn-more
[19]https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing
[20]http://www.experian.com/blogs/data-breach/2017/07/12/increasing-leaderships-engagement-cybersecurity/
[21]https://www.veracode.com/security/penetration-testing
[22] https://www.forbes.com/sites/ericbasu/2013/10/13/what-is-a-penetration-test-and-why-would-i-need-one-for-my-company/#97d333e18a0d
[23/24]https://resources.infosecinstitute.com/benefits-using-third-party-pen-testing-company/#gref
[25]https://www.veracode.com/security/penetration-testing
[26] https://resources.infosecinstitute.com/benefits-using-third-party-pen-testing-company/#gref
[27]http://lca.lawcouncil.asn.au/lawcouncil/cyber-precedent-risk-management/cyber-precedent-insurance
[28/29]https://www.webberinsurance.com.au/cyber-insurance?gclid=EAIaIQobChMIormtrtbk3gIVgoBwCh0mQALdEAAYAyAAEgKpZPD_BwE
[30/31]https://www.brennanit.com.au/wp-content/uploads/2018/04/DR-solution-infographic.pdf
[32/33]https://www.networkworld.com/article/3248969/data-center/what-is-disaster-recovery-how-to-ensure-business-continuity.html
[34]https://phoenixnap.com/blog/enterprise-password-management-solutions
[35/37]https://thycotic.com/company/blog/2018/11/06/enterprise-password-management-smbs-to-corporations/
[36]https://phoenixnap.com/blog/enterprise-password-management-solutions