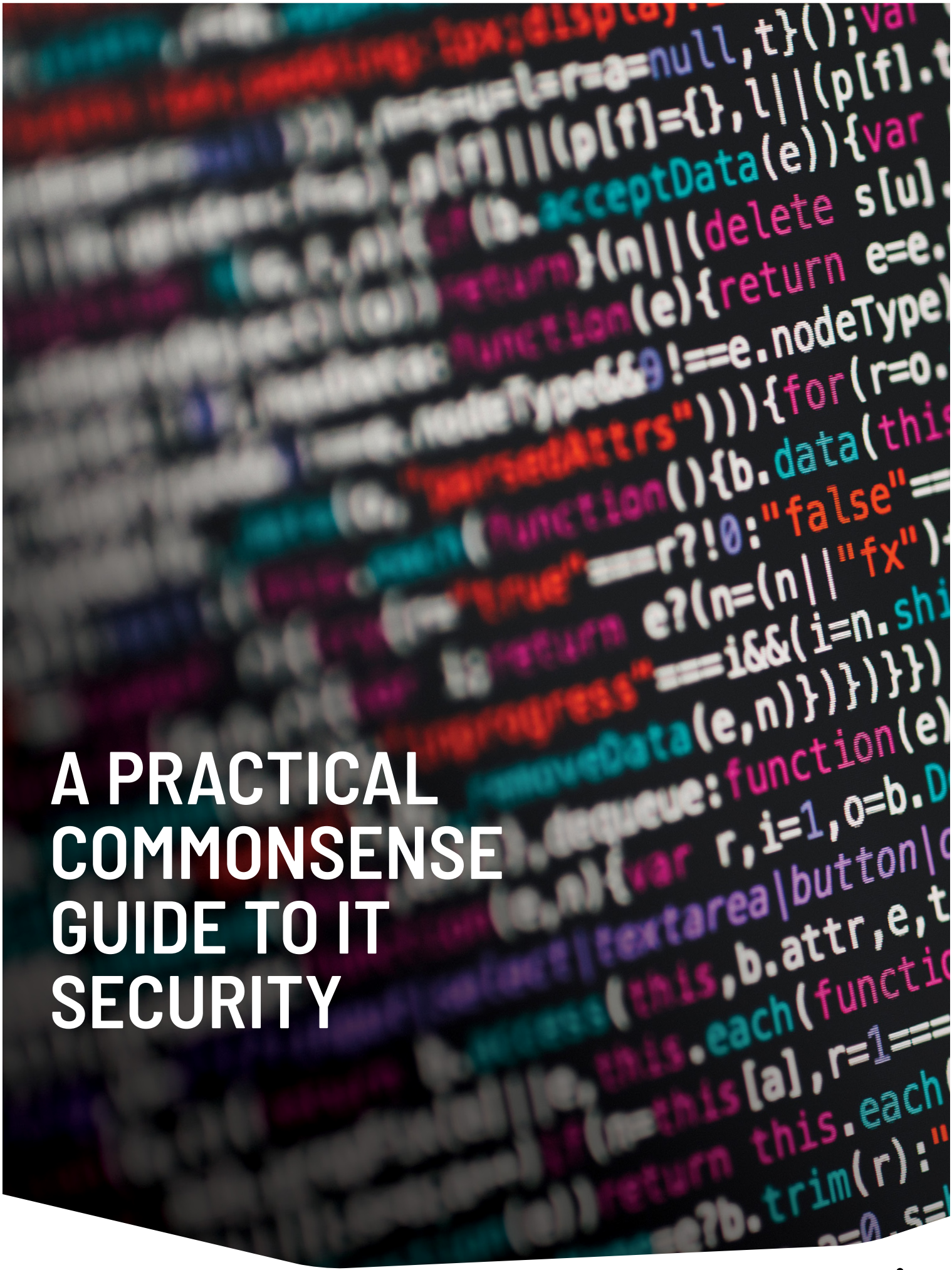


A PRACTICAL COMMONSENSE GUIDE TO IT SECURITY

Kytec

This short paper has been written for people who are responsible for IT security within their organisation and those who would be impacted if security breaches occur.

While vendors have a direct commercial interest in strongly highlighting the need for security, what *is* true is that threats are increasing, constantly changing and the potential business impacts are becoming greater. **Security breaches are up 11% year on year**[1] The IT security landscape is becoming more complex.

This paper will outline some of the common risks, risks that are often ignored, some simple ways to mitigate these risks and advice on how to take a holistic and practical approach to managing IT security.

1 Cisco

Introduction

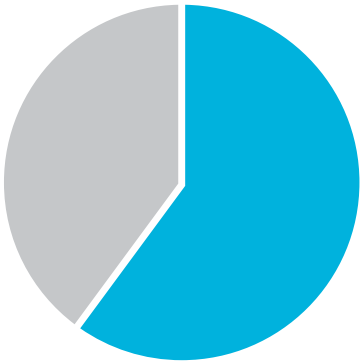
There is a confluence of factors driving the visibility and importance of security. COVID-19 has accelerated the adoption of remote working, working from home and the use of personal devices. This, along with the increased use of cloud computing and cloud applications, means that traditional perimeter security alone is no longer effective. And as the sophistication of hackers, or malicious actors, increases, the risk of a breach is increasing, along with the consequences such breaches.

Some high-profile breaches include Equifax (ex Veda), a global organisation which collects and sells credit history data. In 2017 Equifax had 147 million accounts hacked[2] and personal and credit information accessed.

In 2016, the Census website, operated by the Australian Bureau of Statistics, was maliciously attacked (four denial of service attacks) and the site rendered inoperable[3].

While these high-profile breaches are a wake-up call, they mask the real problem: hackers don't need to, and don't necessarily want to, attack large, sophisticated organisations. Making money through cyber-attacks is a numbers game. Attacking a large number of small to medium businesses, with insufficient or outdated security systems and policies can be very fruitful. In fact, 62% of cyber attacks are targeted at small business and the average value of a compromise is around $1.6M[4]. In addition, what we are seeing is the emergence of nation states as malicious actors as well as overseas individuals that have limited financial means but see significant economic arbitrage in attacking businesses in developed economies.

We recently came across a company (health food) that set up an e-commerce site to sell its products. They were commercially successful in that they transacted with 1,000 customers, but the customer information was scraped - for every online transaction, the credit card details of all 1,000 customers were stolen and subsequently sold. Social engineering is all about gathering the critical information about a person to fully exploit their identity. Credentials are a tradeable commodity and can be sold multiple times to different buyers.



62%

of cyber attacks are targeted at small business and the average value of a compromise is around $1.6M

2 Federal Trade Commission (US)
3 Australian Bureau of Statistics
4 Cisco

Those responsible for an organisation's security are in an increasingly difficult situation. The financial impact of breaches is becoming so significant that security is a critical issue for the CEO, CFO, CIO and the Board. Hackers are becoming more sophisticated, plus there are a plethora of security vendors, solutions and products. And often, the responsibility for IT security does not sit with a dedicated role. It may sit as part of the IT Manager's portfolio. As always, there are competing priorities and limited budgets.

Unfortunately, for every organisation, managing security and minimising the risk of breaches creates friction, process complexity and additional cost, so risks and their impacts need to be assessed against cost when creating a security plan. IT security policy needs to consider the impact on the business, minimise disruption and be conscious of staff productivity.

A good analogy for managing IT security is car insurance. For most days you have car insurance, you are getting nothing for your money – maybe some peace of mind – but for those rare occasions when you have an accident or your car is stolen, the insurance becomes invaluable. Similarly, with security, when things are going well, you wonder why you are spending money on security, but if there is a breach, this is the moment of huge pain and cost. A security plan has the aim of safeguarding against that pain and cost.

"You can't hit a target that you can't see".

Unbelievably, the mean time to detect a threat is 100 days. Yes 100 days. To bring this to life, imagine a robber living in your house for 100 days – observing where you are storing jewellery, cash, watches, where car keys are kept, where passwords are stored and when the house is vacant. After all that information gathering, the robber pounces. You can imagine the scale of your loss.

In the following sections, we will highlight some of the key risks, briefly look at some potential solutions, highlight the three main attack vectors – **email, web and endpoint** - and discuss another important concept – **the human firewall** - an often overlooked, but critical part of a successful security strategy. We will also explore multi-factor authentication and the move to 'zero trust'.

Unbelievably, the mean time to detect a threat is 100 days.

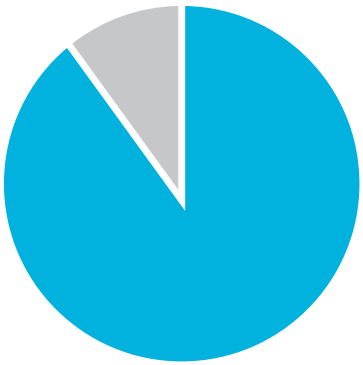
Email

For hackers, email is a numbers game.

For example, it's easy to send a high volume of phishing emails where even a very low strike rate can be lucrative. If you reverse the view, think about how many emails you receive each day or week. A small lapse in concentration, and clicking on a malicious link, can be very costly. Increasingly, malicious emails are looking more legitimate which makes things more difficult and with the huge volume of email each person receives, it's easy to make a mistake.

While back door access to your organisation is harder to crack, email effectively represents the front door - access is easy and email is therefore the number one attack vendor. 90% of attacks begin with email[5].

We are all familiar with phishing emails - and they have varying levels of believability. Some however, can look very legitimate and will entice your staff to click on a link in the email. The objective being to steal a username and password. 80% of security breaches involve compromised passwords[6], so the need to verify identity through multi-factor authentication is critical. Once credentials are captured by the hacker, they are free to navigate through your environment. Here is where the attackers now have the access to the 'crown jewels'. Consider that the attacker might be able to transfer cash to outside bank accounts, steal credit card details, etc.



90%

of attacks begin with email.

80%

of security breaches involve compromised passwords.

5 Verizon
6 Cisco

Hackers can afford to play the waiting game, and may spend days, weeks or months watching a chain of emails before pouncing at a time where they can, acting as your staff member, request, for example, that an invoice be paid into their account rather than your company's account.

So, in this case, the primary weakness in the system is actually your staff member or the 'clicker'. We refer to this as the 'human firewall'.

A real-life problem is that people get distracted or multi-task and may click on a link without too much thought. They may just be intending to have a 'quick look' at whatever it is that has been sent.

There are a couple of solutions here, firstly, education of your staff which is the **human solution** and the technology solution is Multi Factor Authentication which means account access needs to be validated using a second physical device such as an iPhone.

Multi Factor Authentication moves security closer to the user. Users are verified before being granted access.

Most people are familiar with the consulting framework 'People, Process and Technology'. To optimise your security effectiveness, you need to make sure you are covering each of these pillars. Organisations can throw a significant amount of money at the technology pillar because it's concrete and visible, but you also need to ensure you are educating your staff and investing in processes that may require additional layers of approvals. Then look at how you can automate the processes and automate the response to a breach.

"For every lock, there is somebody out there trying to pick it or break in."

Understand traffic patterns

With security, visibility is paramount. You can't shoot a target that you can't see.

An important initial step in understanding risk, is to look at the traffic patterns of your business. Are your staff sending documents to the cloud for PDF conversion? Are your staff transferring files using dropbox? Are your staff using offsite storage? What websites are your staff accessing and what cloud applications are being used? How many attachments are entering and leaving your organisation? And do you know what's in them?

For example, consider the marketing person who is working with a web developer, creating a new website. Not only is your marketing person transferring lots of data and content to a largely unknown third party, they are creating an external facing interface that needs to have security policy and procedure baked in. This is not top of mind for the marketing person, so IT needs to be involved in this process.

Some security products enforce security at DNS and IP layers blocking malware, ransomware and phishing emails before connection is established.

DNS stands for Domain Name Services – think of it as being the 'telephone book' of the internet and each time you click on a URL, say www.apple.com, behind the scenes there is a process that converts the web address into an IP address which is a string of numbers, such as 192.168 0.0 24.

DNS protection is a foundation element for protecting your users. Quite simply, each time a user clicks on a web address, the DNS Protection will look at a number of things before allowing the web address to resolve. For instance, is that web address associated with another domain that is known to be serving malware? In that case, your user will be blocked from accessing that domain.

Shadow IT

Another thing to consider is Shadow IT.

Shadow IT refers to the procuring and operation of IT infrastructure, hardware and software outside the control of IT. It is becoming increasingly prevalent because line of business managers can purchase cloud applications simply, using a credit card. For example, the Marketing Manager might subscribe to a cloud CRM platform or Marketing Automation system without any input from IT.

"By its very nature, shadow IT exists to circumvent IT governance and security controls by employees believing they're doing something beneficial for the company," says Rick Orloff, former Vice President and Chief Security Officer at Code42 and currently Strategic Advisor at Nova Partners.

"The painful truth is that shadow IT is one of the leading causes of insider data threats across any organization. There can be significant dangers associated with shadow IT, including poor IT governance, unnecessary exposure to security breaches and significant privacy risks".

"For example, a marketing organization could end up exporting their entire internal customer list to a cloud-based marketing automation platform that doesn't encrypt sensitive data," said Thomas Phelps IV, Vice President of Corporate Strategy and CIO at Laserfiche.

Shadow IT represents a problem for the IT Manager for many reasons – the solutions won't be integrated or optimised, they may represent a duplication and purchasing power is diluted. However, of most significance is the security risk.

The staff member doing the purchasing may use their personal, 'weaker' credentials which provides an avenue into your network, or they may be entering corporate credit card information into a non-secured or even malicious site.

Or consider a person using drop box instead of organisation's 'official' OneDrive. If they set up the account using their corporate credentials, if there is a breach and their details captured, this can provide access to your network. There is another a problem if they leave your organisation. Access to company data may be lost due to its lack of visibility.

Recently, we came across an organisation that was using eight different vendors for storage. This raises a whole range of issues in terms of security and data protection.

"Cisco found that IT departments estimate their companies are using an average of 51 cloud services, when the reality is those organizations are using around 730 cloud services."

Mitigating the risk of Ransomware

Thinking about ransomware attacks sends shivers up the spine of most IT and Security Managers. This is where a malicious actor gets into your network, encrypts all your data and seeks a ransom payment – most likely in bitcoin - for your data to be decrypted and accessible again. This type of attack can paralyse your business and cost a significant amount of money.

This type of attack isn't necessarily targeted at large companies. It's a game of scale, so attackers can make a substantial income by targeting a large number of mid-sized, even small companies. Often SMB's have less protection in place. Hackers are 'always on' and have scripts continually running, looking for vulnerabilities.

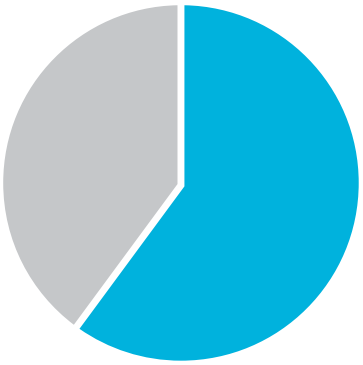
Paying the ransom is one (uncomfortable) way to solve this problem. Typically, like insuring your vehicle **after** an accident, this would then be followed by implementing a security infrastructure and policy that would have prevented the initial attack in the first place. A hard lesson indeed.

Another way to minimise the impact of such an attack is to have an effective **data protection – or back up – solution in place**. This means that you are constantly creating a copy of your data, either onsite or in the cloud, that can be restored in a little as 15 minutes. The mean time to restoration is the critical indicator and will be a function of solution design and policy. A back up, or data protection solution takes the power away from the ransomware hacker.

Often organisations think that because they are using a cloud platform such as Microsoft Office 365, their data is automatically backed up. Unfortunately, this is not the case.

60% of sensitive cloud data is stored in Office documents, and 75% of this is not backed up![7]

Microsoft offers geographical redundancy of stored data but is not ultimately responsible for its protection and restoration. This responsibility remains with the O365 customer. Usually unknowingly, this is a point of vulnerability and risk for many organisations.



60%

of sensitive cloud data is stored in Office documents, and **75%** of this is not backed up!

7 Veeam

Firewalls are no longer the - only - solution

Traditionally, firewalls have been the primary network protection solution They are perimeter devices - much like a moat around a castle or a wall around a city. They control traffic and access into a network. They inspect traffic, and filter based on predetermined policy. They are a barrier to the Internet and company resources and prevent the loss of company data.

However, firewalls have shortcomings. They operate on the basis of predetermined rules. Once a hacker figures out what the rules are, they can circumvent them; in fact, phishing, ransomware, and botnets are just three examples of threats developed to get around firewalls.

Plus, a firewall can't predict what threats are coming down the pipeline. It's a reactive system, not a proactive system. And if you haven't set the right rules, your firewall can't block the latest threats because it doesn't know to defend against them.

Today, firewalls are still an important element in the security mix– but are moving from an physical appliance to having their function being delivered in the cloud.

Unfortunately, a simple firewall solution can no longer be relied upon as the workforce is becoming more distributed – people working remotely or from home and directly accessing cloud applications using the Internet.

Also consider this simple and confronting example. Firewalls stop external threats 'getting in', but what if through misplaced trust, you let somebody in? For example, a contractor is onsite fixing a printer, they are provided access to your network and if ill-intentioned can access files, servers, etc, representing a huge risk to your business. What policies, procedures and protections do you have in place to prevent this type of breach?

Another example is where somebody, posturing as a staff member, speaks to your IT department because they are (supposedly) having access problems and want to re-set their password. Your IT department wants to act in good faith, and help their colleague, but how do they validate the caller? Multi-factor authentication minimises risk in these situations.

Managing your endpoints

Management of endpoints – PC's, phones, tablets – is a critical piece of any security strategy. Traditionally, an SOE (Single Operating Environment) has provided governance here. However, as devices proliferate and working from home becomes more common, there are increasing vulnerabilities as operating systems age or as recommended patches aren't applied.

Managing endpoints is like trying to hit a moving target. Traditional anti-virus solutions do not completely protect endpoints.

Keeping devices patched and updated is one of the strongest ways to prevent bad actors exploiting vulnerabilities and gaining access to a network through insecure devices. Ideally, this process is taken out of human hands because any latency in this process represents risk. And scripts are continually running and looking for vulnerability.

Don't forget that your organisation is part of an ecosystem

In reality, no business is isolated from other organisations in its supply chain. Every business sits within an ecosystem of suppliers, partners, customers and a range of other third parties. So every organisation in a supply chain is a risk to the others. Organisations need to consider supply chain compliance.

This means that **other organisations** may be the source of breaches for **your** business - but also your **customers** may have requirements in terms of compliance and the ability to withstand penetration (pen) testing for you to be an approved supplier. Banks in particular have stringent security requirements for their suppliers, so ineffective security can have a tangible and negative impact on your revenue. As an example, your customers or suppliers may require your organisation to be ISO 27001 certified.

It's what's on the inside that – also – counts

An often-overlooked threat is the 'insider threat' - either somebody with ill-intent who has penetrated your organisation, a disgruntled employee or an ex-employee.

Not only can they do damage, there are also legal problems if emails/docs/ company records are purged by a disgruntled or ex-employee.

Do you know where all your company information is stored? Do you have a back-up solution in place?

Threat Intelligence

So, now you have considered email, web and end point security. The next key piece to consider is **threat intelligence** – this is the 'brains' of the security ecosystem. You should ask your security vendor about how and where they get their 'threat intelligence'. This is critical, particularly in what is called 'a Day Zero attack'. Simply, this is a new threat or malware that emerges. How fast can the vendor identify and reduce the 'time to detect/ time to remediate' such attacks?

As an example, Cisco Talos inspects 600B emails per day and blocks 19.7B threats each day. The research team identifies dodgy links, domain spoofing, malicious intent and spam. Once a threat is identified, Talos shares that intelligence immediately across all organisations that are using a Cisco security product.

The human firewall

One of the biggest vulnerabilities in your security infrastructure is your people.

In fact, 95% of cyber security breaches are due to human error[8]

As somebody responsible for IT security, one of your key roles is awareness, education and behaviour of your staff. This is quite challenging because security isn't everybody else's day job.

The main things to consider are:

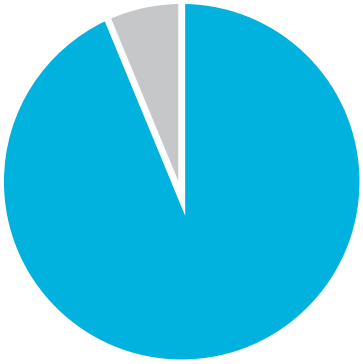
- Helping your staff identify malicious emails and ensuring they don't click on the links in these emails.
- Educating your staff that they should consult IT on any application or software purchases, particularly cloud-based, including storage services.
- Ensure their PC, tablet and phone operating systems are up to date.
- Educate your staff around the need for multi-factor authentication.

In terms of security and risk management, you should identify the 'strategic' staff members in your organisation. These people require more thorough education and additional policy should be considered around their access and behaviour.

Firstly, who has access to budgets and who controls the flow of money? Definitely CFO, Marketing and Accounts Payable. Who else?

Secondly, who has access to company IP or valuable information? This could be R&D, Engineering, Marketing or those who have access to company records or customer information.

Every organisation is different, so you will need to make an assessment as to who the strategic people are.



95%

of cyber security breaches are due to human error.

8 Cisco

Multi Factor Authentication

Multi Factor Authentication is the final important element for securing users, applications and ensuring device health.

We strongly encourage organisations to implement Multi Factor Authentication.

The easiest way to think about this is getting cash out at a Bank's ATM – you have two elements - a card (something you 'have') and a PIN number (something you 'know'). You need both before you can transact at the ATM. This now brings in the concept of ' Zero Trust'. Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture.

With Zero Trust, you will be asked to validate your credentials each time you want to access an application. A common example of Multi Factor Authentication is where you log into a particular application, eg, a banking portal, but to be granted access, you need to enter a code that has been sent to your mobile phone, for example. This means that it's not possible to access the application by simply knowing and using a login name and password. Another, biometric layer, can be added to authentication, where face recognition is required before access is granted.

Not only is Multi Factor Authentication important to for identifying valid users, it can also assess the device health each time your staff are accessing applications. For instance, do they have the latest IOS version? Are they still using a device that has not been upgraded and has known issues? Have all the latest patches been applied?

"Multi Factor Authentication is one of the most effective controls an organisation can implement to prevent an adversary from gaining access to a device or network and accessing sensitive information. When implemented correctly, Multi Factor Authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network. Due to its effectiveness, Multi Factor Authentication is one of the Essential Eight from the Strategies to Mitigate Cyber Security Incidents".

- Australian Cyber Security Centre

Five key takeaways

1

Benchmark where you are today

Understand your current traffic patterns, what domains are accessed, what devices need to be secured and what external applications are being used.

Think about leveraging a trusted partner that can provide a 'Security Gap Analysis' and make relevant recommendations. Gap analysis provides a view on security maturity and assesses business and IT processes to determine vulnerabilities and gaps.

Partners may also be able to run tests over say a seven day period, then provide a detailed assessment report.

2

Understand your risks and their potential business impact

All risks should be assessed against the impact of those risks. And all assets, eg, customer data or IP (intellectual property) need to be identified.

- What is the impact of losing customer data – both immediately to the business and longer term brand reputation? What about loss of trust in your business by customers?
- How much money will you lose if your e-commerce site goes down for 24 hours?
- How much money does it make sense to spend to mitigate these risks?
- What is the impact of having your data locked up by a ransomware attack?

3

Create a plan

Once you have a clear idea of your current environment, traffic, risks and business impact, it's time to create a plan. This is the *do what, when and why* part.

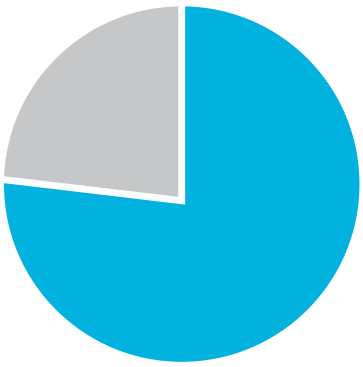
More than 77% of organisations do not have a cyber security response plan[8].

It's not possible to remove all risk from a network, and expenditure on security solutions will reach a point of diminishing returns, so you need to prioritise what needs to be done and remember, the roll out can be phased over time. Budget can be allocated across multiple financial years.

There is no silver bullet and no single solution, but we would warn against a piecemeal, 'product approach' and recommend adopting an architectural approach where there is shared intelligence and policy across all devices and elements of the security infrastructure. Based on your business model, business processes and your current infrastructure, the focus should be on the function and capability required, not the product.

And ideally, select a single vendor with global coverage so they are learning across their entire customer base and sharing those insights. This will result in an integrated and more effective solution.

Your plan should include insights, policies, procedures, communications and a technology solution.



+77%

of organisations do not have a cyber security response plan.

8 Cisco

4

Communicate

Define who your key stakeholders are.

These are the people who will be most impacted by any breaches plus whoever is providing your budget.

You also need to provide updates to the Board, either directly or via the senior leadership, as they are responsible for the overall risks of the business

You need to provide regular updates to the business and give them peace of mind but also explain what you are doing to mitigate risk. The business wants to know that its budget is being used effectively and that their part of the business is secure.

5

Don't forget about **people**

Your people and their behaviour can be a significant security vulnerability but they can also be part of the security solution. We call this the 'human firewall'.

Help them identify potential threats, the impact to the business of these threats and get them onside so they are happy to comply with any security policies and procedures.

It's a delicate balance of education, control and management.

"A robust security system contains more than just hardware or software; there must always be a "wetware" (aka human) defense element as well. A so-called 'human firewall' is a concept in security awareness that empowers a team to fight against hackers in a proactive as well as reactive fashion.

It is essentially a commitment of a group of employees to follow best practices to prevent as well as report any data breaches or suspicious activity".

- Infosec Institute

About Kytec

Kytec designs, deploys and manages a full suite of technology solutions for Australian businesses.

Kytec is certified in collaboration, cloud, security, enterprise networking, data centre, unified communications, contact centre, storage and data protection.

Kytec can provide advice and consulting with the objective of solving business problems and creating business value.

Kytec can perform a security gap analysis, live security tests, Proof of concept (POC) and make recommendations specific to your requirements.

www.kytec.com.au
sales@kytec.com.au

Kytec