NAVIGATING THE MAZE OF ANTI-MALWARE TECHNOLOGIES IN THE SAAS ERA -

Solutions for Small and Large Businesses in 2022

StepFwd IT

INTRODUCTION

Malware is a threat as old as cybersecurity itself, and in the modern era of software-as-a-service, technology is becoming increasingly available to both business leaders and cybercriminals alike.

With the increased availability of defensive technology, often on a per user basis, there has never been a better time to build a cost-effective cyber defence, but increased availability has also resulted in increased complexity.

The challenge facing modern business leaders is not how to build, or budget for, a cyber defence. Rather, it is how to build the best possible defence given the wide and often confusing range of solutions, services, bundled options and licencing models available.

This paper seeks to help business leaders assess the priority of cyber defences to their business, and in line with other operational risks so that informed decisions can be made regarding budget allocation.

This paper also seeks to provide guidance on how to navigate the complexities of cybersecurity by identifying the foundational elements of a good cyber defence.

These foundational elements are low cost/effort, scalable and readily available. This means every business, from the sole trader to the multinational, should consider implementing them. In many cases access to these tools may already be available through existing software licences, or available on a pay per-user basis, allowing easy entry for small organisations. The more advanced solutions, which will be covered in a future publication, require more investment, expertise or ongoing management effort, and should be considered by medium and large sized businesses or those with a high-risk profile.

In all cases, a strong cybersecurity partner will be able to identify solutions that are already packaged and available within existing licence agreements, and what, if any, new solutions best fit the needs of an organisation to ensure maximum risk mitigation is achieved with the budget available.

Malware, short for Malicious Software, is an umbrella term, and includes viruses, spyware and ransomware.

48%
of Australian businesses suffering an attempted malware attack in the past 12 months[1].

The average ransom costs **USD $5,600[2].** However, the average number of days for a businesses to return to normal operations is **16 days[3].**

THE IMPACT OF SAAS

SaaS, or Software as a Service, is the concept of software being run in a centralised fashion by the software developer, and access is sold via a subscription to the user. Spotify is a great example of this. You don't need to install new infrastructure to run Spotify, you simply pay a monthly fee, download the app and gain access to all of Spotify's features and music. This model usually reduces initial set-up costs and often facilitates a consumption or user based commercial model.

This phenomenon has reached the world of cybersecurity. Gone are the days when large amounts of hardware needed to be procured and installed to run an enterprise solution such as an anti-virus or web filtering. Instead, a monthly fee can be paid to a large provider, providing a set number of users access to the service.

This is great news for small and medium sized businesses, who benefit from reduced barriers to entry for many products, and solutions and costs that scale with their business.

This does, however, result in many, many cybersecurity services that were previously cost prohibitive now being available to all businesses. The challenge for today's business leaders and their partners is navigating the potential options and selecting the right strategy and underpinning technologies to give them the best return for the allocated budget.

Unfortunately, SaaS has also become standard in the world of cybercriminals, resulting in a sharp increase in cybercrime.

Historically, only individuals with a combination of very in-depth knowledge of computer programming, and the desire/morality to use it for criminal purposes were capable of committing cybercrimes. This was a rare combination of skills and circumstances.

SaaS, however, has resulted in those capable of developing malware being afforded a second option. Instead of committing cybercrime themselves, they can now sell multiple copies of their malware to other criminals who do not have the capability to launch attacks on their own.

This ultimately results in two different outcomes.
First, a degree of separation is added between the malware developer and the cybercrime event, which makes the practice more appealing to some computer programmers.
Secondly, the number of criminally minded individuals and groups with access to cybercrime capabilities has greatly increased.

This 'deskilling' of cyber-attacks is one of the key factors in the increasing number of cyber-attacks in 2021.

UNDERSTANDING YOUR MALWARE RISK PROFILE

Many businesses struggle with the issue of prioritising malware and other cybersecurity threats. Measuring the return on investment for cybersecurity spend is often difficult as attacks avoided are hard to quantify. Conversely, businesses that have been affected by a successful malware attack often invest heavily, to the point of overinvesting due to the cost and damage incurred.

It is strongly recommended that malware be treated like any other risk to a business's operations, and be assessed by its likelihood and impact, with mitigation activities and budget allocated in alignment with that assessment.

LIKELIHOOD

The unfortunate truth is that due to the ease at which malware 'kits' can be purchased online, the low skill requirements to deploy them, the ability to deploy them from different legal jurisdictions and the often lucrative results, malware is a common occurrence.

Sophos, a security software vendor, commissioned a report in 2020 which surveyed 5000 IT leaders and found that of the Australian respondents, 48% had suffered a successful malware attack in the 12 months prior[1].
To reinforce this, many high profile Australian organisations fell victim to malware in 2020 including Service NSW[4], Lion Australia[5], BlueScope[6] and Toll Group[7].

Three simple questions for business leaders to consider around the likelihood of a malware incident:

1. How confident am I my current cyber defence uses modern practises and technology
2. How I.T. savvy are my team
3. How public is my brand and image

While the threat of malware starts with a probable likelihood for all businesses, some factors can increase an organisations exposure to malware and should be considered when assessing the likelihood of an attack:

- **I.T. competence** – Many malware attack techniques rely on simple methods to gain access, which may be missed by non-savvy or untrained staff.
- **Public image** - A large public image or if the organisation is sometimes covered in mainstream media can increase the likelihood of malware attacks as attackers attempt to create a reputation for themselves.
- **Industry** - Certain industries, such as Financial Services and Healthcare, are disproportionately targeted by malware.
- **A large technology environment**, such as large server estates or highly computerised operations, creates a wider footprint exposed to attack.
- **Current cybersecurity posture** – Cybercriminals are often scanning the internet for weaknesses, meaning leaving holes in defences can attract additional malware attention over and above what the organisation would have received otherwise.
- **Historic attacks** – previous successful attackers are used by attackers as a sign of weak defences, and often result in increased future targeting. This increases exponentially where a ransom has been paid, as it marks the victim organisation as one likely to pay ransoms in future attacks.

[1]https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
[2]https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
[3]https://www.datto.com/resource-downloads/ANZDatto-State-of-the-Channel-Ransomware-Report.pdf
[4]https://www.service.nsw.gov.au/cyber-incident
[5]https://www.smh.com.au/technology/hackers-post-evidence-they-have-beer-giant-lion-s-confidential-files-20200619-p5548s.html
[6]https://www.afr.com/technology/port-kembla-steelworks-hit-as-bluescope-cyber-attack-bites-20200515-p54tb9
[7]https://ia.acs.org.au/article/2020/mytoll-still-down-after-ransomware-attack.html

IMPACT

Assessing the potential impact of a malware attack involves several factors. There are both direct and indirect costs, and in the case of ransomware, there may be a ransom cost to consider. A CrowdStrike study found the costs of a ransom payment alone can be more than USD $1 million[8], although the average is closer to $5,600[2], as attackers tailor their demands to the victim organisations size. The key factors to consider when estimating the impact of malware are:

- **Cost of internal downtime** – If systems are taken offline, employees may be unable to work, leading to not just unproductive time, but a backlog of work once systems are restored. The average downtime suffered as a result of malware is as high as 16 days[3].
- **Lost sales** – There can be a direct loss of sales from system downtime, such as a website, but also future lost sales due to brand and reputational damage.
- **Cost of professional assistance to perform the recovery** – Additional skilled resources may be required to aid in remediation. Overtime or additional services costs may also be incurred.
- **Value of data that may be lost** – Some data may never be recovered after a malware attack, meaning its value is lost, or the data will need to be regenerated at a cost.
- **Damage to brand and reputation** – increasingly consumers and businesses view it as a risk to transact with a business that has fallen victim to malware in the past.

- **Cost of dissatisfied customers** – As customers are unable to interact with the business, they may become increasingly frustrated, negatively affecting sentiment and future repeat business. There is also a risk that customer data may be part of a cyber incident, which if made public could have an impact on that customer, and their relationship with the victim organisation.
- **Increased insurance** – Many cyber insurance policies will increase the cost of premiums following a successful attack.
- **Cost of unmet contractual obligations** - Downtime as a result of malware often results in a business missing its contractual obligations.
- **Regulatory fines** - Fines may be incurred due to data privacy breaches or negligence.

Once a business has an accurate, but not alarmist, view of its risk profile it can determine the appropriate budget to allocate to mitigate this risk. Fortunately, many of the foundational elements of malware defence are standard practice and should not require additional investment.

Three simple questions for business leaders to consider around the impact of a malware incident:

1. What would be the impact of all systems being offline for a day, or a week?
2. How well do I know what critical and confidential data I have, where it is and who has access to it
3. What would my current and future customers think if I were to be the victim of a cyber-attack?

[8]https://www.crowdstrike.com/resources/reports/global-attitude-survey-2020/

THE FOUNDATIONS OF A GOOD DEFENCE

These are the practices that every business should consider, from the sole trader to the multinational. While the technology may change as the business scales, these practices can be put in place with low cost and effort, and so should be considered by all organisations.

Training – Gone are the days when training required an in-house training team. Today, there are many low-cost high-value SaaS solutions available, and many free resources online.
Put simply, if all staff were given a piece of machinery which, if used incorrectly, could cause the entire business to stop operating, would they be given training on how to use it correctly?
The same principle should be applied to the humble laptop.

As users learn to avoid high-risk behaviour and to spot the signs of attempted malware attacks a business's likelihood of being impacted by a malware outbreak reduces considerably.

While the lowest cost solutions can be found for free online in places like YouTube, more mature solutions will involve not just training videos but simulation facilities and management information to provide oversight and governance to leaders.

Simple User Device Hardening – Several simple steps can be taken on user devices by an organisation to reduce the risk and impact of malware. These include activities such as switching off macros in Microsoft Office, blocking flash and java in web browsers, restricting administration privileges, and enabling inbuilt ransomware protection on Microsoft Windows.

Web Filtering – Preventing accidental access to websites that pose a high security risk is a simple and effective way to protect a business from malware infections delivered via drive-by download. This type of malware is hidden within a website and attempts to trick the users into installing it, or in some cases can install itself without the user knowing. SaaS offerings have changed the web filtering market significantly by removing the upfront investment requirements and reducing the ongoing management needs. Modern, market-leading products are now available at per-user costs, with large reductions for very small businesses.

Secure Email Gateway (SEG) – A SEG provides several important functions in the fight against malware by scanning incoming mail and looking for threats. Modern solutions will use threat intelligence aggregated across many organisations, along with AI/ML techniques to determine the trustworthiness of emails, as well as virtual sandbox and scanner technologies to identify and eliminate malware before it reaches the users.

Modern email services, such as Exchange Online and Google Mail provide inbuilt SEG functionality, with more advanced functions often available at an increased licence cost. Businesses at particular risk of cyberattack should consider implementing an additional, independent SEG to complement these systems.

Anti-Virus – Long the cornerstone of cyber defence, anti-virus software is still an important tool in the fight against malware. Market leading anti-virus software contains separate modules to prevent viruses, malware and ransomware. Many operating systems include this kind of protection out of the box, such as XProtect on macOS and Microsoft Defender on Windows 10.

Backups – One of the most undervalued defences against malware is the humble backup. Not often considered a security technology, backups have become more important with the rise in the popularity of ransomware. As malware increasingly tries to remove and monetise access to corporate data, a backup is an incredibly simple and effective countermeasure[9].

Simple backup solutions can be implemented through cloud storage tools, and market-leading solutions have backup frequency tailored to each system based on the value of the data. All backups should be regularly tested and store data away from the operating environment, so when a restore is required the data integrity is assured.

Patching – Did you know on the second Tuesday of every month you are entered into a race with cybercriminals? This is when Microsoft releases its monthly security patches. While this is undoubtedly a good thing, it has a dark side many business leaders do not know about.

The release of patches effectively highlights where systems have vulnerabilities.
Once released cybercriminals will immediately begin reverse engineering each patch, attempting to understand the vulnerability that's being patched and trying to build malware to exploit it. Once ready, they will look for any devices that haven't yet installed the patches. The same is true of all software installed in a business's environment, regardless of the vendor.

Simple patching doesn't require any additional technology, just a small amount of time when patches are released. While occasionally annoying, a small amount of time to install a patch can save a huge about of downtime and cost in the future.

Effective, enterprise grade patching happens as quickly as is possible without introducing undue risk to the business and includes management information to demonstrate the completeness of the process.

Mobile Management – Often mobile devices are not considered when reviewing cybersecurity, but now that mobile devices can perform many of the same functions as laptops, a similar security coverage is required. Web filtering, patching, backups and anti-virus should all be considered in the mobile environment. Often inbuilt technology will exist and be sufficient (depending on the manufacturer and OS) but review and consideration are still required.

Cyber insurance – while cyber insurance is generally well adopted, it's estimated that of organisations that do have cover, 64% do not have adequate cover for malware and ransomware attacks[10]. Good cyber insurance should cover ransomware and social engineering, and premiums should reduce with investment in cyber defences.

The advanced practices, which will be covered in a future publication include a hardened user estate, a malware response plan, regular 'fire drills', updated DR plans, vulnerability scanning, privileged access management, user reporting procedures, network segmentation, next-generation firewalls (IPS/IDS), SIEM, SOC and autonomous AI defence tooling.

[9]In some cases newer ransomware uses been known to use double or triple extortion. This is when access, confidentiality and clients are used to extort payments. Backups are only an effective solution against access extortion, which remains the primary method of ransom.
[10]https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

CONCLUSION

Like the security industry, the malware industry has moved to a SaaS model. The availability of malware kits to the average criminal, coupled with the ease of use, remoteness of use and lucrative rewards have all contributed to the current prevalence of malware.

This, along with the amount and complexity of different security solutions available, and the hard to calculate ROI of defensive spend, creates a trap many Australian businesses fall into, resulting in them falling behind, and falling victim.

However, with the increased availability of security technologies, there has never been a better time to build a cost-effective defence that allows business to continue unaffected in the face of malware attacks.

Businesses need to treat malware like any other risk to operations, and use security expertise, either in-house or outsourced, to avoid selecting solutions that don't suit their needs and burning budget with little return.

An effective defence should make use of 'bang for your buck' solutions that are already available in existing software packages, allowing low cost, highly effective defences, and freeing budget up for other endeavours

Contact Info

hello@stepfwdit.com.au

1300 131 679

https://www.stepfwdit.com.au/

StepFwd IT