Cybersecurity and Data Awareness

A guide to protecting yourself and your customers from a potential threat and how to respond if you have been attacked…

| eBook

DIAMOND

"*There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.*"

John Chambers
Chief Executive Officer
Cisco Systems

Table of Contents

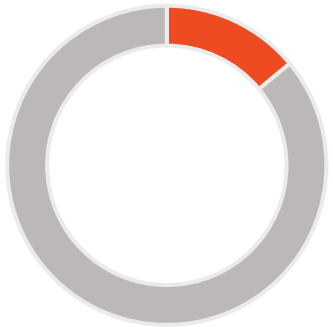
DIAMOND

Cybercrime by the numbers

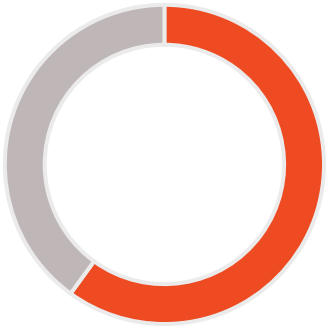
Are you under threat?

62% of attacks target small-to-mid sized businesses

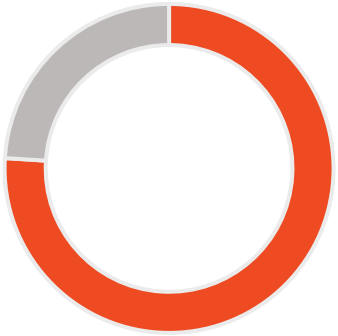
Only 14% of small businesses are “highly effective” at risk mitigation



60% of small businesses attacked fold within 6 months



76% of businesses reported phishing attacks



Today, more than ever, you need to secure your network to keep your operations going, keep your data safe and most importantly keep your customer’s data safe.

“Cyber” threats are constantly evolving and becoming more complex, so it is important to remain proactive and vigilant with respect to IT security.

Cybersecurity has evolved to become more than a technology issue that can impact operations and business information. It can also present legal risks and impact reputation.

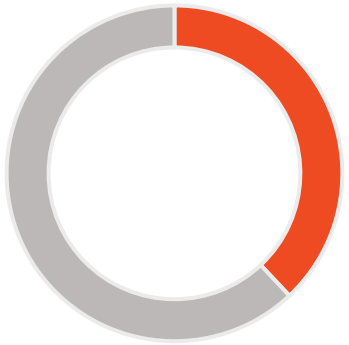
Sources: Denver Post, 2016. Verizon, 2018. Cybint Solutions. Varonis, 2018. Cisco. Wombat Security, 2019. Keeper Security, 2018.

DIAMOND

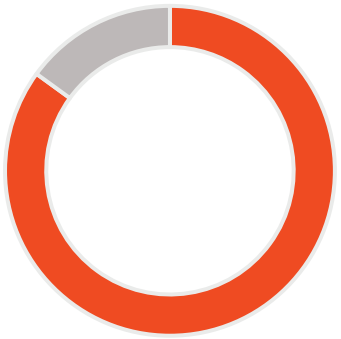
Cybercrime by the numbers

How do they get in?

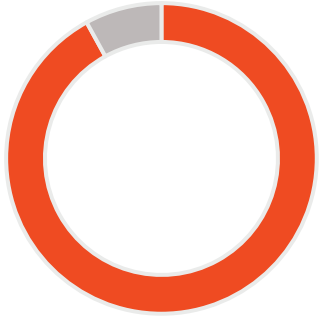
38% of malicious files are in Microsoft Office format



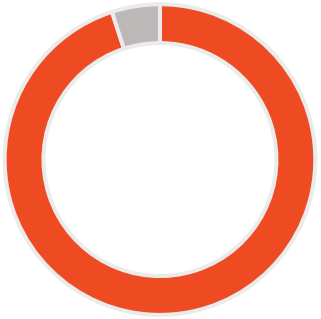
85% of all email attachments are malicious



92% of malware is delivered via email



95% of breaches are due to human error



Cybercriminals are after your data and they want to disrupt your systems.

They are creative and consistently change methods in an attempt to trick you, your staff and even your business partners into divulging confidential information such as usernames and passwords.

Ensuring staff understand how to identify a cyberthreat and how to manage them appropriately can not only help avoid potential attacks but can maintain your reputation as a safe organisation to work with.

Sources: Denver Post, 2016. Verizon, 2018. Cybint Solutions. Varonis, 2018. Cisco. Wombat Security, 2019. Keeper Security, 2018.

DIAMOND

Cybercrime by the numbers

How do they stack up?

350%	Increase in ransomware attacks every year
516,380	SMBs fell victim to cybercrime in 2017
25+ hours	Average downtime for 1 in 4 businesses hit by a cyberattack
$1.9 million	Average cost of data breach in 2017
$1 billion	Annual cost to the Australian Economy in 2018
$6 trillion	Worldwide cybercrime costs by 2021

Sources: ASBFEO, 2017. Norton, 2017. Ponemon Institute, 2017. Cybint Solutions. Varomis, 2018. TechRepublic, 2017. Cybersecurity Ventures, 2018.

DIAMOND

Cybercrime by the numbers

What is the most important number?

1

It only takes one employee to be tricked by a scam in order to gain access to your business' data

DIAMOND

The cost of a cybersecurity breach to your business

The Australian Criminal Intelligence Commission (ACIC) states Australia is an attractive target for serious and organised crime syndicates due to our nation's relative wealth and high use of technology such as social media, online banking and government services.

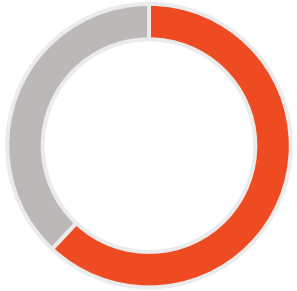
There are three types of costs you may incur if your business experiences a cyberattack.

1. **Economic costs**
2. **Damage to reputation**
3. **Legal costs**

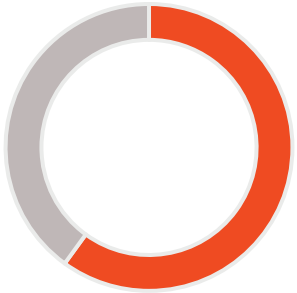
DIAMOND

Cost of a cybersecurity breach #1

62% of attacks target small-to-mid sized businesses



60% of small businesses attacked fold within 6 months



Source: Denver Post, 2016.

Economic costs

Cyberattacks are getting more and more sophisticated with hackers penetrating email systems, intercepting communications and leveraging company and supplier information to their advantage. The types of economic costs can include:

- **Theft of corporate information**
- **Theft of financial information or money**
- **Disruption to trading**
- **Loss of a business or a contract**

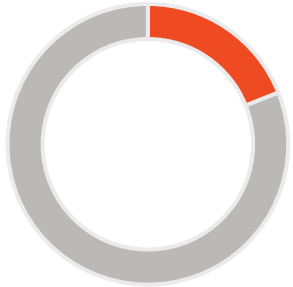
Example: An innocent looking email from a sub contractor recently cost an organisation over $20,000. An email exchange between the business and their supplier resulted in a fraudulent request for bank account details to be updated. This request was accompanied by a more formal request, via email, on letterhead. Unfortunately, due to the official nature of this interaction, the money was paid into the cybercriminals' bank account.

DIAMOND

Cost of a cybersecurity breach #2

46% of organisations suffered brand damage due to a cyberattack

19% of organisations suffered reputation damage due to a third party security breach



Source: Forbes Insights, 2016.

Reputational damage

A company's reputation is paramount. One successful cyberattack can bring years of hard work undone. When subjected to a data breach, how prepared you are and how you respond may be put under the microscope. The types of reputational damage can include:

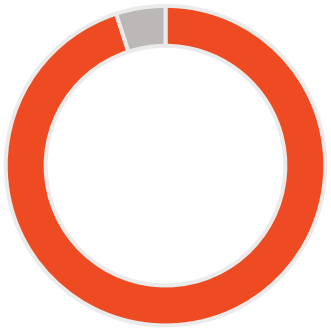
- **Loss of customers**
- **Loss of sales**
- **Reduction in profits**

Example: A local business had a staff member click on a link in an email that contained a CyrptoLocker Virus. It shut the business' systems down for over a week which meant they were unable to see customer information or project status. This resulted in the business not being able to meet customer deadlines, impacting current and future business opportunities.

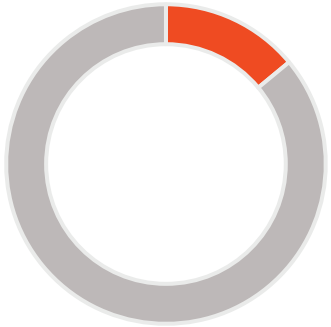
DIAMOND

Cost of a cybersecurity breach #3

95% of breaches are due to human error



Only 14% of small businesses are “highly effective” at risk mitigation



Sources: Cybint Solutions, 2018.
Keeper Security, 2018.

Legal consequences

What your organisation did to prevent the breach and how well you responded will determine financial penalties. The types of legal consequences can include:

- **Penalties for negligence**
- **Legal action from impacted parties**
- **Trading sanctions until a business rectifies the cause of the breach**

Note: Penalties for notifiable data breaches used to be calculated based on the size of the organisation and the amount of data that was confirmed stolen. More recently, the Office of Australian Information Commissioner (OAIC) has tended to base fines on the level of negligence by the business that led to the breach.

The key questions OAIC audit officers will ask include: *“What have you (the breached organisation) done to prevent the breach?”* and *“How did your organisation respond to the breach?”*

DIAMOND

"Where machine-learning mimics human behaviour it becomes artificial intelligence (AI). We can develop programs that mimic humans to fool malicious software. At the same time, AI is used by criminals and by intelligence organisations to mimic human behaviour."

Professor Alana Maurushat
Professor of Cybersecurity and Behaviour, Western Sydney University and Director, IFW Global

Artificial Intelligence

A double-edged sword

DIAMOND

Artificial Intelligence (AI)

Good guys

Due to the vast number of threats and attacks carried out globally each day, companies, such as Fortinet who provide integrated security solutions, rely on sophisticated AI and machine learning to protect their customers.

Application of artificial intelligence in cybersecurity

Like all intelligence, AI needs to be taught. It can be likened to the mind of a child that is gradually "trained" to autonomously collect, analyse and classify threats.

Fortinet's Self-Evolving Detection System (SEDS) has been learning about cyberthreats for years. Now considered mature, this machine learning and AI program features a continuous training model that has proven effective even against next-generation malware.

Once it develops new and effective defence signatures these are distributed across the Fortinet Security Fabric in real-time, designed to provide wholistic protection for businesses from advanced threats.

Source: Observer, 2017. Fortinet, 2019.

vs. Bad guys

Cybercriminals are increasingly leveraging technology, in particular AI, to enhance their scamming abilities.

With AI as a tool, they can net a higher degree of success making it near impossible to distinguish between AI and humans, particularly on social media.

This was demonstrated with SNAP_R (Social Network Automated Phisher with Reconnaissance), a spear phishing tool powered by AI, created by researchers from ZeroFOX.

The tool absorbs data from a target's Twitter account, then writes a personalised *phony* tweet complete with a malicious link. Confirming the theory that social media is ideal for launching a targeted cyberattack with very little overhead.

> *"By using AI, cybercriminals can launch mass attacks that are all automated so they never get tired and they can be very targeted by setting web crawlers that work off a set of parameters based on public information gathered over the internet; which in turn is then used to gain access to a company's system"*
>
> *Professor Alana Maurushat, Director, IFW Global*

Source: IFW Global, eBook (Payment Diversion Fraud - The Impact of AI) 2019.

DIAMOND

Know your enemy

Sophisticated business models

Far from being mavericks operating from basements and dark rooms, some cybercriminal networks are moving towards sophisticated business models that closely resemble legitimate businesses.

An understanding of the nature of these networks is essential in developing a plan to defend against them.

Experts such as Professor Alana Maurushat advise to *“consider these nefarious organisations as business competitors, like any other in the market.”*

These business models include facets such as HR teams (for recruiting and background checking), marketing and sales departments, in-house staff training, disaster recovery, money-back guarantees and 24/7 telephone support.

These sophisticated organisations have become successful in much the same way other businesses do, as functions such as marketing teams help to build their reputation in the cybercriminal community and advertise their services via the dark web.

DIAMOND

Know your enemy

Curious characters

The other end of the scale from cybercrime networks are those curious people prying around networks to enhance their skills.

Students have been known to hack into businesses and university systems as part of their own learning and development.

In most cases these are fairly innocent interactions but can be disruptive as they poke around moving or deleting files and seeing what mischief they can get up too.

In some cases, hackers collect this sensitive information and sell it on the dark web.

Australian National University (ANU) suffers data breach

Situation: Hackers accessed personal data belonging to staff, visitors and students dating back 19 years, including sensitive data such as date of birth, tax file numbers, bank accounts details and academic records.

Solution: The ANU released a statement about their course of action, June 2019.

"*We've been working closely with experts in this area because there is inherent risk involved with any internet connected system, which is why we must always be vigilant.*

There are things we can do to reduce the risk of data breaches, both at an organisational level and an individual level. Organisationally, we have invested heavily in IT security in the past 12 months and that investment has been successful in the sense that it reduced the risk presented by many attackers, and it helped us detect this sophisticated intrusion.

We need to keep investing in security. On an individual level, we can all change our passwords regularly, be vigilant about where we keep our information and be alert to suspicious activity."

How do cybercriminals get in?

Malware

For a long time, the phrase “computer virus” was misappropriated as a term to define every type of attack that intended to harm or hurt your computers and networks. A virus is actually a specific type of self-replicating attack, or malware.

Any software created for the purpose of destroying or unfairly accessing networks and data should be referred to as malware.

An attacker will use a number of methods to get malware installed onto your computer but generally requires a user to take action. This may include clicking a link to download a file or opening an attachment that may look harmless.

Once in your system, malware can take control of your machine, monitor your activity and access and syphon confidential data from your computer or network.

- Word document or PDF attachment
- Malicious email attachment
- Gains foothold and wreaks havoc

DIAMOND

How do cybercriminals get in?

Phishing

Phishing is the act of creating an application or website that impersonates a trustworthy and often well-known business to elicit confidential information.

Just because you received an email that says it's from Australia Post, the Australian Federal Police or even your own bank doesn't mean it should be taken at face value. Always verify the source of any service requesting your sensitive data.

Phishing can be targeted at millions of unknown users or directly at one individual (Spear Phishing), presenting links to malicious URLs in emails, or direct traffic to "spoofed" websites.

Clicking on these links can open the door for attackers to enter your system and access confidential data like bank account details, credit card numbers and passwords.

- Overwhelmingly email based
- Predominantly targets data theft
- Can use email, SMS or websites

DIAMOND

How do cybercriminals get in?

Social engineering

Not all types of malware rely solely on devious computer programming. Experts agree that the majority of attacks require some form of what is called “social engineering” to be successful.

Social engineering is the act of tricking people, rather than computers, into revealing sensitive or guarded information. Complicated software is totally unnecessary if they can just convince potential victims that they're a security professional who needs their password to secure their account.

Often a cybercriminal will impersonate a high-ranking individual in an organisation in an attempt to divert authorised payments to themselves.

These attacks are harder to detect as they rarely contain any malicious links or URLs, so will not be intercepted by security technology.

- Business Email Compromise (BEC)
- Highly targeted social engineering
- Usually uses identity of CEO or CFO
- Often a payment diversion fraud

DIAMOND

“Education, policy and planning…

This is key to protecting your

business from costly cyberattacks.”

Glendin Franklin-Browne
Technology Consulting Manager
Diamond IT

Minimise the Impact of a Cyberattack on your Business

Protection strategies

DIAMOND

Tip #1

1. Implement policies and keep them up-to-date
2. Ensure they are read and understood
3. Review & test regularly, every 12-24 months

Protection strategies

Staff policies

The vast majority of breaches are caused by human error.

Proper staff policies are critical in demonstrating diligence and protecting your organisation from financial and reputational damage.

A cybersecurity policy is more than a document that you don't use or read until something goes wrong. It helps protect your organisation and demonstrates a level of diligence in the protection of your systems and data.

You must ensure every staff member has read the policy, understands it and signs off to say so. Review your policy regularly, every 12-24 months and ensure staff are aware of any changes.

Incorporating a data breach response plan can go a long way to reducing the impact of a cyberattack on your customers' perception.

Policies and response procedures can be tested sporadically with a mock event and should be interactive and facilitated by a specialist.

How your business handles the situation and how well you keep your customers informed and support them though the situation is critical to maintaining your former reputation.

DIAMOND

Tip #2

1. Enable staff to identify threats through training
2. Equip staff on how to manage information
3. Demonstrate diligence ahead of an attack

Protection strategies

Staff awareness

Even world leading cybersecurity organisations can take hours to identify new threats and push out patches. Your staff are the first line of defence against these evolving threats.

Employees can be held personally accountable for breaches so they must be provided with proper training and tools. Staff awareness training demonstrates diligence in ensuring staff are properly educated ahead of an attack and it also shows your customers that you take cyber and data security seriously.

"In the past six months 75% of data breaches that I have been involved in investigating could have been avoided had staff been made aware of the signs."

Glendin Franklin-Browne, Technology Consulting Manager, Diamond IT

It is also important that staff understand their legal obligations when handling your clients' and customers' personally identifiable information.

Both your organisation and your employees will be held accountable by the Office of the Australian Information Commissioner (OAIC) in a data breach situation. It is your responsibility to provide staff with the proper training and tools in a similar fashion to WHS (workplace health and safety).

DIAMOND

Tip #3

1. Reduce impact of attacks
2. Ensure reporting compliance
3. Resume operations speedily

Protection Strategies

Data breach response plan

A data breach or cyberattack is a stressful and disruptive event. If you faced an attack today, who in your organisation would know what to do? How long would it take for customers to be informed?

Could you determine your notification obligations, and what data would be collected for an audit process?

If your business is breached the last thing you want to be doing is figuring out how you're going to address the situation.

Having a proper plan will help you to:

- Quickly mobilise the right resources (who in your organisation knows what to do?)
- Promptly and clearly communicate with customers and staff
- Identify if a notifiable data breach has occurred and respond in a timely manner (30 days)
- Prepare the necessary information if an audit is required

DIAMOND

Tip #4

1. Develop a technology roadmap
2. Ensure & test an integrated security plan
3. Align your network with industry best practise

Protection Strategies

Technology

With networks becoming increasingly disjointed and complex, it is important to have a technology roadmap that addresses all aspects of your business. As your business grows, adding employees, offices, connected devices and business applications, you become more vulnerable to cyberthreats.

To enable an effective defence, the data and security elements across all of your business network's various environments must be well-integrated, able to share intelligence, and be visible.

"Fortinet Security Fabric solutions for small business are based on the industry's best firewall / unified threat management (UTM). These solutions are tightly integrated with other core infrastructure and security components to protect the entire business from advanced threats."

Mark Kovacik, Account Manager, Fortinet

Look for a provider that will keep your network in alignment with industry best practise through proactively assessing and recommending the best technology solutions for your organisations needs, including top of the line security equipment.

DIAMOND

Useful Links

www.scamwatch.gov.au
Provides information to consumers and small businesses about how to recognise, avoid and report scams – subscribe for alerts on the latest scams.

www.cyber.gov.au
The Australian Cyber Security Centre, news and tips on how to better secure yourself or your business online, as well as report a scam, cybercrime or identity theft issue.

www.staysmartonline.gov.au
Australian Government's online safety and security website, designed to help everyone understand the risks and simple steps we can take to protect our personal and financial information online.

https://diamondit.com.au/technology-security
Provides information, tips and examples for Cybersecurity, Ransomware and other related updates – subscribe for monthly eNews.

DIAMOND

How Can We Help?

Diamond have a team of cybersecurity experts with specialised skills in Unified Threat Management (UTM) technologies and staff education and training services including mock events.

We have extensive knowledge in managing data breaches and can assist with Notifiable Data Breach Scheme (NDBS) and General Data Protection Regulation (GDPR) preparation and response.

Cybersecurity is a vast and complex environment. We can help ensure your technology, policy and staff education programs align with best practice.

Let us Help you Secure your Business Today

https://diamondit.com.au/technology-security

DIAMOND