Grant Thornton

An instinct for growth™

Cyber Security for SMEs

Ken Miller

Grant Thornton Consulting

Statistics

Cyber security is a big problem for small business.

- Small business is the target of **43%** of all cybercrimes.
- **22%** of small businesses that were breached by the 2017 Ransomware attacks were so affected they could not continue operating.

Source: Cyber Security Best Practice Research Report at www.asbfeo.gov.au/cybersecurity

- **33%** of businesses with fewer than 100 employees don't take proactive measures against cyber security breaches.
- **87%** of small businesses believe their business is safe from cyberattacks because they use antivirus software alone.
- Cybercrime costs the Australian economy more than **$1bn** annually.

Statistics

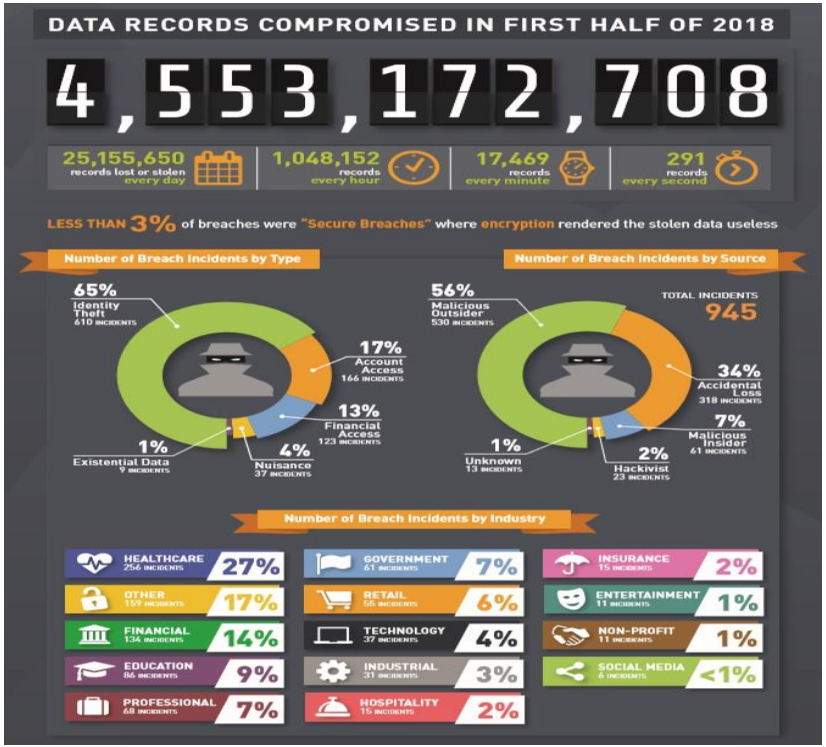
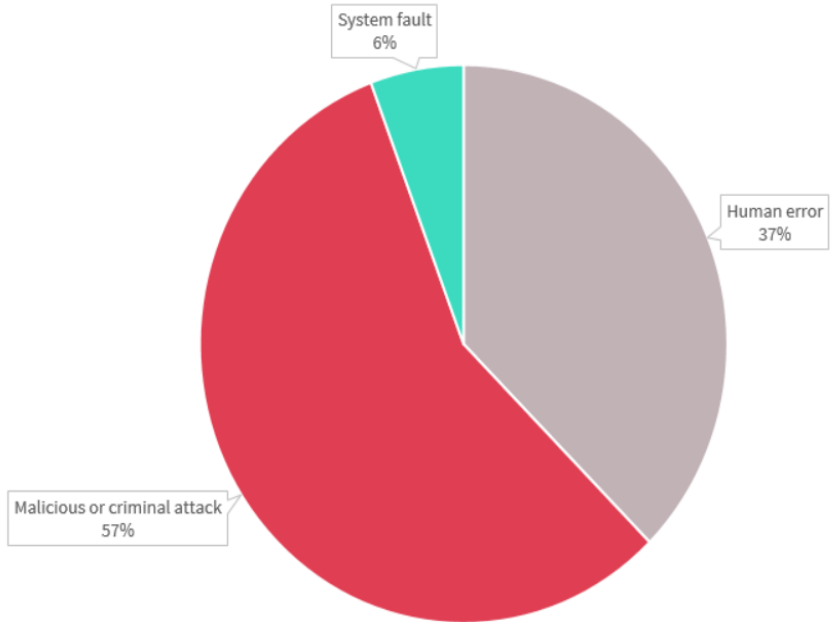


Chart 1.4 — Source of data breaches by percentage — All sectors



https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-july-30-september-2018

Detection and Incident Response

Grant Thornton | An instinct for growth™

Data breaches 2018-19

Australia Post – March 2019

- AusPost's Bill Scanner caught up in Gmail privacy sweep – Works with Google to ensure API permissions aren't revoked

ASUS – March 2019

- ASUS users targeted in large supply chain attack – Users infected via software update utility
- ASUS releases fix after ShadowHammer malware attack – But some users unable to update to non-backdoored software

Bank of Queensland – March 2019

- Bank warns of reported third-party data breach – The Bank of Queensland has announced that it has been made aware of a personal data breach by a third party provider

Kathmandu – March 2019

- Credit cards cancelled as Kathmandu reveals online store hacked – month-long breach during peak discount period
- Kathmandu hit by hackers
- Credit cards cancelled as Kathmandu reveals online store hacked
- Kathmandu flags suspected data breach
- Data breaches have possibility to ruin customer relationships

Citrix – March 2019

- Citrix investigates major security breach – resecurity says it believes at least 6TB of data was downloaded

Melbourne Hospital – February 2019

- A cyber crime syndicate accessed the medical files of 15,000 patients at Melbourne Heart Group at Melbourne's Cabrini Hospital
- 'The crooks are ahead': Cabrini breach a warning for Australia
- Melbourne heart clinic hit by ransomware attack

CoffeeMeetsBagel – February 2019

- Dating site Coffee MeetsBagel warns Aussie users of data breach on Valentines Day
- 'Coffee Meets Bagel' Dating Site Hit by Data Breach

9Honey – February 2019

- Dating app suffers data breach

Toyota Australia – February 2019

- Toyota Australia hit by cyber attack – takes down email and other systems
- Cyber Ransom Attacks On The Rise, Toyota Australia has confirmed it has been subject to an attempted cyber attack
- Millions of customers' data accessed in second Toyota hack – Tokyo sales subsidiaries raided
- Toyota Australia hit by cyber attack

AMP – February 2019

- Chinese AMP contractor pleads guilty to data breach

LandMark White – February 2019

- Australian bank customers caught in valuation firm data breach | Caused by undisclosed 'security vulnerability'
- Home loan details of 100,000 customers hacked in major data breach
- LandMark White blames exposed API for data breach – ANZ confirms it has suspended use of the property valuer
- Valuation firm hit by data breach LandMark White pleads for long share suspension
- Embattled LandMark White shares drop 10.6 pc after data breach
- NAB pulls plug on LandMark White as home loan breach scandal grows
- LandMark White blames ill-informed public commentary on its dark web data breach for further ASX share suspension
- Centrelink keeps LandmarkWhite, says data breach hit 'very small' client group
- LandMark White counts cost of data breach – LandMark White still unsure of financial impact
- LandmarkWhite knew of IT weakness in 2017, a year before data breach
- Landmark White's stolen data re-appears on dark web
- Landmark White data disaster claims CEO scalp
- LandmarkWhite faces regulator scrutiny over IT response, disclosure
- LandMark White CEO exits after data breach – two directors step down from board
- CBA assures itself of LandMark White's post-breach infosec
- LandMark White's data breach just the beginning for cyber criminals

Department of Parliamentary Services – February 2019

- Security breach strikes parliament's IT network – all passwords reset
- Political party networks caught up in parliament's IT breach – but no evidence of electoral interference
- The cyber attack on Parliament was done by a 'state actor'
- Citrix | Australian parliament hackers gain remote access

Bunnings – February 2019

- Bunnings exposed staff performance database – individual staffer did unwanted homework

Facebook – January 2019

- Apple Shuts Down Facebook Data Collecting App – Since 2016, Facebook has been asking users to install a "Facebook Research" VPN that lets the company monitor their phone and online activity, according to Tech Crunch
- Apple punishes Facebook over app that paid users to hand over data
- The Apple-Facebook Feud Hits a Breaking Point
- Facebook stored millions of user passwords in plain text – hundreds of millions of users to be notified
- Facebook says up to 111,813 Aussies in last year's security breach
- Facebook's lax security has left millions of users with a lot to worry about
- Facebook staff had access to millions of users' passwords in plain text, violating security practices

Global Hacking Scare – January 2019

- Global hacking scare nets Queensland MP, Surf Life Saving as millions of passwords breached – websites belonging to Queensland's Deputy Opposition Leader, a real estate business and Surf Life Saving Australia are among thousands of pages caught up in the latest international data breach

SkoolBag – January 2019

- MOQdigital's education software platform SkoolBag caught in global data breach

Optus – January 2019

- 'Mistakenly' Publishes Private Numbers Online And In White Pages

Collection #1 – January 2019

- Breach Exposes a Record 773 Million Email Addresses – The massive trove of leaked data, which was posted to a hacking forum, also includes 21,222,975 unique passwords.
- Experts comment on record 772mil-user data breach – Cybersecurity expert and founder of website Have I Been Pwned Troy Hunt broke the news recently that the largest ever database of breached login details have been leaked on the dark web.
- Data leak – Collection #1 is the just the beginning
- Cyber watchdog warns on dark web PS data – The Australian Cyber Security Centre (ACSC) has urged organisations and individuals across the Australian Public Service to check if their email addresses and/or passwords are included on recently released lists of stolen data.

Fisheries Queensland – January 2019

- Fisheries Qld blames bad update for password 'fault' – allowed fisherman to get into any account.

Types of Incidents

Cyber attack targets

- customer records and personal information
- financial records
- business plans
- new business ideas
- marketing plans
- intellectual properties
- product design
- patent applications
- employee records.

> Cyber security is about protecting your technology and information from accidental or illicit access, corruption, theft or damage.
>
> Cyber security is an ongoing journey in your business and needs to be part of your daily business processes.

Who and What Threats?

'Cyber criminals' (individual or group) that can threaten your technology or data could include:

- criminals - out for financial gain or information, to illegally access your hardware and data or disrupt your business
- clients you do business with – to compromise your information with malicious intent
- business competitors – looking to gain an advantage over your business
- current or former employees – who accidentally or intentionally compromise your information or data.

Information and data on your business, employees and customers. A number of ways are developed to exploit weaknesses in your business such as:

- theft or unauthorised access of hardware, computers and mobile devices
- infect computers with viruses and malware
- attack your technology or website
- attack third party systems
- spam you with emails containing viruses
- gain access to information through your employees.

Jargon

- Email phishing
  - Attempts to trick you by sending hoax emails, getting you to click on a dangerous link, or providing personal or financial information to an unauthorised source.
- Malware
  - Malicious or intrusive software, including viruses, worms, Trojans, ransomware, spyware and adware.
- Ransomware
  - Hijacking your files and locking you out of your system, then ransoming access back to you.
- Denial of Service
  - Using a network of computers to send requests to your system and overload it to make it unavailable.
- Watering Hole Attack
  - Setting up a fake (or compromised) website you are known to go to, then using it to infect visiting users.

Impacts

- Financial loss – from theft of money, information, disruption to business
- Business loss – damage to reputation, damage to other companies you rely on to do business
- Costs – getting your affected systems up and running
- Investment loss - time notifying the relevant authorities and institutions of the incident.

- Develop clear policies and procedures for your business and employees.
- Develop a cyber security incident response management plan to support your policies and procedures.
- Train new and existing staff on your cyber security policies and procedures and the steps to take if a cyber threat or cyber incident occurs.
- Keep your computers, website and Point-of-Sale (POS) systems up-to-date with all software release updates or patches.
- Back-up important data and information regularly to lessen the damage in case a breach occurs to your systems.

Mandatory Data Breach Disclosure

- https://www.oaic.gov.au

Which data breaches require notification

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

The NDB scheme only applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'.

Examples of a data breach include the following incidents:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

There are a few exceptions, which may mean notification is not required for certain eligible data breaches.

Enforcement powers of the Office of the Australian Information Commissioner

- The Privacy Act confers a range of enforcement powers on the Commissioner, including:
  - accept an enforceable undertaking (s 33E)
  - bring proceedings to enforce an enforceable undertaking (s 33F)
  - make a determination (s 52)
  - bring proceedings to enforce a determination (ss 55A and 62)
  - report to the Minister in certain circumstances following a CII, monitoring activity or assessment (ss 30 and 32)
  - seek an injunction including before, during or after an investigation or the exercise of another regulatory power (s 98)
  - apply to the court for a civil penalty order for a breach of a civil penalty provision (s 80W).
- The 'civil penalty provisions' in the Privacy Act include:
  - A serious or repeated interference with privacy (s 13G) – 2000 penalty units (current total is $420,000)
  - The maximum penalty that the court can order for a body corporate is five times the amount listed in the civil penalty provision (current maximum $2.1 million).

3 Key Steps

1. **Prevention – Protect your assets**

- Back-up regularly to protect against loss.
- Patch applications by installing security updates.
- Use complex passwords and use two-step authentication.
- Limit access to administrator accounts and sensitive information.

2. **Well-being – Do things safely**

- Communicate safe practice and talk about cyber security frequently.
- Browse safe sites and ensure your staff do too.
- Only allow applications you trust on your computers.

3. **Respond – Report and recover from an attack**

- If you think an attack has happened, tell staff and tell the authorities.
- Restore backups from before the incident.
- Consider cyber insurance.

Responsibilities

- Starts at the top
- Starts and finishes with people in management.
- Get everyone on board
  - You need to have support from everyone in the business.
  - From top to bottom.

- A hands-on effort
  - There is no single-fix for cyber security. You can't solely rely on antivirus software to keep you safe from attacks
- Know your risks and vulnerabilities
  - If you use the internet, you are at risk
- Protect your business
  - The right approach for you depends on your business, the people in it, and the information you need to protect

Basic Protections

- Install anti-virus software or check existing software is up to date on all employees' computers and laptops.

  It is one of the simplest ways to prevent employees downloading potentially harmful malware that could lead to a data breach.

  And ask your IT team to check firewall settings.

- Have clear policies in place to create a cyber-conscious culture in the workplace (everything from password rules and backing up work to use of WhatsApp groups and what data employees can keep on their computers).

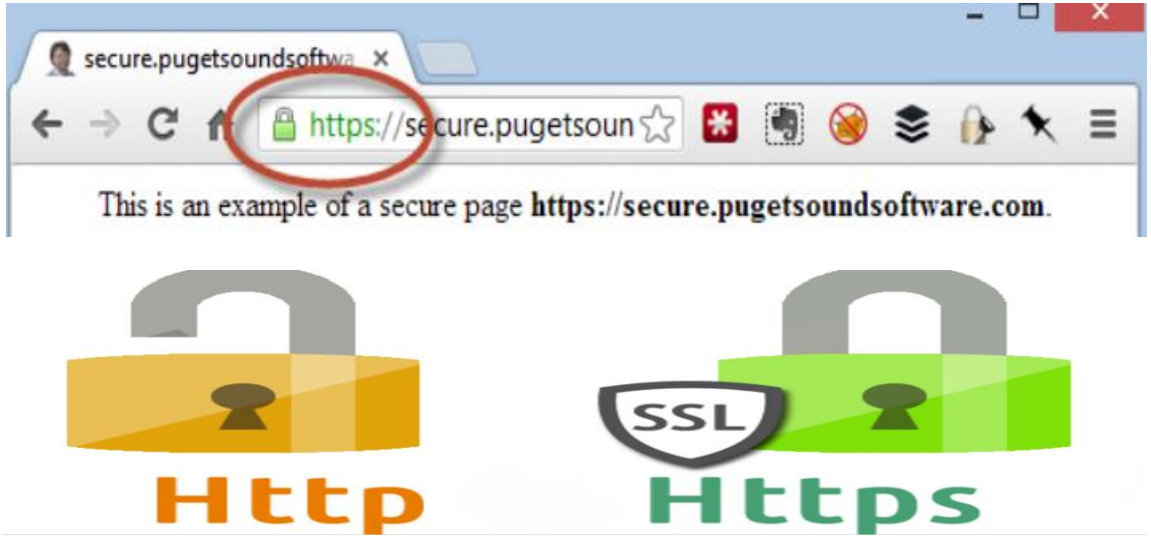
- Check what your PII or business insurance covers and consider buying cyber insurance.

  This can cover the cost of responding to a breach, as well as damages, and also give you access to specialist support ensuring the breach will be dealt with in line with the General Data Protection Requirements ('GDPR') / Mandatory Data Breach Requirements ('MDBR').

- Make sure any cyber insurance comes with a pre-approved panel of providers who are immediately available in the event of a breach.

HTTPS and HTTP

- HyperText Transfer Protocol (**HTTP**), uses HyperText Transfer Protocol Secure (**HTTPS**).
- Using **HTTPS**, the computers agree on a "code" **between** them, and then they scramble the messages using that "code" so that no one in **between** can read them. This keeps your information safe from hackers.



Hover

In the image above, you can see the mouse pointer is hovering over a link that appears as...
www.ups.com/delivery/verify-customer

However, the yellow-tinted pop-up underneath the mouse pointer indicates the actual destination URL is...
http://www.eicar.org/download/eicar.com

Appendix 1 - Types of Cyber Attacks

Denial of Service (DoS) Attack

- This type of attack send enough information and data all at once from multiple computers to overload your system so it shuts down. These are common and one of the best ways to prevent against this kind of malicious cyber traffic jam is using analytics to monitor unusual spikes in traffic flow. Regular security software updates are another routine way of preventing these types of issues.

Malware

- That's one word that should set of off alarms bells whether you're running an eCommerce store or a brick and mortar shop with an online presence. Malware is the catchphrase for any of the malicious software that lurks in the weeds of cyberspace looking to gain access to your system to cause some kind of damage. The phrase covers a large swath of worms, viruses, Trojan Horses and other pests like Ransomware. Antivirus software creates a good moat around your business, and you should always be wary of opening emails from people you don't know.
- Watch for pop ups promising needed updates that are really masking rogue software. Updating your firewall is a good move too.

Password Attacks

- Unfortunately, there are some very good reasons why internet security experts tell you to make sure your small business passwords don't use common words and phrases or easy to remember terms like a variation on the name of your company.
- Cyber criminals can unlock the door to your sensitive data using just one password as the key. It's such a common scenario, the pundits have even divided these types of attacks into three subcategories:

Ransomware

- Hijacking your files and locking you out of your system, then ransoming access back to you.

The Brute Force Attack

- Imagine an old school safe cracker here. Instead of a stethoscope to listen for the clicks telling them they've found the right combinations, these modern day criminals use a program to try different sets of common words. If a hacker has a list of employee names, they'll get to work with easiest-to-guess passwords based on first and last names and pet names.
- Changing passwords frequently can throw any hackers off your trail. Stay away from simple keyboard progressions like qwerty and away from slang terms and common misspellings. Once again comprehensive security software works wonders for your small business.

The Dictionary Attack

- Pretty much the same as the brute force version with a more narrowed focus. This attack gets it's name from the fact that many people tend to choose passwords that are seven characters or fewer — the kind that can be found in the dictionary.
- Where you login plays an important role. Unsecured WiFi connections are public and more open to being hacked.

Key Logger Attack

- Imagine someone being able to use a program capable of tracking every keystroke you make? Hackers have access to programs capable of this, programs capable of putting your passwords and sign in IDs in their hands. If you've ever logged onto a computer or into a portal using a username and password, you could be vulnerable.
- Fight back using multifactor authentication. Here, you'll outfit everyone with a password and some other form of authentication that slows hackers down. Quite often an access code is used as an added form of protection.