The Risk of Data Breaches.

Cybercrime is a growing phenomenon worldwide, costing hundreds of billions of dollars globally and affecting organisations of all sizes, across all industries. In Australia, new data breach laws are raising the stakes for any company holding personal information about their customers.



The HP Elite range of desktops, tablets, laptops and printers are engineered with effective, easy to use bios-level security features designed to beat the growing cybersecurity threats companies face. Features include:

HP SURE CLICK

Provides hardware-enforced security for web browsers, protecting your PC from websites infected with malware, ransomware or viruses.

HP SURE START

Monitors in-memory BIOS, recovers the platform without intervention, restores the BIOS to a custom state, and is enterprise ready for centralized management.

HP SUREVIEW

Protects mobile workers from visual hacking using screens engineered with 'privacy mode' reducing up to 95 percent of visible light when viewed at an angle.

HP SECURE PRINTERS

Protects mobile workers from visual hacking using screens engineered with 'privacy mode' reducing up to 95 percent of visible light when viewed at an angle.

Threat matrix: What are the data threats?

1.1 Cybercrime: The Global threat and its cost

Today, cybercrime poses the greatest single threat to business, in recorded history. That's a big call to make: and the numbers back it up. A 2017 Cybersecurity Ventures report projects that the annual cost of cybercrime globally will reach USD $6 trillion by 2021.

Already, cybercrime costs the world 0.8% of global GDP – almost USD $600 billion – according to a February 2018 report, The Economic Impact Of Cybercrime, by the Washington DC-based Center for Strategic and International Studies (CSIS), which also estimates that the cost of cybercrime has grown by 20 percent since 2014 – and that the rate of increase is accelerating.

$USD 6 trillion
cybercrime cost

> "Cybercrime is relentless, undiminished and unlikely to stop."
>
> *- Center for Strategic and International Studies (CSIS), 2018*



1.2 Why is cybercrime increasing?

There are a number of reasons for the growth in cybercrime. These include:



- Rapid adoption of new technologies by cybercriminals
- Rising numbers of new internet users from low-income countries with weak cybersecurity.
- The Cybercrime-As-A-Service phenomenon - where a small number of highly skilled perpetrators build and sell attack tools and core infrastructure to millions of unskilled cybercriminals, making cybercrime much easier to commit.
- A growth in cybercrime hot-spots, which now include Brazil, China, Ghana, India, Nigeria, North Korea, Russia, the USA and Vietnam.
- Rise of digital black markets and financial sophistication of top-tier cybercriminals

1.3 How new ways of working can raise the cybersecurity threat

We know that the way we work has changed: it is mobile, it is digitally collaborative and it is increasingly reliant on cloud-based systems. This is occurring at a time when cybercrime has become highly lucrative, with malicious software easy and cheap to access and cybercrime becoming more lucrative and highly organised.



Cyber attacks are increasingly targeting these new modes of work, using phishing, malware and visual hacking to perpetrate attacks such as Business Email Compromise and data theft.



80 billion
malicious scans per day

1.4 What happens to stolen data?

Stolen data such as credit card numbers and personally identifiable information (PII) is often traded between criminals on the Dark Net - a virtual black market which has aallowed cybercrime to proliferate in recent years, facilitated by untraceable, borderless and mobile digital currencies like Bitcoin. Ransomware payments are also booming thanks to Bitcoin, while scammers, hackers and other financial thieves will route money through a series of bank transfers disguising the end destination: a criminal's personal bank account. Stolen intellectual property is often sold to unscrupulous businesses across the globe.

Stolen data now fuels a multi-billion dollar criminal industry – and the increased ease of monetising these crimes has ramped up the overall threat level because it makes stealing less risky and more well paid. That has also lowered the barriers to commit crime - and boosted the scale of cybercrime.



The incidence of malicious internet activity is astonishing, with The Center for Strategic and International Studies (CSIS) reporting that one major internet service provider (ISP) sees 80 billion malicious scans a day, thanks to cybercrime 'bots' seeking vulnerable targets. Researchers estimate that the amount of new malware released, ranges from 300,000 to a million viruses and other malicious software products created every day. According to the Anti-Phishing Working Group, phishing remains the most popular and easiest way to commit cybercrime, and the incidence of unique phishing email campaigns is continually rising, currently recorded at around 100,000 unique campaigns each month.

2. Data breaches worldwide – and the cost

2.1 'Best Case' data breach: Australian Red Cross Blood Service

The Red Cross blood donor service was lucky to escape serious repercussions from a 2016 data breach when a file containing details of over half a million prospective blood donors was inadvertently saved to a public-facing web server by a contractor. Fortunately the breach was discovered almost immediately and the Blood Service closed the website and notified people who may have been affected. An investigation by the Australian Information Commissioner took almost six months and found that, while most information security measures were in place, third party contractor arrangements and length of data retention were inadequate. An enforceable undertaking to improve arrangements was agreed in July 2017. The costs were limited to reputational damage and the extensive labour involved in preparing for, and responding to, the investigation.

2.2. 'Worst Case' data breach: Ashley Madison

In 2015, online extra-marital dating site Ashley Madison experienced a severe cybersecurity breach and over 300 GB of data was stolen, including users' personal details, financial information including credit card numbers and transactions and intimate information. Hackers threatened to release the information publicly unless the company closed the website, but when the company refused to close its website and reported the hack to police, the hackers released users' personal information on the Dark Web, along with over 12 GB of corporate emails including those of the company's CEO. Some users later received threats to publish their details unless they agreed to pay a Bitcoin ransom for their data.

According to Panda Security CEO Diego Navarrete: "Ashley Madison went from being a sleazy site of questionable taste to becoming the perfect example of security management malpractice."

Early estimates suggested the breach could cost up to US$200 million. While the consequences for the company are ongoing, various penalties and legal suits have ensued including

- A class action citing over 37 million users, settled by the site's Toronto-based parent company Avid Life Media in 2017 for US $11.2 million
- $1.66 million fine by US Federal Trade Commission for lax security and deceptive practices

300 GB
stolen data



2.3 Cost of Data Breaches worldwide

The 2017 Internet Organised Crime Threat Assessment (IOCTA) produced by Europol, outlines the growing problem of Business Email compromise (BEC). This usually involves mimicking or hacking a senior executive's email, and directing an employee to make payments to accounts under the control of the cybercriminal. BECs can occur via malware, such as key loggers, but more likely occur using phishing. BEC was the most commonly reported fraud in the EU in 2016, and victims are `usually small to medium sized businesses.

In August 2016, a BEC scam reportedly cost German company Leoni AG US $80 million, and known BEC frauds have cost companies over US $5 billion since 2013.



2.4 Cost of Data Breaches in Australia

HP Australia's Nov '17 Security Study found:

- 57% of SMBs had done no IT Security Risk Assessment in past year
- 49% of SMBs were not prepared for mandatory data breach disclosure laws

Top consequences SMBs expect from data breach:

- 67% - Disruption to business operations
- 48% - Financial costs
- 44% - Potential loss of IP
- 40% - Legal or compliance issues

2.5 Europe and US: Data breach growth - and successful actions

The 2017 Internet Organised Crime Threat Assessment (IOCTA) produced by Europol, shows that social engineering (CEO Fraud), malware, and attacks on critical infrastructure are rising exponentially. There seems to be a regional flavour to some attacks, with France and Norway each reporting over 2 per cent per cent of global BEC attacks. Around 16 per cent of global ransomware detections come from Germany, Italy, the Netherlands, and the UK, with banking malware rates highest in Germany and Russia.

However, in the UK, the government's National Cyber Security Centre, a branch of the UK Security Agency GCHQ, recently introduced an Active Cyber Defence program which has reduced the UK's share of global phishing attacks from 5.3 per cent to 3.1 per cent.

3. Australia's new data breach laws

3.1 New laws

Australia's Notifiable Data Breach scheme began operating from 22 Feb 2018. The scheme is administered by the Office of the Australian Information Commissioner (OAIC) and applies to any organisations with an annual turnover of $3 million or more, plus any sized credit reporting bodies, health service providers, and TFN recipients.

Organisations must notify people whose data was breached, plus file notification with the OAIC, if they discover any unauthorised access, disclosure or loss of data involving personal information that is "likely to result in serious harm to any individual affected." Examples include information about a person's health or finances or which could be used for identity fraud. Companies have just 30 days to determine whether a breach might have caused serious harm, before they notify individuals and the OAIC.

3.2 Data breach examples

In the first month following the implementation of Australia's data breach laws, 31 cases were reported to the OAIC. These included a data breach by shipping company Svitzer that affected the emails of half its Australian employees.

Data Breach reports in Australia have started high and will continue to climb, according to HP security expert Mohammed Khan. "This trend will increase because companies are not prepared for the level of cybercrime activity that is the new normal," says Khan, who is a Business Process Consultant at Hewlett Packard Australia.

The OAIC will release quarterly statistical information on the data breach notifications it receives.

3.3 Potential costs

Reputational cost, stolen data and potential redress to customers are among the costs that data breaches could now incur. The Ponemon Institute reports that the average cost of a data breach in Australia in 2017 is $2.5 million, with an average cost of $139 per lost or stolen record.

$AUD 2.5 million
average cost per breach

3.4 Expectations

The bar has been raised for companies in Australia that collect any information about their customers. Australian law now includes thirteen provisions under The Privacy Act regulating how organisations handle personal information and how they protect that information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. There's now requirements to destroy or de-identify information as soon as it is not used for approved purposes. Organisations in financial services or health sectors are subject to other laws about personal information security.

Companies can no longer afford to be complacent about information security as investigations and public expectations demand a comprehensive approach to data protection. Listed companies have the added pressure of shareholder expectations, when the costs of data breaches are so well known and potentially so high.

4. Solutions

4.1 Policy and procedures

Tap into the extensive resources from OAIC and other government bodies which include privacy protection procedure documents, templates for the information you supply to customers at the time you collect their data and formal processes to secure and maintain or destroy personal data. Make life easier for yourself by streamlining your processes with technology. Protect your corporate reputation - and reduce potential penalties or legal actions, by listing the processes that your company has in place to deal with data and secure against breaches.







4.2 Biometric Protection

Ensure data protection across your company's devices by implementing biometric identity protection against unauthorised access – such as fingerprint, facial or iris identification. Biometric access is easy to use, which makes it far more likely that users will comply; and it's also difficult to circumvent, adding another layer of complexity against cyber attacks. HP's Elite range of technology provides secure biometric protection across the platform.

4.3 Phishing protection

Protect against malware and phishing scams by instituting and enforcing anti-virus software and constant signature downloads. Use hardware to close the gaps that software always leaves. Today's most malevolent and destructive attackers use BIOS-level code, which once opened, infects the computer's Basic Input/ Output Operating System – a critical system component which loads before the operating system and before user authentication is required. The only protection against this level of attack is BIOS-level security which detects any change to the BIOS and restores it to default before an attack can proceed – HP's SureStart technology will get rid of malware before extensive damage can be done.

BIOS-level
security



4.4 Implementing data protection policies company wide

Millions of devices can potentially access your network. Your WiFi network should require the highest encryption protocol, your web servers hold sturdy firewalls that are constantly updated.

Cybercrime statistics worldwide show that humans are the weakest link on any network. Using HP Technology can reduce the risks; adding education and awareness raising can ensure that your company has the best levels of protection in place.

The IT security at your workplace may be at an all-time high – but mix it up with today's digital threats and things may get a whole lot murkier. The 2018 HP Australia Security Study found that less than half of Australian SMEs have conducted an IT risk assessment in the last year. If you haven't acted on your data protection strategy: do it now, before it's too late.