platinum
TECHNOLOGY

We live in a data driven economy. Regardless of industry type or organisation size, your data is your most critical asset which must be protected.

Data is your business

We live in a data driven economy. Regardless of industry type or organisation size, your data is your most critical asset which must be protected. With the global pandemic accelerating digital transformation, and of course work from home becoming the new normal, the increase in volume and value of data has created an unprecedented opportunity for cyber criminals.

While many of us have spent the last 18 months reimagining the way we live and work, cyber criminals have used this as an opportunity to hone in on our vulnerabilities. They're exploiting distributed networks and taking advantage of the rapid IT changes businesses had to implement almost overnight. They're also targeting vulnerable people, SMB businesses, government, and health services to conduct espionage, as well as steal money and sensitive data.

The picture we're painting might sound like something out of an episode of the television series Get Smart but unfortunately, it's a stark reality of the times. Research from the Australian Cyber Security Centre reinforces this; in the 12 months to June 30, 2021, they received more than 67,000 reports of cybercrime incidents essentially equating to one every 8 minutes. [1]

The top five industry sectors to report data breaches were health service providers, finance (including superannuation), legal, account and management services firms, government, and insurance firms.[2] Self-reported losses from attacks in Australia were estimated at $33 billion.[3]

What is a data breach?

A data breach occurs when confidential, private, or other sensitive information is accessed without authorisation or is lost. A data breach can occur accidentally, or because of a deliberate attack.

What is a cyber-attack?

A cyber-attack is any attempt to gain unauthorized access to a computer or computer network with the intent to cause damage. An attack can be launched from anywhere by an individual or an organised crime syndicate with the aim to disable, disrupt, destroy, or control computer systems.

The most common form of attack in Australia is ransomware – where the attacker will encrypt important data or information and then ask the owner of the data for money to release it back.

Financial gain is the prime motivation followed by social or political sabotage.

---

[1] ACSC Annual Cyber Threat Report 2020–21

[2] Office of the Australian Information Commissioner's Notifiable Data Breaches Report: Jan – June 2021

[3] Cyber Threat Report 2020–21

Local examples

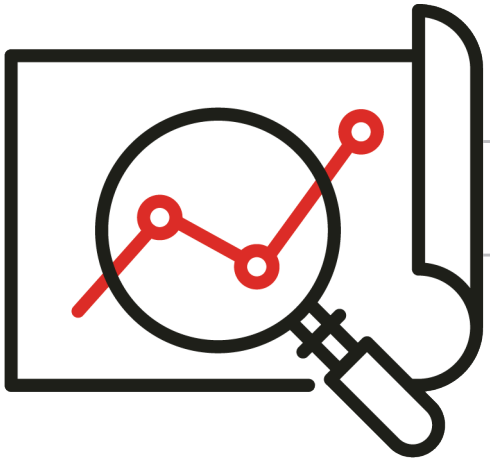
In December 2020, it was determined a national Australian travel retailer had disclosed personal information of almost 7,000 customers to third parties without consent. Data including credit card and passport information was leaked due to human error - three years earlier. In addition to the reputational damage, the retailer paid $68,500 to lessen the affect on customers impacted and was subject to a government enquiry.

In May 2021, a ransomware group claimed access to tens of thousands of records from a mid-sized Australian telecommunications provider. The criminals implored the company to communicate and co-operate before 'valuable company documents' would be leaked. The hackers posted a disturbing ransom note, a ticking timer, took down the company's website and gave them 240 hours to respond to their extortion attempt.

Raising visibility on the importance of a cyber resiliency plan

With the increase in frequency and seriousness of attacks, mid-sized businesses can no longer ignore the statistics. It's common practice to have risk management plans in place as well as insurance to cover organisations in the event of a workplace fire, theft, flood, or damage to property and now more than ever is the time to make sure you also have a data protection and business continuance strategy in the event of a cyber-attack.

In the past discussions about data protection, business continuity or cyber resiliency were a conversation limited to the IT department. However, with the outcome of a breach shifting in severity over the last few years (from theft to data ransom and destruction) cyber resiliency must be a senior management or board level discussion. Organisations that don't have a vigorous and effective response plan are not taking their risk management or governance duties seriously otherwise.



Tackling risk head-on: Mitigation strategies for counteracting threats

The threat landscape is constantly evolving. Unfortunately, it's not a matter of "if" an organisation will be targeted by cyber criminals but "when" and how severe the impact will be to the business.

The key is to be proactive and based on experience here are our top five mitigation strategies:

1. Conduct a Risk Assessment to determine vulnerabilities

A risk assessment will offer insight into the assets that need to be protected and the security controls currently in place. In addition, conducting an assessment will help your IT department identify areas of vulnerability that could be exploited, and subsequently prioritize which steps should be taken first to address concerns.

2. Governance

Create a cross-functional team who will be responsible for assessing, developing, and implementing your resiliency plan. The stakes are high and as a result we recommend the plan is overseen by senior management and includes members of the IT Department, HR and even Marketing.

3. Best Practice System Configuration and Hygiene

Establish a systematic process for managing standard system hygiene and most importantly ensure your applications are configured in line with best practice.

A recent report from CoreView revealed:

- Approximately 80% of data breaches involve privileged credentials - so setting appropriate admin controls should be IT's first job when giving access to employees.
- 97% of Microsoft 365 users do not use multi-factor authentication. This is unfortunate given research from SANS Software Security Institute indicates that 99% of data breaches can be prevented using multi-factor authentication.[4]

4. Backup data and ensure Anti-Virus Software is up to date

A data breach can negatively affect your businesses profitability and competitiveness which is why having a data backup solution is critical to recovery.

For best results, backup copies are made on a consistent, regular basis to minimize the amount of data lost between backups. It's also important to test backup services regularly for any issues which might prevent you from accessing your data during critical times.

It's equally important to make sure your anti-virus software is up-to-date, and we recommend automating updates to ensure your defense is always on.

5. Build an Incident Response Plan

Data breaches or attacks are not just IT problems – they are business problems. The sooner they can be mitigated the less damage they can cause which is why it's important to have an incident response plan in place to ensure everyone (from the IT department through to non-technical employees) know what they're responsible for in the event of a data breach or attack.

---

[4] CoreView: Microsoft 365 App Security Governance Shadow IT Report

Take the next step with Platinum

IT security is a necessity for business. There is no room for complacency, poor practices or technology products which might compromise your IT infrastructure. A set and forget strategy will not work and neither will burying your head in the sand.

We're committed to helping our customers manage the security posture of their organisation and can help you wherever you are on your IT journey. We have over 10 years' experience servicing Australian and International organisations. We also have broad industry knowledge, deep expertise, and the commitment you need to get results.

Where to next?

Contact Platinum Technology for a no obligation consultation to see if this is the right choice for the future of your business.

Joseph Girgis
Director – Sales and Operations
Platinum Technology
www.platinumtechnology.com.au

Mobile: 0447 498 560
Australia: 1300 544 815
Vietnam: +84 284 458 1717
Singapore: +65 31 38 3770
New Zealand: +64 4928 3030

Platinum Cyber Security Assessment

Contact us to book your free Cyber Security Assessment.

We will perform an assessment based on the NIST and CIS standards across OnPrem endpoints, Active Directory and Office 365.

Organisations are looking for a way to check their security status quickly and simply. They want insight into their vulnerabilities, based on data from the company infrastructure and Office 365.

This is the basis on which we can provide recommendations and an action plan to improve your security. It's the perfect way to maximize security and demonstrate that your organisation takes security seriously.

platinum TECHNOLOGY