BYTE

A complete guide to protecting your business from cyber security threats.

A cyber security whitepaper

Prepared by Byte
www.byte.com.au

Contents.

Introduction.

Cyber attacks are on the rise among Australian organisations. The average cost of a cybercrime attack is around $276,000[1], in addition to reputation damage which has a significant impact on the bottom line and future viability of the business.

With COVID-19 pandemic forcing many organisations and its employees to operate from home, security issues have never been a more important reputation risk to address. Data from various sources[2] indicate an increase in the number of security breaches during the first half of 2020 as more people work from home.

Phishing is the most prolific method of cyberattack that results in compromised credentials. Such attacks pose significant threats to an organisation as they typically include unauthorised access to customer data including personal information, sensitive information and user credentials.

The human factor is also a vulnerable link in data security. Whether through human error, such as sending personal information to an unauthorised recipient, a general lack of security awareness, or where a cyber breach is traced back to a human compromise, employees are centrally involved in most data breaches. It is therefore important that organisations put individuals first in designing a comprehensive security solution.

[1] Australian Cybercrime Online Reporting Network (ACORN)
[2] Office of the Australian Information Commissioner, Australian Cyber Security Centre, Security In Depth, ACCC

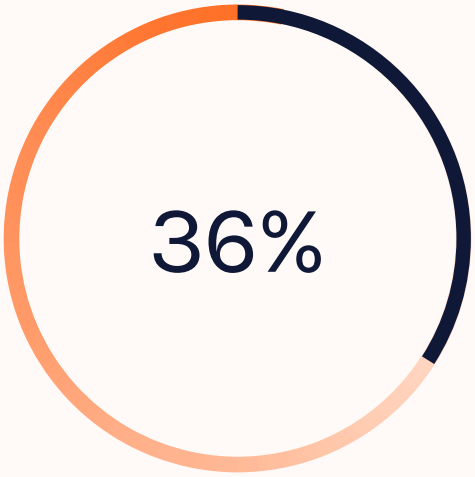
Security threats impacting Australian business right now.

1. Phishing
2. Compromised credentials
3. Ransomware
4. Malware
5. Lack of cyber security culture

1 Phishing

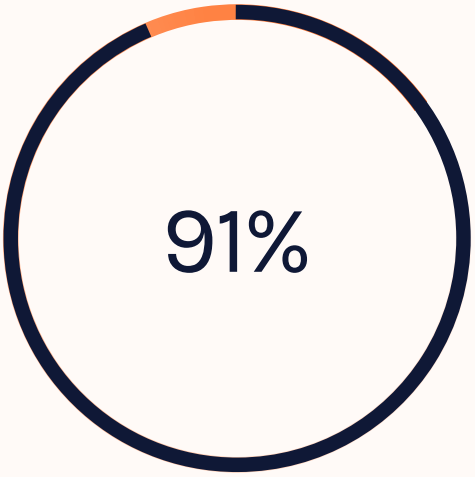
Phishing or "spear phishing", a more targeted attack directed at an individual or company, is the most prolific and highly effective method used by malicious actors to steal sensitive information. It can be in the form of a text message or email from someone that masquerades as a reputable source or as a legitimate institution that lures an individual into providing personal information, sensitive data or login credentials.

According to research by Security in Depth, 91% of cyber attacks begin with a phishing email. Employees are often unaware of the methods to identify a fake email and accidentally click on embedded links or respond to the email's call-to-action.



of compromised credentials between January to June 2020 were a result of phishing

Notifiable Data Breaches Report, January - June 2020, Office of the Australian Information Commissioner



of cyber attacks start with a phishing email

(Security In Depth, Sept. 2020)

Mitigation Practices

Phishing

- Prevent phishing emails from reaching users with effective anti-phishing software that can handle zero-day vulnerabilities.
- Educate staff on how to identify fraudulent emails and set policies and guidance on how to handle suspect communications.
- Watch out for suspect grammar and spelling, sender address, attachments, shortened links, login pages, urgent deadlines, alarming content full of warnings and consequences for not taking action.
- Avoid using public networks.

SECURITY SOLUTION

Microsoft 365 prevents phishing attacks with built-in machine learning models and impersonation detection that quickly identify and block suspicious activity on email.

2 Compromised or stolen credentials

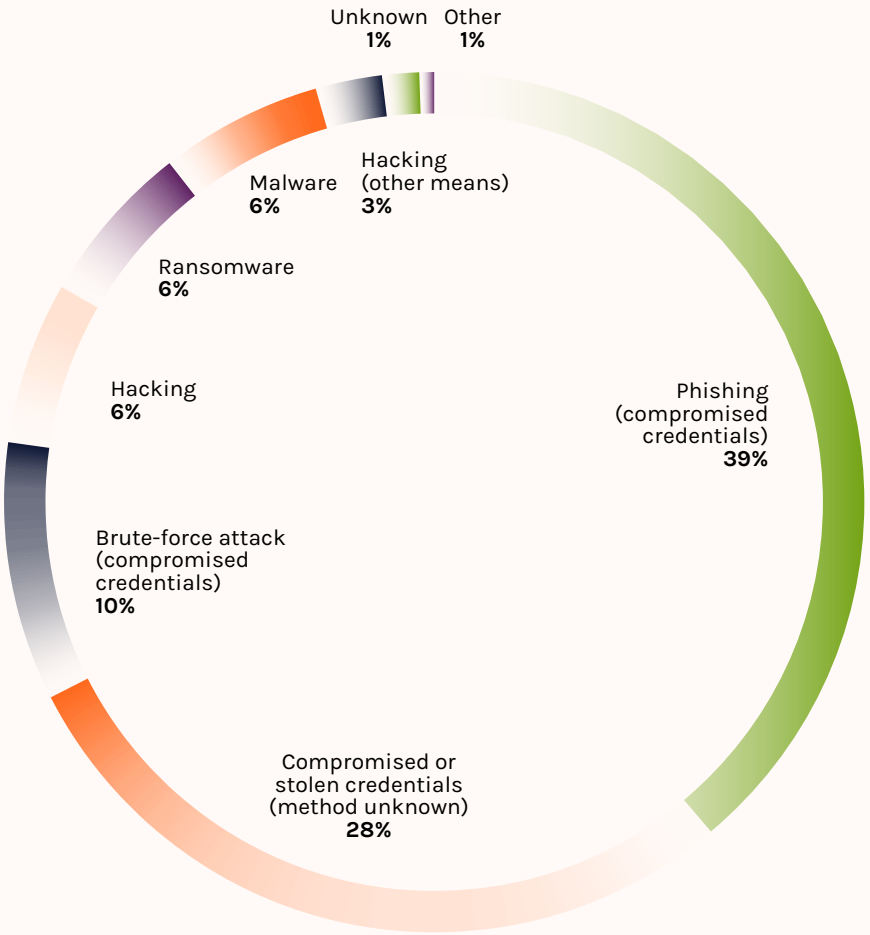
Credential compromise typically starts with a phishing email that tricks a person into giving up their login details. A common example is a phising email that, at a quick glance, looks like a legitimate password reset requests from Gmail or Outlook. When the user enters their login details into the fraudulent site, they are handing over their username and password to cyber attackers, providing access to their email account.

Outside of phishing, compromised credentials via an unknown method is the second most prevalent cyber incident that can be attributed to data breaches that have been reported to the Office of the Australian Information Commissioner (OAIC) during the second half of 2019 and the first half of 2020.

> The **#2 most prevalent cyber incident** is credential compromise from unknown means
>
> (OAIC)

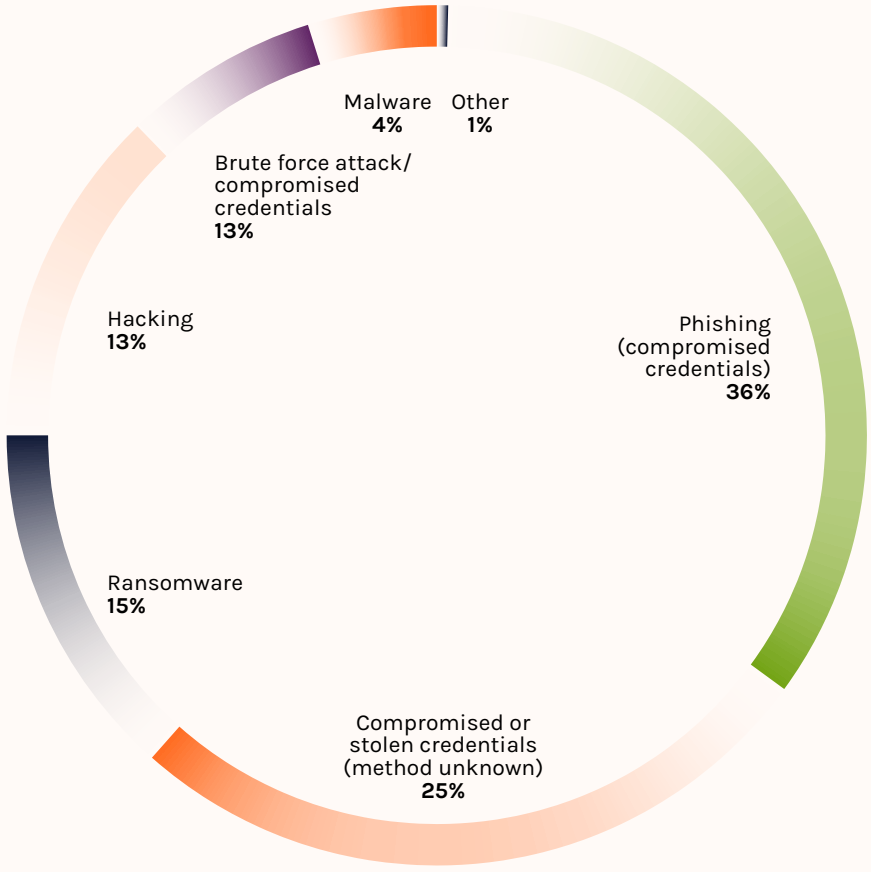
This is the result of 'credential stuffing' attacks whereby attackers use login credentials obtained from breached user credentials that have been leaked or posted online.

The primary reason credential stuffing is so effective is because most people re-use the same username and password for multiple services.



Cyber Incident Breakdown (2019)

Notifiable Data Breaches Report, June - December 2019, Office of the Australian Information Commissioner



Cyber Incident Breakdown (2020)

Notifiable Data Breaches Report, January - June 2020, Office of the Australian Information Commissioner

Mitigation Practices

Compromised or stolen credentials

- Use unique passwords for each account or service.
- Password managers such as Lastpass or Dashlane are useful in managing secure access to multiple accounts.
- Enable two-factor or multi-factor authentication.
- Education programs to increase security awareness of employees.

SECURITY SOLUTION

Multi-factor authentication along with Windows Defender makes it difficult for hackers to access information. It is a simple but important step to securing your company data and devices.

3 Ransomware

From January to June 2020, the OAIC reported more than 150% increase in data breaches (from 13 to 33) attributed to ransomware attacks compared to the previous six months. There are many forms of ransomware attacks, but one of the most common forms is where a malicious individual encrypts a user's important files and then demands something from the user, such as money or information, in exchange for the key to decrypt them. Some of these attacks result in the exfiltration and release of information by the attacker.

Ransomware attacks are on the rise, particularly those that encrypt files that are stored in the user's cloud storage. It can be installed on a system through a malicious email attachment, a fraudulent software download or by visiting a malicious webpage. When a company is attacked by ransomware, they lose access to their own system making it difficult to understand the extent of the data breach.

Data breaches from ransomware attacks **increased by 150%** in January to June 2020 compared to the previous period.

Office of the Australian Information Commissioner, Notifiable Data Breaches Report: January - June 2020

Mitigation Practices

Ransomware

- Keep your software and operating system updated.
- Backup your data.
- Only download from sites you trust.
- Do not open untrusted email attachments.
- Use VPN when accessing public wifi.
- Don’t use unfamiliar USBs and external hard drives.
- Get ransomware detection and recovery with Microsoft 365 advanced protection.

SECURITY SOLUTION

A business needs a comprehensive solution that includes security awareness and training for employees, a data backup and recovery plan and a security solution such as Microsoft 365 with advanced security and device management to safeguard the business. It is built to protect company data at scale, secure every device that connects to work emails and files, and detects and defends against cyberthreats.

4 Malware

Malware consists of viruses, spyware and other malicious software that is designed to disrupt, damage or gain unauthorised access to sensitive data. In July to December 2019, this accounted for 10% of cyber incident data breaches reported to the OAIC. With the blurring lines between personal and work systems, and work from home arrangements since March 2020 which is predicted to remain permanent for many, business face greater risks of malware infection from home networks. However, prevention can be as simple as having security software in place.

Mitigation Practices

Malware

- Ensure all security updates and patches are installed.

SECURITY SOLUTION

Windows 10 and Microsoft 365 includes protection mechanisms to detect and prevent computer viruses, malware, rootkits, worms, and other malicious software from being introduced.

5 Lack of cyber security culture

The employee is arguably the most vulnerable part of a cybersecurity setting in the business. Studies have shown that employees often lack security awareness training which increases a company's exposure to data breaches and security issues that result in reputation loss. There is an urgent need for business and IT leaders to invest in training and awareness programs, combined with the implementation of a comprehensive security solution.

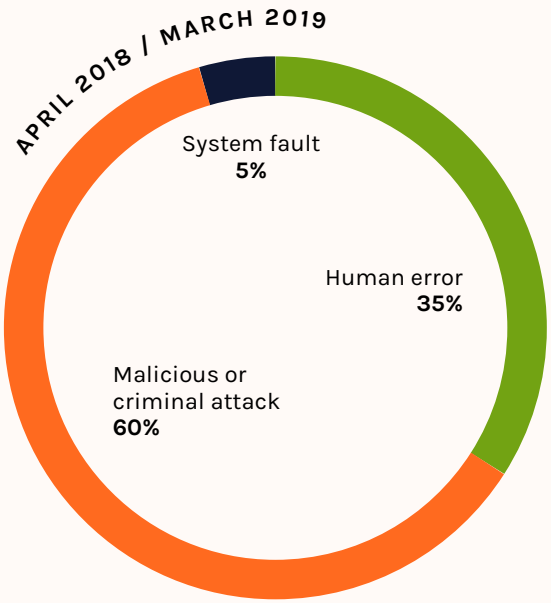
A security awareness and training program should address common security issues:

- Using weak passwords or the same passwords across multiple apps or services.
- Leaving their work devices unattended whether at work or at home or lending them to family members.
- Using the same password for business and personal accounts.
- Using malicious USBs, external drives and external devices.
- Accessing public wi-fi.
- Spotting fake emails.
- Sending sensitive information via email.
- Disclosing login credentials or other sensitive data.

Poor practices in password management often leaves an organisation open to malicious attacks. They are easily by-passed by Brute Force Attack - a method of decoding sensitive data using trial-and-error at scale. Typically done using scripts or bots to crack passwords and encryption keys, it generates a large number of consecutive guesses until the correct combination is found.

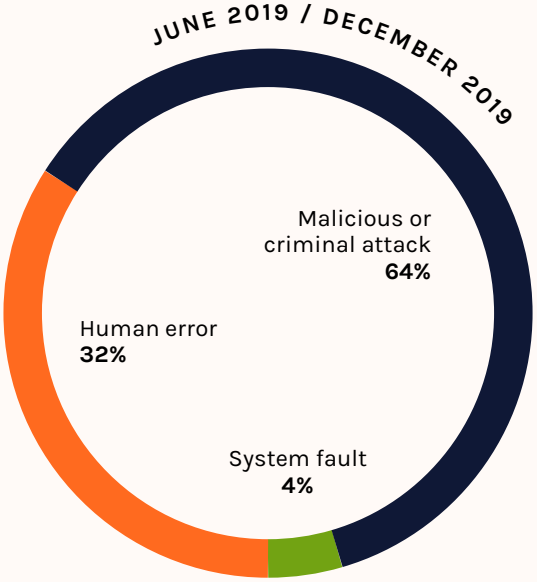
Human error and insider threats.

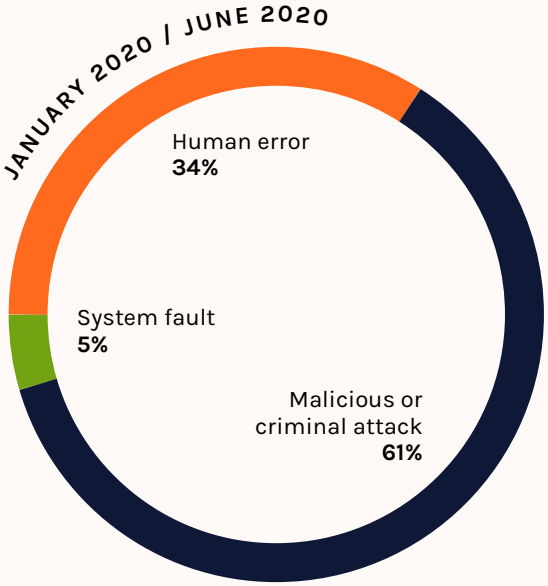
The OAIC reports point to human factor as a vulnerable link in data security, which is consistently the second highest source of data breach. Whether through direct human errors, such as sending personal information to an unauthorised recipient, or where cyber breaches were traced back to a human compromise, employees are centrally involved in most of the data breaches reported to the OAIC. It is important that organisations put individuals first.



Employees are involved in most data breaches, including many cyber attacks that exploit human factor vulnerabilities.

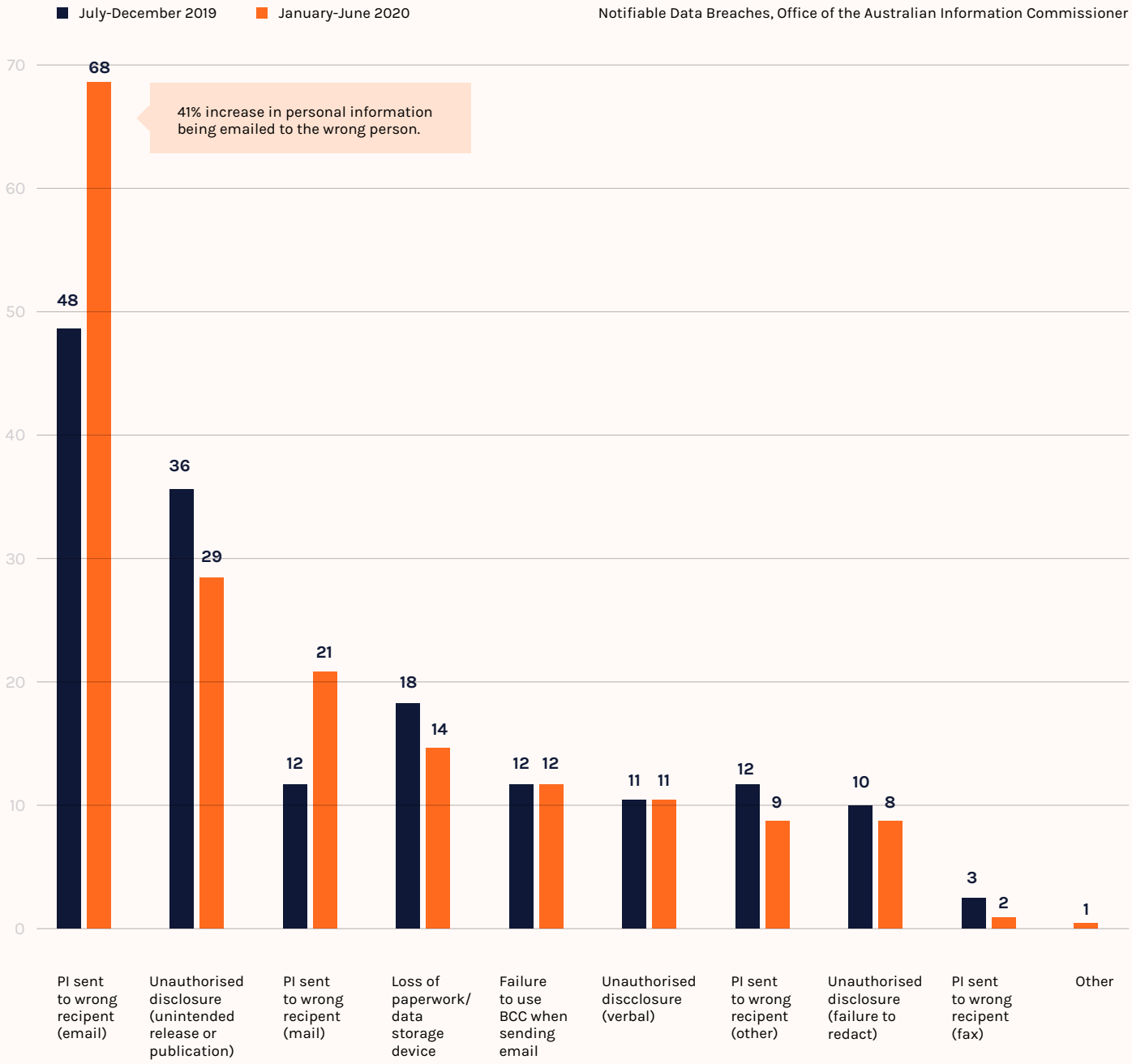
Notifiable Data Breaches, Office of the Australian Information Commissioner





The first half of 2020 saw a sharp rise (around 41%) in personal information being sent to the wrong recipients via email, compared to the previous period. Interestingly, this coincides with the Australian workforce shifting to work from home. A survey by Security In Depth of approximately 1500 businesses indicate that this may be explained by an increase from 9% to 20% of employees using their personal email accounts for business.

Human Error Breakdown



Many cyber incidents exploit vulnerabilities involving a human factor as they often require a person to do something that results in a security or data breach.

- Phishing emails require tricking a person to click on a link or disclose passwords
- The use of weak passwords or reuse of the same password across multiple services and accounts
- The general complacency and lack of security awareness which leads to poor security practices at work and at home

KEY TAKEAWAYS FOR YOUR TEAM:

Work from home security best practice.

With work from home arrangements becoming more common in organisations, it's important to establish best practice security guidelines across the business.

1. Restrict administrative privileges for remote access.

2. Use unique passwords for every account or service to limit the reach that a compromised credential has in your business.

3. Use multi-factor authentication (MFA).

4. Use VPN for secure web browsing and remote network access.

5. Update your software and operating systems to combat the latest cybersecurity threats.

6. Avoid public wifi as it increases exposure to cyber threats.

A simple security solution to growing cyber threats.

Protect your intellectual property and customer data with the advanced security features of **Office 365** and **Microsoft 365**.

- Begin with protecting your identities as they are the keys to your environment.
- Protect yourself against sophisticated threats such as phishing and zero-day malware and automatically investigate and remediate attacks.
- Meet compliance requirements with comprehensive information protection backed by cloud based machine learning.

1 Protect

What if you could protect your company's data?

Ensure that no one can share your personal and financial information outside your business. SMBs are turning to Microsoft 365 to protect their business data because of the scale of Microsoft security, with over 470 B emails analyzed per month and 3,500 security professionals protecting customers.

2 Secure

Would you like to secure every device that connects to work emails and files?

Effectively control which devices and users have access to your business information at any given time. With the emergence of new regulatory requirements for different industries and states, SMBs are considering Microsoft 365 because of the higher security functionality.

3 Defend

How would you like to defend your business from threats?

Take advantage of always-up-to-date security that automatically detects and defends against cyberthreats. Every day, Microsoft analyzes 6.5 trillion signals—the largest threat-related optics. Anytime a new threat is detected anywhere in the world, Microsoft updates its network to ensure our security software can protect your company from both old and new forms of malware.

Prevent costly cyberattacks from happening:

- **Detect threats early** with Advanced Threat Protection (ATP) Safe Links and Safe Attachments that automatically scan and analyze email links or attachments.
- **Prevent phishing attacks** with built-in machine learning models and impersonation detection that quickly identify suspicious activity on email.
- **Protect company devices** with multifactor authentication and Windows Defender to make it difficult for hackers to access information.

Give your organization greater data protection:

- **Protect sensitive data** from leaks with built-in Data Loss Prevention that can automatically detect when an email includes sensitive information.
- **Encrypt sensitive emails** with one click to ensure that only the right individuals can access information.
- **Control who has access to files** with Information Protection that lets you apply restrictions to emails and to prevent data from ending up in the wrong hands.

Secure every device that connects to your business data:

- **Control who has access to your data** with Conditional Access to decide which devices can connect to business applications.
- **Apply security policies** like PINs or fingerprints to protect business data in iOS and Android devices. If a device goes missing, remotely wipe business information.
- **Manage business apps** with mobile application management that lets you determine who has access to business apps on personal devices.

Byte's people first approach to data security.

We consider ourselves a people business first, technology second. We know technology – it is our expertise, however our focus is on the user experience: how technology impacts the end user and how it can help transform a business.

Over the past two decades we have specialised in the financial services, professional services and accounting sector. We have the depth of expertise to solve their specific challenges with an understanding of the legal, regulatory and compliance frameworks within which to operate. Our process is based on Microsoft best practice and utilizes the methodology of Microsoft Cloud Accelerator Program for Secure Work.

Our process includes:

Assessment

(Security Workshop)

Helps assess client's security readiness and define client's environment and needs and developing a road map for creating a secure workplace.

Validation

(Proof of Value)

Activate relevant trial licenses to demonstrate the value and benefits.

Implementation

(Migration to new solution)

Setting up solution (building, migrating and installing a bespoke solution tailored to the client's needs discovered in the assessment phase) and training personnel to use it.

Optimisation

(The modernisation of the environment as part of Managed Services)

Setting up solution (building, migrating and installing a bespoke solution tailored to the client's needs discovered in the assessment phase) and training personnel to use it.

Customer stories.

Accru+
Harris Orchard

"Byte maintains security for us. The security of our data is really important to us because we are the custodians for our clients' information. I definitely recommend Byte. Nothing is too difficult for them and we are comfortable that they have our clients' data security and our security at heart in their structure."

- Ainsley Coggins, Director, Accru Harris

SYGROUP
CHARTERED ACCOUNTANTS

"It was vital that we found a solution that could provide us with the utmost security and that the data was retained within Australia to reduce the risk of overseas influence. And Byte was able to accommodate all of that for us. Our client security is the most important thing to the SY Group way."

- Sarah Foley, Practice Manager, SY Group


BYTE