Ever since the inception of the internet’s public usage almost three decades ago, protection mechanisms for information assets and the practice of cyber security have enormously evolved. Cyber-attacks are increasing in number and sophistication, while our dependence on the internet and other networks is growing simultaneously. As much as the digital world is interconnected with a chain of cloud computing, smartphones, intelligent transport systems, e-governance, e-banking, etc., it is also making it impossible to avoid threats in the cyber space.

**What is Cybersecurity?**

Despite the global nature of today’s computer systems and networks, there isn’t one universally accepted definition of Cyber Security. If defined in its true sense, Cybersecurity is the practice of protecting networks, systems and programs from digital attacks. These attacks are aimed at retrieving, changing, misusing or destroying critical information and result in disrupting business processes or incurring financial losses to the victims.

**Why is Cyber Security Important?**

Enterprises, governments, financial institutions, hospitals, etc. gather, store and process huge amounts of confidential data on their computers and transmit critical information across their networks. The growing numbers of sophisticated cyber-attacks have made these entities realize that malware is now a readily available commodity.

Realizing this trend, global spending on cyber security has been continually growing in the past years. According to Australian Cyber Security Growth Network, the current [global market for cybersecurity](https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#3b322236381d) in 2020 is $173B, with expected growth to $270B by the year 2026. By that year, about 77 percent of spending for cybersecurity will be in externally managed security services. It is expected that by 2026, global spending on external products and services for cybersecurity will annually increase by 8.4 percent.

**Common Types of Cyber Attacks**

Though individuals and businesses have found ways to prevent cyber-attacks for the most part, by no means does it indicate that they are totally safe from the risks they pose.

Let’s briefly describe some of the most common cyber threats that individuals and small businesses face and how they can be avoided.

**Malware**

Malware is a short form of malicious software. It refers to any software that is specifically designed to get access into and damage the owner’s computer system without their knowledge. Malwares are of different types with different purposes such as using your system to send spam, stealing login information or crashing your operating systems. Some common types of malware programs include viruses, spyware, worms, trojan horse and botnets.

**Social Engineering**

In a social engineering attack, a cyber-criminal manipulates people psychologically into giving away sensitive information such as credit card or login information. Phishing is one of the most common social engineering techniques where a criminal sends a deceptive email and asks a user to click on a given link or give away personal information by mentioning false scenarios, for instance, winning a lottery, free air tickets, and likewise.

**Advanced Persistent Threats (APTs)**

In APT attacks, an unauthorized user will infiltrate into a network without getting noticed and stay there for a long time. The intention behind APTs is to continuously steal data without harming the network. APT attacks often target industries with highly-sensitive information, such as finance or defense sector.

**Ransomware**

It is a type of malware that locks your device and holds your files hostage until you pay a ransom amount to get the access back to your data. Common ransomware types include lockers, crypto malware and scareware.

**Why Small Businesses are at Risk?**

Small and medium businesses are now more at risk at the hands of cyber criminals as compared to large enterprises. This is because big corporations are now investing and implementing strict security measures as part of their compulsory fulfillment of business requirements. Small businesses on the other hand have still not realized the importance of security and potential consequences of information theft. On the attacker’s end, automation has made it much easier for them to attack thousands of small businesses at one time, most of which are easy and vulnerable targets.

**Cybersecurity for Small and Medium Businesses in Australia**

On 6th August, 2020, the Australian government released its [Cybersecurity strategy](https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf), which has re-emphasized the importance of cybersecurity resilience at national level. But the SME sector in Australia is still struggling to achieve the required cybersecurity standards.

According to a [survey by the Australian Cyber Security Center](https://www.cyber.gov.au/acsc/view-all-content/news/largest-survey-improve-cyber-security-australias-small-businesses) in 2019, the country’s SME sector is highly vulnerable to cyber threats. Though only 1,763 small and medium businesses responded, which accounts to less than 0.1% of total SMEs, it’s still a first of its kind report which clearly draws attention. It mentions that a significant proportion of SMEs in Australia have inadequate cyber security practices in place. The fact that this sector contributes substantially to the Australian economy, this statistic indicates a potential risk to the economy at national level.

The survey report also mentions that though most SMEs are aware of their exposure to cyber risks, they don’t completely understand the severity of underlying vulnerabilities and threats that cause the risk factors.

**How can Small Businesses Ensure Cybersecurity in Australia?**

ACSC has released its [Small Business Cyber Security Guide](https://www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide), which provides information about all potential cyber threats and related cybersecurity measures, such as risk mitigation, vulnerability reduction and threat protection. However, instead of a broader approach, business owners understand clear and easy explanations of applicable threats, with examples specific to their industry. Even better would be to break down information into smaller aspects, focusing on specific areas to reduce confusion. For instance, an email policy or an access control policy for small and medium businesses.

To protect against cyber threats, SMEs must adopt security best practices by

* ensuring password management
* avoiding phishing scams
* conducting regular information security awareness sessions for employees
* implementing access control and network security practices
* securing workstations, servers, and all personal devices of employees
* securing employee browsing experience

SMEs must adopt these best practices along with security solutions such as Intrusion Detection Systems, Firewalls and Antimalware programs, data encryption and backup, and data leakage prevention tools to create and ensure an environment of cybersecurity in Australia for small and medium businesses.

With guides such as that of ACSC, SMEs also need guidance on how to choose effective cybersecurity service providers that provide [impressive managed IT services](http://www.kmtech.com.au/) with real outcomes.

With the 2020 cybersecurity strategy introducing new initiatives for the SME sector, it is hoped that targeted solutions are designed and implemented for the SME sector. The coming 12 months are critical in seeing how these solutions are brought to life to reflect a positive change in overall cybersecurity resiliency of Australian Small and Medium businesses.