AUSCSEC

What is your Cyber resilience worth?

The cost of not being Cybersecure could be your reputation and revenue. What is it worth to you to be Cybersecure?

Consider this: if your IT spend each year is less than 1% of your annual turnover, and your Cybersecurity spend is less than 25% of your IT spend you **will** be at risk.

Cybercriminals can detect and monitor transactions between organisations and financial institutions simply by monitoring internet traffic. Sophisticated criminals will analyse that data and decide who they're interested in.

Running your business without Cybersecurity protection is like being in a James Bond movie; consider the opening scene in Daniel's first Bond movie, "*Casino Royale*". The villain already has your credentials, and James is pursuing him on foot relentlessly through a myriad of difficult and dangerous situations in Madagascar: he must eventually resort to the most brutal of force to retrieve those precious credentials.

Or imagine that Jason Bourne has possession of your credentials as he tried to escape the Russian KGB and Moscow police, driving your “taxi” on a single lane. The villains are in pursuit, and there’s heavy traffic coming head on, through the streets and you’re expecting him not only to survive but also escape with your precious credentials intact and hand them safely back to you.

But is it only a matter of time before you're caught? Without cybersecurity protection, it most certainly is!

Most adversaries – regardless of their objectives – must be able to gain initial access, escalate privileges, steal credentials, move within and across assets, evade defences, and persist in networks without being recognised. They sneak around in the background, finding out exactly what you have and what price they can get on the black market for your personal details. Or they may work with other cybercriminals to take away your freedom and security.

Consider for a moment the story of the three little pigs sent out into the world to "seek out their fame and fortune".

The first little pig builds a house of straw, but along comes the wolf and says:

"Little pig, little pig, let me come in”.,
The first little pig replies
"no, no not by the hair on my chinny chin chin."; The wolf then says:
"Then I'll huff, and I'll puff, and I'll blow your house in."

And sure enough, the wolf then blows the house down and devours the first little pig.

The second little pig builds a house of sticks; the wolf also blows that house down and eats the second little pig.
The third little pig builds a house of bricks, and the wolf can't blow that house down.
The wolf then tries to trick the pig out of the house by asking to meet him at various places, but each time the third little pig outwits him. Finally, the wolf climbs down the chimney, at which point the pig catches the wolf in a pot of boiling water, slams the lid on, and then cooks and eats him.

Today, individuals, businesses, communities and nations find themselves in the very same predicament, trying to stay one step ahead of the Cyber wolves.

The Cyber wolves are either attacking you inside your homes and organisation or trying to lure you out so that they can steal or destroy your most valuable assets. Your credentials are the master keys to the door of the room containing those assets.

It's only a matter of time before they break down the door. The door that you have been meaning to fix for ages but never got around to it. But be aware that any decision to defer and waive remediation activity potentially exposes you to vulnerabilities and therefore, an attack.
From our experience dealing with various individuals and organisations, there is little understanding of what it means to be cyber secure and cyber-resilient, and how to get there.

But know that you are not alone. Many of our clients, partners, and vendors have shared why they continue to drive the "taxi" to escape those villains.

You must demonstrate vigilance of those who may have your keys or even part of them. Similarly, you must be relentless in your endeavours to escape their clutches. And it is the same reason why we continue to live in houses made from "straw" and "sticks".

Every mitigation strategy should be on the table to secure your defence.

You can learn from the third little pig and build your house out of bricks at the start, or we can help you on a journey of upgrading your home to brick while keeping you as cyber safe as possible along the way. There may be iterations as you progress from straw and sticks to brick veneer and finally, full brick.

As technology improves, you can continue evolving and building to keep these Cyber wolves at bay.

We know from experience that it's less complicated than you think to implement foundational building blocks to take your organisation from vulnerable to cyber resilient. Organisations need to invest now, rather than wait for an incident to happen. When that happens, you will be dealing with recovery plus business as usual, loss of face with clients and fellow vendors. There's also the inevitable backlog of business activity, existing responsibilities for data/privacy issues and any liabilities above and beyond that.

You need to change your mindset from reactive to proactive.

We need to ensure we have plans in place to mitigate cyber-attacks. You can't run away from it; there is no Mighty Mo - the USS Missouri with its 17 inches of steel doors slamming shut behind you to keep you safe.

The motto of the Mighty Mo was "Strength for Freedom". Even the mightiest need to be upgraded. In the summer of 1984, the ship was updated with the most advanced weaponry available; including upgrades to radar and fire control systems for her guns and missiles, and improved electronic warfare capabilities to ensure she was battle-ready for the future. That future became the Gulf war.

But even the mightiest of defences have weaknesses, ships like the USS Missouri are highly susceptible to attacks from submarines and guided missiles, and so require appropriate protections and countermeasures.

To make it too hard for attackers to succeed, we need to utilise emerging technologies to harden our organisations and assets to enable us to withstand an attack from an adversary.

Similarly, we must ensure your business has the tools (People, Process and Technology) to not only survive being hunted but to continue and grow.

Today's adversaries pose similar threats to organisations as the USS Missouri did to other enemies of her time. These days, cyber enemies are far less visible but just as damaging. Some are highly skilled and primarily rely on tools and techniques they develop, while others rely mostly or entirely on tools developed and distributed elsewhere. Some adversaries are lone-wolf actors, but others are teams and groups such as nation-states, criminal organisations, and hacktivist groups.

While most adversaries are external, many breaches are performed by people within the organisation: the internal human factor.

We know from the latest Office of the Australian Information Commissioner (OAIC) Notifiable Data Breach Report, July to December 2019, that the human factor, the trusted insider statistics, have increased every year. Key statistics reported that for this period, a total of 537 notifications broken down as follows:

- **32% human error**;
- **64% malicious or criminal attacks, and;**
- **4% system faults.**

While the focus is pointing at the external adversaries, we need to be mindful and watchful about trusted insiders and the threats they pose to their own organisations, either intended or not.

Trusted insiders are often disgruntled employees and occasionally just criminals, particularly in larger organisations of 100 employees or more. But in smaller organisations, trusted insiders are often employees unaware of the tricks employed by cyber criminals and fall prey to sophisticated phishing attacks or unknowingly invite the wolves in from surfing the web in their spare time.
These are the most dangerous trusted insiders: those that are naively using the internet for their personal use.

What sets today's adversaries apart from previous generations is the sophistication of techniques. Adversaries are increasingly employing never-before-seen tools and tactics, including custom and polymorphic malware that defeats existing security technologies. They are building evasion techniques into their exploits and malware to disable or circumvent traditional security tools and gain access to networks and the assets connected to them.

The OAI Commissioner discussed the international landscape and reflected that still, the most data breaches—including those resulting from a cyber incident—involved a human element, such as an employee sending information to the wrong person or clicking on a link that resulted in the compromise of user credentials.

Organisations should seek to understand what data they hold, and what information is considered critical.

By working with AUSCSEC to secure and protect their customers from harm in the event of a data breach, they can reduce the risks associated with the human factor – the trusted insiders.