LOGICALIS
Architects of Change

Opinion article

Cybersecurity lessons that board directors and senior executives can learn from the Three Musketeers

Australian companies face increasing risks from external threats in our digital society. One of the biggest challenges is the growing threat of cybercrime. According to the Australian Cyber Security Centre (ACSC), an average of 164 cybercrimes were reported each day, or one every 10 minutes, from 1 July 2019 to 30 June 2020.[1]

Australian organisations across many sectors including business, education, health, and all levels of government were put on high alert after a sophisticated, state-based cyberattack targeted the country in January 2021. Similarly, the recent cyberattack on Australia's Nine Entertainment has highlighted the increased prevalence of these attacks.

It's clear that cyberattacks are a major threat to Australian businesses. Data breaches and cyberattacks have far-reaching impacts. Not only do organisations face the risk of compromised data, but there are significant financial risks associated with data breaches, as well potential damage to image and brand reputation, and a lack of customer confidence in a company.

Despite the risks, many organisations continue to believe that cybersecurity is solely the responsibility of the IT team. Today, this couldn't be further from the truth.

All for one and one for all

While the Three Musketeers may not be the first thing that comes to mind when thinking about cybersecurity, Australian organisations can learn a lot from the musketeers' motto. It's easy to associate cybersecurity with the IT team; however, maintaining a strong cybersecurity posture shouldn't sit entirely on the IT team's shoulders. On a fundamental level, IT technologies and expertise are a critical method of defence for organisational security, but cybersecurity breaches affect all employees, and can easily be caused by any individual employee within any part of the organisation.

Security breaches can take down an entire business, as we saw with Nine Entertainment. Depending on their effectiveness, cyberattacks can have a domino effect on a company. While a threat or attack may only target one small part of a company's defence, they can take technologies offline that prevent employees from doing their jobs, which can delay delivering work for clients. Furthermore, these impacts may be felt across the business's bottom line, which can impact on shareholders, and even global economies.

As such, it's essential that cybersecurity is a priority for all business functions, not just IT. In fact, cybersecurity needs to be prioritised from the top to the bottom of a business, starting with senior executives and board directors, and filtering down into the wider business. Everyone must understand the unique and important role they play as individuals in keeping the company secure, embracing the motto of all for one and one for all.

[1] https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Taking a top-down approach to cybersecurity

Implementing a strong cybersecurity approach into an organisation requires buy-in from the top, not only from a financial perspective, but from a broad operational and cultural perspective as well. It is essential to integrate cybersecurity into the wider business strategy, and closely align it with business objectives. To achieve this, CISOs and other C-level executives need to work in tandem to ensure that cybersecurity is considered at every level of the business.

For many organisations, this involves considering how cybersecurity can help other departments deliver work to clients without impacting on the company's security posture. Everything from file sharing to workflow management and video collaboration technologies need to be assessed for impacts to cybersecurity while simultaneously helping to improve worker productivity across the business. This is why the IT team and C-level executives must work together to ensure strategies and technologies are aligned for the best possible organisational defence.

Creating a strong cybersecurity culture

While it's essential that executives and board directors work closely with the IT team to ensure a strong cybersecurity strategy, senior management also needs to ensure the strategy complements wider business objectives and the organisation's culture. Executives need to align the workplace culture with a strong cybersecurity culture and promote good cybersecurity hygiene across the business.

Rob Mattlin, national practice manager for modern workspace, Logicalis Australia, said, "For organisations to build a strong cybersecurity culture, business executives must lead by example and encourage employees to adopt better cybersecurity hygiene practices. This includes engaging workers with cybersecurity training and introducing security best practice for things like password management and file sharing.

"While the IT team is primarily responsible for cybersecurity, executives can support the IT team by engaging workers on a daily basis, and demonstrating cybersecurity best practice in their own actions. This means executives and board members attending cybersecurity training, following cybersecurity policies and processes correctly, and using the right tools and technologies to conduct business."

Investing in the right supporting technologies

In addition to maintaining a strong cybersecurity culture in the workplace, it's essential that employees are empowered with the right tools and technologies that provide critical layers of defence against external threats. This includes network and endpoint security tools, like VMware Carbon Black, that integrate with existing digital infrastructures to create a strong cybersecurity posture.

Naveen Shettar, general manager of consulting and advisory, Logicalis Australia, said, "While it's incredibly important that employees and executives work to maintain a strong internal cybersecurity culture, digital societies have digital threats, which means we need to invest in digital defences. Without the support of the right technologies such as network and endpoint security, firewalls, secured networks, encryption, and more, our organisations will always be at risk from successful attacks by cybercriminals.

"When all of these elements work in tandem, organisations can provide the best level of security for every area of the business, from the top of the company to the bottom, and at every technological layer in between."

Are all members of your team—both human and technological—working together to protect your business? It can be challenging to know which step to take first to strengthen your approach to cybersecurity. However, investing in the right partner can help simplify this process. Logicalis Australia has a range of security assessment services to help organisations determine what controls and practices are most appropriate for the business. For more information on implementing pragmatic and risk-based cybersecurity plans suitable for your organisation, contact Logicalis Australia today.