VAN Radar 2019

Roundtable session summary

Session: Cyber smart – protecting your business

Presenter: Mike Reynolds, Macquarie

As business people, you need to be curious about security.
*Even though it's highly technical and a challenge – you need to **get this**.*

The most commonly hacked businesses are medium-sized companies like yours – large enough to manage a valuable pool of client funds but small enough to have fewer security and fraud controls.

Meet your hackers

A third of them have been hacking for more than a decade, and nearly half are tertiary educated. The vast majority (86%) hack because of the challenge in learning and applying new skills. They see hacking as a puzzle to solve.

Many hacks are business models providing features such as customer service to make the transaction as easy as possible. They invest in skills, such as native English speakers and graphic designers. It is important to remember to 'park the criminality' and see them as businesses.

How are they doing it?

- **Ransomware:** A type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. They do not usually negotiate.
- **Phishing:** Authentic-looking—but bogus—emails, USBs or phone calls, requesting information from users or directing them to a fake web site that conduct dodgy dealings or distribute malware.
- **Email compromise:** Convincingly taking over a digital identity that gives a wealth of information on a person, their business and finances.
- **Malware:** Malicious computer software that, once downloaded to your computer, accesses passwords and steals data.
- **Supply chain attacks:** If you rely on vendors, consider who is weak within your network? This form of attack is slow and cautious while the hackers develop a way to monetise the data.

How do we defend ourselves?

90% of breaches are due to human error. At Macquarie, solutions we've turned off auto-complete functions for email addresses and email content and removed email attachment functions for back office staff. These measures were not popular but immediately effective in preventing information going to the wrong people.

- Staff education is critical
- Invest in technologists
- Define your risk appetite and align your investment to a framework
- Define what's important to your business and invest in protecting that (client data, not Christmas photos)
- Be sceptical

Invest in low-cost but high-value solutions ($500-$40,000)

- Firewall set up consultancy
- Email and web filtering
- Security education program for staff
- Antivirus
- Application whitelisting
- Phising email simulations
- Threat intelligence service
- Daily backup of critical data
- Remove local admin privileges
- Restrict USB thumb drives
- User account monitoring
- Strong password requirements
- Control office network ports
- System hardening

Mike Reynolds is the Chief Information Security Officer in BFS at Macquarie