EXTRA, EXTRA - READ ALL ABOUT IT!

All too often in today's world we see headlines like the one above where SME's fall victim to Cyber criminals placing Business owners, (and sometimes their livelihood), into severe jeopardy and disarray due to a targeted Cyber-attack. Businesses who form part of the Complementary Health Industry can also be targets whether you are an importer, exporter, manufacturer, distributor, or retailer. All such businesses hold valuable customer and employee information that Cyber criminals seek to steal.

Impacts experienced can range in scale and severity. From a client's Business needing to close as it cannot operate with a virus infected computer system. Other impacts may be brand damage to the Business due to private and confidential company information and client/staff records released onto social media platforms, or the sale of such information on the Dark Web. It might be the financial burden on the Business where a ransom must be paid to retrieve information so your business can be back up and running.

Infiltrating a Business is becoming relatively simple as these criminals become more and more sophisticated in their methods of social engineering fraud aimed at you making a mistake and falling into their clutches giving them your system access.

Let us look at some of the techniques employed in the world of social engineering.

What is Social Engineering? One definition (in the context of information security), defines social engineering as the psychological manipulation of people into performing actions or divulging confidential information.

Common types of social engineering attacks to be aware of are:

Phishing ... this refers to the practice of sending fraudulent email communications that appear to originate from a trusted source, with the aim of gaining personal information, or influencing the target to do something.

Whaling ... this is a highly targeted phishing attack at the most senior management level of a Business and is designed to make those who fall victim to it take steps moving the Cybercriminal closer to their aim, such as transferring funds from the company to their bank accounts.

Malware (or Malicious Software) … means any unwanted software installed in your systems without consent. This software can be created purely to destroy all your records, causing havoc.

Diversion Theft ... where Cyber criminals try to manipulate transport companies to deliver products and services for their financial gain.

Baiting ... as the saying goes "come into my parlour said the spider to the fly." Baiting involves the scammer using a false promise to lure the unfortunate into a trap which may have an aim to take personal and financial information or infect the system with malware.

Pretexting ... Pretexting is a form of social engineering in which an attacker tries to convince a victim to give up valuable information or access to a service or computer system. The distinguishing feature of this kind of attack is that the scam artists come up with a story — or pretext — in order to fool the victim.

SMS Phishing ... Utilisation of text messaging fraud to lure victims into again revealing personal account information or installing malware to infect their systems.

Scareware … Scareware is malicious software that tricks computer users into visiting malware-infested websites. Also known as deception software, rogue scanner software, or fraud ware, scareware may come in the form of pop-ups.

Examples of Major Cyber incidents

- Security researchers uncovered Russian hackers infiltrating United States utility companies.
- A large International Hotel Chain had five hundred million guests' data stolen including passport information.
- A major International Airline had 380,000 customers' personal data stolen from their app.
- Online customers of a large Retail Chain in the USA were hacked, stealing sensitive personal information.
- Closer to home- Valuation in Australia. A Property Valuation company had their customer data breached for 100,000 of its Bank related clients.
- 30,000 Victorian Public servants' personal information was stolen due to a data breach.

Examples of Cyber Insurance Claims

1. A Property Developer was required to make a payment of $400,000 to a services provider upon settlement of Properties. On the day the payment was due, the Insured received an email from the service provider advising their banking details had changed. The Insured requested that this be sent to them in writing on the service providers letterhead which they received, including the signature of the director of the company. A couple of weeks later, the Insured was sent an email, following up the payment at which time it was discovered that the email and letter had been fraudulent. The Insured contacted their bank to stop the payment and were informed that the money had already been withdrawn and transferred overseas.

<u>Outcome</u>
The Insured made a claim on their Cyber policy which triggered the optional Social Engineering cover. The insurer appointed an IT forensic consultant who identified that the hacker had infiltrated the consultant's system and intercepted correspondence between the Insured and the service provider firm. The Insured was reimbursed for the outstanding funds (capped at the Social Engineering sub limit of $250,000).

2. The Insured, a Medical Services provider, which held confidential medical information on their patients, was compromised by a ransomware attack. As the Insured could not access their patients' medical data, they were unable to operate.

<u>Outcome</u>
The Insured's policy was triggered, and the insurer appointed an IT Forensic Consultant to fix the damage to the Insured's system and investigate if the hacker still had access to the system. A law firm was also appointed to assist the remediation process and advise if the client had to report the matter to the Privacy Commissioner. Payment was made to the value of $63,000 in relation to business interruption loss, forensics, and legal costs.

Mitigating Cyber Incident related costs

Every Business in this day and age is reliant upon computer systems, online platforms, etc., where employees are using PC's, laptops, tablets, mobile phones, and other devices and should consider mitigating Cyber-attack costs and purchase Cyber Insurance.

The Complementary Health Industry is no stranger to these practices be it internal systems to run operations or selling products online through a website platform.

Cyber Insurance policies can cover a range of Cyber related activities such as Computer System Security Failure, Cyber Business Interruption Costs, Cyber Claim Defence Costs, Cyber Extortion Event, Data Breach, Media Claim Defence Costs & Regulatory Investigation, Social Engineering & Phishing. Policies also provide the value added back up when needed of a 24/7 emergency assistance to help you out in your time of need.

The insurance cost can be minimal when compared to the consequences of the unexpected losses that can be incurred. If you are unsure about Cyber Insurance and need a professional advisor to talk to, please contact our friendly team at IME Insurance Brokers - Insurance Made Easy for personal assistance to discuss your own individual circumstance **1800 641 260** or visit us at: www.imeinsurance.com.au

Our website address link to Cyber Insurance is https://imeinsurance.com.au/cyber-insurance/

James Gillard
Managing Director

IME INSURANCE MADE EASY
BROKERS SINCE 1992

cma Complementary Medicines Australia