Social Engineering isn't just a buzz word

So, what is Social Engineering anyway?

It's the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Hopefully by reading this article it will alert you to the fact, whatever the size of your business , you are a target and need to be constantly aware of IT Risks.

Deception by hackers wanting to steal your identity, or destroy your hard earned business reputation , disrupt your day to day business activities , steal/lock your data, demand ransoms to get it back, and possibly spread or sell your client's information to all and sundry.

So, what types of Social Engineering are there?

- **Phishing**, where attackers use emails, social media, instant messaging, and SMS to draw in targeted victims into providing sensitive and private information with an aim to compromise business systems. An example of this is "Business Email Compromise" (BEC), where hackers create a fictitious appearance as known Executives of a firm to force those in Account Payable areas into transferring significant sums of the company's money into the hackers own bank account.
- **Watering hole** means implanting malicious code into the public website pages of sites that the targets visit such as online shopping sites.

- **Whaling attack.** Same as phishing but this time the hackers are out their trawling with an aim to catch a whale which are big PHISH, in other words, Board Members & Senior Executives of private business and government agencies.
- **Pretexting.** Hackers create a fictitious identify of a person to gain private information then once in hand manipulate that information for criminal intent.
- **Baiting** where hackers use an infected computer file which looks just like an authentic software update. Case in point, a hacker infects USB sticks , leaves them around public areas and the unknowing public insert them into their own computers potentially destroying data on their hard drive due to an infected program on the USB stick.
- **Tailgating** where a hacker can infiltrate entry to a restricted area by walking in behind a person who is authorized to access the area. Someone for example in a building who enters the lift but gets off behind the person that works on that floor. Possibly disguised as a tradesman where no questions are asked of the intruder.

Businesses are not bullet proof

Businesses MUST do everything in their power to protect themselves from being exposed and vulnerable when it comes to forms of social engineering by 3rd parties. Undertake checks on vendors, install fraud detection systems, separate financial duties of employees, and roll out education programs for staff on how to detect fraud and what steps to take.

Despite these measures' businesses can still and do become victims of social engineering.

Three example cases

A. The case of the fake invoice.

An employee for a distributor of component parts was accountable for making regular vendor payments. After several months of this arrangement in place the employee one day received an email appearing to come from the vendor. The proposed vendor said they were having banking issues and asked for the payments to be made to a new bank and attached a new invoice. The employee was finding it difficult to verify the request and the proposed vendor applied pressure for the payment to be made. The employee paid the false invoice. The real vendor chased a payment they did not receive and realised through social engineering techniques they had been hacked and the cost to the distributor was $250,000.

B. The case of the imaginary CEO

A regional CFO of a subsidiary of a large public listed company received an email purporting to be the Assistant of the CEO in the United States. The email requested the CFO transfer a significant sum of money immediately to cover a tax payment in China. The CFO questioned the request and then the fake Assistant of the CEO made a phone call to the CFO insisting and proving over the phone the request was legitimate. The fake Assistant to the CEO knew all about the companies polices, operations, people, processes, etc. The CFO transferred the money however the scam was detected after another attempt at transferring the funds was stopped by the subsidiaries bank. The company only recovered a small portion of the transfer and the resultant loss to the company was $1,000,000.

C. The case of the Hacked emails

A Business Manager (external consultant) who is responsible for Account Payments received an email, purportedly from their client enquiring about her bank balances and availability of funds. The email seemed very authentic as it included details regarding full descriptions of account numbers, names and some recent transactions. The Business Manager communicated back to their client with the requested details. A further email came back from the client requesting $100,000 be sent to a specific account offshore to purchase real estate. The Business Manager trusted the instructions and the payment was made into the hacker's bank account. All too late, as the $100,000 had been sent.

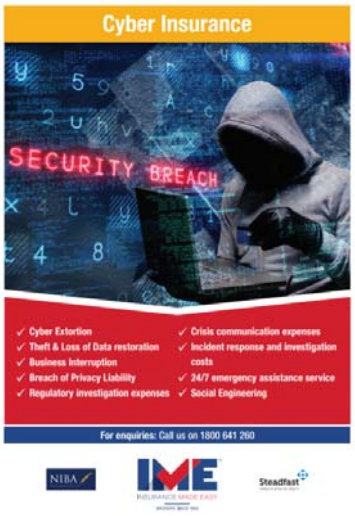
Can Cyber Insurance help?

Cyber Insurance can at least be a safety net consideration which business should seriously look at. In the event a business falls victim to being hacked, Cyber Insurance cover provides some relief to the devasting repercussions to the Business and provides financial reimbursement to rectify the damage done under the terms and conditions of the insurance policy.

There is standalone Cyber Insurance and Cyber cover is also part of an overall Management Liability insurance policy.

If you would like to know more about Cyber Insurance and Management Liability Insurance please contact the friendly team at IME Insurance Brokers - Insurance Made Easy for personal assistance to discuss your own individual circumstance **1800 641 260** or visit us www.imeinsurance.com.au

James Gillard
Managing Director
Insurance Made Easy


Cyber Insurance
SECURITY BREACH
✓ Cyber Extortion
✓ Theft & Loss of Data restoration
✓ Business Interruption
✓ Breach of Privacy Liability
✓ Regulatory investigation expenses
✓ Crisis communication expenses
✓ Incident response and investigation costs
✓ 24/7 emergency assistance service
✓ Social Engineering
For enquiries: Call us on 1800 641 260
NIBA
IME
Steadfast


Management Liability Insurance
Why Every Business Should Have It?
IME