TRENDING TOPICS

Risk Management

Social engineering fraud
– prevention is the best approach

The volume of social engineering scams deployed by cyber criminals is rapidly rising. The financial loss and reputational damage to organisations that fall victim to these scams is significant.

By increasing employee awareness, and implementing systems and operational controls, organisations can significantly reduce the risk of being affected by social engineering threats.

Liberty International Underwriters

CLYDE&CO

What is social engineering?

Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that is then used for fraudulent purposes.

It's a process by which cyber-criminals take advantage of unsuspecting victims to financially gain from access to their sensitive information. Social engineering attacks can take many forms: online, over the phone, or in person. Whilst attacks can involve exploiting weaknesses in technology, human error often plays a role.

Common forms of social engineering attacks

1. Business email compromise scams

Impersonating businesses for financial gain

Cyber-criminals commonly compromise a senior employee's or financial controller's mailbox, and then fraudulently instruct the organisation's clients to replace the bank details that they use to pay the organisation, with the cyber-criminal's bank details, in order to misdirect funds. Spoofing emails are the key to executing the attack, and typically requests are made in a situation of urgency to circumvent fraud detection processes and increase the chances of success.

2. Email phishing

Emails or websites that trick people into giving out sensitive information

Phishing campaigns are typically indiscriminate wide scale campaigns to increase the potential scope of victims. Spear phishing attacks target a particular organisation, or person(s) within an organisation.

A common example is an email that appears to be genuine, which contains an attachment that in order to be opened requires the user to enter their login details. Once provided, the cyber-criminal can hijack the user's mailbox.

3. Pretexting

Creating a fake scenario or persona to obtain systems access or funds

A common example is an individual receiving a fake phone call from the 'IT department' requesting login details to fix an 'error', or a cyber-criminal sending an email to an individual threatening to disclose salacious web browsing history unless they pay money to the cyber-criminal (usually in the form of crypto-currency such as bitcoin).

The impact for organisations

Social engineering attacks cause significant financial harm.

In addition to the direct financial losses, social engineering attacks can cause significant reputational damage which can lead to loss of clientele. There are also privacy concerns which can lead to regulatory and third party claims exposure.

> Recent figures suggest that by 2021 cyber crime will cost the world $6 trillion annually, up from $3 trillion in 2015.
>
> Source: 2017 Cybercrime Report, Cybersecurity Ventures

3 steps to reduce exposure

Prevention is the best cure to combatting social engineering attacks. With the appropriate systems and processes in place, organisations can reduce their risk profile.

By preparing for an incident organisations can significantly improve their ability to detect and respond, thereby minimising the operational and financial impact of an attack.

Organisations can take three steps to reduce the chances of falling victim to social engineering attacks, by focusing on: people, processes and technology.

1. People

- Train employees to increase awareness of the various forms of social engineering attacks, and how to recognise and appropriately respond to them.
- Test employees by running simulated phishing campaigns.
- Develop a system so that employees can quickly and easily report incidents and suspicious activity to the appropriate IT and risk management functions for review.

2. Processes

- Establish, implement and enforce policies for internet usage, facilitating financial transactions, and protect information from unauthorised access, disclosure or loss.
- Employees should be suspicious of any emails seeking to change bank account and/or payment details and verify the legitimacy of the email by calling the sender using official contact details, not those provided in the suspicious email.
- Develop and test incident response plans, to minimise the impact of an incident in the event that one occurs. This includes understanding the role and benefit of working with external legal, IT security, forensic providers, financial institutions and law enforcement post incident.

3. Technology

- Implement complex password requirements. Consider the use of implementing multi-factor authentication to protect sensitive systems from unauthorised access.
- Back up data and ensure the backup systems are regularly tested.
- Implement logging capabilities to identify and track suspicious network activity. This is critical for investigations post incident.

A relationship that protects what you value most

No matter what business sector you are in, or the complexity of your insurance needs, **Liberty** will find a way to speak your language. Liberty's fully integrated team of underwriters, risk engineers and claims professionals combine their experience and expertise to truly understand your business, provide tailored levels of cover, and offer practical guidance.

Clyde & Co advises clients on a broad range of privacy and incident response related matters, including in assisting organisations address their legal and regulatory obligations as well as in preparing for and responding to data breaches and other cyber incidents. Clyde & Co works with a number of IT security and forensics organisations in providing these services.

For more information, please contact

liuasiapacific.com

clydeco.com

Liberty International Underwriters | CLYDE&CO

02/19.v4