Cyber | **Insight**

Summary: Social engineering considerations for Investment Managers

Asia Pacific

Liberty

nccgroup

Investment firms require an insurance solution that is broad, compliant, relevant and customisable. Liberty, along with cyber security advisers NCC Group, aim to provide an overview of recent social engineering developments and some practical tips on how investment managers can protect their firms from these manipulation techniques.

What is social engineering?

Social engineering is a manipulation technique designed to 'exploit humans' to gain access to private information or coerce an action to be performed. Some of the most common and well-known forms of social engineering include the use of phishing emails, spoofed SMS message and even directly calling users, where the social engineer attempts to impersonate a legitimate third party.

When targeted by an adversary seeking to use social engineering to exploit a user or organisation, it is likely this adversary will combine several social engineering techniques to achieve their end goal.

A real-world example of a successful social engineering attack on an Australian hedge fund involved the use of a malicious Zoom meeting invite to plant malware and gain access to the organisation's network. This access was ultimately used to approve A$8.7 million in fraudulent invoices.

What can be done to protect your organisation?

Cyber security awareness training should be provided to all personnel in order to assist them in understanding their security responsibilities, alongside providing them with the techniques to identify attempted social engineering attacks.

When dealing with suspected social engineering attacks, users should be trained to consider the following and the legitimacy of the request:

- Is there a sense of urgency to perform an action?
- Why am I being asked to open the attachment?
- Why do I need to click the link?
- Why do I need to give permission?
- Why do I need to perform a specific action?
- Am I being asked for information they wouldn't necessarily need to know?

Employees should also be aware of how to report suspicious requests, understand the dangers of using weak passwords, and appreciate that the information they post online via social media can be used against them.

As well as raising awareness amongst employees as to what a social engineering attack may consist of, investment firms should establish processes that provide a fail-safe mechanism to employees to either prevent a social engineering attack from initially succeeding or to detect it prior to a significant impact occurring. This could include introducing additional verification for certain fund transfer requests, or additional verification requirements prior to authorising a change of registered member details.

Organisations should ensure their systems have security controls enabled that meet the recommendations of good industry practice. The Australian Cyber Security Centre (ACSC) recommends eight security controls organisations should implement to mitigate the likelihood of a cyber security incident. These controls are known as the ACSC Essential Eight.[1]

At a minimum, organisations should implement these controls on any computer within the organisation capable of initiating a financial transaction.

1 https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

Responding to a social engineering attack

It is important that investment firms have a well-rehearsed incident response plan in place, enabling them to swiftly detect and respond to a computer security incident. Successfully detecting, containing and recovering from a social engineering attack requires that an organisation has predefined and well-rehearsed steps regarding how to respond once an incident is identified.

The success of preventing critical repercussions as a result of the attack often depends on at which point the attack is detected. If the attack is detected early in the life cycle, such as upon receiving a suspicious email or phone call, there is a greater chance of preventing either financial impact or reputational damage to the organisation.

Good industry practice is to align an organisation's incident response plan with a well-known standard, for example the National Institute of Technology (NIST) SP 800-61.[2] NIST recommends the plan includes the following phases of incident response life cycle:

Those tasked with responding to the social engineering attack must be correctly equipped and trained to do so. A mishandled incident response effort may provide an adversary an opportunity to further compromise the organisation. Organisations should establish an incident response retainer with a third party specialist.

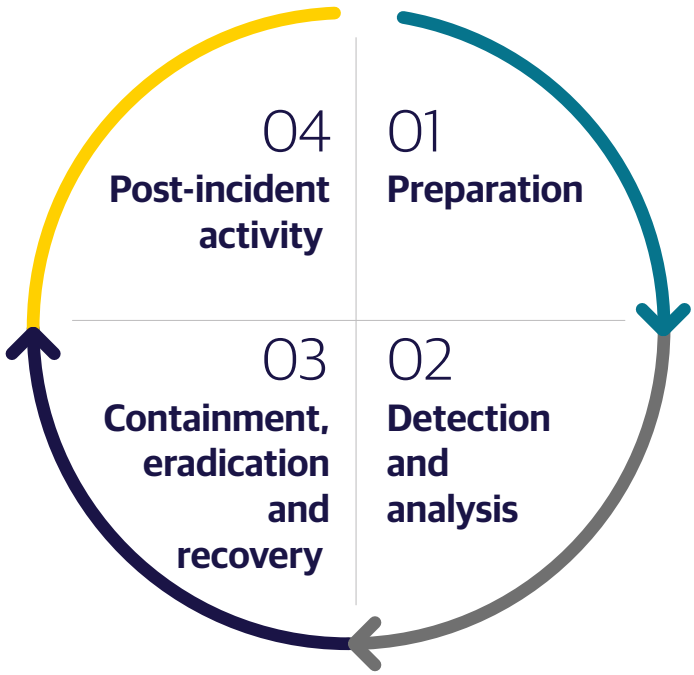
In the event of an incident response scenario, Liberty clients can contact NCC Group to ensure to-the-minute expert advice is provided that is specific to the situation the organisation is facing. Alongside being capable of responding to real-world attacks, the provider can be engaged to perform proactive 'threat hunts' to comb through an organisation's IT environment and identify any sign of intrusion and remediate as required.

Liberty can also help investment firms engage specialist third party legal and financial accounting organisations to assist in recovering fraudulently initiated financial transactions.

Conclusion and next steps

Social engineering attacks can be a successful mechanism for adversaries seeking to exploit organisations and are likely to remain a consistent ongoing threat in the future. It is imperative that investment funds prepare staff to be able to detect and defend themselves against social engineering attacks, alongside implementing appropriate mechanisms and processes to respond to such attacks.

Liberty and NCC Group are well-positioned to provide organisations with the support they require to implement adequate defences against social engineering attacks, and through NCC Group's incident response retainer service, act as first responders on behalf of an organisation during an ongoing security incident.



2 https://www.nist.gov/privacy-framework/nist-sp-800-61

About NCC Group

Liberty engages NCC Group as a cyber security adviser to support clients underwriting Professional and Financial Risk policies.

NCC Group is trusted by more than 15,000 clients to protect their most critical assets from cyber threats. With NCC Group's knowledge, experience and global footprint, they are well placed to help clients identify, assess and treat risks. NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

NCC Group has more than 1,800 colleagues in 12 countries. NCC Group's Technical and Risk Consulting, Incident Response and Managed Services have significant market presence in North America, Europe and Asia Pacific.

For more information please visit:
libertyinternational.com

Office locations

Connect with Liberty

Global reach. Financial strength. Local authority.

Distinct, complex and constantly evolving – every business is as unique as their insurance needs. To confidently progress in the face of risk and uncertainty requires a level of security you can only achieve through working with specialists.

Liberty offers a breadth of world-class insurance and reinsurance services to brokers and insured clients. We bring value and solutions to business and government organisations across Asia Pacific – helping protect what they earn, build and own.