beazley

Article

Social engineering: an analogue trick in a digital age

January 19, 2024

What is social engineering?

Social engineering is used by criminals to trick employees into doing something that enables the criminal to defraud a company of money or to gain access to IT networks evading usual security protocols to steal funds.

Social engineering scams are becoming even more successful and seemingly authentic as hackers use personal information about the target, such as their name and phone number – usually easily available on social media. The rise of remote working and virtual meetings has led to an increase in online scams often using ‘deepfake’ videos and audio files impersonating senior executives requesting other members of staff to transfer urgent payments to ‘clients’.

Once the victim has fallen for the initial approach and taken the desired action, the fraudster will manipulate and mislead the unsuspecting Employee into voluntarily releasing funds or sharing valuable data. Social engineering scams can remain undetected for a long period of time, causing significant losses, embarrassment and potential reputational damage to both individuals and the organization.

Why should you care?

Social engineering claims can fall into the grey area between crime and cyber exposures, leaving clients without adequate insurance coverage for this risk.

Our 2023 Q2 Cyber Services Snapshot reveals that phishing attacks are on the rise again. Businesses and individuals alike need to be aware. It is still extremely difficult to prevent attacks. Regular staff training that can help to identify and respond to this type of attack is important, alongside encouraging the adoption of general best practices, such as multi-factor authentication, penetration testing and wire transfer protocols.

However, because of how social engineering works, this is not a ‘catch-all’ plan; it is important to have an insurance safety net that suits the needs of the business.

Our solution

We offer a Commercial Crime policy that protects against digital crime, including fraudulent instruction coverage for losses resulting from theft, fraud or deception from social engineering.

Additionally, whilst social engineering cover is available in our cyber insurance offerings, some insureds may find that they need even more coverage. To help, our US Crime team now offers social engineering coverage on an excess basis, adding a valuable layer of financial protection.

For more information please visit: Fidelity and Crime | beazley

beazley