CITYNET
LLOYD'S BROKER

SOCIAL ENGINEERING CYBER CLAIM

A company fell victim to a sophisticated social engineering cyberattack. The attacker, posing as a high-ranking executive within the company, initiated contact with the accounting department via email, requesting an urgent funds transfer to a designated external account. The email was crafted meticulously, using the executive's name, official signature, and language consistent with previous communications.

In this well-planned attack, the cybercriminal leveraged publicly available information about the executive and the company's hierarchy, allowing them to convincingly imitate the executive's communication style. The email appeared genuine and raised no suspicion among the accounting staff.

Unfortunately, without verifying the request through additional channels or protocols, the accounting department processed the funds transfer, resulting in a significant loss from the company's accounts. The incident was discovered only after the legitimate executive in question inquired about the unauthorized transfer several days later.

RESPONSE AND IMPACT

Upon discovering the fraudulent transaction, the company immediately launched an internal investigation and notified the appropriate law enforcement agencies. They also engaged a cyber incident response team to assess the extent of the breach and implement measures to prevent similar incidents in the future.

Despite these prompt actions, the stolen funds could not be entirely recovered, and the company suffered a severe financial setback as well as reputational damage.

INSURANCE CLAIM

The company had a comprehensive cyber insurance policy in place that covered various cyber risks, including social engineering attacks. The company promptly filed a claim with their insurer detailing the incident, providing evidence of the social engineering attack, and the resulting financial losses and expenses related to incident response and recovery efforts.

After thoroughly investigating the claim, the insurance company determined that the incident fell within the scope of coverage, as social engineering attacks were explicitly included in the policy. The insurer agreed to cover the financial loss, less any applicable deductibles, enabling the company to partially recover from the incident's financial implications.

KEY TAKEAWAYS

This example highlights the importance of cyber insurance coverage, especially in today's evolving threat landscape, where social engineering attacks are becoming increasingly sophisticated and prevalent.
Companies should proactively assess their cybersecurity measures, conduct employee training on identifying social engineering attempts, and have appropriate insurance policies in place to mitigate the financial and reputational risks associated with cyber incidents.