Vol. 24 No. 1 The Journal of the Allegheny County Bar Association January 14, 2022

LAWYERS JOURNAL

LAW PRACTICE MANAGEMENT

Tips to prevent skyrocketing costs related to social engineering fraud

By USI Affinity

Since 2020, social engineering attacks have increased dramatically in frequency and severity. Business email compromise (BEC) scams are occurring 15 times more frequently than last year, and severity has increased by 179%, with average losses nearly tripling to more than $326,000.

Risk management and insurance programs are not keeping up with this escalating threat, according to recent studies. About 75% of companies fail to equip employees with minimal social engineering awareness training, and 70% of small businesses say they are unprepared to deal with a social engineering attack.

Social engineering defined: A confidence scheme that intentionally misleads an employee into sending money or diverting a payment. The employee is misled by fraudulent information in a written or verbal communication, such as an email, a fax, a letter or even a phone call.

Particularly in a remote workforce environment, cybercriminals are targeting organizations for false payments. Social engineering plays off the electronic nature of modern payment processes and funds transfers. Examples of social engineering include phishing, smishing and vishing scams.

- Phishing: Nontechnical or highly skilled technical manipulation of email servers to induce people to break normal security protocols. Phishing has led to massive financial losses for organizations. Hackers often impersonate a legitimate trading partner or fellow employee; by impersonating a trusted contact, the hacker convinces the employee to send money or confidential data.
- Smishing: The use of text messaging to convince people to pay money or click on suspicious links.
- Vishing: Over-the-phone scams. By posing as bank staff or other financial service employees, the scammers try to persuade people to share information.

Risk Management Best Practices That Help Prevent Social Engineering Attacks

While social engineering security threats will never vanish, organizations can prevent them by taking proactive steps.

1. Train employees. Ensure employees know what to look for in a phishing email and how to spot other social engineering threats. Give employees clear policies on protecting sensitive information, sound password practices, effective security, and visitor management.

2. Document specific verification procedures for any wire/money transfers. Structure prearranged call backs or other verification procedures in contracts or service agreements with third parties, such as customers, clients and vendors. For example, a phone call to a specific person at the third party will help confirm banking and routing information that is not on a particular invoice or email. The phone call should not involve a telephone number in a recently received email.

3. Implement procedures for responding to a scam. If an organization falls victim to a fraudulent transfer scam, it should act quickly and 1) contact its financial institution and request it contact the financial institution where the transfer was sent, 2) contact the local FBI field office to report the crime, and 3) file a complaint with the FBI's Internet Crime Complaint Center.

Insurance Policy Considerations

After a social engineering event, it's critical to place all applicable insurance carriers on notice.

How USI Can Help

In the event of a social engineering incident, standard or "off the shelf" crime and cyber policies may have coverage gaps, which can lead to uninsured losses. USI can review an organization's existing insurance policies and provisions to determine the total amount of coverage potentially available and the nature and extent of any verification requirements.

USI has prenegotiated social engineering coverage on crime policies (ExecuSafe) and cyber policies (PrivaSafe). We help clients prevent and mitigate losses by moving coverage to ExecuSafe or PrivaSafe with both insured and client social engineering loss coverage. We can also modify crime policies to interact with cyber coverages, as well as assist in implementing training programs, awareness updates and recovery plans. If additional coverage is needed, USI may suggest a standalone social engineering fraud policy, if appropriate for the company's risk profile. ■

To learn more about mitigating cybercrime losses with insurance and risk management, contact your USI consultant or email us at pcinquiries@usi.com.