CYBER CRIME

Social Engineering Fraud
&
Data Breaches

What Is Social Engineering Fraud?

Social engineering fraud is defined as “the use of deception to manipulate individuals into divulging confidential information that may be used for fraudulent purposes.”

Criminals use various forms of communication such as email, the Internet, telephone, and even face-to-face interaction to infiltrate companies. The main objective for these criminals is **financial gain**.

Humans tend to be the weakest link in the security chain, resulting in a vulnerability that can have serious operational impacts. All of us are vulnerable to being deceived because people can misplace their trust if manipulated in certain ways. Social engineers focus their attention on locating vital data while gathering information.

Social Engineering Fraud Strategies Used:

- Impersonation
- Phishing/spamming
- Phone phishing
- Forensic Recovery
- Quid pro quo (“give and take”)
- Baiting
- Direct physical access
- Diversion Theft

The best defence for combating social engineering fraud **before** a loss occurs is awareness through organizational culture and training.

Impacts of Social Engineering Fraud

Nearly half of global businesses surveyed in 2011 reported being the victim of one or more social engineering attacks that resulted in losses ranging anywhere from **$25,000 to $100,000 per occurrence.**

Not only does social engineering fraud have a significant financial impact on organizations, organizational productivity and reputation may be affected greatly.

Prevention is KEY!

Because social engineering is continually progressing and is a **huge threat** to organizations in today's day and age, it is essential that all employees are educated and trained on how to detect and prevent these types of fraud.

Communities should consider creating a **training program** that highlights measures specific to their organization, and can include the following examples:

- Identify which employees have access to what types of information and levels of sensitive company information. **REMEMBER: All employees are at risk!**
- Never release confidential or sensitive information to anyone you don't know.
- Establish procedures to verify incoming cheques and ensure clearance prior to transferring any money electronically.
- Reduce the reliance on email for all financial transactions. Establish call-back procedures for all payment approvals and outgoing fund transfers to a previously established phone number.
- Only open emails from trusted sources.
- Avoid responding to any offers made over the phone or via email. **If it sounds too good to be true, it probably is.**
- Physical documents and computer hardware should always be shredded prior to disposal.

Specific policies for employees should be implemented outlining what is defined as confidential information, how to keep it safe, and how to respond to an attack. A security policy should include a component for raising awareness amount employees and educating those who are most vulnerable (ie: new hires, reception personnel, finance personnel, and IT employees to name a few).

CASE STUDY

The finance controller of an organization was responsible for making regular payments to a service vendor that the provided monthly maintenance services. The controller received an email that appeared to come from his contact, indicating that the vendor's bank was having issues accepting payments, and asked if the future payments could be made to a new bank account. This did not seem out of the ordinary to the controller as the emails appeared to be from a trusted source.

Following multiple payments, the vendor contacted the organization after they realized their loyal customer was late on payments. An investigation determined that the vendor's email was hacked, and the company had been socially engineered into believing the bank change was authentic.

In the end, almost $50,000 was handed over the to fraudster!

How Can We Help?

COVERAGE

NORCIX has arranged coverage for social engineering fraud through Beazley Group. This coverage offers a **$1,000,000 limit**, and is available to all member communities that have submitted their application and received confirmation of coverage.

WHEN A BREACH OCCURS…

If your organization experiences a breach, it may be difficult to determine where to begin and what steps should be taken. We request that you follow the steps outlined so we can assist you as quickly as possible before any additional issues arise.

1. BREACH

It is brought to your attention that a breach has occurred.

2. NOTIFY

Contact our office immediately using the contact information below.

3. ASSIST

We will report the loss to Beazley, who will help:
- Manage the breach successfully.
- Help select data breach counsel and if needed, a forensic expert to investigate.
- Provide you with guidance along with counsel to help you meet regulatory requirements.
- Maintain continuous contact with your organization and our office regarding the breach status.

4. EFFECTIVENESS

By contacting our office as soon as possible and working with Beazley, these efforts all lead to a breach being handled as effectively as possible.

REMEMBER

Do NOT try to resolve on your own—we are here to help!

CONTACT US!

Tel: 867.873.8359 **Toll-Free:** 1.866.973.8359

Karen Kuronen: karen@nwtac.com
Cynthia Horton: cynthia@nwtac.com
Sarah Hodgins: sarah@nwtac.com