THE HARTWELL CORPORATION

Bonds ■ Benefits ■ Insurance ■ Risk Management

AN EMPLOYEE-OWNED COMPANY

Social Engineering Fraud is on the Rise

This material is provided for informational purposes only. Before taking any action that could have legal or other important consequences, confer with a qualified professional who can provide guidance that considers your unique circumstances.

It was a typical morning for Ingrid, an accounting clerk at A&J Engineering Services. As she was going through her new emails she came across one from Jack Williams, the new financial manager at key vendor Johnson Supply Company. Jack had called her a couple of days prior to introduce himself and alert Ingrid that Johnson Supply would be making some changes to their banking accounts. Ingrid smiled as she recalled the friendly conversation they had about their pet pugs. Nice guy, she thought.

She opened the email, noticed the usual Johnson Supply logo at the top of the page and read Jack's note. He had included three smiley face emojis following his request to have all future payments wired directly to their new checking account. He included the account number and asked Ingrid if she would get this set up right away. He wrote that he really wanted to impress owner George Johnson with his quick and efficient work and hoped Ingrid would help him.

Ingrid noticed an email trail below Jack's note, where Ingrid's boss Tom had welcomed Jack and said he'd OK'd the new wire transfer deposit plan. Since Tom was good with it, Ingrid was happy to oblige and changed the bank account information for Johnson Supply. She let Jack know everything was set up.

A month or so later, Ingrid was surprised, when Tom stormed into her cubicle visibly upset. He waived a stack of invoices from Johnson Supply in her face asking why she hadn't paid their most important vendor. Ingrid explained that she had paid all the invoices and followed Jack's new payment instructions exactly.

"Jack?" her boss said. "Who in the heck is Jack?" Ingrid felt a sinking feeling in her stomach.

It was later discovered that the payments had been deposited in an anonymous offshore account. A textbook case of social engineering fraud.

What It Is

Social engineering fraud (SEF) is the process of intentionally getting people to divulge or act on information under false pretenses by exploiting human nature. It is the act of deceiving and manipulating an individual in order to gain access to information, monetary resources or other assets.

Unfortunately, SEF is growing at a rapid pace. The Federal Bureau of Investigation reports that between October 2013 and August 2015, in the United States alone, more than 8,000 SEF victims were defrauded of nearly $800 million.

The average loss: $130,000.Travelers Insurance reports that SEF cases have increased by more than 90% annually, with more than 100,000 social engineering attacks launched daily. **Approximately one in three businesses are targeted by SEF perpetrators**. While large businesses are a favored target, small firms are becoming common victims as well.

Social engineering fraud takes many forms, but most have the following characteristics:

Investigation
The perpetrator cases the company looking for vulnerabilities and identifying likely targets among its employees. In our example above, the perpetrator identified a lower-level clerk who had access to financial accounts.

Impersonation
The SEF perpetrator typically impersonates a real or fictitious individual with a supposed connection to the company -- a vendor, a customer, an employee, a banker, etc.

Relationship Building
The perpetrator builds a social relationship with the target employee in order to create friendship and trust. Our perpetrator discovered that Ingrid had a pet pug through her Facebook account and used that information to create a positive, friendly bond.

Exploitation
The perpetrator uses the friendship and trust built with the targeted victim to convince them to do something they wouldn't otherwise do. In our example, Ingrid willingly changed the vendor's bank account number without verifying the change with the vendor or her boss.

Execution
It used to be that attempts to defraud companies and individuals via the Internet were fairly easy to spot because of bad grammar, spelling errors and sloppy graphics on emails and Websites. Not anymore. SEF perpetrators create Websites, emails, attachments and other documents that look exactly like the real thing. Ingrid was convinced that the email came from Johnson Supply, and the email trail clearly showed that her boss was on board with the change.

Education, Training and Safeguards Imperative
When it comes to social engineering fraud, the best offense is a good defense. That defense begins with awareness training for all employees. Make SEF a well-known acronym from the front desk receptionist to the board room. Employee ignorance is your company's greatest vulnerability when it comes to SEF.
Explain to employees how SEF works. Warn them to be vigilant and report to management when a potential perpetrator tries to convince them to take actions that could make the company vulnerable.

Management should identify what company information and resources might attract a SEF attack and, equally important, who has access to those resources. Identify primary employee targets and focus ongoing training and monitoring there.

Examine your policies for handling financial and other sensitive information. Prohibit any single employee from releasing such information without specific high-level clearance. Don't allow any individual to single-handedly complete a financial transaction above a certain dollar threshold. Require managerial review and approval for any requests for changes to customer or vendor accounts. If you receive a phone or email request from a vendor or customer to change account information, follow up by phone or an in-person meeting to verify that the request is legitimate.

Work with your accounting firm to set up these and other fraud safeguards. You might want to consider hiring a consulting firm to conduct SEF penetration tests by phone and email to probe for vulnerabilities.

Are You Insured?
Despite your best efforts, you cannot make your company 100% safe from social engineering fraud. Insurance is your final financial safeguard to minimize or eliminate SEF losses.

Companies who have purchased cyber insurance may be shocked to find that this type of insurance likely does not cover losses from social engineering fraud. Most cyber policies cover losses resulting from unauthorized entry into or the failure of the company's computer network. With SEF, the targeted employee is typically

authorized to enter the network, which is likely working just fine.

Similarly, some crime policies may deny coverage for SEF losses. These policies may have language that limits coverage to "direct" fraud and excludes coverage when losses are the result of a "voluntary parting" with company resources -- i.e., when assets are released with the knowledge and consent of an employee.

Fortunately, forward-thinking insurance companies are now offering specific social engineering fraud endorsements to their crime and fidelity policies. These endorsements bridge the SEF coverage gaps created by traditional cyber and crime policies. Indeed, they extend coverage to specifically include instances of social engineering fraud perpetuated by perceived vendors, clients and others.

To obtain SEF coverage, you may be required to fill out a supplemental application outlining the policies and procedures you have in place to combat SEF. Insurance limits can be as low as $10,000 or as high as $1 million or more.

SEF Risk Analysis

We would be happy to help you analyze your current insurance policies and identify potential coverage gaps that leave you vulnerable to SEF losses. We can also get you quotes on an SEF policy endorsement that matches your exposure. Don't wait until you're the next victim of social engineering fraud.

We may be able to help you by providing referrals to consultants, and by providing guidance relative to insurance issues, and even to certain preventives, from construction observation through the development and application of sound human resources management policies and procedures. Please call on us for assistance. We're a member of the Professional Liability Agents Network (PLAN). We're here to help.

THC
THE HARTWELL CORPORATION
Bonds ■ Benefits ■ Insurance ■ Risk Management
AN EMPLOYEE-OWNED COMPANY

1220 Cleveland Blvd. • PO Box 400
Caldwell ID 83606-0400
(208) 459-1678 • (800) 828-7835
FAX 454-1114

1 Airport Plaza • PO Box 51019
Idaho Falls ID 83405-1019
(208) 522-5656 • (800) 243-6344
FAX 524-5721