

News & Views

How many “outsiders” have access to your financial accounts? The answer could be surprising.

Social Engineering – Can Your Employees Be Hacked?

Our physical security initiatives serve to create an “illusion of security”.

We are all familiar with the term “hacker” and we associate hacking with penetrating our computer security to obtain access to our electronic information. To protect ourselves we spend large sums of money on securing our network and our systems. We install firewalls, intrusion detection systems, authentication devices, anti-spam software, anti-virus software and the list goes on. As security vulnerabilities are announced we install the recommended patches within the recommended time frame. We continue to upgrade our security as new technologies become available spending even more money. Yet, we remain totally vulnerable!

A security system is only as strong as its weakest link. Often, the weakest links are people. Organizations are “customer service” driven. Their employees are trained to respond to customers’ inquiries as quickly as possible and without inconveniencing the customer. Yet, do we train our employees in what is considered appropriate versus inappropriate customer response? How do we protect our stakeholders’ information from being released to a third party by an inadvertent but accommodating employee action? Do our employees accept someone’s word over the telephone? Is a callback required when a change of banking, change of name or change of address is requested? Have we trained our employees to be aware of the social engineer?

“Social engineering” is the human side of stealing information or assets. It can be defined as outsiders tricking insiders to perform illicit acts such as allowing inappropriate access to corporate systems or providing proprietary information. Social engineers use influence and persuasion to engage an employee in committing a fraud. An employee unknowingly gives away information in an email, answers questions over the telephone to someone they don’t know, or follows directions to make changes to a stakeholder’s account without verification. It

is not a new concept. It has been inferred that social engineering tactics placed the wooden horse behind the walls of Troy. The social engineer is a “con man” who exploits human vulnerabilities such as an individual’s desire to be helpful.

Social engineering attacks can be computer-based or human-based. Examples of computer-based attacks are email attachments containing malicious software, phishing or a counterfeit pop-up window. Human-based attacks exploit human nature. The information is obtained by asking questions of trusting employees, through impersonation, wandering through premises unescorted to observe employee workstations (looking for the yellow sticky note with the password stuck to the computer), obtaining employment within the organization, dumpster diving and studying the information on corporate websites.

How can the organization protect itself?

Successful social engineering attacks rely on the employees of the organization. Organizations need to create a culture of security through clear and strong security policies and “standard operating procedures” to guard against social engineering. Employees must be trained in recognizing social engineering attacks and trained in the organization’s policies and procedures. Security companies advise that up to 40% of an organization’s security budget should be spent on employee training.

The first step in preventing an attack is “spotting” the attack. Some signs of an attack by a caller are:

- *Caller refuses to give contact information*
- *Caller rushes through the request*
- *Name dropping throughout the conversation*
- *Resorts to intimidation when questioned*
- *Asks “odd” questions*
- *States a senior member in the organization needs the information now*
- *Requests confidential information*
- *Requests changes to confidential information*

...continued on page 2

News & Views

How many “outsiders” have access to your financial accounts? The answer could be surprising.

This list is by no means exhaustive and we recommend that organizations work with security firms that specialize in training employees against social engineering attacks.

Though the telephone is a popular method of gaining “inside” access, it is not the only method used. How many “intruders” are allowed to wander through your organization in a given day? Does anyone question the telephone repairman, computer technician or electrician? How about the well-dressed individual who appears to belong?

Not all Risks Faced by the Organization are Insurable

The organization can suffer a financial loss as a result of a social engineering attack and find itself without an insurance recovery. Money and securities are not covered property under a Property Policy. Employee Dishonesty coverage responds when an employee steals from the organization but not when an employee is used unknowingly as a pawn in the commission of fraud. Errors and Omissions Policies respond to third party financial losses not to first party losses. Since there is no bodily injury or property damage the CGL is not involved.

Only by creating a culture of security and implementing reasonable controls can the organization take a proactive defense against social engineering attacks. Why is this necessary? Because times have changed.