As headlines continue to report cases of ACH, wire fraud, and corporate account takeover with the focus put on the need for enhanced technical controls, the role of the commercial customer—both as a target of cyber criminals and as another line of defense against them—is often lost in the analysis.

Introduction

Protecting and enhancing the value of our information and IT systems has become a central strategic objective in most organizations, second only to making profits. Information security is not just a simple matter of having user-names and passwords. Regulations such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley (GLBA), Basel II, Sarbanes Oxley Act (SOX), Federal Information Security Management Act (FISMA), and various privacy/data protection laws impose a raft of obligations on us. While, viruses, worms, hackers, phish-ers and social engineers threaten us on all sides. Employees sometimes make careless mistakes and open the door to fraud.

An organization’s best defense against cyber fraud is not technology alone; it’s a culture of security within an organization, one that promotes automatic and intuitive behavior in support of information security.

Formal security policies no matter how carefully they are written are of little value unless your customer’s and their employees know about them and understand their obligations. What’s more, there are some security threats for which there are no effective technical controls. Social engineering, for example, can only be countered by broad awareness throughout the organization.

Security awareness is one of the most cost-effective measures an organization can employ to protect confidential information assets. When your customers and their employees are made aware of the risks and how to mitigate them, they take personal responsibility for the information entrusted to them, and a robust security-minded environment naturally occurs.

Components of the Program

With that said, how do you create a Customer Security Awareness Program? Let’s first look at what the Program consists of.

A successful security program consists of: 1) developing an IT security policy that reflects business needs and compliance with regulations, and considers known risks; 2) informing users of their IT security responsibilities, 3) developing awareness material; and 4) establishing processes for monitoring and reviewing the program.
(1) Developing an IT Security Policy
A security policy is the primary way in which your security expectations are translated into specific, measurable, and testable goals and objectives. You have one for your employees, but do you have one for your customers?

The primary purpose of a security policy is to inform your users and customers of those essential requirements for protecting various assets including people, hardware, and software resources, and data assets. Another purpose is to provide a baseline from which your customers can acquire, configure, and audit own their computer systems and networks. This also allows them to develop operational procedures, establish access control rules of their own and various application, system, network, and physical controls and parameters.

If your customer’s computers are protected from threats, this reduces the risk of ACH and wire fraud.

The basic structure of a security policy should contain the following components:
- A statement of the issue that policy addresses.
- A statement about your position on the policy.
- How the policy applies to the online environment.
- The customers’ roles and responsibilities.
- What actions, activities and processes are allowed and which are not.
- What are the consequences of a breach.

(2) Developing an IT Security Policy
Once security policies have been established, they must be disseminated. Another essential part of this process is establishing a record that those involved have read, understood, and agreed to abide by the policy.

(3) Developing the Awareness Education Material
Once your security policy is in place, it’s time to turn your attention to the Customer Security Awareness Program itself. An awareness and training program is crucial because it is the instrument for disseminating information that customers and their users, need in order to remain secure.

What is Security Awareness?
Security awareness efforts are designed to change behavior or reinforce good security practices. The purpose of awareness is simply to focus attention on security. An awareness program is intended to allow individuals to recognize IT security concerns and respond accordingly.

An example of a topic for a customer security awareness program (or awareness material to be distributed) is social engineering. The subject can simply and briefly be addressed by describing what social engineering is, common techniques used to ‘socialize’ individuals, what customers should do to protect corporate and confidential information, and what they should do once they have been targeted. A list of possible security awareness topics can be found at the end of this document.

The basic security awareness material is a core set of terms, topics, and concepts. Once an organization has established a program that increases the general level of security awareness and vigilance, the basic material allows for the development or evolution of a more robust awareness program. It can also provide the foundation for additional training.
Developing the Awareness Model

The awareness material should be developed with the following in mind:

- What behavior do we want to reinforce?
- What skill or skills do we want the users to learn and apply?

The focus should be on specific material that the participants should integrate into their online habits. Participants will pay attention and incorporate what they see or hear in a session if they feel that the material is relevant and developed specifically for them. An awareness and training program can be effective, if the material is interesting and current, as opposed to stagnant.

The first step in building the material is to decide if it will be developed in-house or contracted out. Some key issues to consider in making the decision to develop a program in-house or to outsource include:

1. Do we have the in-house resources to do the job? This includes people with the right skills and enough people to do the work.
2. Is it more cost-effective to develop the material in-house versus outsourcing?
3. Is there a budget in place?
4. Do we have a person on staff that can oversee, refresh and effectively monitor the content?
5. Do we have the necessary resources (e.g., funding and staff with necessary expertise) to maintain the material?
6. Will outsourcing allow us to quickly fulfill compliance requirements?

If your organization doesn’t have in-house expertise and can’t afford to allocate the necessary resources to develop the material and implement the program, you might begin looking at professional organizations, who provide a customer security awareness program for a fee.

Continuous improvement should always be the theme for security awareness initiatives, as this is one area where “you can never do enough.” To ensure that your policies and materials do not become obsolete, you should establish processes for monitoring and reviewing them.

(4) Establishing Processes for Monitoring and Reviewing the Program

Once the program has been implemented, processes must be put in place to monitor compliance and effectiveness. A specific department, such as the security or compliance department, should be charged with the custodianship of your policy and security awareness training program. That department would then be responsible for conducting a regular review and as applicable, updating your security policy and program. The process should include some form of update mechanism so that changes in your organization’s online operating environment or multi-factor authentication technology can be quickly translated into your security policy and awareness initiatives.

A. Evaluation and Reporting

Evaluation and reporting mechanisms are critical components of any customer security awareness program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the reporting mechanism, will validate your compliance efforts to auditors. It is essential to realize that there is no silver bullet for security. Security awareness programs, controls, and policies are only effective in the context of an integrated and comprehensive data security architecture; that is, all access control, risk management, awareness programs, and IT security tools must work in a coordinated, cohesive and coherent fashion. Thus, in order to provide security, it is not enough to simply implement
some security features in an IT system. Real security requires us to holistically integrate risk management controls including processes, and technology together with customer awareness training.

**B. Sample Security Awareness Topics**
A significant number of topics can be mentioned and briefly discussed in any awareness program. Topics may include:

- Password usage and management – including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code
- Spam, and unknown e-mail/attachments
- Web usage – allowed versus prohibited; monitoring of user activity (for your customer’s users)
- Social media security
- Social engineering
- Policy – implications of noncompliance
- Data backup and storage – centralized or decentralized approach
- Incident response – contact whom? “What do I do?”
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
- Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
- Personal use and gain issues – systems at work and home
- Handheld device security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work
- Software license restriction issues – address when copies are allowed and not allowed
- Timely application of system patches – part of configuration management
- Access control issues – address least privilege and separation of duties
- Individual accountability – explain what this means in the organization
- Use of acknowledgement statements – passwords, access to systems and data, personal use and gain
- Visitor control and physical access to spaces
- Desktop security – discuss use of screensavers, restricting visitors’ view of information on screen, battery backup devices, allowed access to systems
- Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form
About InfoSight Inc.

InfoSight’s Customer Security Awareness Program
InfoSight Inc. offers a variety of services to help you develop appropriate policies, implementation tools, controls and monitoring that are aligned with your organization’s overall information security management program objectives. Your Customer Security Awareness Programs needs to be comprehensive and well designed in order to ensure that customers and contractors are aware of their responsibilities to protect valuable information.

Benefit from a policy solution developed by a strong leader in information management and compliance. InfoSight understands information-centric security, and how to make the information itself secure.

InfoSight’s Security Awareness Training Portal
Besides offering a Customer Security Awareness Program, InfoSight also offers formal security awareness training courses that are suitable for particular audiences from users to executive managers on a variety of topics. We also customize material for specific audiences. InfoSight’s awareness and training material can be accessed through a variety of means, including an online portal and all training material is easy to use and scalable for various audience sizes and locations.

InfoSight, Inc. offers proven, affordable Managed Security, IT Compliance and Vulnerability services that protect and optimize how an organization’s critical information is processed, managed and stored. For more than 10 years, InfoSight has served organizations nationwide minimizing risk exposure and providing the highest levels of security assurance and IT regulatory compliance. InfoSight services combine consulting with technology including Perimeter Security & Infrastructure Monitoring Services, Email and Internet Content Services, Data Leakage & Data Privacy/ Policy Enforcement Services, IT Risk Assessment & Compliance Consulting, and Enterprise Network Implementation Solutions. For more information, visit www.InfoSightInc.com or contact us at 305-828-1003 x101.

For more information on our Customer Security Awareness Program, and/or security awareness training portal, contact 305-828-1003 x101 today, or visit www.InfoSightInc.com.