The Business Need for Information Security and Privacy Education

by Rebecca Herold, CISSP, CISM, CISA, FLMI ***July 2006***

Your personnel hold the security and privacy of your company information in their hands; both figuratively and literally. Businesses depend upon their personnel to handle their valuable data responsibly and securely. Without effective personnel education, businesses face significant negative business impact and even possible business failure from the consequences.

There are many compelling reasons for businesses to implement an effective information security and privacy education program—three of particular significance include:

- Growing numbers of laws and regulations require information security and privacy education.
- Personnel must be educated to understand how to effectively follow the procedures that support the privacy promises.
- Education will help to reduce the insider threat of personnel committing computer crime and disruption.

Organizations must know how to create an effective education program, deliver the program, and target groups who need specialized training and awareness to protect their business by improving personnel knowledge.

Meet Legal and Regulatory Requirements

There are a growing number of laws and regulations that require, either directly or indirectly, businesses to implement formal information security and privacy education programs. Lawmakers recognize the importance of educating personnel about how to properly protect data as evidenced by the laws that include requirements to educate personnel on how to securely handle personal information.

A few of the laws that include some type of information security and privacy education requirements include:

- Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA)
- European Union Data Protection Directive
- Japan’s Personal Information Protection Law
- U.S. 21 CFR Part 11 (Electronic Records/Electronic Signatures)
- U.S. Fair Credit Reporting Act (FCRA)
- U.S. Federal Information Security Management Act (FISMA)
- U.S. Gramm-Leach-Bliley Act (GLBA)
- U.S. Health Insurance Portability and Accountability Act (HIPAA)
- U.S. Sarbanes-Oxley Act (SOX)

The Organization for Economic Cooperation and Development (OECD) Privacy Principles, which serve as a framework for the majority of data protection laws throughout the world, stress the importance of education for ensuring the privacy of personal information. Judgments and consent orders specifically require organizations to establish formal information security and privacy training and awareness programs.

> An SQL attack was conducted on Petco in June 2003. The attacker was able to read clear-text credit card numbers stored in Petco's database. The FTC consent order required, among other things, that Petco must not misrepresent the extent to which it maintains the privacy and security of personal information. It ordered Petco to establish, implement, and maintain "a comprehensive information security program that is reasonably designed to protect" the security of consumer personal information that included a formal information security and privacy training program. Petco also must obtain an assessment that the program and training is reasonable from a qualified independent third party biennially for 20 years. Petco must also provide copies of the assessments, including training materials, to the FTC within 10 days of each assessment.

Having a formally documented information security and privacy education program that is clearly supported from executive management helps to demonstrate your organization's due diligence for reasonably protecting personally identifiable information (PII). It is also much less expensive for your organization to invest in an effective information security and privacy program than it is to pay for 20 years of expensive ongoing consent order compliance activities following the aftermath of an incident that could have been prevented with proper awareness.

Prevent Mistakes and Actions Based Upon Lack of Knowledge

Mistakes happen during the course of business. Actions are often performed by workers with good intent, but result in devastating consequences, just because they did not know any better.

> On March 30, 2006, the Connecticut Post reported that the Social Security numbers of 1250 teachers and school administrators in the Connecticut Technical High School System were mistakenly sent via email to "the system's 17 principals...to inform them about a coming workshop. The file with the Social Security numbers was attached to the email by mistake…At least one principal...then forwarded the email to 77 staff members without opening the attachment containing the Social Security numbers."

You cannot expect your personnel to protect company information if you do not communicate effectively with them about how to protect the information. The greater awareness personnel have about information security and privacy, the more securely they will handle PII and other sensitive information, reducing the likelihood of mistakes and actions that put PII and your business at risk.

Your organization cannot protect PII and other mission-critical data without ensuring all your personnel:

- Understand their roles and responsibilities for protecting the information as part of their job
- Understand your organization's information security and privacy policies, standards, procedures, practices, and expectations
- Possess the knowledge enabling them to protect the information and related technology resources for which they are responsible

People are the weakest link in your information security and privacy program. The key to actually attaining a reasonable and appropriate level of security and privacy is educating your personnel. An efficient enterprise-wide information security and privacy education program is critical to ensure your personnel understand their information security and privacy responsibilities, then to appropriately use and protect the information resources entrusted to them.

> Without effective information security and privacy education programs, incidents will occur that could have a devastating impact to your business.

Prevent Deliberate Fraud and Disruption

Trusted insiders can do bad things with the information that they are authorized to use. Your authorized users are, and will always be, a threat to the information to which they have access.

> On May 25, 2006, Computerworld reported that a former Red Cross worker allegedly used the information to which she had authorized access, including names, Social Security numbers, and birthdates, to open credit card numbers using their names and then go on shopping sprees. As of the report date, at least four people had been confirmed as being victims in this identity/credit card fraud incident.

> The U.S. Department of Justice site reported on March 1, 2006 that a systems auditor who had access to place software on the computer he was auditing "used that access on numerous occasions to view his supervisor's email and Internet activity as well as other communications, and to share those communications with others in his office. Kwak carried out his crime and invaded his supervisor's privacy for personal entertainment; there is no indication he profited financially from his actions." The auditor pleaded guilty and "faces a maximum penalty of five years in prison and a fine of $250,000 for the crimes to which he pled guilty."

Providing ongoing awareness and training for information security and privacy will help all your personnel not only know what they should be doing but also know how to identify when others they work with are doing something wrong. Establish, and consistently enforce, sanctions for policy non-compliance. Doing so will help to dissuade at least some potential crooks.

> For more statistics and information about insider threats, see the joint CERT/CC Carnegie Mellon University and U.S. Secret Service insider threat studies at http://www.cert.org/insider_threat.

Use actual examples within your awareness messages and training content to get your messages across even more effectively.

> 🕮 You can find more actual examples of insider threat incidents in my blog, http://realtime-itcompliance.typepad.com/.

Target Training and Awareness Messages

Education must be ongoing, delivered in multiple ways, and tailored to different groups within your organization. Training and awareness content for target groups must be specialized for the specific issues that they need to understand as it relates to their job responsibilities.

Some training and awareness should be given to all your employees. You also need to have different training and awareness content and information for specific target groups to directly address their job responsibilities. You need to identify your target groups based upon your own unique organization, environment, industry, and regulatory requirements. The following list highlights potential target groups to include:

Executive management

Legal personnel

Mid-level managers

IT personnel

Marketers and sales representatives

Physical security personnel

Research and development personnel

Internal audit personnel

Public relations personnel

Human Resources personnel

Information security and privacy personnel

Third parties (vendors, outsourced companies, and so on)

Physicians and medical providers

Trainers

Customer service and call center personnel

For example, the type of information you could cover within customer service and call center awareness and training materials includes:

How to respond to customer privacy and security concerns and complaints

Customer security and privacy compliant procedures and forms

Identity validation methods

How to identify social engineering

How to identify fraud attempts

Who to contact when an incident is reported

How customers can opt-in and opt-out

Customer opt-in and opt-out procedures

How to give access to customers' corresponding PII

How to update incorrect customer information

Invest Adequate Resources in Privacy Education

There are many business benefits of an effective information security and privacy education program. Unfortunately, many businesses do not invest nearly enough time, effort, personnel, or resources to their information security and privacy education efforts—and even more alarming, most do not allocate an information security and privacy education budget at all.

> ✎ According to the 2006 Deloitte Global Security Study, less than half of organizations allocate a budget specifically for information security and privacy awareness and training activities.

Take time to create an effective education program, and realistically determine the budget you will need to fulfill the program. The investment will be small compared with the impact of incidents, penalties, and judgments that can occur without an effective education program.

Your Business Needs Information Security and Privacy Education

There are many convincing benefits for establishing an effective privacy education program that is built around your business processes and goals and addresses your unique business challenges:

- Reducing numbers of privacy and security incidents
- Preventing privacy and security incidents from occurring
- Motivating personnel to do the right thing during the course of performing their business responsibilities
- Making personnel aware of the risks involved with handling PII and, in turn, having them work in a more secure manner
- Retaining customers who can see the business is protecting their personal information
- Demonstrating due diligence within business activities where personal information is handled, stored, and accessed
- Ensuring business partners and outsourced businesses appropriately protect the data that your organization has entrusted to them
- Meeting legal and regulatory compliance requirements for appropriate awareness and training
- Meeting the organization’s privacy policy and other contractual obligations and promises
- Strengthening personnel trust and confidence in your organization management and leadership

The bottom line is that organizations must have an effective information security and privacy education program. Not only do laws require it, but it demonstrates due diligence and helps reduce the number of costly incidents and fraud.