FEATURE

The Benefits of Information Security and Privacy Awareness Training Programs

In today's world of hackers and identity thieves, there is an underlying need for every government and commercial organization/business to have an awareness training program for both information security and privacy, either separate or combined. Information security and privacy regulatory requirements vary by country, but there is commonality in purpose and benefits.

The reasons for an awareness program are many, and they include regulatory mandates, ethical considerations (particularly in the handling of personal information), and basic best practices to protect enterprises from potential threats and unnecessary risk (e.g., financial, public image). The key to having a good information security and privacy program is to practice good behavior in the work and home environments.

Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL V3, PMP
Is a senior consultant at Coalfire-Federal with more than 19 years of experience in information security and privacy. Wlosinski has been a speaker on a variety of IT security and privacy topics at US government and professional conferences and meetings. He has written numerous articles for magazines and newspapers, including articles for the *ISACA® Journal*.

There are three basic awareness program perspectives: regulatory, business and personal. The information that follows identifies how an information security and privacy awareness training program benefits the organization, the individual and employees.

Regulatory Benefits

Information security and privacy laws and regulations are put in place to protect a nation's citizens and because not protecting data can severely affect the organization. Regulatory requirements benefit the organization in the following ways:

- **Shows compliance with information security laws and regulations**—Having an information security awareness training program provides proof that the organization is in compliance with the law. This type of training is normally required for all employees, but there can be custom courses for executives.
- **Supports privacy laws and regulations**—In-house courses can provide custom privacy awareness training to support the government's regulations. Examples of the information that requires protection include personally identifiable information (PII) and protected health information (PHI).[1] This type of training can not only educate employees who directly work with the information, but also those who are exposed to it. One of the concerns every organization has is insider threats. To heighten the level of awareness, the training would include negative outcomes to the organization (e.g., fines of US $5,000 for each offense, or four percent of the organization's annual worldwide turnover) and the personal ramifications of misuse (e.g., loss of job).
- **Protects employees' data**—If security and privacy programs were not in place, no one's information would be safe. If the data were

© 2019 ISACA. All rights reserved. *www.isaca.org*

accessed by criminals, they could find ways to take money, assume the victim's identity, blackmail the victim and their family, and more. Every organization where a victim applied for a job or worked stores personal information about potential applicants and current employees in their human resources (HR) systems, and those systems need to be protected.

- **Safeguards the organization's sensitive data**—An information security awareness system can include instructions about the handling of classified, secret, proprietary and sensitive information.[2] Special data handling instructions can be incorporated into the training to address media labeling, information storage and other protective measures.

Benefits to Business Organizations

Having an on-demand information security and privacy awareness program (or two) in a business has many benefits, including:

- **Establishes organization policy and program**—It is a best practice for an organization to have an information technology security awareness program. Awareness teaches staff about management's information security strategy, goals and objectives, and it supports and promotes management's commitment to protect the organization.
- **Establishes a secure environment**—An organizational commitment promotes good information security practices at work (e.g., proper disposal of credit card applications, patient data). A secure environment not only protects the organization where an individual works and its sensitive data, but it teaches the importance of denying access to the organization's information to unauthorized personnel.
- **Establishes a common security posture**—A common posture includes:
  - Defining the organization's information security and privacy policies that lay the foundation for regulatory compliance
  - Providing commonality and standards among a diverse organizational culture
  - Providing a starting point for the ongoing improvement of the awareness program and practices because the threats keep evolving and criminals adapt to countermeasures
  - Training new hires and the uninformed about security and privacy threats, risk and concerns (because employees may not have prior knowledge about the threats)
- **Provides point of contact information**—Having contact information in the training program is important so that people know how to react in an emergency response situation. Points of contact should include:
  - Incident response team (IRT), which is responsible for information security incident response and handling
  - Chief information security officer (CISO), who is responsible for enterprise policies and procedures, and the staff who support it
  - Privacy officer (PO), who is responsible for privacy policy, procedures, processes, standards and privacy incident response
  - Help desk personnel because they know what to do in the event that a machine or the network is having problems or is acting unusual or erratic
  - Building security, because it would inform employees of protective measures and procedures related to the building, the people and the working environment
- **Identifies types of sensitive data**—In some organizations, there are levels and types of data sensitivity. Classified, confidential, intellectual and proprietary data require a higher level of vigilance and stronger protective controls. Privacy-related data require quicker reporting and could mean the difference between an organization going under or surviving in this competitive world.
- **Highlights the concerns of mobile media**—The course could provide information about installing encryption on mobile media (e.g., discs, thumb drives) and defining best practices on how to keep media safe. Protective controls include

© 2019 ISACA. All rights reserved. *www.isaca.org*

not taking sensitive information out of the office and not copying the data to remote computing devices.

> "EMPLOYEES SHOULD SHARE THEIR KNOWLEDGE AND EXPERIENCE WITH COLLEAGUES IF THEY SEE WEAKNESSES OR LAPSES IN SECURITY."

- **Identities theft prevention practices**—If an enterprise handles people's social security numbers, addresses, dates of birth or medical information, it has the very important responsibility of protecting that data. An awareness course can tell an employee how to protect printed information within his or her working area and around others. Additionally, employees should share their knowledge and experience with colleagues if they see weaknesses or lapses in security.
- **Provides data sanitization instructions**—Training can enlighten employees to the fact that the data can exist on discarded computer equipment, mobile storage devices and hard copy reports. The training program can also tell employees how to handle the data and who to contact should they need to discard or destroy the information (locally stored, replicated, extracted or backed up).
- **Protects the organization's reputation**—Awareness reinforces the organization's efforts and procedures to protect the data, which, if not implemented, could lead to public embarrassment, reduced stock value, loss of market share or worse. Bad security and privacy practices can cause the organization to fail because of lost corporate secrets, the mishandling of personally identifiable information (PII), security breach notifications, cyberblackmail or lost revenue from the unavailability of the organization's Internet services, to name a few.
- **Provides organizational recognition**—An awareness program can be recognized as a best practice among other organizations. An excellent program can earn awards and notoriety among peers from organizations such as the US Federal Information Systems Security Educators' Association (FISSEA).[3] They have annual conferences where new and best practices are demonstrated.
- **Provides links to other information**—An awareness training program can contain URLs/links to helpful information such as the organization's policies, emergency response and handling procedures, guidance, standards, and regional and business contingency plans.
- **Identifies risk and threats to the business**—Some examples of this include:
  - An awareness program can inform employees that the organization's information is always at risk from various localized threat actors, such as a malicious network administrator, an insider, a visitor, and possibly friends and family.
  - Other organizations, such as foreign governments, criminal organizations, criminals and identity thieves, can also be threats that increase the risk to the organization.
  - An awareness program can provide information about how the organization enforces protective controls against the threats from malicious acts and negligence via processes, procedures and technology.
  - Awareness combined with vigilance helps reduce the threat of an insider attack and the theft of computing equipment, mobile data storage media and hard copy information.
  - Employees' awareness of the security ramifications of misusing the most powerful computer (i.e., the human brain). Instilling and promoting security is up to users and everyone around them.
  - Highlights the risk scenarios associated with poor security and privacy practices, and it discourages these bad practices. By teaching staff to protect their work, the enterprise is discouraging malicious behavior such as selling secrets and PII.

© 2019 ISACA. All rights reserved. *www.isaca.org*

- Recognizes when there is the potential risk of losing current, potential and past employee and customer information (e.g., PII and protected health information [PHI]). Loss of the data can be costly to the organization both financially and in reputation. The worst-case scenario is business closure.
- In financial institutions, there are business and personal risk factors associated with customer account information. Identity thieves have many ways to exploit loan, savings, checking and money market accounts and credit information. Tax information can also be exploited by malicious individuals for fraudulent purposes and monetary gain.

> "AN ORGANIZATION'S AWARENESS PROGRAM CAN TEACH EMPLOYEES HOW TO IMPROVE SECURITY AND PRIVACY IN THEIR PERSONAL LIVES."

Personal and Employee Benefits

An organization's awareness program can teach employees how to improve security and privacy in their personal lives. Security awareness can have a positive effect on employees, their families, friends, neighbors and homes. Having an awareness that vulnerabilities exist in wireless portable computing devices, home networks and mobile computing devices (e.g., smartphone, laptop, computer tablets) provides people a base from which to implement protective controls. Some benefits include:

- **Legal**—There is an awareness that individuals can be held personally liable for the mishandling of personal and sensitive data at work. Penalties vary by organization.
- **Ethical**—Individuals can be taught the ramifications (e.g., fines, jail time) of pirating software such as music, games and videos.
- **Employment status**—Not following security policies can cause employees to get reprimanded and/or penalized, even fired. It is everyone's responsibility to protect the organization and the data it acquires.
- **Mentoring**—By learning about the organization's regulatory compliance requirements (and the law), employees can become more law-abiding and can be mentors to others. Information that can be shared with others includes how to avoid email and phishing scams, tricks used by cyberpredators, personal safety practices, preventative and reactive action to take in a cyberemergency, and more.
- **System access**—An awareness program can inform users about the system access rules and guidance related to password strength, length, composition (i.e., combination of characters), number of attempts allowed, entry duration, etc. Access controls not only apply to the devices that are used, but also to network devices. The access training received at work should be taught to those in the household to help prevent intrusions to personal information and the home/family environment.
- **Computer weaknesses**—An awareness course can teach users about vulnerabilities in personal mobile computing devices and desktop computers and the need for software patches and upgrades.
- **Social media**—Social media software applications (e.g., Facebook, Twitter, Skype, LinkedIn, blogs) can expose users to a variety of malicious threats such as identity theft, cyberbullying, kidnapping and more. An awareness course can teach people what not to put into the public domain that can be used against them.
- **Family activities**—Information security awareness and data loss prevention training obtained at a place of employment can be used to mentor the employee's family and to prevent the misuse of information about the family's habits and routines. If misused, the information can provide burglars an opportunity to enter a home and take valuables.

© 2019 ISACA. All rights reserved. *www.isaca.org*

Conclusion

The human brain is the most complex computer, and individuals are in charge of educating it. It is very important that the brain be aware of what it can and should do to protect the organization, the individual, the home and everyone around them. Remember that everyone can be affected by one person's actions or lack thereof. Investing in developing and implementing a security and privacy awareness program that covers the topics discussed not only helps to protect the organization and the data, but can help people and trading partners as these best practices are spread.

There are many organizations that can be found on the Internet that provide security and privacy awareness training. Three publicly available organizations that provide good information security awareness material and programs are the SANS Institute,[4] Stay Safe Online[5] and the International Information System Security Certification Consortium (ISC)[2] Safe and Secure Online.[6]

Endnotes

1. Wlosinski, L.; "Key Ingredients to Information Privacy Planning," *ISACA® Journal*, volume 4, 2017, *www.isaca.org/Journal/archives/*
2. Wlosinski, L.; "Data Loss Prevention—Next Steps," *ISACA Journal*, volume 1, 2018, *www.isaca.org/Journal/archives/*
3. National Institute of Standards and Technology, "Federal Information Systems Security Educators' Association (FISSEA)," USA, *http://csrc.nist.gov/organizations/fissea/home/index.shtml*
4. SANS Institute, *https://www.sans.org/security-awareness-training*
5. StaySafeOnline, *https://staysafeonline.org/ncsam/*
6. International Information System Security Certification Consortium, Safe and Secure Online, USA, *https://safeandsecureonline.org/*

© 2019 ISACA. All rights reserved. *www.isaca.org*