Building a Case for IT Security Awareness: Best Practices for Increasing Impact and Promoting Cultural Change

Ellen Roth-Perreault, SPHR, GSLC

Abstract – Since the Federal Information Security Management Act (FISMA) was signed into law in 2002, Federal agencies have struggled to establish agency-wide information security programs that meet baseline requirements for protecting information assets. Since the government performs important missions that require the storage and use of sensitive information, implementation of FISMA's provisions and establishment of program cohesiveness is essential.

During the last three years, agencies have experienced serious security incidents that have left the public questioning the security of data. Though organizations continue to spend money on technology and software, technology solutions are not the complete answer. As incidents rise, the government must recognize the impact that human factors have on IT security, and support IT security awareness programs appropriately as value-added cultural change components of the IT security program.

This paper presents five best practices that agencies can use to rethink traditional awareness program structure. Using these practices, agencies can develop programs with messages and content that create positive behavior change within the workforce, and make a clear case for the value of awareness programs.

Index terms – Security Awareness, Cultural Change, IT Security

I. Introduction

It is common knowledge that the Federal government has experienced challenges establishing agency-wide information security programs that adequately safeguard information assets. Since the government established Title III of the E-Government Act of 2002 (H.R. 2458/S. 803), entitled the Federal Information Security Management Act (FISMA), agencies have struggled to meet the baseline requirements that will reasonably ensure the security of our government's information. Auditing organizations such as the Government Accountability Office (GAO), agency Inspectors General (IGs), and Congress have examined agency progress each year, citing widespread deficiencies across all agencies, as well as those items that individual agencies must address. With government agencies providing critical services from veteran healthcare to national defense, agencies process, access, and store vast amounts of sensitive data. Overall, the government has some of the most extensive requirements for protecting the confidentiality, integrity, and availability of data, and bears great responsibility for security of a large public constituency's information.

II. Recent Security Incidents Within the Federal Government

It is also no secret that in the last three years, agencies were a part of several widely-publicized security incidents. One of the most jarring occurred on May 3, 2006, when the Department of Veterans Affairs (VA) was involved in a critical event in which an employee's personal laptop and external hard drive were stolen from his residence. The hard drive contained privacy data of over 26 million veterans—data which could easily be used for identity theft, and should absolutely not have been in public hands. The incident revealed the perils of having unclear or fragmented data security policy. It also revealed the confusion that can occur when employees do not have a full understanding of incident reporting procedures and the grave damage that security breaches can have on an agency's reputation.

Realizing that data security incidents are by no means limited to the VA, the Committee on Government Reform required all agencies to submit the details of security incidents involving the loss of sensitive information since January 1, 2003. The Committee issued a report [1] in October 2006, revealing several startling facts, the most alarming of which is that all 19 Departments and agencies had at least one data security incident since January 1, 2003. The report details incidents in which across government, thousands of laptops containing agency data

Ellen Roth-Perreault is an IT security workforce development, training, and awareness consultant for the worldwide firm Booz Allen Hamilton. Throughout her career, she has consulted on workforce issues to Federal agencies. She holds a M.A. in Organization Development from Marymount University, and is interested in applying change management principles to Federal IT security program development.

have been stolen, and thousands of records containing personal information such as social security numbers have been compromised. The Committee report also cites that "only a small number of the data breaches reported to the Committee were caused by hackers breaking into computer systems online. The vast majority of data losses arose from physical thefts of portable computers, drives, and disks, or unauthorized use of data by employees." This point clearly supports the widely-held belief that the human factor is the weakest part of an agency's information security equation. It also demonstrates that the scope of Federal security policy and programs must expand to accommodate the fact that data is not simply resident on networks. Data is transported everywhere individuals go.

A. Security Awareness: A Question of Priority

Although improving the ability of employees to avoid and respond to situations in which security can be breached has been discussed as a way to reduce the number of agency security incidents, human factors have not consistently received the funding or attention necessary to make significant, sustained improvements. A *CSO Magazine* research report [2] from 2003 demonstrates this fact: "When asked what their organization's security management priorities were for the coming year, respondents listed training/educating employees (72%), assuring business continuity (68%), disaster recovery (68%), enforcing security policy (65%) and assessing risk (61%), in that order. When asked about spending priorities, CSOs said they would invest in security software (38%), services (21%) and security hardware (14%) in 2003." In this example, there is a clear conflict between the priorities expressed by executives, and where money is channeled.

A *CIO Magazine* report titled "The Global State of Information Security 2006" reveals that the importance of security awareness may be declining. In 2005, when survey respondents were asked to list their priorities for the year, employee awareness programs ranked number two. In 2006, employee awareness programs ranked tenth, tied with efforts to monitor compliance with security policy [3]. The number two priority in 2006 was network firewalls, followed by application firewalls—very different solutions than trying to influence employee behavior. Data from recent GAO reports suggests that the Federal government may have decreased its emphasis on employee awareness as well. The March 2006 report "Federal Agencies Show Mixed Progress in Implementing Statutory Requirements" states: "In their FISMA submissions for fiscal year 2005, agencies reported that they provided security awareness training to the majority of their employees and contractors. However, while 19 agencies reported that they had trained more than 90 percent of their employees and contractors in basic security awareness the overall percentage of employees trained among the 24 major federal agencies reviewed dropped from 88 percent in 2004 to 81 percent in 2005, a level almost equal to that reported in 2003" [4].

B. Measuring Security Awareness Program Effectiveness

With the data that is available, it would be nearly impossible to correlate the increase of serious data security incidents to the decline of the importance and implementation of security awareness training. It is curious, however, that the technology solutions that have taken priority over people-centered initiatives solutions have not provided fool-proof value.

Establishing effectiveness metrics for security awareness programs is difficult since awareness programs seek to change the behavior and attitudes of the entire workforce. The cause of human behavior is much more difficult to isolate because humans are influenced by a variety of factors. Measuring whether an employee understands basic IT security principles at the end of an annual awareness course—the traditional method of measuring awareness—barely scratches the surface of whether an employee is better equipped to perform responsibly in the workplace. A better measure of the likelihood that responsible behavior will result from awareness activities is whether employees understand the importance of IT security to the organization, can relate to IT security as an organizational component that enables their ability to perform their duties, and can translate this understanding to performing responsible IT security behaviors in the workplace. Understanding IT security principles at this level shows that cultural change is occurring.

III. Best Practices in Establishing Value-Added Security Awareness Programs

The remainder of this paper focuses on five best practices that security awareness program administrators can use to build more meaningful, contemporary awareness programs that assist organizations in achieving cultural change. By implementing these practices, security awareness personnel will be able to reenergize the mission of security awareness programs and demonstrate the strategic value of awareness initiatives, while building true understanding within the employee community.

A. View Awareness as a Cultural Change Mechanism

Security awareness programs have the ability to positively shape organizational culture if program leaders understand the components of organizational culture and use awareness program initiatives in a manner that will

drive messages into the heart of the organization. Often, the goal of "cultural change" is as an abstract notion. However, organizational culture is composed of several components. By understanding each component or level, security awareness professionals can transform the way in which they view their mission and how they develop awareness messages.

An organization's culture can be thought of as its personality or attitude. Just as an individual's attitude affects his dress, speech, and priorities, an organization's attitude is expressed by artifacts, norms, values, and assumptions. The four layers that make up an organization's personality can be described as follow, according to Thomas Cummings and Christopher Worley's model [5]:

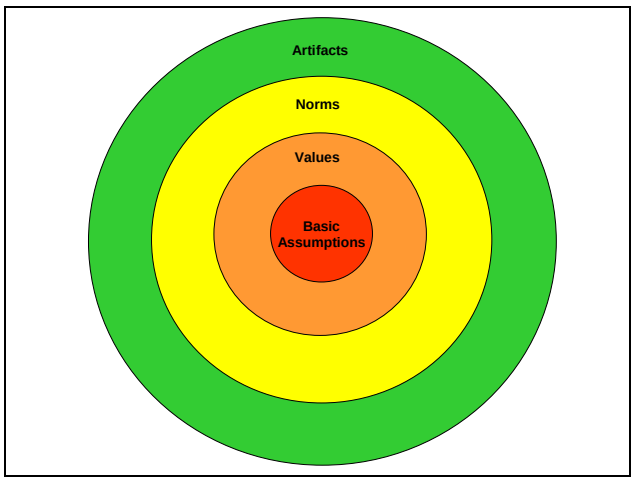

Figure 1: Cummings and Worley's Model of Cultural Layers

Artifacts: Visible manifestations of an organization's norms, values, and basic assumptions; the most outward expressions. Example: The observable, security-related behavior of an employee.

Norms: Unwritten rules that determine the range of acceptable behavior in an organization. Example: It is ok for me to go out of my way to make processes efficient so that I can serve my customer better. But, it is not ok for me to do this if my actions circumvent security policy.

Values: Core beliefs about what is important in an organization, generally established by leadership. Example: We are a customer-centric business, and our ability to provide service depends on the confidence our customers have in us. Therefore, I will go out of my way to protect sensitive information to ensure the confidence of our customers.

Basic Assumptions: Underlying assumptions that determine how organizational problems are solved based on organizational values. Example: My laptop, containing sensitive data on millions of individuals has been stolen! I need to report this to my Information Security Officer right away, because this violation of organizational security policy is serious!

In a functional organization with a strong culture, routine behavior will reflect the organization's values because basic assumptions are well-established. If there is a conflict between behavior and values, this means that there is inconsistency in the values that are communicated or enforced. Once basic assumptions are embedded within the culture, they are reinforced every day as employees observe other employees and senior executives acting in accordance with the culture.

In an IT security organization, values are articulated through policy, which is set by leadership. Policy articulates the security standards the organization must meet, and specifies the penalties associated with non-compliance. Through ongoing, consistent exposure to policy in various media, the values articulated by policy become basic assumptions. However, without consistent communication of policy and enforcement of expectations, an unreliable culture develops where "anything goes."

Since awareness programs are the communications component of an organization's IT security program, they should be structured to support the mechanics of cultural change. First, awareness program administrators should be certain to tie awareness messages to organizational policy, and to repeat themes within several forms of media—from posters and trinkets, to informational bulletins and events—to drive them into the culture of the organization. Second, visible senior management support is critical to transforming simple messages into expressions of firm values. Consider adding a message from senior leaders at the beginning of annual awareness training, or involving leadership in launching the year's awareness event series. These practices will enhance the effectiveness of awareness programs by demonstrating that the organization not only "talks the talk" of security, but it also "walks the walk." Synchronization is essential to delving beyond the surface and shaping culture.

B. Consider Awareness a Multi-Audience Activity, and Structure Content Accordingly

Although awareness programs are traditionally structured to treat all employee groups the same, awareness program content should be structured with specific employee subgroups in mind. All Federal agencies include senior executives, IT security professionals, and general

employees, each of which can be considered a distinct audience with specific awareness needs. In this context, "awareness" does not just mean being aware of basic IT security principles—it means awareness of current IT security issues that concern the audience. The most obvious example is the awareness needs of IT security professionals. These individuals must be acutely aware of the latest security threats, and of organizational policy. They must also be aware of the hot topics and annual objectives of the agency IT security program. By creating audience-specific awareness content rather than limiting the scope of the agency awareness program to the general user, awareness messages become valuable strategic communications that enable IT security program execution.

C. Put General Awareness Message in a Useful, Recognizable Context

Though there are individuals with needs beyond the bounds of traditional IT security awareness programs, most employees are functional experts in fields outside IT security. Annual awareness training, awareness program activities, and program materials are usually the only way that employees come into contact with the organization's IT security office.

Security awareness program administrators should keep this in mind when developing ideas and content. For messages to "stick" they must be demonstrate how following good IT security practices will make an individual's job easier, or will prevent a negative consequence. For example, if an organization is composed primarily of scientists, a useful awareness program communication may provide tips for protecting data gathered through countless hours of research. In reality, the same practices of backing up information and not transporting sensitive data outside of the organization are as important to researchers as to other personnel. It is the way in which the message is packaged that establishes a clear relationship between the IT security best practice and the individual. If messages are personal and relevant, they are more likely to translate into action and be internalized as values.

D. Incorporate Contemporary Topics to Keep Content Fresh and Useful

The other way in which content can be made more relevant is by ensuring that it is contemporary. A recent Darkreading.com article [6] emphasizes the importance of refreshing content rather than discussing the same security concerns every year: "In general, our readers didn't find our stories about Windows vulnerabilities, lost laptops, NAC, or HP pretexting to be as interesting [as 2007 content]…. Could it be that [they] actually want to read about something *different* for a change?" The article describes six new threats that face the public, which would be excellent content for a proactive awareness program.

One relevant, timely topic is phishing, which is described by Webopedia.com [7] as "the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has." Agencies have already begun to proactively equip employees with information about how to avoid this new type of attack that can impact not just the agency, but an employee's personal finances as well. As reported by Federal Computer Week [8], the United States Coast Guard mandated that all employees attend phishing awareness training by January 17, 2007.

Newspapers, trade journals, and online sources provide ample information on the latest threats in a language that the general public can understand. Integrate information from these sources into awareness newsletters or bulletins, or use them as interesting content for annual refresher training. Learning will be reinforced each time an individual is reminded of an awareness topic by the media or experiences a related issue at work or at home.

E. Share Organizational Lessons Learned to Highlight the "Big Picture"

As we have seen within the last several years, no matter what, IT security incidents will happen. Since incidents are a given, a smart organization will do everything possible to learn from each incident and build organizational resistance and resilience. Just as the recovery phase of incident handling focuses on tightening procedures and updating system configurations so that the incident is less likely to happen in the future, organizations should take the time to make employees aware of the consequences that particularly challenging incidents caused, and issue tips a general user can use to help avoid similar occurrences. Employees will develop a stronger sense of the "big picture" of IT security, and awareness programs will have the potential to help reduce the number of incidents that occur. Fewer repeat incidents or incidents caused by lack of employee awareness mean an organization has achieved stronger confidentiality, availability, and integrity of information, and that awareness activities have contributed to the ultimate goals of IT security.

IV. Conclusion

Signs point to the fact that financial and organizational support for IT security awareness programs may not currently be as high as for system-level initiatives. Even so, initiatives geared toward human factors are essential for preventing serious incidents that threaten public trust. Developing an effective IT security organization requires cultural change, and change is encouraged through the IT security awareness portion of the program. Awareness programs target improving the ability of all employees to help prevent IT security incidents through exposure to relevant content that shapes behavior and attitudes. The business case for funding and support for awareness initiatives lies in demonstrating that IT security awareness programs add value to the overall IT security program. It can be a challenge to accomplish this quantitatively, but IT security program administrators can implement best practices that shift the perception of awareness programs from one-size-fits-all annual training and generic awareness poster programs, to strategically driven messages designed to enable cultural change. By establishing IT security awareness as a strategic initiative with observable results, the value of well-structured awareness programs will become evident.

V. References

[1] Government Reform Committee, "Staff Report: Agency Data Breaches Since January 1, 2003," October 13, 2006.
http://oversight.house.gov/Documents/20061013145352-82231.pdf
Last Accessed: 27 January, 2007.

[2] Cosgrove Ware, Lorraine, "CSOs Prioritize Security Spending for 2003," *CSO Magazine Online*.
http://www.csoonline.com/csoresearch/report50.html
Last Accessed: 28 January, 2007.

[3] Holmes, Allan, "Security Survey: The Global State of Information Security 2006," *CIO Magazine Online*, September 16, 2006.
http://www.cio.com/archive/091506/security_survey.html?page=1
Last Accessed: 28 January, 2007.

[4] United States Government Accountability Office, "GAO-06-527T: Information Security: Federal Agencies Show Mixed Progress in Implementing Statutory Requirements," Testimony Before the House Committee on Government Reform, March 16, 2006.

[5] Cummings, Thomas G. and Worley, Christopher, Organization Development and Change, Seventh Edition, 2001.

[6] Wilson, Tim. "The Six Dirtiest Tricks of 2006," Dark Reading.com, December 27, 2006.
http://www.darkreading.com/document.asp?doc_id=113460
Last Accessed: 27 January, 2007.

[7] Webopedia.com
http://www.webopedia.com/TERM/p/phishing.html
Last Accessed: 27 January, 2007.

[8] Brewin, Bob, "Coast Guard Mandates E-mail Phishing Training," Federal Computer Week News, December 28, 2006.
http://www.fcw.com/article97216-12-28-06-Web
Last Accessed: 27 January, 2007.