

Skills and the Human Factor: How Smart Organizations are Closing the Employee Information Security Gap

A password written on a notepad compromises an entire network security system.

A helpful customer service representative unwittingly gives a network access code to a malicious hacker.

A company implements a sophisticated firewall, only to have an employee import a virus from home through a CD-ROM.

The scenarios above may sound intimidating, but they are common risks faced by every organization that relies on electronic networks in daily operations. While organizations invest millions of dollars on firewalls and security services, employee abuse or misuse of electronic information remains one of today's most urgent information security vulnerabilities. But there's good news—these risks can be dramatically reduced simply by increasing employee awareness.

Companies and government agencies are recognizing that employee knowledge of best practices is vital to a secure electronic environment. A federal mandate on information security, the White House National Strategy to Secure Cyberspace, underscores the need for what it calls "A National Cyberspace Security Awareness and Training Program."

According to the report, "solutions to cybersecurity issues exist, but the people who need them do not know they exist or...may not even be aware of the need to make a network element secure."* To address the problem, the report outlines several components of an effective awareness-building strategy, including a combination of security education and certification.

ITAA Sponsors Information Security Awareness Certification Program

For IT specialists, information security certification is nothing new. Reputable organizations such as the CISSP, SANS Institute, and CompTIA offer certifications in this area. Unfortunately, most of these certifications are designed for information security professionals, costing up to \$175 per person.

Now, one organization is offering a new type of awareness program—a general awareness certification aimed at every employee who interacts with electronic information. That organization is the Information Technology Association of America (ITAA), one of the largest IT industry associations in the US. Its program, the ITAA Information Security Awareness Certification, combines educational material with online skills measurement and certification to build employee awareness, establish accountability, and achieve readiness.

The ITAA program and study guide (available through online skills measurement provider Brainbench on May 21) provides valuable advantages for building security awareness. First, the program delivers unbiased, objective data about employee awareness. Secondly, it enables a repeatable process that can easily be implemented across the organization. Finally, by combining skills assessment and learning resources, it gives companies a self-contained solution without the risk of corporate "scope creep," at a fraction of the cost of specialized security certifications.

(Editor's note: scope creep applies to the tendency for organizational projects to grow in size and expense during implementation—see subhead below, Vendor-Neutral Program Provides a Cost-effective Solution.)

Online ITAA Information Security Awareness Test Makes Assessment Available to All Employees

At the heart of the ITAA program is an assessment delivered at the employee desktop through an online skills measurement system. Designed to build and measure knowledge across the enterprise, the online assessment system leverages key features for building information security awareness, including:

A Challenging Assessment—The ITAA awareness test covers topics such as computer security, Internet security, passwords, viruses and harmful software, computer ethics, physical security, sensitive information, and ID and data information theft.

Users can take the ITAA test in one session and repeat the test as needed to achieve a passing grade. The secret behind the repeatable test is a Computer Adaptive Testing technology that selects and delivers challenging questions based on the test-taker's answer to previous questions. The test will not waste time with easy questions, nor will it frustrate the user with questions beyond the individual's level of knowledge.

Objective Results—Traditionally, employee skills are measured through subjective means such as self-assessments or supervisor reviews. Reviews and self-assessments, however, are prone to inconsistent results, with no clear standard for determining proficiency across the organization. As a result, decision makers are often left asking themselves, "How do we know what our employees know?"

The ITAA awareness test enables consistent measurement across the enterprise. It is delivered through a common administration and reporting platform, and delivers results immediately after a test is taken. Through a single testing platform that spans the organization, administrators can learn exactly how much employees know about information security and how much needs to be learned.

Alignment with Learning Materials—The truth is, most employees prefer to spend as little time as possible learning about information security. In the ITAA program, every test-taker receives a single study guide that covers all major topics in the security awareness assessment—a refreshingly concise knowledge resource. The result is a program that appeals to non-IT employees, providing a highly cost-effective turnkey strategy for establishing and documenting basic information security awareness.

A Repeatable Process Builds Awareness Across the Organization

One of the primary business benefits of any online assessment and certification program is that it enables a repeatable awareness building process. Companies can offer testing to select employees and then scale the program across the organization as needed. Key components of the awareness-building process include:

Skills Identification—The first task of an awareness program is to identify the key information security issues that employees need to learn. In the ITAA example, information security issues are directly outlined in the reference material and covered on the test. As a result, each participant knows exactly what is expected in the way of information security knowledge requirements.

An online measurement system offers a snapshot of quantifiable skills data. Once a participant feels prepared, he or she can take an assessment online without the burdens of scheduling or company administration. Results are delivered immediately, providing a detailed measurement of skills levels across the organization, including relative strengths and areas for improvement.

Education—An effective awareness building process includes a significant but low-maintenance self-education component. In the case of the ITAA program, a print reference booklet maps directly to the test. Employees can use it to learn what they need to know without burdening corporate learning or training resources.

Analysis and Reporting—With immediate results delivered through an online testing system, companies can track employee skills to identify information security awareness vulnerabilities. Detailed results provide an objective measure of employee readiness, with a consistent rating system for tracking strengths, weaknesses and improvement over time.

Resolution—One of the primary benefits of online skills measurement is that it is repeatable. If a minimum score is not achieved, an employee can simply study the necessary topics and retake the assessment as needed. In the process, the assessment provides both the motivation and learning structure to help the individual improve security skills.

Certification—Once an individual achieves a minimum score in the online information security assessment, a certification is then available. This certification can be an important tool for validating information security readiness to prospective customers and partners.



Vendor-neutral Program Provides a Cost-effective Solution

Past experiences have made many decision makers wary of security strategies that tend to grow in size and budget after their implementation. The classic scenario of project “scope creep” includes a service-intensive implementation followed by timeline issues and subsequent planning that reveals more work to be done.

The advantage of the ITAA program is that it is not a precursor to a vendor service. The online assessment, educational material and reporting system is delivered as an end-to-end vendor-neutral program, providing a self-contained solution that delivers an unbiased view of security awareness across the enterprise. However, companies that seek to deploy additional training resources in a post-assessment phase can do so with a clear picture of organizational strengths and weaknesses, resulting in a significant increase in training efficiency.

Putting Information Security Awareness Into Practice

Companies and government agencies are recognizing the need to build awareness and establish accountability for information security knowledge. Major federal agencies such as the USDA are exploring strategies in these areas, and critical information networks such as those that run the New York Stock Exchange are also turning to a skills-based approach to build information security skills of system administrators.

Using online skills measurement to build awareness is a relatively new approach to improving information security. However, it is an approach that is delivering results, helping organizations track and improve employee awareness with a new level of consistency, objectivity, and ease. The ITAA Information Security Awareness Certification program provides a model example of how online skills measurement can help companies and government agencies improve the information security readiness of employees across the enterprise environment.

* From The National Strategy to Secure Cyberspace,
February 2003. p. 38.
Available at www.whitehouse.gov/pcipb/