Raising Cyber Security Awareness for Healthcare Professionals

An NJVC® Executive White Paper

Robert J. Michalsky

Principal, Cyber Security

November 2013

NJVC

Driven by Your Mission®

I. Executive Summary

Healthcare professionals should rightly be focused on providing quality healthcare services to patients. Does that mean that the industry should ignore a non-related technical topic, such as cyber security? Hardly, if the data breach history captured by the U.S. Department of Health and Human Services (HHS)[1] is any indication. Data breaches are rampant and increasing in size and frequency.

A large percentage of the reported breaches can be traced back to human error. Physical security controls break down because a door is left open. Technical controls break down because a user ID or password is posted via a sticky note on a computer monitor or because account credentials are shared and the task at hand absolutely positively need to be done right now.

Professionals working in the healthcare industry possess a zeal for protecting the health of their patients and improving how that support is provided. No legitimate employee wants to intentionally do something to adversely impact the health of a patient.

Health IT is about promoting the use of IT to support the healthcare mission. Health IT is all about providing high-quality care more efficiently, faster and cost effectively by using software and hardware technologies that have transformed countless other industries. However, these technologies cannot be deployed without considering the potential new cyber risks introduced to an organization.

An obvious manifestation of healthcare IT is the continuing transition from paper-based records to digital health records. But it does not end there, as wireless technologies have enabled medical devices to become extended diagnostic and reporting nodes on an increasingly networked IT infrastructure that shares patient medical records, billing records, financial records and burgeoning software applications—all accessing databases housed in common server structures.

How can this extended enterprise be protected? One approach can be extracted from the Stop. Think. Connect campaign[2] administered by the U.S. Department of Homeland Security (DHS). The intent is not to make everyone a cyber security expert or to unduly raise fear, uncertainty and doubt—the intent is to bring some sense of awareness of cyber security to the general population. The goal of this campaign is to make someone think—even for half a second—before they take action online.

Do you have a secure connection to the server where you are about to input your credit card information? Are you authorized to access the data records you are about to request? Should you

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

[2] http://www.dhs.gov/stopthinkconnect

post personal information online for anyone to see? Simply hesitating to consider your actions before blindly clicking on that link can help prevent obvious human errors from occurring.

The board of directors of a healthcare organization has a myriad of concerns—providing sound patient care, maintaining financial viability and leveraging IT to enhance their operations. Just like healthcare professionals run their departments, the IT infrastructure should utilize cyber security experts cognizant of the constantly evolving threats and mitigating the resultant risks to the organization. As there is never enough budget or staff to throw at a non- mission essential, yet critical, area such as cyber security—how can the board cope?

Raise the cyber security awareness of the overall organization with role-appropriate cognizance of the consequences of individual actions and how easily one click on an inappropriate link can compromise an entire network—ultimately leading to the compromise of personal health records.

What is one effective way to overcome this challenge? Establish a cyber security awareness program.

Creating and operating a cyber security awareness program does not mean transforming staff into cyber engineers able to reverse engineer malware samples. Instead, the intent, like the DHS Stop. Think. Connect. campaign, is to have individuals realize that they play key roles in protecting the **digital** health of patients—just as they play direct roles in protecting the **physical** health of patients.

STOP | THINK | CONNECT™

Further information on what actions an organization should take after an awareness campaign is conducted can be found at: http://www.njvc.com/healthcare/white-papers-and-case-studies/cyber-security-for-healthcare-white-papers.

II. Rationale for a Security Awareness Program

There is a surprising amount of negative commentary on running a cyber security awareness program in the blogosphere and other social media. Comments usually run along the lines of a company becoming complacent or overly dependent on such a program, that employees are human and will continue to fall prey to determined network intruders or that employees should be focused on their healthcare missions—not on cyber security.

Here we can refer to the shared responsibility implied by the DHS If you See Something, Say Something campaign (which actually originated with the New York Metropolitan Transportation Authority)[3]. Suspicious activities of people, email messages or software activities should be reported and investigated by someone with domain expertise. In a shared IT network environment, a suspicious person is anyone who can enable malware to gain a foothold from where it can propagate and ultimately do damage. General practitioners refer patients to specialists all the time … why not the same for cyber-related issues?

A cyber security awareness program should never be considered the ultimate objective. Instead, it should be viewed as a line of defense in a defense-in-depth approach where multiple lines of defense are put in place to protect electronic medical records when created, accessed or transferred inside or outside a healthcare organization's network and those of its suppliers and other interconnected parties.

if you
SEE something
SAY something™
If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

[3] http://www.dhs.gov/if-you-see-something-say-something

III. The Human Threat

Employees represent the weakest link in the security posture of virtually all organizations. That most basic human trait—a desire to help others (without rigorous verification of identity)—has led to numerous account compromises. It is through these account compromises that malicious software is introduced which leads to data breaches.

The Verizon Data Investigations Report for the Healthcare Industry reports that 93 percent of all breaches were caused by malware or hacking techniques.

Why do healthcare organizations need a cyber security awareness program? Let's run through a number of reasons. First, there is the matter of compliance—various laws and regulations that impose the requirements for security awareness training programs. Next, let's evaluate the approach taken by other industries that have experienced cyber attacks much longer than has the healthcare industry.

Compliance

Healthcare is highly regulated, and with the 2010 passage of the Accountable Care Act, those regulations are only increasing. Below are some compliance-related examples that require some type of security awareness program to be put in place.

Standard	Background
HIPAA	The Health Insurance Portability and Accountability Act (HIPAA; passed in 1996) requires a covered entity or business associate to implement a security awareness and training program for all members of its workforce (including management) (Section 164.308 (a) (5)).
PCI	Any organization that processes transactions utilizing a payment card is subject to the Payment Card Industry (PCI) Data Security Standards. Requirement 12.6 (of the Requirements and Security Assessment Procedures) that states that an organization must "implement a formal security awareness program to make all personnel aware of the importance of cardholder data security."
FISMA	The Federal Information Security and Management Act (FISMA) requires organizations that support federal agencies to protect information collected or maintained on behalf of those particular agencies. Any contractors that fall under these applicability guidelines must provide some type of security awareness training to inform personnel of the information security risks of the particular agency and their responsibilities in complying with relevant policies and procedures.

NIST	Founded in 1901, the National Institute of Standards and Technology (NIST) is a non-regulatory federal agency whose mission is to promote U.S. innovation and industrial competiveness. To that end, NIST produces various special publications intended to serve as examples and templates for a wide range of technologies. NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," and contains about 40 pages of content on the components and materials needed to establish, operate and maintain a high-quality security awareness program. This document provides detailed guidance that ensures FISMA compliance.

Best Practices

Many industries and professional organizations also support security awareness and training programs in an indirect manner by requiring various certification credentials be obtained. Certification is a standard methodology for conducting business and ensuring that professionals have a minimum baseline set of knowledge and skills. Obtaining and maintaining these credentials typically involve an ongoing education component, with professional credits obtained every year to maintain current certifications.

SANS – Securing the Human	The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. Its Securing the Human[4] initiative is aimed at changing user behavior and reducing overall security risks. The SANS Institute features certified instructors who are true subject matter experts and a rigorous updating of course curriculum. The institute also offers newsletters, posters and screensavers emphasizing its mission.
ISC$^{(2)}$	ISC$^{(2)}$[5] is a global non-profit organization that provides vendor-neutral education products, career services and gold-standard credentials to professionals in more than 135 countries. It has built an elite network of nearly 90,000 certified industry professionals worldwide.
DoDD 8570	Department of Defense Directive (DoDD) 8570 provides guidance and procedures for the training, certification and management of all government employees who conduct information assurance (IA) functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. Any full- or part-time military service member, contractor or local nationals with privileged access to a DoD information system performing IA (security) functions—regardless of job or occupational series—are required to have one or more of these certifications.

[4] http://www.securingthehuman.org/

[5] https://www.isc2.org/default.aspx

HITRUST	HITRUST[6] is an organization that in collaboration with healthcare, business, technology and information security leaders established the Common Security Framework (CSF)—a certifiable framework that can be used by any organizations that create, access, store or exchange personal health and financial information. The CSF is an information security framework that synchronizes the requirements of existing standards and regulations, including federal (HIPAA, HITECH), third-party (PCI, COBIT) and government (NIST, FTC). HITRUST requires its assessors and practitioners to attend training updates annually to maintain their designations.
CMMI	Capability Maturity Model Integration (CMMI) is a process improvement training and certification program and supporting services administered by Carnegie Mellon University. Attaining Level 4 means processes are being measured and controlled. Level 5 is process improvement through feedback and optimization. While neither of these levels mandates a training program, implementing one can bring uniformity to the engineering process and allow measures, such as cyber security awareness, to be generated from user surveys.
ISA	The Internet Security Alliance (ISA) is an industry trade group seeking to demonstrate thought leadership by: 1. Advancing the development of sustainable systems of cyber security 2. Advocating for public policy that will advance the interests of cyber security 3. Creating increased awareness and programs that will result in more rapid adoption of cyber security standards, practices and technologies. ISA has published a number of reference sources. One of its recommended practices is to conduct periodic security awareness training.

[6] http://hitrustalliance.net/

Healthcare-Related Certifications

Health IT	Health IT Certification[7] provides professional training and certification for those responsible for planning, selecting, implementing and managing electronic health records and other health IT; those engaged in the creation and management of health information exchanges); and those responsible for the technical and business operations implementation of the Affordable Care Act operating rules.
ISC$^{(2)}$	ISC$^{(2)}$'s new HealthCare Information Security and Privacy Practitioner (HCISPP^{SM}) credential is designed to ensure that practitioners have the foundational knowledge, skills and abilities to protect and keep vital healthcare information secure. HCISPP is ideal for individuals who implement, manage or assess security and privacy controls that address the unique data protection needs of healthcare information.

By requiring various certifications, these organizations not only establish a professional baseline for individuals to enter the field, through the maintenance requirements, they ensure that individuals must undergo annual training to accumulate continuing professional education credits and remain current with the fast-moving landscape of cyber security topics.

Certified professionals typically need some type of continuing education credits in order to maintain their professional standing. Designing, documenting or conducting cyber security awareness programs can count towards this objective. In addition, those sessions allow the educated employees to also gain professional credits—another incentive to attend and participate. As these individuals need continuing education credits to maintain their certifications, it can be argued that a best-practice approach is to educate employees on a regular basis to ensure the organization is improving its cyber security program processes. **Cyber security is not a product, but a process.**

Beyond requirements to do so from a compliance standpoint, the reasons to conduct security awareness programs are:

- Fulfill compliance requirements
- Reduce an organization's risk profile
- Support defense in depth
- Support the implementation of sound security controls

Compliance alone does not equate to sufficient security. It should be considered a base—or starting point—at which to establish a more robust set of controls.

[7] http://www.healthitcertification.com/

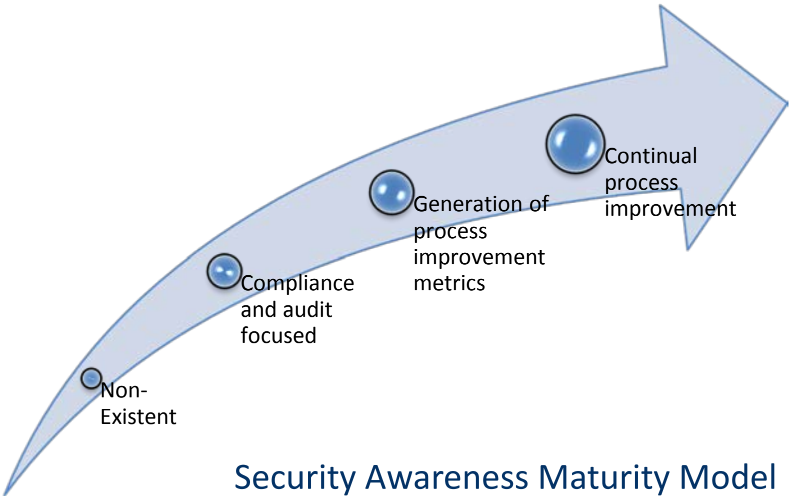
Just as the concept of performing continuous risk assessments can lead to a reduction in an IT operational risk profile, so can conducting ongoing security awareness activities lead to greater staff awareness of evolving cyber threats and new mitigation techniques, and the latest best practices and policies.

IV. Security Awareness Program Essentials

The entire security awareness program can be thought of as series of activities to improve processes that can mature over time into a program that meets the explicit needs of an organization.

Success Metrics

Measurements are useful to assess the maturity of a security awareness program. They can also be used to drive some sense of precision into an often-ambiguous program.


Non-Existent
Compliance and audit focused
Generation of process improvement metrics
Continual process improvement

Security Awareness Maturity Model

Sitting in a classroom running through PowerPoint slides often is not the best way to educate an adult workforce on cyber security. Instead, look for activities that are interactive, more directly involve personnel and reinforce the importance of cyber security to their specific jobs.

Conduct a Mock Data Breach

The most likely scenario for a healthcare organization is that it experiences a data breach. Running a simulation in a controlled environment can be an extremely effective technique to prepare an organization for a potential data breach.

Conducting a mock data breach can be done as a role-play exercise with individuals participating across the entire enterprise. This exercise can reinforce the role of each individual and group prior to an actual data-reporting situation. In particular, it can ensure an organization is ready to meet HIPAA timelines on breach reporting.

A primary objective is to make sure personnel know their roles and that crisis communications plans are in place to handle all external communications regarding the breach. Doing this on an annual basis reduces risk profiles and can lessen the financial fines levied by the HHS Office for Civil Rights for non-compliance.

Examine Recent Health Identity Theft Cases

Let personnel know not only what **can** happen in a data breach, but what actually **has** happened. This approach can make an abstract concept, such as cyber security, more tangible to healthcare professionals by letting them see the consequences of real actions.

Probably the best place to start is to review the previously mentioned HHS "wall of shame" Website and establish an organizational goal to avoid becoming the newest member. Each breach incident also is typically picked up by multiple news media outlets, negatively impacting an organization's reputation..

One objective in each case study would be to make sure an appropriate mix of managerial and technical controls are in place to prevent a similar breach from occurring.

Other topics that can be covered in security awareness training include:

- Reviewing results from an internal phishing campaign
- Reviewing results from recent penetration testing.
- Going through the relevant organization security policies and procedures
- Confirming the nature of organization intellectual property along with physical assets and
- Reviewing personal health information (PHI) being collected and stored
- Identifying what software applications access protected data
- Reviewing employee and contractor responsibilities in handling PHI and sensitive information
- Review of employee non-disclosure agreements
- Evaluating the requirements for proper handling of sensitive material in physical form, including marking, transmission, storage and destruction
- Reviewing IT password policy and authorization methods, such as two-factor authentication.
- Going through physical security issues, such as security badges, door locking and work area security

The focus of all this awareness is to build a culture of security cognizance, and to promote an ongoing series of tips that when followed, enhance the organization's security posture.

Don’t Forget Internal IT Technical Staff

IT professionals are in need of job-specific training that is more technical in nature than that provided to the remainder of a healthcare organization’s staff. These folks are on the front lines of computer network defense.

A lab environment may be used to provide a hands-on, but safe, environment that is not connected to mission-critical systems or nor uses any real patient data. In such an environment, new technologies and techniques can be evaluated for their effectiveness in protecting the organization’s IT infrastructure.

Some additional topics for security awareness training for IT professionals are:

- Understanding the business driver for information security
- Latest wireless protocols and their inherent security
- Top-10 information security best practices
- Security principles for IT system owners
- Fundamentals of cryptography
- Understanding threats: hackers, malware and insiders
- Network attacks and remediation steps
- Host attacks and remediation steps
- Wireless insecurity and remediation
- Securing Windows workstations
- Securing Windows servers
- Securing Linux/Unix servers
- Securing mobile devices

V. Success Factors

The collection and utilization of metrics are essential to measuring the success of a security awareness program. Senior management will want to see that its financial support is paying off. The ultimate goal is to develop and maintain a high-quality program—making incremental improvements over time should also not be discounted. If the humans in the enterprise can be recruited as sensors to and alert the IT security staff to potential environment security gaps, improved security will result. Changed behavior is the objective. Plenty of methods and tools are available to assist in this effort:

- **Surveys** can establish a normal baseline, and then measure on an annual basis if overall organizational security awareness has improved.
- **Portal site** can be created to post all security-related content. Articles, tips and current events make the site lively and content deep so those truly interested can find relevant information. Intrusion identifiers can be provided, along with information on malware threats seen in the wild and relevant prevention techniques. An occasional article by a C-level executive on cyber security will emphasize the importance of the topic to the overall organization. All departments should be recruited for content consider relevant to their roles in the enterprises securing PHI and personally identifiable information.
- **FAQs** can be created on important cyber topics. Employees can also submit questions to be answered.
- **Security tips** can be provided. Personal motivations should be emphasized: what is in it for the employee? How does the employee personally benefit from paying attention to this topic? Creativity is essential to make the content compelling.
- **Professional development** information can entice those with an interest to consider pursuing the field of cyber security full time. Details on professional certifications can be provided, along with links to job postings requiring those credentials.
- **Newsletters** can be used to maintain low-level background awareness by mixing current industry security-related events with internal security news topics.
- **Blogs** can make content available to those who would not normally read cyber security-related trade journals and other sources.
- **Event listings** can tie internal events to external events. Information on industry conferences and Webinars can be provided to support the gathering of relevant continuing education credits to maintain professional certifications.
- **Employee recognition** can reward individuals who have done something noteworthy that has improved organization security.

With all of these activities, persistence and good humor will go a long way in establishing a culture based on using sound security principles without imposing mandatory rigorous processes that might do more harm than good. No one-size-fits-all approach will work. Over time, all security awareness programs should be tweaked to maintain and enhance their effectiveness.

About the Author

Robert J. Michalsky possesses more than 30 years of IT industry experience with both government and commercial customers. As NJVC Principal, Cyber Security, he quantifies and pursues new business opportunities, leveraging the skills and services of the professional staff. Mr. Michalsky has spent more than 15 years providing cyber security-related IT engineering services for classified Intelligence Community and Department of Defense customers.

Mr. Michalsky's cyber security background encompasses a mix of technical and business objectives: computer network defense architecture design, application security testing, security requirements and policy establishment, network operations center management, IT system vulnerability analysis, disaster recovery planning, business continuity management, fraud pattern analysis and network modeling and performance analysis. In addition, Mr. Michalsky has played a lead role in lead business development, technical and project management for a variety of companies. He ran his own consulting company for more than five years, providing IT engineering services to multiple Fortune 500 clients.

Mr. Michalsky ran the training department at AGI (visual modeling software) and has taught IT professional education classes at both Pennsylvania State University and Villanova University. He presented at three Rational Software User Conferences (now IBM) on requirements and IT system performance topics, and published eight articles for the Rational Developer Network and .NET magazine.

Mr. Michalsky possesses a Master of Science in Computer Science from Villanova University, an Executive MBA from Temple University and an undergraduate degree in Mathematics from Kutztown University. He is a graduate of two GE Project Leadership Courses and additional leadership training from Unisys and Dale Carnegie. Mr. Michalsky is a member of the Institute of Electrical and Electronics Engineers, and is a former member of the Computer Measurement Group, where he authored three technical papers, participated on their editorial panel board and presented at three international conferences. Mr. Michalsky holds CISSP and CSSLP cyber security certifications from ISC$^{(2)}$.

About NJVC

NJVC provides customers with innovative solutions to critical mission, business and technology challenges. As a proven systems integrator for more than a decade, NJVC offers a wide breadth of IT and strategic solutions to clients focusing on IT automation and services integration, secure cloud services, managed security services and printing solutions. NJVC provides services to both government and commercial customers whose operations depend on high performance, agility and advanced security. We partner with our clients to support their missions with security-cleared, dedicated and talented employees ready to deploy globally.

NJVC offers various managed services and in person tutorials and workshops designed to raise the awareness of any organization to the dangers of inadequate cyber security practices. Once identified, mitigations processes are put in place. To learn more, visit www.njvc.com/healthcare-it

.

NJVC

14295 Park Meadow Drive
Chantilly, VA 20151
703.429.9000

www.njvc.com

Learn more about NJVC Cyber Security solutions