IT WORLD

Security Concerns Offer Opportunities

Jeff Kabachinski

About the Author

Jeff Kabachinski, MS-T, BS-ETE, MCNE, has more than 20 years of experience as an organizational development and training professional. Web site: kabachinski.vpweb.com; e-mail: JKabachinski@wi.rr.com

Keeping tabs on information technology (IT) security in healthcare is not getting any easier. It's tough to predict the future of healthcare IT growth and what general IT advances are looming that will impact healthcare security. The pace of technological growth shows no sign of slowing down. In fact, the complexity of IT security spirals as new networking devices and features add to the levels of network systems interaction and the growing number of systems of systems. This leaves healthcare technology management professionals in a constant learning mode to stay abreast to support their "client" base. It's probably not as bad as it sounds since we are accustomed to and have an affinity for constant learning. In addition, as we tune into to what's new, we're assessing its effects on IT fundamentals. These days, there is nothing more fundamental to all we do than the omnipresent, underlying IT security. It's been growing as an issue as we get new networking features, such as clouds and virtualization, up and running. In addition, the timing is right, bringing new opportunity for those wanting to become more involved in the IT side of the business.

IT security is one of those things that you can't let up on. Let your guard down and you open yourself to cyberattacks. It happens at all levels of hardware and for all sizes of companies.

IT security is one of those things that you can't let up on. Let your guard down and you open yourself to cyberattacks.

Consider the massive security breach at Sony in April of this year. It was the second largest security cyberattack in U.S. history, effecting the data of some 100 million customers, as described in an article by *The Epoch Times*.[1] Sony had its Play Station 3 network hacked via an anomaly involving Amazon's virtual cloud service called the Elastic Computer Cloud (EC2). It's a service for customers to manage information through the cloud platform. Instead of buying server hardware, cloud service customers can rent it on demand use or pay in advance to keep it reserved and pay a lower "by the drink" rate.

EC2 costs are based on things such as whether you use LINUX/UNIX or Windows, small, medium, or large on-demand availability, and high or standard central processing unit (CPU) use. To subscribe to a service, you give your name, snail mail and e-mail addresses, phone numbers, choose a password, and, of course, submit a credit card number with expiration date and the "secret" three-digit security code. Lots of juicy data for the cyber-criminal!

Despite spending several weeks making repairs, Sony's Chief Executive Officer Howard Stringer told *The Wall Street Journal* that he still couldn't guarantee the security of Sony's videogame network or any other web system in the "bad new world" of cybercrime. He went on to say that maintaining IT security is a "never-

One way to learn and ensure that you're hitting all the right security topics is by choosing a certification path to follow as a guide. Why reinvent the wheel? Use the cert exam's list of objectives as a checklist of what topics you'll need to know.

ending" process and doesn't know anyone that's 100% secure.[2]

They're saying scary things. In *The Epoch Times* article, Pete Malcolm, CEO of Abiquo Inc., said, "Anyone can go get an Amazon account and use it anonymously...If they have computers in their back bedroom, they are much easier to trace than if they are on Amazon's web Services." Sony's Stringer said that this could lead the way to much larger problems where the global financial system, power grid, or air traffic control systems are compromised. "It's the beginning, unfortunately, or the shape of things to come," he told the *Journal*. Commenting on the six-day delay in alerting customers of the breach he said, "If your house has been burglarized, you find out if you've lost something before you call the police." Wait a second; that's no comparison. I don't know about you, but I don't have sensitive financial data for 100 million people at my house. I'd also call the police immediately in case the criminal was still lurking about.

In another cloud related security issue, a Federal Trade Commission complaint charges the Dropbox file-sharing service has not been truthful about security and privacy.[3] Dropbox offers file synchronization and online backup, and it uses a data deduplication process to determine if a file had been previously uploaded by another user. If it had, then DropBox links the file to the previously uploaded data, enabling DropBox to determine specific file users in spite of its claims that DropBox employees are not able to access user files. They also use a single data encryption key instead of a unique key per user like other cloud services, such as Spideroak and Tarsnap. Understanding deduplication processes and encryption keys are just a couple of important aspects of developing a strong IT security policy.

In April, *InformationWeek* received 699 responses to its 2011 Strategic IT Security Survey. Managing security complexity, enforcing security policies, preventing data breaches from outside attackers, and spreading user awareness top the list of challenges cited by the IT professionals surveyed. The problems caused by attacks included loss of access to applications and business operations, intellectual property stolen or compromised, customer records compromised and identity theft. There were also second-order effects, such as customer alienation. It's only natural to distrust a company that doesn't seem to take your protection serious enough. An interesting survey result was found in the replies to the question of who poses the greatest threat of espionage or security breaches. It was a toss-up with 65% saying cybercriminals and 64% saying authorized users and employees.

We continue to hear about security holes in the rush to use new technology. IT risk assessment has grown in use and importance throughout healthcare, and other industries and markets. This renewed focus had one survey respondent saying that his organization has evolved past risk awareness to risk intelligence. Beyond the regulations, businesses now understand that IT risks are indeed business risks requiring serious attention.

InformationWeek found that companies that manage risk more effectively than their peers perform better financially. In its Analytics IT Risk Management Survey in January, 35% of respondents said their companies' IT risk management programs will get more funding in 2011 than they did the previous year. Very few said they expected to see cuts, important priority clues in today's economy. The survey also pointed to the need for security training to ensure employees have a firm understanding of

Exam Objectives Covered by CompTIA's Security+

1.0 Systems Security

- 1.1 Differentiate among various systems security threats.
- 1.2 Explain the security risks pertaining to system hardware and peripherals.
- 1.3 Implement OS hardening practices and procedures to achieve workstation and server security.
- 1.4 Carry out the appropriate procedures to establish application security.
- 1.5 Implement security applications.
- 1.6 Explain the purpose and application of virtualization technology.

2.0 Network Infrastructure

- 2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.
- 2.2 Distinguish between network design elements and components.
- 2.3 Determine the appropriate use of network security tools to facilitate network security.
- 2.4 Apply the appropriate network tools to facilitate network security.
- 2.5 Explain the vulnerabilities and mitigations associated with network devices.
- 2.6 Explain the vulnerabilities and mitigations associated with various transmission media.
- 2.7 Explain the vulnerabilities and implement mitigations associated with wireless networking.

3.0 Access Control

- 3.1 Identify and apply industry best practices for access control methods.
- 3.2 Explain common access control models and the differences between each.
- 3.3 Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.
- 3.4 Apply appropriate security controls to file and print resources.
- 3.5 Compare and implement logical access control methods.
- 3.6 Summarize the various authentication models and identify the components of each.
- 3.7 Deploy various authentication models and identify the components of each.
- 3.8 Explain the difference between identification and authentication (identity proofing).
- 3.9 Explain and apply physical access security methods.

4.0 Assessments & Audits

- 4.1 Conduct risk assessments and implement risk mitigation.
- 4.2 Carry out vulnerability assessments using common tools.
- 4.3 Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.
- 4.4 Use monitoring tools on systems and networks and detect security-related anomalies.
- 4.5 Compare and contrast various types of monitoring methodologies.
- 4.6 Execute proper logging procedures and evaluate the results.
- 4.7 Conduct periodic audits of system security settings.

5.0 Cryptography

- 5.1 Explain general cryptography concepts.
- 5.2 Explain basic hashing concepts and map various algorithms to appropriate applications.
- 5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.
- 5.4 Explain and implement protocols.
- 5.5 Explain core concepts of public key cryptography.
- 5.6 Implement PKI and certificate management.

6.0 Organizational Security

- 6.1 Explain redundancy planning and its components.
- 6.2 Implement disaster recovery procedures.
- 6.3 Differentiate between and execute appropriate incident response procedures.
- 6.4 Identify and explain applicable legislation and organizational policies.
- 6.5 Explain the importance of environmental controls.
- 6.6 Explain the concept of and how to reduce the risks of social engineering.

the organization's security policies. The focus on risk, the understanding of the ties to business success, and clear funding may offer healthcare technology management professionals new opportunities in healthcare IT security.

Keeping Abreast of IT Security

One way to learn and ensure that you're hitting all the right security topics is by choosing a certification path to follow as a guide. Why reinvent the wheel? Use the cert exam's list of objectives as a checklist of what topics you'll need to know. Since, scope creep—adding non-essential content—is always easy, sticking to a good list can help you stay focused and on track. A checklist will also help ensure you don't miss something basic.

There are several worthwhile certification paths to follow, including Cisco's Certified Security Professional (CCSP) and the internationally recognized Certified Information System Security Professional (CISSP). To see a full listing, check out www.networkingcertifications.com.

For a good grounding, take a look at **Security+** from the Computing Technology Industry Association (CompTIA). It's rated as #3 among *all* IT certifications from TechWeb. **Security+** started in 2002 as a response to need. There are now more than 45,000 certified. **Security+** deals with IT security topics, such as cryptography and access control, and includes more business-related topics, such as disaster recovery and risk management. As with all of CompTIA's certifications, this one is also well managed and controlled. Another vote of confidence comes from the Department of Defense as it accepts **Security+** as fulfillment of Level II Information Assurance Technical (IAT) and Level I Information Assurance Management (IAM) in its Information Assurance Workforce Improvement Program (DoD 8570.01-M). The **Security+** exam can also be applied as an elective to Microsoft's MCSA: Security and the MCSE: security specializations. (See the sidebar for a general list of exam objectives covered by **Security+**.)

To build comprehensive checklists, get the competency-by-competency details from the full exam objectives document at the CompTIA web site www.comptia.com. Take note: If you plan on taking the test, be sure your study materials cover the current version of the exam by checking the exam ID number. Also watch for expiration dates for specific exams.

In addition, some free chapters from the *CompTIA Security+ Study Guide (5th Edition, Exam ID: SY0-301)* provide a good start to building your personal IT security reference library. The free chapters are available at the publisher's site. The easiest way to find them is by Googling the filenames—**security_ch01_headstart[1].pdf** and **security_ch02_headstart[1].pdf.** They contain end-of-chapter test questions (and answers) to give you an idea of study materials available, the specific topics in IT security, and also a taste for the exam.

With the attention and renewed risk assessment focus, healthcare IT presents another opportunity and career path for the healthcare technology management professional.

There is no turning back the clock. IT security complexity can only grow with the technology you're trying to protect. It's important that we keep asking ourselves questions about how we're doing in terms of IT security—individually and organizationally. With the attention and renewed risk assessment focus, healthcare IT presents another opportunity and career path for the healthcare technology management professional. ■

References

1. **Dobson C.** Amazon Cloud Linked to Sony's Recent Global Security Breach. *The Epoch Times.* Available at: www.theepochtimes.com/n2/business/amazon-cloud-linked-to-sonys-recent-global-security-breach-56385.html. Accessed May 18, 2011.
2. **Wakabayashi D.** Sony CEO Warns of 'Bad New World.' *The Wall Street Journal*. Available at: http://online.wsj.com/article/SB10001424052748703421204576328982377107892.html#ixzz1McLh3ueV. Accessed May 18, 2011.
3. **Schwartz, M.** Dropbox Accused Of Misleading Customers on Security. *InformationWeek*. Available at: www.informationweek.com/news/storage/security/229500683. Accessed May 18, 2011.