

IBM Podcast

[MUSIC]

MATHENY: Welcome to this IBM podcast, Are security and compliance risk within the healthcare industry on the rise?

I'm Angelique Matheny with IBM. As more information is available electronically, the threat of this sensitive data is increased.

Hackers are focused on Web enabled applications where valuable personal data is exchanged. Web application vulnerabilities continually represent the largest category of vulnerability disclosures.

And today Valerie Hamilton, Worldwide Marketing Manager for Healthcare and Life Sciences, will share with us how the changing landscape of the healthcare industry may be driving the increase of security and compliance risk, and the various ways to reduce the possibility and the impact of security vulnerabilities. Hi, Valerie. Welcome to the podcast. Thanks for joining us.

HAMILTON: Great. Hello Angelique. Thank you for having me.

MATHENY: Valerie, I'm going to start with this, of

course, the most obvious question. Are security and compliance risk within the healthcare industry truly on the rise?

HAMILTON: Well, yes, they are. Security and privacy vulnerabilities have long been an area of concern in the healthcare industry. But even with increased focus on security and compliance, perhaps driven by HIPAA and the HITECH Act, breaches in the healthcare industry appear to be increasing.

It's a trend that's likely to continue as attackers tend to target areas where sensitive personal information is shared, and in the healthcare industry certainly this information is available and out there. Let me share some alarming statistics.

According to an article on darkreading.com, in 2010, surprisingly, healthcare suffered more data breaches than financial services -- in fact, more than three times the number of data breaches. And truly, I could go on and on with alarming statistics about security breaches. Just a quick Internet search shows reports from the Washington Post, Healthcare and Technology, eWeek, Healthcare IT News, all listing some type of security and Web site breach of information in the healthcare industry.

MATHENY: You're right, Valerie. We hear about it all the time. Why is that?

HAMILTON: Well, there are several drivers. First of all, due to the increased regulatory mandates from the Health Insurance Portability and Accountability Act, known as HIPAA, and the HITECH Act, there are increased regulations for protecting the privacy and security of health information. So, security requirements are tougher. And there's also an increase in breach disclosure, meaning security breaches are more visible to the public, if you will.

And I believe that user demand is indirectly a driver. Customers expect data to be available online, real time at their fingertips. The public is demanding rich applications requiring advanced coding techniques, which introduces more risk and threats to this valuable data.

Modernization, in general, is a driver. Traditional applications are being driven to an online world, being Web enabled, increasing corporate risk. Also, cost cutting with today's current economic climate. Today, we have increased demands and perhaps decreased efficiencies. Hackers are becoming smarter and more creative looking at ways to get this private information. It's been said that stealing information is the second highest motivation for Web

application attacks.

And finally, the healthcare industry is becoming more interconnected -- meaning that data, including patient information, such as medical records, flows between physicians, providers, health plans, pharmacies, labs and more. Wherever data is exchanged there's a security risk.

MATHENY: What about for the industry itself? Is this a major concern? What's the impact of a security breach?

HAMILTON: I've recently seen several articles about security concerns in the healthcare industry, and one article cites that about 80 percent of IT professionals at hospitals state that locking down patient information from breaches and unauthorized access is one of their top priorities.

And I've seen more similar articles from experts stating that security's a main concern overall in the healthcare field. And the impacts are significant. Failure to comply to HIPAA, for example, can mean both civil and criminal penalties, including fines and possible jail time.

And think about this. If you look at the average cost of a security breach, at \$6.6 million, this translates to about \$200 per record for client notifications alone. And fines

can be as high as \$15 million, not to mention the loss of reputation, and brand name and other related lawsuits, as well as a disruption to business operations.

MATHENY: Those are some pretty big numbers, Valerie. What are some of the top strategies for avoiding a security breach?

HAMILTON: Well, securing Web applications should be a top priority. This is where data is exchanged and is one of the most vulnerable areas for intrusion. Top strategies include centralizing and automating application content analysis to proactively identify these security vulnerabilities.

And assess compliance requirements, helping to improve the accuracy and reliability of these online systems where this valuable data is exchanged. So, centralizing and automating Web applications, security and compliance analysis includes security testing of Web applications for vulnerabilities and accessibility issues.

And utilizing Web site content scanning and analysis can help ensure compliance with privacy, accessibility and key industry regulations, such as HIPAA and the HITECH Act. The cost savings of automated versus manual security can compliance testing is significant.

Automated testing provides tremendous productivity savings.

For example, outsourced audits can cost anywhere from 10,000 to 50,000 per application. Imagine multiplying that by the number of applications within an organization and by multiple audits, perhaps quarterly. This can be a significant cost to your organization.

And for those organizations creating Web applications, secure coding practices are not typically part of core development activities. In general, development is lacking the tools to automate, mitigate risk and test security. Vulnerabilities are continually introduced in application code. And think about this: 80 percent of development costs are spent identifying and correcting defects.

Another key strategy is to embed security and compliance across the development lifecycle through automation, audit trails, controlled access and also scans of the codes as it's being developed. And even if applications are created by and purchased from third parties, the bottom line is that your organization is still responsible for the security of this information.

So, the key takeaway strategy is to centralize and automate Web application security and compliance analysis to avoid the risk of a data breach, to avoid exposing unsuspecting visitors to malware attacks and falling out of compliance

with security, privacy and accessibility requirements.

MATHENY: Valerie, thank you so much for sharing your time today. This was some great information. We really appreciate you being here.

HAMILTON: Thank you for having me. Appreciate it.

MATHENY: That was Rational's Valerie Hamilton, talking about how security and compliance risk within the healthcare industry are on the rise. To share this podcast with your colleagues or if you're interested in more podcasts like this one, check out the Rational Talks to You podcast page at www.ibm.com/rational/podcasts.

We'll post a link to the security and compliance for healthcare e-kit to help you get started. This has been an IBM podcast. I'm Angelique Matheny. Thanks for listening. Keep tuning in as Rational Talks To You.

IBM Podcast

[MUSIC] [END OF SEGMENT]