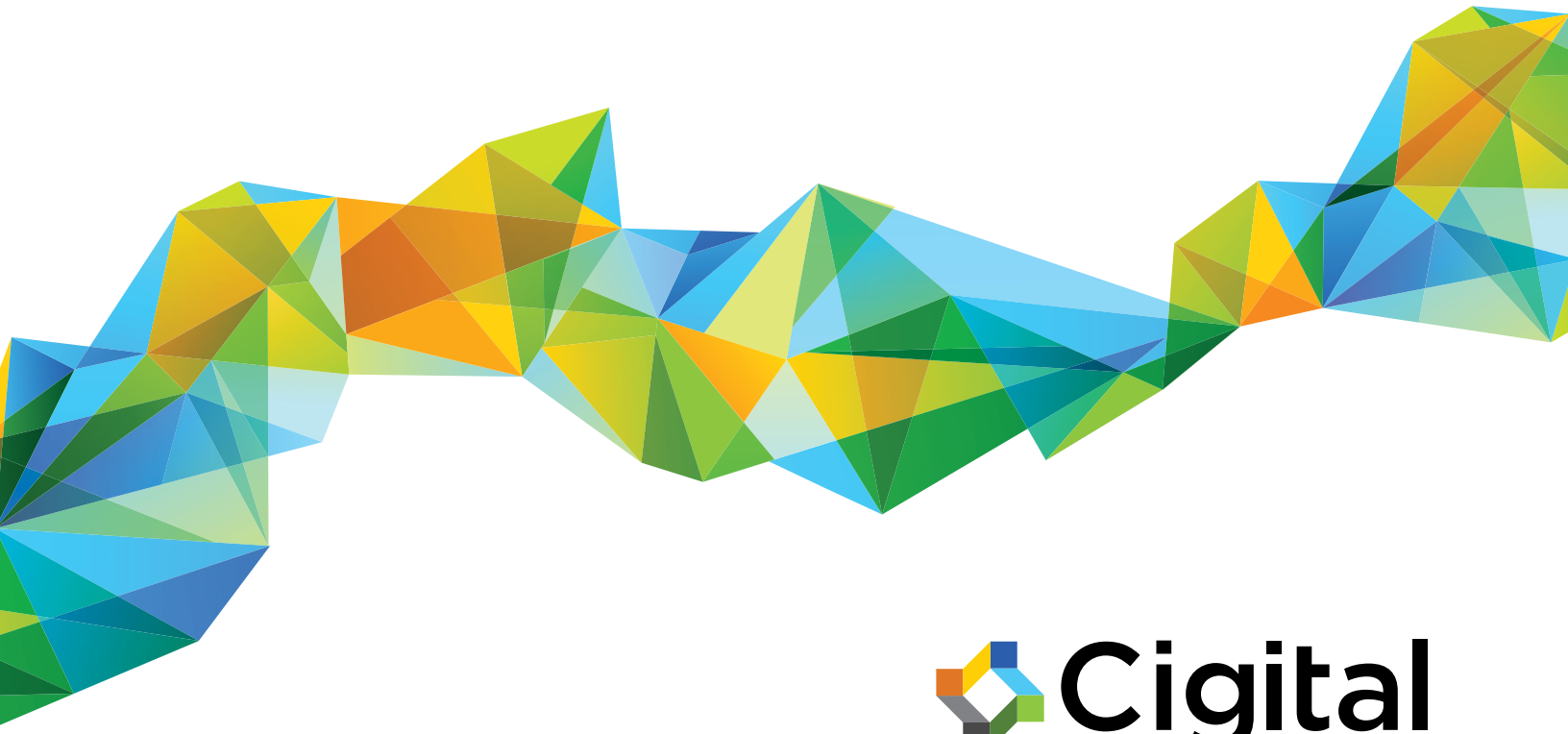
What We've Learned About Security In the Healthcare Industry



Cigital
BUILDING SECURITY IN

Contents

Overview

Patient care is of the utmost importance within the healthcare industry. The **Health Insurance Portability and Accountability Act (HIPAA)** is a driving regulation in the healthcare field affecting the information security and privacy of patient information. HIPAA was passed in 1996, but the privacy and security rules didn't take effect until 2003.

The results of the sixth iteration of **BSIMM** show the healthcare industry lagging in comparison to the 78 other participating BSIMM firms.

Before 2003, if a visitor walked into a hospital requiring medical assistance, it was acceptable protocol for the receptionist to direct the patient to the correct department along with their full medical record. This protocol was put in place to emphasize customer service—ensuring the patient was directed to the correct department with a file of sensitive personal data for the doctor to use to make their most informed diagnosis.

With HIPAA implementation in 2003, there was a significant cultural shift. Daily operations were re-adjusted to focus on the protection of patient information over and above the convenience of customer service protocols. This shift resulted in procedural changes involving people, processes, and technology that in turn impacted patients, doctors, insurance companies, and medical device manufacturers.

The results of the sixth iteration of the **Building Security In Maturity Model (BSIMM)** show the healthcare industry lagging in comparison to the other participating BSIMM firms (a total of 78 firms participated in BSIMM6) over 12 industry verticals. The model is descriptive, measuring real-world security initiatives. But the numbers alone do not tell the full story of information security within the healthcare industry. This case study highlights the past, present, and potential for the future of security in the healthcare industry based on BSIMM research.

The Healthcare Ecosystem

The healthcare industry contains many sub-industries that need to work together in the protection of personal health information (PHI). These sub-industries ensure the security of systems that deliver patient care. Here's a look at the role each type of organization plays in the healthcare ecosystem as it relates to software security:

Healthcare Delivery Organizations (HDOs)	HDOs include hospitals and medical device manufacturers. Hospitals typically buy a majority of their software. Their role in software security is to configure their software using the guidelines provided by HIPAA, along with their own risk management processes.
Medical Device Manufacturers	Medical device manufacturers write both the software that is used to control the device along with the systems that often accumulate patient data and provide it to hospitals and doctors.
Pharmacies	Pharmacies interact with hospitals, doctors, and insurance companies using software they often write themselves. Smaller pharmacies buy software from a few major providers of pharmacy management software.
Pharmacy Benefits Managers (PBMs)	PBMs typically provide mail-order drugs for patients who need them over long periods of time. They interact with the same people that the pharmacy does, but mail the drugs to the patients. They typically write all of their software.

Health Insurance Companies	Health insurance companies write most of the software used to manage interactions with HDOs.

The goal for these types of organizations is to consistently and efficiently share data with one another so the processes currently in place work smoothly together. Changing a component of the process often impacts the sub-industries by requiring them to adjust their software accordingly.

In 2014 and 2015, there was a **cluster of security breaches** that highlighted some of the information security gaps throughout the healthcare industry. The majority of the industry was moving towards improvements in the security of their software and infrastructure; the breaches accelerated their timelines.

Healthcare Industry Security Objectives

The primary objective of security assessment programs is to enable higher quality patient care while optimizing efficiency and impact of security spending. We search for ways that the organization can use the same funds—or slightly increased funds—to get a better return on their security investment.

A secondary objective involves regulators. Regulation in the healthcare industry is typically reactive rather than proactive. There is only spot-checking for compliance with regulations, but when a breach occurs, regulators step in. With the increase in breaches in recent years, many healthcare organizations want to be ready to respond to a regulator in the event of a breach.

Security Implementation Strategies

To improve healthcare organization software security, there are four strategies we've seen implemented successfully:

1. **Allocate resources to be directly responsible for improving software security.** Given the current supply and demand mismatch regarding security professionals, organizations often look within the organization to move development or architectural resources into a security role.
2. **Provide security training throughout the organization.** Training directly impacts key metrics like bug density ratios and time to remediation. **Educating developers** helps prevent the introduction of bugs in the coding process through the application of best practices. When bugs do enter the code, educated staff are required to interpret the results from code assessment and scanning tools, and to identify the proper mitigation technique to fix what is found. Thus, an educated staff will introduce fewer vulnerabilities, and will remediate discovered vulnerabilities faster.
3. **Apply automation tools that look for security vulnerabilities** (such as **SAST** and **DAST**). Integrate these tools into the software development lifecycle (SDLC) to get coverage across all portfolio applications.
4. **Acquire consulting services** based on specific software security needs and areas lacking in the organization's internal team capabilities. **BSIMM measures 112 software security activities** which organizations have implemented both internally and in coordination with consultants.

These activities include training developers and implementing processes to find vulnerabilities faster or on a broader scale. Healthcare organizations often turn to **eLearning or instructor-led security training** to maintain security requirements and improve security processes.

Getting Started In Your Organization

While it seems easy enough to pick a few activities and begin to implement them, we usually recommend a few

strategic pre-requisites to ensure an effective implementation.

The first is to put someone in charge of software security. If nobody is in charge, nobody is going to move the security program forward. During a BSIMM measurement, one of the first questions we always ask is, "who is in charge of software security?" The objective is to ensure that people writing the code and building the software know who to contact with questions. The leader of this software security group (SSG) should be able to communicate with the development team, understand both the business requirements and regulatory requirements, and help the teams implement them.

If nobody is in charge of your software security, nobody is going to move the security program forward.

A quick survey of our healthcare clients and their heads of SSG show that most are pulling that leader role from within other parts of the organization. That may be a lead developer or someone in an architectural role. One of the keys to success for this role is a good relationship with the development teams, so having someone who really understands how software is developed in the company can be a significant asset.

Once an SSG leader has been named, the security initiative should be kicked off with specific activities. One of the early missteps we've seen is unclear expectations between security and development. Setting secure development standards is an easy way to set those expectations. These are usually in the form of a language-specific document that guides developers on the proper practice of writing secure code.

Finally, the head of the SSG should conduct an analysis of the gaps currently in existence which are causing the most impact to the organization. Check **HIPAA** and **HITECH requirements** to determine where process improvements should be made.

The overall objective is to perform security functions as early as possible. Many healthcare organizations are performing penetration testing. Successful companies have ensured the secure coding guidelines prevent many of the vulnerabilities they have been finding.

Execution

Almost every healthcare company we've spoken to has had trouble answering the question, "what does your application inventory look like?" Our medical device clients have a clear understanding of the products they create, but don't always have a view of the applications which support those products. Likewise, the insurance companies understand the key applications which support the major business processes, but they don't have a clear understanding of the full application portfolio.

There are two key tasks to understand the application portfolio:

- Collect an inventory of all of the applications in your environment
- Understand and **risk rank the portfolio** into a few buckets

Almost all healthcare organizations we've engaged with started with an inventory including two buckets: the high risk applications (typically those on the internet or those which contain PHI) and lower risk applications. During execution of the risk ranking processes, clients further defined each bucket to provide a more risk-based analysis of each application. Most have resulted in high, medium, and low buckets. Two organizations implemented something similar to marquee, high, medium, and low. The marquee bucket contains the five to 10 applications most important to the entire organization. This is where the most energy and efforts should be placed from an overall security standpoint.

Most organizations are also looking for quick wins—those activities which won't require significant political efforts to implement and have a good return on investment. It is common for many healthcare organizations to implement developer training and perform static and dynamic security testing for this reason.

Static code testing is relatively new to healthcare organizations (some big insurers are ahead of the game, but not many). Static code testing often results in a large amount of data. Since organizations are looking for quick wins, they are often challenged by the large quantities of data resulting from static testing.

Healthcare Hurdles

Healthcare organizations are historically reactive when it comes to security. They are quick to fix problems when found, but aren't building processes to reduce the likelihood that the same thing won't happen again in the future. Due to this reactive industry tendency toward security, when proactive measures are proposed, the SSG leads we have worked with don't immediately welcome these activities. While training and testing have been easy to implement in these organizations, moving additional testing closer to the development of code has been a challenge.

Very good SSG leads have been able to use metrics to show improvements in things like training and secure coding guidelines to gain buy-in for the implementation of more proactive activities. Additionally, with the increasing "pile of bugs" generated by assessment activities, executives are asking for a more efficient way to reduce the number of vulnerabilities. Proactive approaches solve this issue.

When budgets are analyzed, healthcare organizations are still spending considerable dollars on network and governance activities while not increasing spend for application security activities. The question often asked by internal auditors and other risk managers is whether the spend supersedes the risk. The historical assumption in healthcare is that the network poses the greatest risk. In hospitals, most of the effort is spent securing the network. Medical device manufacturers often assume the network of a hospital is secure when building security into their devices.

We are slowly seeing that model change where applications and devices are taking a greater role in the security of the enterprise. For hospitals, this often means pushing vendors who provide the software and devices that sit on the network to build more secure applications and devices.

Three Primary Results

There are three primary results we've seen from healthcare organizations who have implemented the proactive security measures.

More security coverage for the spend. Organizations are starting to optimize how they use their budgets to get more security coverage. This is due to a better understanding of various security activities that are appropriate for various types of hardware and software. There are also many different options available today when it comes to software security assessment tools and services that organizations can easily access.

Increased breadth and depth of testing. Tool and assessment technologies have improved significantly over the last five years. As such, organizations are able to increase the number of applications they can assess and the level of depth to which they can be analyzed.

Better relationship between security and development. Development groups within organizations are starting to understand and appreciate the need for software security and building security into their software. Developers are starting to accept the fact that building secure software is the norm and the expectation. Therefore, the development organizations are embracing tools that help them build more secure code earlier in the SDLC.

Summary

We've seen significant changes in the healthcare industry suggesting that healthcare security leaders are starting to change the industry mindset and build more effective security programs. The processes we undertake in BSIMM assessments in have resulted in significant improvements in the software security of healthcare organizations..

If the pattern we're witnessing continues, and more and more SSG leaders are brought on to implement security measures, sub-industries and industry leaders will discover the importance of proactive security measures. Healthcare organizations will increase their spend on dedicated security initiatives which will in turn save their organization a great deal of time and money by preventing breaches.

Cowritten by Jay Schulman and Nabil Hannan. Technical review by Dan Lyon.

Learn more about how Cigital can help your healthcare organization become more secure at https://www.cigital.com/healthcare.

About Cigital

Cigital is one of the world's largest application security firms. We go beyond traditional testing services to help organizations identify, remediate, and prevent vulnerabilities in the applications that power their business. Our holistic approach to application security offers a balance of managed services, professional services, and products tailored to fit your specific needs. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure applications.

Our proactive methods helps clients reduce costs, speed time to market, improve agility to respond to changing business pressures and threats, and focus resources where they are needed most. Cigital's managed services maximize client flexibility, while reducing operational friction and cost. Cigital gives organizations of any size access to the scale, security expertise, and practices needed to build a successful software security initiative.

For more information, visit us at **https://www.Cigital.com.**