Overview

In 2015, healthcare became the industry with the most cyber attacks, replacing financial services. Between 2009 and 2017, there were over 2,000 data breaches, exposing a total of more than 177 million healthcare records and resulting in over $75 million in HIPAA violation fines. And those breaches are just the ones we know about.

Misalignment between HIPAA and software security

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996. However, the compliance date of HIPAA’s Privacy Rule and Security Rule didn’t take effect until 2003. These rules were created as a way to implement and enforce industry-wide security safeguards on protected health information (PHI).

The Security Rule focuses on technical defenses around access controls and technology protecting electronic PHI. The requirements state what is expected, but not how to meet them. Thus, the rule’s guidelines can leave health organizations with the burden of implementing effective controls without enough guidance. Organizations may not have the current capability to determine what they are accomplishing from a software security perspective. This is where the Building Security In Maturity Model (BSIMM) becomes a valuable asset.

The BSIMM acts as a measuring stick, assessing security activities performed by an organization. The model also sheds light onto the wider software security community—quantifying practices of many different industry verticals. The BSIMM is not a how-to guide, nor is it a one-size-fits-all prescription. Instead, it is a reflection of the current state of software security. BSIMM measurements can be used to plan, structure, and execute the evolution of an organization’s software security initiative (SSI). Over time, firms participating in the study show measurable improvement in their security stance.

This case study shares one organization’s BSIMM journey in their own words.

Getting started: The wake-up call

In 2013, the number of publicly disclosed healthcare breaches was quickly rising. Patient data was being leaked and incredibly damaging effects were unfolding for the organizations at the center of each scandal.

Our leadership established that security needed to become a top priority. The main constraint at the time was figuring out where to start. So, we gathered the information we did know. Our software portfolio at the time consisted of nearly 3,000 applications. The majority of these applications were developed in-house. However, there was a catalog of third-party software in operation.

Next, we wanted to understand what other firms were doing—both right and wrong. After some digging, we understood a few critical points:

1. We didn’t have a dedicated global software security organization within the firm. Creating one would allow us to define software security goals, roles, and responsibilities, and then propagate these within the organization.

2. We needed to create a multi-year plan to strengthen our existing security program. While the organization was performing security activities throughout, we didn’t aggregate data throughout. No comprehensive plan existed.

The head of our internal Software Security Initiative (SSI) had experience with the BSIMM previously when he worked for another large healthcare organization. He determined that it would be best to bring in a third-party and undergo a BSIMM assessment to establish an unbiased view of the security activities performed throughout our organization. To further benefit our strategy, he recommended that our firm become active in the BSIMM community. This would give us insight into what other firms were doing in light of the current security crisis. We were particularly interested to see successful security approaches, failed approaches, and what new strategic techniques were popping up in the industry.
The BSIMM assessment process

The BSIMM process took two business days and required minimal overhead. It involved a series of 60-minute interviews with key security members of the organization to evaluate various security activities that we performed internally. The first interview was scheduled with our SSI lead. Additional interviews were conducted with team members responsible for day-to-day security activities. The topics covered during these interviews aligned with the BSIMM Software Security Framework:

Topics covered during the interviews

- Our software security policy
- Secure software development life cycle (SDLC) and gates
- Application compliance obligations
- Metrics
- Software security training
- SSI outreach
- Software security standards
- Data classification
- Application risk ranking
- Security defect discovery
- Vendor management

Who staff members interviewed

- Software security process leaders
- Business analysts driving non-functional security requirements into development projects
- Architects driving software security
- Development and QA managers
- Risk, threat, and attack intelligence managers working with SSI and engineering teams
- Security operations managers and incident response managers focusing on application-level events
- Compliance, legal, and risk representatives
- Those instrumental in defining and enforcing software security-related activities
- Audit and project management office (PMO) group representatives responsible for monitoring and enforcing security-focused SDLC gates

Minimal preparation was required for the interviewees. The BSIMM assessors distributed a brief description of the BSIMM to interview candidates so they would have a better understanding of the interview objectives, which was very helpful.

Shortly after the interview process was complete, we received a report of the results. A BSIMM scorecard provided a high-level overview and a detailed score comparison outlining the differences between our commonly observed security activities and those performed by similar organizations.

In total, the entire BSIMM assessment process spanned a period of three weeks.
The BSIMM results

We weren’t expecting very promising results. Because our software security program was quite young, our feedback was daunting. This spider graph illustrates the results of our assessment in comparison to BSIMM firms in the financial services industry.

At the time we were assessed, the BSIMM did not have data to compare us to peers in the healthcare industry. This assessment reaffirmed our SSI lead’s perspective that the healthcare industry’s BSIMM score ranked lower than the average financial services industry score.

In Figure 1, the high water marks of BSIMM financial services participants are similar to our results in the Compliance & Policy results and the Standards & Requirements results. However, we scored below average for the remaining areas. Clearly, our organization’s security program had a lot of room for improvement.

This data allowed us to formulate short-term preventative measures until a long-term security strategy could be established.

Developing a strategy

After examining the report internally and breaking it down with BSIMM assessors over an hour-long read-out meeting, we developed three actionable short-term goals based on our available budget:

1. Create a software security group (SSG). We achieved this by allocating resources that would be directly responsible for improving the software security program. A global SSG standardized a process for relaying a concise, consistent message across the organization. It continuously serves as the ideal platform to track progress and effectiveness of the security program.

2. Conduct role-specific security training. In addition to offering annual compliance-based training, our organization implemented a training strategy that involved all team members working in the development life cycle. Security training impacts key metrics like bug density ratios and time to remediation. Targeted developer training reduces the number of security bugs introduced in the coding process.

   We also introduced an executive-level training program to educate our firm’s primary decision makers so that they are better equipped to fully understand the current state of our security program.

3. Implement automated tools in coordination with manual review. We integrated automated tools for static and dynamic testing into our SDLC, so we can identify vulnerabilities earlier in the development process. Now, when bugs are discovered in code through static application security testing and real-time scanning tools, developers are required to interpret the results and identify the proper mitigation technique to remediate findings. The purpose of this is to mitigate vulnerabilities faster and introduce fewer issues into the code in the first place.
With guidance from BSIMM assessors, we then created a two-year roadmap based on the initial benchmarks and BSIMM results.

We also made the decision to undergo a BSIMM assessment annually to measure our security initiative and examine progress over time. It was decided that annual measurements would provide us with the data needed to make decisions on budget allocations, where and how to focus our security activities, and how to continue improving our security stance.

Our first BSIMM assessment was four years ago.

**Moving forward**

Fast forward to today. Figure 2 below illustrates the progress we’ve made over the last three years. Now that recent BSIMM data includes healthcare industry results, we can compare our most recent BSIMM results to those of our healthcare peers.

We created a stronger security program by performing targeted security activities throughout the SDLC.

![Figure 2. BSIMM results three years after initial assessment vs. the BSIMM healthcare vertical](image)

With our roadmap based on the initial assessment, we were able to plan the high-priority (i.e., weaker security) areas to include within each year’s budget. The roadmap along with annual BSIMM assessments allowed us to gauge the process. Additionally, we were better able to strategize where and how we were working to create a stronger security program by performing targeted security activities throughout the SDLC.
Synopsys takeaways

Working with this particular organization provided highly valuable insight into the healthcare industry based on the data we collected. More importantly, our BSIMM assessors were able to help this organization to create a proactive software security program. In an industry driven by HIPAA compliance, healthcare organizations often take a reactive security approach. With data gained from the BSIMM, this particular firm committed to a proactive software security approach.

Our contact at the organization was able to convey to executives that their internal security team was doing everything in their power to protect the organization's assets. They were able to show SSI progress with metrics year over year from each subsequent BSIMM assessment.

BSIMM data supports the claim that the healthcare industry is making progress. Firms are beginning to take security seriously, approaching it proactively. The graph above illustrates a comparison between BSIMM industry verticals.

BSIMM assessments throughout the healthcare industry have shown that once organizations are HIPAA compliant, there is often little direction or effort focusing on security. After undergoing a BSIMM assessment, these organizations look beyond compliance and toward building a mature software security program to stay ahead of attackers.

More information on the BSIMM can be found at bsimm.com.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com