Application Security in the Financial Services Industry

Myths vs. reality

Introduction

As organizations work to transform their AppSec practices and streamline their DevOps development model, they continue to struggle to implement tools and processes that can scale and keep pace. The complexities of managing and maintaining open source, and the adoption of cloud-native architectures and their associated microservices all increase the degree of difficulty. Further, supply chain intricacies make it very difficult to get a full picture of an organization's risk profile. So it's no surprise that AppSec continues to be an increasingly complex challenge for organizations adopting modern development practices.

This is particularly true for the financial services industry (FSI), where the stakes are high. In 2019, the global financial services market was valued at a whopping $22 trillion.[1] Opportunities for exploit abound, and financial services firms are often high-profile targets. In the shadow of unrelenting real-world challenges, these firms are often a first-choice target for attackers. During the first year of the COVID-19 pandemic, over 70% of financial services firms experienced a successful cyber attack, and COVID-related business conditions were perceived as being to blame.[2] In the event of a breach, companies must cover millions in losses. In 2019, the average cost per breach was $5.86 million.[3]

Problems that existed before COVID, like supply chain risk management, budgeting and resource constrains, and a lack of security training, have only worsened. This is the reality facing financial services firms. As stated in a prominent cyber security community, "There are two types of financial services companies: Those who have experienced a cyber attack and those who will in the future."[4]

There are many myths and misconceptions that linger in the financial services industry in regard to application security. So we used the 2020 "Building Security in Maturity Model" (BSIMM) report research data to debunk and explain seven of the biggest myths, in an effort to provide clarity and guidance. Regardless of your personal experiences and perception of these myths, there are concrete steps you can and should take to ensure your AppSec program is on track.

During the first year of the COVID-19 pandemic, over 70% of financial services firms experienced a successful cyber attack.

The seven myths of FSI application security

Myth 1: Financial services firms are secure because they must be

Overall, the perception of financial services is that the industry is secure. This is based on no evidence or data, but rather on the belief that as the gatekeepers of everyone's sensitive data, it simply **must** be secure.

Because the industry is highly regulated, financial services firms tend to be very good at remaining compliant. This has helped lull security leaders and customers into a false sense of security. While an organization may indeed gain short-term comfort from successfully meeting compliance requirements, long-term problems arise when organizations fail to scrutinize their security practices beyond compliance.

If you're feeling ill-prepared to tackle the onslaught of security challenges in your firm, you're not alone. Most organizations don't have a firm grasp on what activities they need to be implementing beyond basic penetration (pen) testing.

Reality

Financial services firms are not so secure. In a recent independent study commissioned by Synopsys with the Ponemon Institute, "The State of Software Security in the Financial Services Industry," the findings highlight the misconception of FSI security. Ponemon discovered that 50% of financial services firms experienced data theft due to unsecure software. This undoubtedly stems from the fact that only 34% of FSI software is tested (beyond pen testing) for security vulnerabilities. And only 45% of financial services firms believe they have adequate security budget to address their risks, while 76% say it's difficult to detect security vulnerabilities in financial software systems before going to market.[5]

Myth 2: Financial software is different than other software (and therefore can't change)

A lot of financial services firms still believe their software is inherently different from other types of software, and it is therefore incapable of change. They believe they cannot afford to make important shifts toward DevOps, and place unwarranted trust in tried and true practices such as the waterfall methodology. The perception is that what has worked in the past will continue to work.

Reality

There are no special snowflakes. Financial software is written, managed, and tested in the same manner as any other software. Outdated development models inhibit development velocity and hinder go-to-market speeds. Organizations that refuse to adapt to the modern software landscape will fall behind, if they haven't already.

Attracting top talent will also be a challenge for firms unwilling to modernize; developers are uninterested in working for organizations stuck in the past. The future success of your firm relies on a move to DevOps, which will help make your software better, your development faster, and your overhead lower.

Myth 3: Little financial services firms have different AppSec needs than big financial services firms

There is a misconception that small banks and large banks have different AppSec needs and relative levels of security.

Smaller banks often buy their software, while larger banks build their own. It is therefore believed that when purchasing software, the burden of security falls to the vendor, not the purchaser.

Additionally, the erroneous belief that smaller banks use different software than larger banks often results in critical security practices being overlooked. More troubling still is that many smaller banks believe they are simply too small to be a viable target.

Reality

Size doesn't matter. All financial services firms regardless of size depend on open source software and software supply chains—even those who build their software themselves. All organizations bear the same relative level of AppSec responsibilities.

Customers expect the same security from a small bank as they do from a larger bank. So all banks are responsible for implementing robust and comprehensive AppSec strategies and taking ownership of their security risk profile. Troublingly, the Ponemon report showed that only 43% of financial services firms require third parties to adhere to strict cyber security requirements or verify the security practices of third parties. This highlights a false belief in the security of third-party software and indicates a failure to take on the burden of security internally.[6]

The idea that smaller banks are impervious to attacks is simply wrong. Attackers target systems via automated strategies; they don't care who or how large the target is. Attacks are always opportunistic in nature; if you're small and vulnerable, you're just as appetizing a target as something large and vulnerable.

FACT: Only 43% of financial services firms require third parties to adhere to strict cyber security requirements or verify the security practices of third parties.

Myth 4: You control everything that's in your deployed software

Many financial services firms believe they have a good understanding of all the components and elements in their deployed software. But knowledge of everything in a software stack is not a complete picture of everything going into production—not even close. Even larger financial services firms struggle with this misconception.

Reality

You have an incomplete picture. Today, all financial services firms use some form of open source software, and it covers a broad range of AppSec activities and environments. From Docker and Kubernetes to supply chains, cloud deployments, and shared responsibility models, you need to understand all the code and every component in your environment. Mastery of exactly what you're deploying and each of their respective security stances is critically important.

Myth 5: Cloud security is the job of cloud operators and owners

Similar to the idea about third-party responsibility, financial services firms often believe that the cloud "does it for them" when it comes to security. Assuming cloud security is the responsibility of the cloud operators and owners, financial services firms often do little to nothing to secure their cloud deployments.

In 2019, Capital One fell victim to this very misconception. Capital One's misplaced trust in AWS to perform adequate security practices resulted in a massive breach. Reports found that despite the exploit being known and reported, "major players like AWS are not doing anything to fix it."[7]

Reality

Cloud security is your responsibility. GitHub, GitLab, and various other cloud services work hard to secure their users' deployments. However, responsibility still lies with your firm's internal AppSec program. In order to run a secure cloud deployment, security teams must deploy secure containers into their cloud.

Additionally, the responsibility for overall security best practices, identity and access management, and crypto security is yours. Without internal security activities, you may be functional, but you are certainly not secure.

Myth 6: Pen testing, gate testing, and final step security is sufficient

Financial services firms tend to believe that pen testing, often the path of least resistance, is enough. Teams have more resources that are skilled enough to perform these tests, and portions of the process can be easily automated.

The simplicity of this testing method, along with a firm's typical lack of resources, results in the misconception that they're doing the best they can with what they have.

Reality

AppSec must be built in. While pen testing does serve a critical role in application security, it's insufficient when used alone. Synopsys industry experience shows that 50% of all defects found in software are architectural flaws, which go undetected by pen testing.

Organizations need to adopt deep-dive architecture risk analysis (ARA) practices or threat modeling in order to identify these critical risks.

Myth 7: Developers can learn AppSec skills on their own with experience

Financial services firms often lack the resources needed to perform important security activities. Despite this shortcoming, they believe that given enough time and self-taught experience, their developers can take care of any security needs within the software development life cycle.

While this could be true for a select few, the consequences of what could occur during a developer's learning curve constitute a large risk. Questions of how long it will take a developer to become an expert, plus a lack of structure and metrics by which to assess their skills, leave a dangerous gap in security.

Reality

Security training is necessary. The Ponemon report shows that only 38% of financial services firms have employees with the cyber security skills required to secure their software. And 25% percent of employees have no security training at all, yet they are still tasked with AppSec responsibilities.

Most organizations don't have the budget to address today's risk environment, let alone provide the security training to bring developers up to speed for the future. And only 45% of financial services firms believe they have an adequate security budget.

FACT: Only 38% of financial services firms have employees with the cyber security skills required to secure their software.

What's your AppSec myth?

Most organizations hold onto at least one misguided idea that can pose a risk to the integrity of its software. Whether you're just starting out on your application security transformation or you're well on your way to modernizing and reinforcing your security program, there are concrete steps you can take today to replace that myth with data-based strategies to improve your AppSec processes.

BSIMM and Maturity Action Plan services from Synopsys

Rooted in our commitment to provide clear and actionable feedback about your application security program, the Synopsys BSIMM and MAP offerings provide a wide range of support.

- **BSIMM.** A BSIMM assessment from Synopsys allows you to gauge your program relative to trends, best practices, and your peers. BSIMM experts carefully examine your security program and then provide a scorecard that details your security stance relative to your industry peers and leaders. This gives you a snapshot of how well or how poorly you're performing in areas that are critical to AppSec success.

- **MAP.** A Synopsys Maturity Action Plan (MAP) is a custom-tailored roadmap based on BSIMM data and scores. It offers the security strategies, capabilities, and activities your company should employ on its path to effectively mature its security program and provides key guidance.

Using these proven assessment methods to analyze your existing security program, Synopsys identifies gaps and areas of improvement, while also giving actionable guidance on what remediation steps to take.

Security is a journey

Synopsys recognizes that security is a journey. Maturing your security program requires a clear roadmap and concrete steps to take over time. We help you build a long-term plan that starts by assessing where you are, and then provides tangible steps to address existing gaps.

Our plans are organized with different stages in mind and are designed to easily keep up with changes in your portfolio. We identify weak links in your system design and highlight areas where additional security testing is necessary. We also use threat modeling on the systems, software, and people involved in your program to identify tangible threats and help you build security into development workflows.

Clearly communicating program improvements, security practices, and vulnerability remediation is critical to your program's success. Our roadmap ensures visibility into and accountability for the management of your security program. You get a clear picture of defect discovery, policy compliance, and security training, as well as professional help with improving risk reduction and risk prevention.

We can help: Synopsys offerings

Participating in a BSIMM assessment gives you ongoing access to a unique and private community of software security leaders in financial services and other industries, where you can discuss common issues and find solutions. Your assessment provides a clear picture of how well your security program operates and where you need to make improvements.

A Maturity Action Plan delivers a step-by-step plan with actionable guidance to help prioritize your security program funding, streamline resources, and reduce the overall risks of application vulnerabilities. We remove the guesswork and stress of beginning your security program transformation.

Ready to get started? Let's talk.

Visit our website to get started on your AppSec transformation today. www.synopsys.com/software-integrity/contact-sales.html

References

1. Steven Bowcut, Cybersecurity in the financial services industry, Cybersecurity Guide, Feb. 25, 2021.
2. Phil Muncaster, Most Financial Services Have Suffered COVID-Linked Cyber-Attacks, Infosecurity magazine, Jan. 19, 2021.
3. Steven Bowcut, Cybersecurity in the financial services industry, Cybersecurity Guide, Feb. 25, 2021.
4. ibid.
5. Ponemon Institute, Synopsys Cybersecurity Research Center, The State of Software Security in the Financial Services Industry, Aug. 1, 2019.
6. ibid.
7. Brian Krebs, What We Can Learn from the Capital One Hack, Krebs on Security, Aug. 2, 2019.

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.
690 E Middlefield Road
Mountain View, CA 94043 USA

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