Hard lessons

The financial sector is among the most heavily targeted – and the most advanced when it comes to security validation and breach simulation. Evan Schuman explores the industry's hard lessons and what security teams across industries can learn from them.

Businesses in the financial sector are among the toughest when it comes to data security. Years of around-the-clock breach attempts and heavy regulation have pushed banking and finance firms to spend more on the people and technology needed to better protect intellectual property and customer data.

"Because of the availability of money, financial companies are attacked by anyone and everyone," said Todd Inskeep, a consultant and former security executive at Booz Allen Hamilton and Bank of America. "Every other industry has assets that you can convert to money somehow. The financial industry actually has the money."

With that in mind, companies have invested heavily on continuous security validation (CSV) and breach/attack simulation (BAS), which encompass everything from pen testing, red-, blue- and purple- teaming and vulnerability management to proactive threat hunting and external attack surface management.

In these areas, companies have had some successes, and made plenty of mistakes along the way.

One area of success is in how financial firms segment their systems, making it harder for attackers to move around in the network.

On the downside, because these companies are risk-averse, they are often slow to embrace new technology and improve processes.

This is the story of where financial firms have struggled, where they've succeeded and what security teams in other industries can learn from their experiences.

Complexity and segmentation

In the financial sector, the complexity of how business is done can be both a strength and weakness.

Selim Aissi has seen this dynamic up close, having spent more than six years as CISO at Ellie Mae following a stint as vice president of global information security for Visa. He details the complexity – particularly when it comes to money transfers:

"We had several hundred financial institutions connected to Fannie Mae. That's a huge attack surface," he said. "What magnifies the risk is that a lot of the protocols used for those money transfers, such as SWIFT, haven't been upgraded for some time. Do they need to be redesigned for modern communications? From a practical perspective, it is very difficult to transform communications between financial

OUR EXPERTS: CSV/BAS

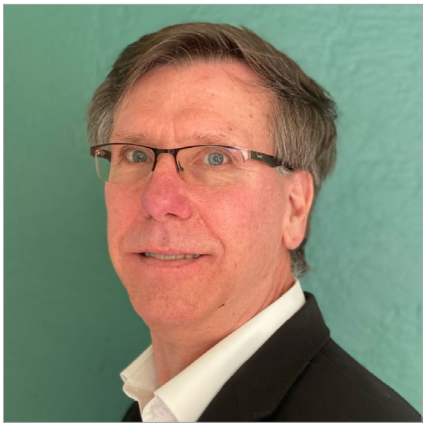
Todd Inskeep: Security consultant
Selim Aissi: Former CISO, Ellie Mae & VP/global information security, Visa
Umesh Yerram: Global CISO, Cboe Global Markets, former vice president, information security & chief data protection officer, AmerisourceBergen
Steve Zalewski: Former CISO, Levi Strauss & Co.
Jeff Farinich: CISO, New American Funding
Aaron Card: Director, digital forensics and incident response, NTT
Jacob Ansari: CISO, Schellman & Company
Jeff Dimmock: SpecterOps director, Adversary Simulation
Daniel Wallance: Associate partner, McKinsey
Joseph Krull: Senior analyst, Aite Group
Rob Ragan: Principal security researcher, Bishop Fox
Bryce Austin: Security consultant

71%
of all data breaches are financially motivated

— Verizon

institutions."

Because so many financial institutions use these networks, any communication change would have to be adopted by all of them. Financial institutions, as a rule, are extra-careful and therefore slow — resistant, even — when it comes to adopting changes.



Steve Zalewski: Former CISO, Levi Strauss & Co.

One of the security strengths in finance that differentiates it from almost all other verticals is a far more sophisticated and strict level of segmentation, something that began decades ago with trader activity on trading floors.

"The trading floor systems are definitely very isolated systems," said Umesh Yerram, the global CISO at Cboe Global Markets, which owns the Chicago Board Options Exchange and stock exchange operator BATS Global Markets. "Traders still have the old system hardened that they use on the floor."

Before he joined CBOE, Yerram was vice president of information security and the chief data protection officer at AmerisourceBergen, a Fortune 8 enterprise with $190 billion in revenue last year.

Patch management: a moving target

That high level of network isolation illustrates the core advantages — and struggles — financial institutions face while tweaking CSV and BAS strategies.

Consider, for example, patch management. There is little debate that it is simply impossible for enterprises to keep on top of patch management, given the torrent of vendor patches and new holes discovered daily. The typical response is to triage, to only patch the most sensitive parts of the system and/or the segments that house the most valuable data.

The problem with that strategy is that it creates a porousness in the environment that allows an attacker to reside anywhere — especially in a seemingly innocuous low-priority area such as within a networked scanner or the menus-sharing portion of the cafeteria page — and then slowly move to anywhere else, such as payroll or R&D or another high-priority target.

"With patch management, there is simply never enough money, time or resources. We are literally playing a shell game," said Steve Zalewski, former CISO at Levi Strauss & Co. Though not a financial company, Levi Strauss interfaces heavily with the financial sector as a retailer processing customer credit cards. This is where automated CSV can help. It correlates vulnerabilities found in the network to real threats by operationalizing threat intelligence, so you know which vulnerabilities in the organization's network are being exploited by threats found in the wild.

(Lack of) visibility in the cloud

Zalewski also expresses concerns about the sharp increase in enterprise data residing in the cloud, whether it is authorized or shadow IT. And although cloud systems can be reasonably secure, they do not provide anywhere near the level of visibility and controls that exists in the rapidly disappearing on-prem systems. He argues, too, that cloud strategy can pit CIOs against CISOs.

"Cloud impacts negatively. CIOs are measured on efficiency; CISOs are measured on effectiveness," Zalewski said. "The drive to cloud is an efficiency play."

Given that security controls are less in most cloud environments compared with on-prem, "CSV and BAS are having to be revisited," Zalewski said. That is because

70%

of financial companies experienced a cybersecurity incident in 2018 and 2019

— Clearswift

the environment has changed so sharply since the enterprise's CSV and BAS strategies were likely crafted. "The foundational assumptions may no longer be valid, especially about perimeters I can control. We must adapt. We now have this push for effectiveness when efficiency is driving us into new areas. The rules of engagement have changed."

Jeff Farinich: CISO, New American Funding

Another financial industry CISO, Jeff Farinich of mortgage company New American Funding, sees the lack of visibility and controls in most cloud environments as something that must be addressed going forward.

"(Cloud vendors) make changes constantly" without the knowledge or approval of their enterprise tenants, Farinich said. "Where are all of your objects in the cloud?"

Meanwhile, pen testing in cloud environments raises contractual and legal issues, with few of the largest cloud platforms (where most Fortune 1000 enterprises are found) permitting such efforts. Officially, it is to try and avoid problems that could disrupt other corporate tenants, but some suspect it is more about the fear of what tenants would find.

"I don't have an answer to how I am going to pen test my AWS and Azure environments — yet," Farinich said. "I don't think the tools have caught up to go into deep pen testing in your cloud environment."

The problem with "checklist" pen testing

The most controversial of the CSV tactics is penetration testing. Whether it should be done is not the question. Depending on the CISO involved, the questions focus on who is to do the pen testing (internal or external), how far should they go and the frequency.

Pen testing itself has two very different functions. One tests defenses and the other is an open-ended examination of what is left, such as PII, credentials, sensitive intellectual property or even a decryption key. Most internal executions focus on defense testing, ignoring the "let's see what we can find" function.

Internal versus external has its own set of pros and cons. Internal is usually a lot less expensive, but it suffers from the company politics problem of familiarity. When internal people find sloppy work and other headaches, they may know the people involved in such errors. Do the internal people not want to get their friends in trouble? Will they hold back reporting what they find? Will they inappropriately tone it down? A third-party pen tester is more likely to report everything, without hesitation.

> "I don't have an answer to how I am going to pen test my AWS and Azure environments – yet. I don't think the tools have caught up to go into deep pen testing in your cloud environment."
>
> *– Jeff Farinich: CISO, New American Funding*

Ellie Mae's Aissi says he opted for both. "We used external independent pen testing to augment the internal pen testing," he said.

Another cybersecurity consultant, Aaron Card, director of digital forensics and incident response at NTT, also expresses concern that pen testing results vary far too widely and are at the mercy of individual approach differences.

"For many penetration testing scenarios, the results can be unrealistic or not useful, lulling the organization into a sense of well-being. This is due to the varying methods of attack that are left up to the tester. Many

65%

of the top 100 US banks failed web security testing in 2017

— IBS Intelligence

organizations/CISOs simply name the targets for the testers," Card said, adding:

"They do not put together any form of attack planning or methodology, so the result is that your results are only as good as the tester and their methodology."

He warned: "If (pen testers) don't use a clear threat modeling framework, then they are just kind of shooting from the hip based on knowledge and experience." Another issue that can be remedied by incorporating an automated CSV platform: The issue of familiarity goes way. The results are captured and recorded. Once known, they can't be unknown unless someone criminally deletes the reports.

Jacob Ansari: CISO, Schellman & Company

Getting back to the original mission

Much has changed in the decades since pen testing began, and Jacob Ansari, CISO at security and compliance assessor Schellman & Company, argues that it is worth noting how pen testing has drifted away from its original intent and design.

"It's easy to get lost in the thicket of CSV and BAS terminology and ideas, but we should remember that the original idea of penetration testing in the 1980s and 1990s was simulating actual attacks to evaluate the effectiveness of our defenses," he said. "Somewhere along the way, many organizations decided that what they wanted was a relatively tame exercise in shaking the vulnerability tree to see what falls loose. Then each item could be shorn of its context and explained away."

He added: "The idea of red teaming tries to recreate that original intent: How can an attacker link these events together to create a serious adverse impact? How can we grow our capability for imagining what an attacker might do, and how do we prevent these from happening? New technologies and suppliers can help us with these elements, but an organization that isn't willing or capable of considering these kinds of actions or that wants to constrain these kinds of tests because they fear — perhaps fairly — disruption to production or findings that require a lot of investment to remedy won't realize much benefit from them."

This forces the key issue: When problems are discovered, does security have the time and resources to adequately chase each down and affect repair? Sometimes, especially with the largest enterprises, this can get into another internal political problem, with one security team being pitted against another, a tactic that can undermine the desired harmony of the security operation.

This worries Jeff Dimmock, SpecterOps director at consulting firm Adversary Simulation.

> "If (pen testers) don't use a clear threat modeling framework, then they are just kind of shooting from the hip based on knowledge and experience."
>
> *– Aaron Card: Director, digital forensics and incident response, NTT*

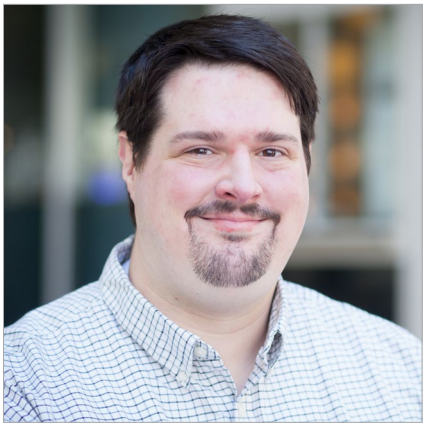
"CSV or BAS offerings — whether services or products — are ultimately just another tool to be used as part of a larger security program to achieve a desired effect, yet enterprises often adversarially architect these components against detection teams. This leads to attempts to game/bias testing, increasing tensions between teams and [delivering] a lack of meaningful progress," Dimmock argued.

$18.3 million

Average cost of a cyberattack in the banking sector

— Accenture

He added: "The correct approach is one that encourages collaboration. The myriad CSV or BAS offerings should be designed with a focus of stress-testing response efficacy and finding gaps in detection capabilities. Deficiencies found through validation testing within an organization should not be viewed as a black eye for detection teams."



Jeff Dimmock: SpecterOps director, Adversary Simulation

Even if an enterprise security operation properly identifies and addresses/fixes every hole and errant PII record found in its systems, does the team take it to the next logical step? Does it investigate how that problem happened? The argument goes: If the root cause is not identified, is the system any more secure than it was beforehand?

This is a key concern for Daniel Wallance, an associate partner at consultancy McKinsey. He worries that many CISOs are not, indeed, taking the next step. "They're not asking 'Why and how did that PII get there? Was there a deficiency in the controls? They need to look at how it got there as an after-the-fact analysis. If it's the discovery of intruders on the network, do they explore how they got there? Are the controls actually leading to information that will prevent and block PII from leaving in the future?"

Joseph Krull, senior analyst for cybersecurity at consulting firm Aite Group, still sees the checklist mentality surfacing.

"The majority of organizations — including financial services companies — are still stuck in the past with regard to cybersecurity validation," he said. "Executives commission penetration tests because either their internal audit departments put it on the annual audit calendars, or their regulators are looking for evidence that a penetration test has been performed in the recent past. To be sure, penetration testing can be a highly effective detective control. The problem is that we are not doing them often enough."

Most compliance-driven penetration testing is done annually, and forward-leaning companies may do quarterly or even monthly tests, he said. But these tests are simply snapshots in time. If even one administrator makes a mistake, such as a poorly executed configuration change, this can open an exploitable weakness that might not be detected or stopped until the next penetration test.

The lesson here: Incorporate automated CSV to be able to test more frequently, weekly or even daily, and use a mix of human-powered pen testing and automated CSV.

> "The correct approach is one that encourages collaboration. The myriad CSV or BAS offerings should be designed with a focus of stress-testing response efficacy and finding gaps in detection capabilities. Deficiencies found through validation testing within an organization should not be viewed as a black eye for detection teams."
>
> *– Jeff Dimmock: SpecterOps director, Adversary Simulation*

Another long-standing concern — as relevant in 2021 as it was 10 years ago — are security operations that are quick to embrace the latest security tools, even if their environments have massive security holes in the fundamentals.

"Red teaming and pen testing are sexy," said security consultant Bryce Austin. "But for 90% of the companies I work for, it's

127 days

How long stolen cardholder data remains captured

— SecurityMetrics

wasted money. Some of these enterprises have ERP that still run on Windows Server 2008; They are authenticating people in clear text. And yet they are still spending money on red teaming.

"I tell them, 'If you want to bullet-proof your car windows, OK, but maybe you should get your brakes fixed first.'"

Automation pros/cons

The challenges described by our experts brings us to a solution many organizations clamor for: automation. In theory, automation would address a lot of the problems discussed. Automated CSV platforms put the adversary in the hands of the blue (detection) team. They can test their detection capabilities — tech, processes and SIEM rules, for example — and make improvements more quickly, thus reducing stress.

> "I tell them, 'If you want to bullet-proof your car windows, OK, but maybe you should get your brakes fixed first."
>
> – *Bryce Austin: Security consultant*

The challenge inside the CISO's office right now is that automation forces theory to collide with reality.

CISOs "are underwhelmed by many fully automated solutions," said Rob Ragan, principal security researcher at consulting firm Bishop Fox.

To be fair, Ragan adds, much of that stems from the CISO's staff not putting in sufficient time to customize and otherwise tweak these applications for their environments. That said, the cybersecurity market suffers as a whole from inflated expectations.

CISOs need to push harder to better understand what they are buying.

"Did [CISOs] not understand that they have to invest hours of their own team's time into this? That's important because no one [on those CISO teams] has time to do anything with it," Ragan said. Before making any of these automated purchases, security teams must "insist on a detailed meeting with the technical folk.

"Get a trial, proof of value, a full demo trial. Try it for a few months and have a quick out-clause. Understand how much it is to set it up properly," Ragan said. ■

LESSONS LEARNED:

Suggestions for effective security validation and breach simulation programs, based on the experiences of the financial sector:

- Consider incorporating automated CSV with manual pen testing to achieve consistency and objectiveness.
- Automated tools have pros and cons when deployed as standalone. But as a supplement to manual (internal and external) testing, it can catch much that humans might miss and automate repetitive testing — allowing pen-testers to do more.
- Porousness is your enemy.
- Emulate the financial sector's robust use of segmentation, which will help in many areas of defense, especially patching.

92%

of ATM machines are vulnerable to hacks

— Positive Technologies