ATTACKIQ®

Case Study

Efficiently Assessing Cybersecurity Risk Across a Leading National Bank's People, Processes, and Technology

"Financial services is an industry in the crosshairs of cyberattacks," says the vice president and manager of corporate information security for a leading commercial bank in the United States. Concern about security risks permeates the institution, from front-line employees to the board of directors.

This bank has dozens of branches and hundreds of ATMs across multiple states. Across all its business units, the company's culture is very customer-focused, an approach that feeds the emphasis on cybersecurity.

> *"What intrigues me about the AttackIQ platform is that it enables us to more easily perform risk assessments on our internal assets. Our testing processes need to ensure we have all the right controls in place, and if one security solution isn't supporting a particular control, another one is."*
>
> – Bank Vice President and Manager of Corporate Information Security

"As an organization, we always think of the customer's perspective first," says a senior information security analyst at the bank. *"They are relying on the bank to keep their money and data safe, and depending on our business units to work smoothly every day, without interruption. Effective cybersecurity is key to meeting customer expectations."*

Achieving the bank's cybersecurity objective requires constant vigilance on the part of the information security team. *"Threats are sophisticated these days; we can't just patch the well-known vulnerabilities,"* the senior analyst says. *"Attackers can pivot and navigate throughout a network without being detected. That makes it difficult to lock down the network using only hardware configurations, software patches, and user access policies."*

Adds the vice president and manager of corporate information security, *"What keeps me up at night is fear that we might miss a significant threat or vulnerability. It is imperative that we have the best possible tools in place for protecting our systems and data, and ensure that they are all working together properly."* To that end, when the VP and their colleagues learned about breach and attack simulation (BAS) software, they immediately understood the prospective benefits of adding such a solution to their security infrastructure.

Legacy Approach to Cybersecurity Testing

This bank invests significant resources in cybersecurity, and management wants proof that technology solutions are working as intended. The bank formerly engaged external penetration (pen) testers annually to determine how well its security controls were working.

CUSTOMER

A Leading National Bank

LOCATION

United States

INDUSTRY

Financial Services

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Control Auditing
- Investment Decision Support
- Post-Incident Response Remediation

PROJECT BUSINESS IMPACT

- Continued customer confidence in security, for a competitive advantage
- Evidence to potentially support a higher maturity rating with the Office of the Comptroller of the Currency (OCC)
- Same-day answers to management inquiries about whether bank assets are safe from new or prominent types of attacks
- Better technology investment decisions

> *"The more I see of the AttackIQ solution, the more impressed I am. Its integration with MITRE ATT&CK allows us to take a real-world attack scenario, understand each of the attack's components, and then unit-test those individual components in our environment."*
>
> - Bank Senior Information Security Analyst

Legacy Approach to Cybersecurity Testing (cont.)

The security team was concerned about the ongoing efficacy of this approach. *"Hiring a pen tester once a year to produce a report does not provide us with all the information, we would like to mitigate all threats we may face,"* the senior analyst says. "*The attack landscape is ever-changing, and we never know when an employee might inadvertently open a new gap in security controls by changing a configuration."*

"To stay a step ahead of the bad guys," they continue, *"we needed visibility into our controls' effectiveness that was closer to real time. We couldn't perform pen tests much more frequently because they were expensive, and because scheduling, onboarding, and preparing for the tests was very labor-intensive. We needed a solution that would streamline testing."*

The bank wanted to automate assessments of preventative and detective security controls. It also needed to demonstrate to regulators that its security met compliance standards. *"We needed evidence that settings and processes were in line with expectations for a bank of our size,"* the corporate information security VP says. *"Most important, we wanted the ability to see what would happen if a particular attack threatened our environment. We knew breach and attack simulations could give us the information we needed to mitigate the risk of future attacks from being successful."*

Investment in Automation and Insights to Controls Validation

AttackIQ provides a security optimization platform to automatically run testing scenarios that mimic the likely tactics, techniques, and procedures (TTPs) of attacks the organization might face. It enables security teams to consistently validate the effectiveness of those security controls that are working, while revealing whether organizational response to the attack meets expectations — in terms of not just technology, but also people and processes. And if controls fail to thwart a simulated attack, then the security team gains insight into areas of the security infrastructure (technology, processes, and people) that need shoring up.

Among the options to continually validate security controls, the AttackIQ Security Optimization Platform stood out. *"What intrigues me about the AttackIQ platform is that it enables us to more easily perform risk assessments on our internal assets,"* the corporate information security VP says. *"We need defense in depth, so we utilize a range of security solutions. Our testing processes need to ensure we have all the right controls in place, and if one security solution isn't supporting a particular control, another one is."*

The VP and their team wanted to understand how the bank's security solutions were communicating with one another, as well as how staff were using those systems to protect the bank's assets. However, they did not have much excess time to dedicate to testing. Automation in the AttackIQ platform, along with the solution's integration with the MITRE ATT&CK framework, put ongoing, routine, best-practice testing within the bank's reach.

> *"To have regular pen testing, you would need a full-time staff member just to manage the back end. With AttackIQ, we can just fire up the tool, choose a scenario, and tell it to run. The difference in resource requirements is night and day."*
>
> - Bank Senior Information Security Analyst

Investment in Automation and Insights to Controls Validation (cont.)

"AttackIQ makes it easy to integrate this industry-standard framework into our risk assessment process," the VP says. *"The Security Optimization Platform also enables us to frequently test our detective and preventive controls. It also helps inform our incident-response process with an understanding of what would happen in an actual attack."*

The senior analyst agrees. *"The more I see of the AttackIQ solution, the more impressed I am,"* they say. *"Its integration with MITRE ATT&CK allows us to take a real-world attack scenario, understand each of the attack's components, and then unit-test those individual components in our environment. Every attack is different. The endgame might be to exfiltrate data or install ransomware, but there might be six different types of attacks that can reach that end. It doesn't make sense to just say 'We're protected against ransomware,' because what type of ransomware attack are you talking about? You have to cover all the different attack vectors to actually be prepared."*

Equally important for a midsize financial institution, the Security Optimization Platform comes with templates of common attack scenarios, as well as blueprints that guide staff through establishing a BAS strategy, setting goals, and defining how the organization will use the solution.

Leveraging the AttackIQ Platform

The information security team has run its first assessment in the Security Optimization Platform, simulating an attack against a few server groups. The bank's security operations center (SOC) is currently evaluating the results. *"They are looking at gaps the simulation revealed and planning remediation,"* the VP says. The next step is to run a simulation that tests the bank's incident management staff. *"We plan to use the AttackIQ platform to regularly put our technology infrastructure through its paces, but we also will test our people and processes to be sure that everyone and everything is responding properly to threats."*

When testing reveals that a control is ineffective, the bank will attempt to mitigate the problem, then retest. *"We want to make sure subsequent attack simulations do not identify the same issue, which would indicate we were unable to lock it down,"* the senior analyst says. *"It is important to have the AttackIQ platform to let us know whether the problem is fixed."* Along the same lines, security controls validation reports from AttackIQ will provide support for the bank's efforts to achieve a higher level of cybersecurity maturity as determined by its U.S. federal government regulatory agency.

Leveraging the AttackIQ Platform (cont.)

This leading bank will also use the Security Optimization Platform to perform one-off tests when needed. *"This tool gives us the flexibility to answer ad hoc questions about the state of our security controls,"* the senior analyst says. *"If our CIO reads about a new type of attack and wants to know how our controls perform against that particular threat, we can set up a scenario that emulates the attack in question. We can let her know the results by the end of the day."*

Another use case that this bank envisions is investment decision support. *"If our tests reveal a gap between security controls, we can run simulations to compare different options for eliminating that gap,"* the VP says. *"The AttackIQ platform can help us build a case for one tool over another. It's powerful to show upper management: 'Here's the scenario we're concerned about, and here's what this new security solution would do if we were attacked.'"*

All these use cases are possible because the platform automates scenario testing, thus minimizing the staff time required. *"To have regular pen testing, you would need a full-time staff member just to manage the back end,"* the senior analyst says. *"With AttackIQ, we can make simulations a routine part of operations, because we can just fire up the tool, choose a scenario, and tell it to run. The difference in resource requirements is night and day."*

ATTACKIQ®

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.