White Paper

The CISO's Guide to MITRE ATT&CK® for the Financial Services Sector

How to build a program of threat-informed defense in an industry under regular cyberattack.

Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an *"as is"* basis. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

Executive Summary

Financial Services Firms Need Threat-Informed Defense

Chief information security officers (CISOs) in the financial services sector are well aware of the cybersecurity risks their institutions face. Across every type of organization, the frequency of threats continues to accelerate. The FBI reports that its Internet Crime Complaint Center (IC3) received 69 percent more complaints in 2020 than the year before, and Americans lost more than $4 billion to cybercrime in 2020 alone.[1]

Within the burgeoning cyberattack industry, financial institutions are in practitioners' crosshairs. That's why financial firms' CISOs have been investing heavily in cybersecurity for years. But is it enough? Unfortunately, many CISOs don't know. They lack a data-driven method for determining whether their controls would be effective against the threats with the most potential to harm their institution. That's where MITRE ATT&CK® plus breach and attack simulation for automated control validation comes in.

Chief information security officers in financial services businesses need to build a security program based on the concept of threat-informed defense. To do so, they can leverage the MITRE ATT&CK framework to understand the tactics, techniques, and procedures (TTPs) that attackers are most likely to use against their institution, as well as the potential impact an attack using those TTPs might have. Then they need to develop an assessment program that simulates real-world breaches and attacks to determine the effectiveness of their institution's technologies, processes, and people in defending against the threats they've identified as high-priority.

Data gathered in this process is extremely helpful in both guiding security investment decisions and supporting regulatory compliance. It can also build confidence among the financial institution's risk and security teams, compliance and auditing teams, board members, and executives that the institution's security program is proactive, strategic, and threat-informed.

Breach and Attack Simulation for Automated Security Control Validation

Gartner defines breach and attack simulation (BAS) technologies as capabilities "that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means." The primary use case (of many) for a breach and attack simulation platform is automated security control validation. By continuously and automatically testing security controls against real-world threat behaviors aligned to the MITRE ATT&CK framework, cybersecurity leaders can measure security program performance, identify security gaps, and prioritize program investments. With real-time data about their program's performance, security leaders can make better informed decisions to optimize business outcomes across the organization.

Leading-Edge Doesn't Mean Impenetrable

The institutions holding society's riches for safekeeping have always proven an attractive mark for prospective thieves. Twentieth-century brick-and-mortar bank robber Willie Sutton reportedly explained why he targeted banks by saying "because that's where the money is." And interest in robbing banks has only grown in the digital era.

Ever since the internet emerged as a driving force in global communication flows, financial institutions have been under cyberattack. The Carnegie Endowment for International Peace has collected information on 200 cybersecurity incidents targeting financial institutions across a little more than a decade.[2] Those are all major incidents that were made public, so it's likely that many more security events with a smaller impact failed to make the list. By 2017, the G20 was worried that "the malicious use of information and communication technologies (ICT) could ... undermine security and confidence and endanger financial stability."[3]

> *"Malicious actors are taking advantage of digital transformation and pose a growing threat to the global financial system."*[7]

As the International Monetary Fund more recently put it: "Today, the assessment that a major cyberattack poses a threat to financial stability is axiomatic — not a question of if, but when."[4] And the Federal Reserve Bank of New York delineates the scope of the risk by estimating that "the impairment of any of the five most active U.S. banks will result in significant spillovers to other banks, with 38 percent of the network affected on average."[5]

Financial institutions' need for highly effective cybersecurity has been demonstrated time and time again. One of the largest cyberattacks of all time was hackers' attempted theft of nearly $1 billion from Bangladesh's central bank.[6] In February 2016, hackers launched malware within the Bangladesh Bank network, stealing the bank's credentials for the SWIFT funds transfer system. Posing as employees of the Bangladesh Bank, the hackers issued 35 fraudulent funds transfer requests to the New York Fed. Only four of the 35 succeeded, simply by chance: One of the fraudulent requests included a misspelled word, while others requested funds be transferred to a bank whose name is similar to that of a company on a sanctions blacklist. Still, the attackers got away with $81 million, making this one of the richest bank heists ever.

Are the Industry's Substantial Investments Enough?

Chief information security officers in financial institutions are inundated with information about the risks, and their sector tends to lead the way in terms of cybersecurity innovation. Financial services firms typically have large security teams with access to substantial resources. Banks that may not be sufficiently motivated by the threat landscape are compelled by external regulators to put stringent security controls in place. From PCI DSS[8] to the New York Department of Financial Services (NYDFS) Cybersecurity Regulation,[9] financial services CISOs are under scrutiny. Most go to great lengths to protect their organizations' applications, data, and people.

That work will never be done. The threat landscape is continuously evolving, which means financial institutions' defenses must always be improving as well. Ongoing innovation is absolutely crucial for security teams within the financial services sector. So is making sure that those innovations — and the overall security infrastructure — can effectively thwart any prospective attacks. And that's where some financial institutions are currently falling short.

Chief information security officers need to be confident that all their carefully constructed controls are working as intended and protecting what they're supposed to protect. To build this confidence, they need to continuously validate those controls; a traditional red team exercise a couple of times a year is no longer enough to protect organizations from the onslaught of new and more sophisticated attacks.

For CISOs looking to build a more dynamic, efficient, and effective approach to understanding if their controls are working to protect their organizations, what's the best place to start?

Start by Leveraging the MITRE ATT&CK Framework

Developed by the nonprofit MITRE Corporation, the MITRE ATT&CK framework is a knowledge base of adversary TTPs that have been observed in cyberattacks around the world. The framework also provides a detailed description of sub-techniques for each TTP, lists threat actors known to use it, and maps the threats to specific security controls designed to thwart them. It is widely regarded as the most authoritative and comprehensive explanation of TTPs available to cybersecurity professionals.

MITRE ATT&CK is crucial in developing a program of threat-informed defense because it helps an organization's defenders zero in on the threats most likely to have the greatest impact on their institution. A financial institution's security team can't protect their IT infrastructure against every threat it might someday face. Limited time and resources mean that even the most robust security program must focus on the subset of TTPs that pose the biggest risk.

A security team can leverage the MITRE ATT&CK framework to determine what attackers or organizations are most likely to come after its institution, and how they're likely to do it. From there, the team can establish a list of high-priority adversary TTPs, with a detailed description of each and an inventory of threat actors known to use those techniques. The CISO can then map out the potential ramifications for the institution of each TTP. Some leading CISOs have developed a security risk rating that gauges the threat level posed by each tactic, technique, or procedure. The end game of this process is to develop a "most wanted" list of attackers and TTPs that the company's control assessments should focus on.

> *"There is long-term value to be gained through ATT&CK. It's a unifying effort and a way that we can all refer back to it. It's the mother brain."*[10]
>
> — Pete Luban, Head of Cybersecurity and IT Risk
> Dimensional Fund Advisors,
> AttackIQ Customer Case Study

Following this analysis, the financial institution's security team can map the defenses they currently have in place to the most problematic threats. This process presents an opportunity to identify clear gaps in coverage and to prioritize security investments that address the most glaring deficiencies in the institution's current state.

The next step is to develop an assessment program through which the security team can determine whether the measures they have in place — including technology, processes, and people — are actually working.

Three Key Principles Should Drive Security Control Validation

The financial institution's assessment strategy should revolve around three key principles. One is that information about threats, controls, and the effectiveness of those controls needs to be consistent throughout the organization. It's crucial for everyone involved in security management to be on the same page about the TTPs that pose the greatest risk to the organization and about their ability to defend against them. This is another benefit of utilizing the MITRE ATT&CK framework: Prioritizing TTPs based on this authoritative external source can help build internal consensus that may otherwise be more difficult to come by.

As testing gets underway, information sharing will become even more crucial. Data — on both real-world security events and controls' performance in security assessments — should be amalgamated so that everyone, at all levels of the company, is working off the same information. All security data should flow into a data lake, where users at different levels can derive their own views, pull their own reports, and draw their own conclusions. Such democratization of data leads to better security decisions on a daily basis, and provides a more fertile ground for ongoing security innovation throughout the financial institution.

A second guiding principle for designing the security assessment program is to make sure routine testing is forward-looking, not just a review of historical analyses in the security information and event management (SIEM) system. Keeping a future focus is necessary because the ability to make data-driven decisions is evolving. The financial institution CISO needs processes and tools for evaluating how effective the security program is, and building block number one is the evaluation of individual security controls. Security teams need a clear view of how each control is currently performing against specific TTPs on the "most wanted" list — not how well it performed two years ago or even six months ago.

The third key principle is that threat-informed defense must be built on an ongoing cycle of assessments performed via attack simulations and organizational mitigation efforts. A wide range of assessments should test the people, processes, and technology the company has in place, from many different angles. These assessments should seek to uncover any gaps in protection that require mitigation through technology investment, process change, or staff education. Their results can support the business case for investing in needed changes.

In an effective security program, these assessments run regularly, year-round. Once-a-year testing doesn't cut it for financial institutions operating under the cloud of constantly changing threats. The more frequently assessments happen, the more likely they are to quickly discover any change to the security environment, such as a new software configuration or staffing change, that alters the controls' effectiveness. Moreover, any time financial institutions mitigate control gaps uncovered by their assessment program, they should re-test the controls that previously failed to make sure their mitigation efforts solved the problem.

Enter Automated Security Control Validation

Even the largest financial institutions struggle to staff a red team that can test protections against the full scope of threats to all their business groups and geographic locations. Testing should be ongoing and continuous, against all the prioritized attack vectors the financial institution's different divisions and branches might be exposed to, and it's nearly impossible for a human team to provide such an assessment regime.

Alternatively, breach and attack simulation software can run assessments on a regular basis, making them a routine part of security operations. Leveraging a BAS tool can make the red team staff more productive. The team can leave routine tests to the software and take on more complex or one-off tests themselves, expanding the breadth of organizational activities that the assessment program can evaluate. Leveraging a BAS tool that ties in with the MITRE ATT&CK framework gives a financial institution CISO a leg up in developing a cohesive, integrated assessment program.

> *"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."*[11]
>
> ***— Bank Vice President and Manager of Corporate Information Security, AttackIQ Customer Case Study***

The AttackIQ Security Optimization Platform, for example, provides scenarios to automatically assess your security controls against specific TTPs in the MITRE ATT&CK framework. Security teams can leverage these attack simulation templates to test controls targeting their institution's "most wanted" threats. Once the tests are set up, they run automatically and staff can launch them with the press of a button. This means that even for red teams capable of performing some ongoing penetration testing internally, the Security Optimization Platform extends their reach by assessing the security infrastructure against a broader swath of threats and by testing more frequently.

By the same token, automated testing enables the optimization of regulatory compliance. The frequent and thorough control assessments help prove to regulators that a financial institution's security controls are effective.

Keep in Mind During Program Design

A CISO designing an assessment strategy around automated control validation software should keep in mind that testing isn't a project, it's a program. Infrequent penetration tests are not adequate for any business, and especially not for a financial institution in the crosshairs of attackers worldwide.

In the Bangladesh Bank heist, for example, the hackers used a custom malware toolkit they had developed to cover their tracks in the SWIFT Alliance Access system. The toolkit enabled them to delete records of their logins and transfer requests, bypass validity checks, manipulate balance reporting, and prevent the printing of transaction logs.[12] These attackers specifically targeted the Bangladeshi central bank, but every financial institution faces the risk that attackers might pull off a highly sophisticated heist. It is unacceptable for a financial institution to allow for the risk that attackers may be able to navigate around its network for weeks or months before the breach is detected.

It's important to keep in mind that you cannot fix every issue at once. Continuous testing supports continuous improvement. The ideal approach to control validation is to find gaps through testing, incrementally improve control effectiveness, retest, identify new opportunities for improvement, and then continue the cycle. Such a regime of continuous testing and improvement will refine the security team's detection capabilities and enable an increasingly difficult set of scenarios, thus continuously improving the institution's threat detection capabilities.

Conclusion

Shift to a Threat-Informed Defense Mindset

Perhaps most critical for a financial institution CISO is to create the cultural change they envision. Routine assessments are a key element of threat-informed defense, but so too is a shift in the mindset of the entire security organization. The CISO needs to advocate for the benefits of building a security program around data on controls' effectiveness. External statistics on control failures support this shift: too many enterprise breaches succeed despite the presence of security controls. Research from a Poneman Insitute survey found that amongst over 500 information technology and security leaders across sectors, 53 percent said they were uncertain about the effectiveness and performance of their cybersecurity capabilities.[13] Such a lack of confidence in the organization's security readiness is unacceptable.

> *"MITRE ATT&CK gave us the ideal framework to meet our target use cases with AttackIQ's breach and attack simulation platform. It also made it easier to objectively manage accountability between the security operations, information technology, and our internal networking group. MITRE ATT&CK gave us a common language to use for precise communication amongst all of our cyberdefender stakeholders and clear and measurable data that we can all use."*[14]
>
> — Hedge Fund Analyst,
> AttackIQ Customer Case Study

Chief information security officers of financial services firms should communicate to the rest of their organization how the security infrastructure would be transformed by placing data at the center of all decision-making. Intelligence about specific TTPs from the MITRE ATT&CK framework would provide a better understanding of expected adversary behaviors and visibility into the institution's control effectiveness. Security teams can use authoritative MITRE ATT&CK information to rally around the true threats to their institution.

For financial institution CISOs, there's no time like the present to move to threat-informed defense. Overall, the FBI received more than 2,000 complaints about internet crimes every day in 2020,[15] and there's no sign that attacks will slow anytime soon. Confirming that security controls are effective is crucial to financial firms' regulatory compliance. It's also imperative for institutions seeking to avoid headlines such as "US Insurance Firm Hit by Cyberattack," "Wall Street Targeted in New Capital Call Fraud Scheme," or "Bank XYZ Data Breach."[16]

Financial institutions will inevitably become stronger when the security team has visibility into controls' effectiveness, as well as clarity on what is required to stay ahead of threats. Attackers looking for financial institutions to target are moving fast. Those institutions' CISOs should not delay their move to threat-informed defense.

Learn more about how to achieve cybersecurity readiness and effectiveness by signing up for AttackIQ Academy's free courses on uniting threat and risk management, purple team operations, and putting MITRE ATT&CK into practice at academy.attackiq.com.

Additional Resources

- Automation Transformation Calculator
- Podcast: Pete Luban of Dimensional Fund Advisors on MITRE ATT&CK and Security Optimization
- Customer Case Study: Hedge Fund

Citation

[1] "Internet Crime Report 2020," FBI Internet Crime Complaint Center, March 17, 2021.

[2] Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions."

[3] G20 Finance Managers and Central Bank Governors Meeting Communiqué, March 17-18, 2017.

[4] Tim Maurer and Arthur Nelson, "The Global Cyber Threat," International Monetary Fund, Spring 2021.

[5] Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis" Federal Reserve Bank of New York, revised May 2021.

[6] "The Billion-Dollar Bank Job," New York Times Magazine, May 3, 2018.

[7] Tim Maurer and Arthur Nelson, "The Global Cyber Threat," International Monetary Fund, Spring 2021.

[8] "Mapping PCI DSS to the NIST Cybersecurity Framework," PCI Security Standards Council, 2019.

[9] "Cybersecurity Requirements for Financial Services Companies," New York State Department of Financial Services, March 1, 2017.

[10] Pete Luban, quoted in "Dimensional Fund Advisors: Security Optimization in a Top Asset Manager," AttackIQ Customer Case Study.

[11] AttackIQ Customer Case Study, "Efficiently Assessing Cybersecurity Risk Across a Leading National Bank's People, Processes, and Technology."

[12] Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions."

[13] Jessica Davis, "Security Investments Increasing, But 53% Leaders Unsure of Effectiveness," Health IT Security, July 20, 2019.

[14] AttackIQ Customer Case Study, "Case Study: Financial Industry."

[15] "Internet Crime Report 2020," FBI Internet Crime Complaint Center, March 17, 2021.

[16] Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions."

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.