ATTACKIQ®

White Paper

The CISO's Guide to Cybersecurity Readiness

How to elevate cybersecurity program effectiveness and readiness through data-driven visibility.

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

Notice 2

Executive Summary 4

Threat-Informed Defense Improves Protection 4

Between a Rock and a Hard Place 5

Leading Causes of Opacity 5

Reimagining Cybersecurity Controls 6

Automation Makes Control Assessments Routine and Efficient 6

What Should the CISO Do? 7

Choose Metrics Wisely 8

Develop a Testing Strategy 8

Drive Testing Through Purple Team Operations 9

Establish an Overarching Assessment Program 9

Identify Underlying Organizational Issues 10

Shift to a Threat-Informed Defense Mindset 10

Conclusion: CISOs Steering in the Right Direction 11

Executive Summary

Threat-Informed Defense Improves Protection

It's not a question of if, but when, an attacker will break past an organization's cyberdefenses and intrude into the interior of its network infrastructure. Protecting against such threats is table stakes for chief information security officers (CISOs). What sets the best cybersecurity teams apart is their ability to understand the threats with the most potential to impact the organization and to plan how they will defend themselves and recover should such an attack occur.

The U.S. Department of Defense defines readiness as "the ability … to fight and meet the demands of assigned missions."[1] In cybersecurity, readiness means being fully prepared to defend the organization against a cyberattack. To achieve readiness, the organization should make decisions on the basis of real data and evidence of security outcomes. To generate data and ensure security outcomes, the security team needs to focus on strategies and solutions that answer several key questions:

- What attacks might happen to us?
- Are adversaries able to steal our data or hold us ransom?
- How well is our security program performing in relation to known threats?
- Are we getting the most out of our security investments?
- How effectively have we trained our team to counter incoming intruders?

Guesswork won't help with these questions. Security leaders need to understand whether the controls they have in place are effective and whether the organization is ready for the attacks that are sure to come. The question is if security teams have clear, data-driven visibility into their cybersecurity readiness. Their answers must be based on real-time performance data that can be shared with risk and security teams, compliance and auditing teams, board members, and executives. When they are, the CISO can be confident that the organization's security program is proactive, strategic, and threat-informed.

[1] Congressional Research Service, "The Fundamentals of Military Readiness," October 2, 2020.

Between a Rock and a Hard Place

As the frequency of cyberattacks continues to increase, CISOs are getting squeezed.

The transition to remote work for large swaths of the global workforce, combined with businesses' growing reliance on digital and cloud solutions for core capabilities, presents prospective attackers with seemingly limitless opportunities.[2] Meanwhile, corporate leaders conscious of the expanding cyberthreat landscape expect reassurances from security executives that their company's systems are safe. They also want to know that security investments are working as expected.

These assurances can be hard to produce. Spending on cybersecurity technologies continues to rise, yet successful attacks and data breaches keep occurring. The problem? Companies are putting dollars toward good technology — from endpoint detection to security segmentation — but those solutions aren't meeting expectations.

In some cases, that's because organizations failed to deploy best-in-class defenses. The SolarWinds intrusion revealed that some U.S. federal agencies had not adopted internal defense capabilities, like zero trust, that could have prevented an intruder from moving laterally. In other cases, organizations that have deployed best-in-class capabilities failed to test them against known threats. The best endpoint detection and response (EDR) functionality won't help if the system is not configured correctly or if the security team is struggling to operate effectively. Finally, some organizations' security teams, processes, and technologies are simply focused on the wrong threats.

Leading Causes of Opacity

Visibility into security effectiveness can also be stymied by personnel silos. For example, unless information flows freely between the blue team (responsible for defending the network) and the red team (responsible for testing the network's defenses), and the two teams are collaborating with a threat-informed mindset, issues uncovered through red team testing are unlikely to be resolved in a timely, efficient, and effective way to elevate security program performance.

How might this play out in practice? A major global bank recently analyzed the structure of its large security team to identify structural weaknesses. It discovered even more silos than it feared: three different red teams were operating independently, in different divisions of the company. Not only were the teams not communicating with one another, but they were operating outside the line of sight of executive management. The situation was inefficient, as each red team was reinventing the testing wheel. The siloed nature of their work prevented company-wide visibility into security effectiveness. Testing was happening, but the results were unavailable at the corporate level. As a result, the team lacked comprehensive visibility into its security program.

When the CISO lacks an overarching view of security events and testing results, crucial security decisions are based on only a subset of the company's information. And as the large bank's experience indicates, staffing silos may inadvertently result in data silos. In other cases, data silos are intentional: security teams may isolate and filter information as it moves up the corporate ladder so that senior management sees only the picture that middle management wants to paint. Limited visibility into the organization's security situation results in poorly informed decisions at the corporate level and ineffective controls.

[2] Scott Ikeda, "New Security Report Breaks Down Increase in Cyber Attacks Due to Remote Work: Lack of Training,Overwhelmed IT Departments Are the Main Issues," CPO Magazine, October 16, 2020.

Many businesses have implemented security information and event management (SIEM) technologies, with the goal of consolidating data across intractable silos. Unfortunately, the SIEM's information is, by nature, historical — it consolidates log file data, which can provide a view only of what happened in the past. It doesn't provide any insight into how well the security program might perform if and when it's tested by the adversary. Although logs are important for understanding the historic state of security information, relying on them to prepare for future threats leaves open the question of how well a security program will perform against a prospective real-world attack.

Reimagining Cybersecurity Controls

The purpose of security controls is to defend the organization against prospective attacks. Chief information security officers need to evaluate whether they have enough information to determine the readiness of those defenses. Several questions should be central to that analysis:

- What is our impact tolerance? What are the business processes we need to protect, and what would be the impact on those processes in the event of data corruption, malware, or a distributed denial of service attack?
- Are security decisions driven by data about the greatest threats to those business processes?
- Are routine security assessments forward-looking and predictive of controls' effectiveness, instead of being focused on the events and threats of the past?
- Do decision-makers have visibility to security effectiveness companywide, or is information siloed by geography, business unit, function, or another differentiator?
- Is data about controls' performance disintermediated so that security, risk, and compliance teams are working off of the same data?

A strategic security organization uses routine assessments to evaluate how controls are performing against the specific tactics, techniques, and procedures (TTPs) that adversaries are most likely to use against it. The control assessments are a routine part of security operations, performed on an ongoing basis, with performance against key adversary TTPs tested on a weekly or monthly basis.

Such regular and consistent assessments of controls' effectiveness enable the CISO to evaluate whether the company is prepared for likely attacks. They provide evidence for the executive team that the company is appropriately prepared, and highlight areas in which the program needs further investment or where the team could divest in controls that are no longer performing or needed.

Automation Makes Control Assessments Routine and Efficient

A security architecture built on routine assessments of controls' performance against real-world attacks enables threat-informed defense and cybersecurity readiness. The assessments gauge the effectiveness of both security staff and technology solutions at recognizing and thwarting attempted breaches and attacks. Successful tests validate that the security infrastructure is working as intended. Control failures highlight areas in which security needs to improve.

While red teams and penetration testing services could, in theory, provide such frequent testing, automation makes the breach and attack simulation environment more agile and up to date. Tests can run as often as security decision-makers want them to — including one-off assessments when new attacks happen to competitors or ransomware events hit other industries — so they can evaluate controls' performance from many different angles over any time period, rather than a single point in time. Controls that require mitigation can be re-tested at will.

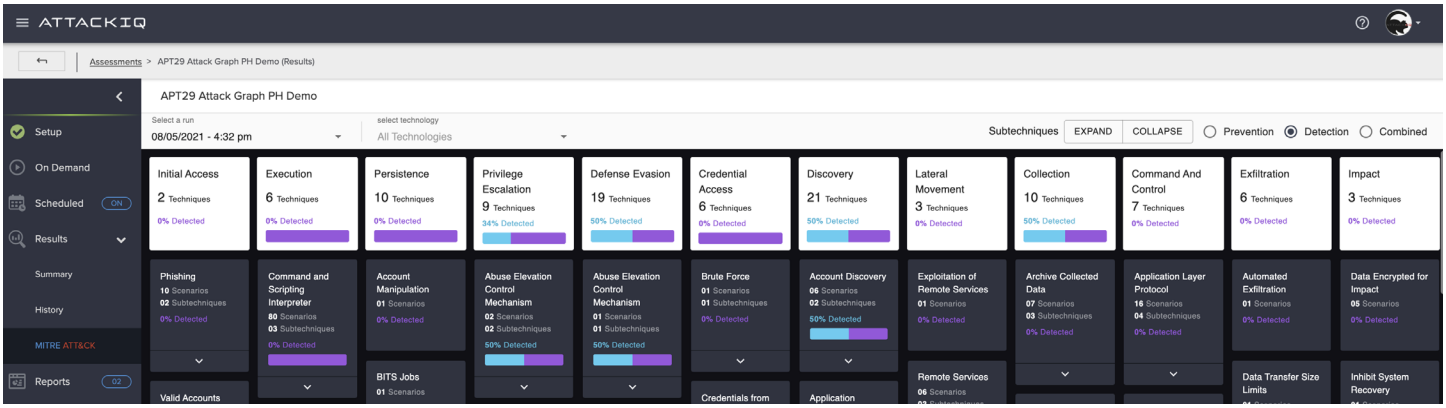
Automated testing also optimizes use of the CISO's limited resources. Manual testing can be expensive and inefficient. Penetration testers are typically external consultants who charge a premium for their expertise. In contrast, automated security control testing solves both cost and inefficiency challenges. CISOs wanting to explore the costs and benefits of their various options may find return on investment (ROI) calculations demonstrate that automation enables much more frequent and broad-based testing is available at the same cost.

Manual Testing Costs*	Automated Testing Costs*
$11,460,708	$586,704

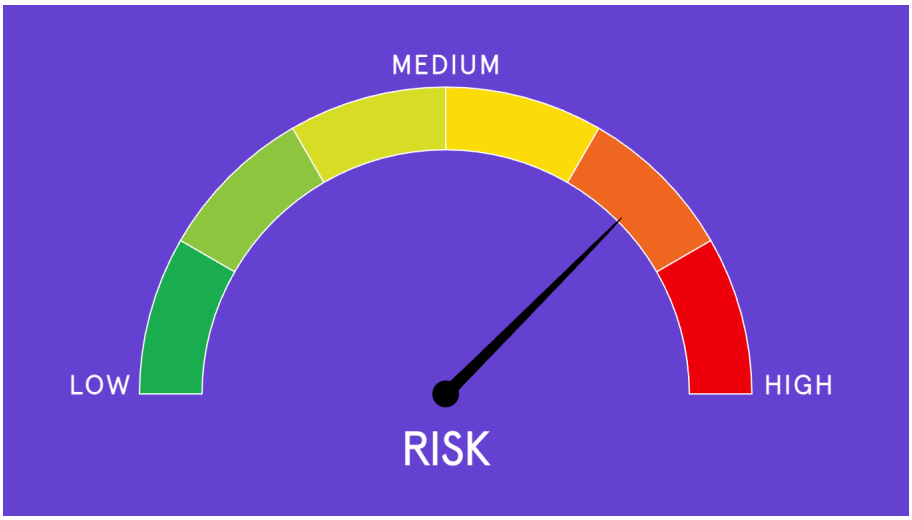
*Cost estimates include capital expenses such as hardware, software licenses, and vendor maintenance. Your total savings may be greater when you factor in operating cost reductions. Total cost is factored for one year.

What Should the CISO Do?

Chief information security officers that want to move their organization toward better control assessments and cybersecurity readiness need to develop a deep understanding of the threat landscape. The MITRE ATT&CK® framework is a great resource for determining which individuals or groups are most likely to attack an organization and which TTPs they would likely use to do so. Developed by the nonprofit MITRE Corporation, ATT&CK is a comprehensive knowledge base of adversary TTPs that have been observed in cyberattacks around the world. It provides a detailed description of every TTP and a list of the threat actors known to use it. CISOs can leverage this information to define the highest-priority TTPs for their security organization. From there, they can collaborate with other internal executives to map out the prospective ramifications for their specific organization.



CISOs should also look at creating a risk rating that gauges the threat level posed by each TTP. One option is to give each tactic, technique, or procedure a security risk score similar to the credit score the company's risk management team might create for customers and financial counterparties.



One goal of this stage of the process is to develop a "most wanted" list of attackers and TTPs that the company's control assessments should focus on. The security team can't protect the corporate infrastructure against every potential threat; limited resources and limited time to execute mean every security program must focus on the subset of TTPs that are most likely to do the most damage.

Choose Metrics Wisely

Once the CISO has defined the TTPs that matter most to the organization, the security team is prepared to plan their testing strategy. Step one is to develop metrics that will effectively evaluate each security control's performance. Each measure needs to gauge whether the control is detecting what it's supposed to detect and preventing everything it's supposed to prevent. Choosing the right metrics is vital to the success of a data-driven security program.

Develop a Testing Strategy

Next, the CISO and team are ready to flesh out the company's new assessment strategy. For each TTP on the "most wanted" list, the security team needs to determine how they will understand whether controls are capable of fending off that type of attack.

An effective controls assessment program revolves around three questions:

- Do our defenses actually map to likely threats?
- Do the security measures we have in place work?
- Are we prepared to respond effectively if something goes wrong?

A breach and attack simulation (BAS) platform that aligns with the MITRE ATT&CK framework can answer these questions by simulating, on a regular basis, the most likely adversary attacks the company is likely to face. These automated tests reveal gaps in security technologies, as well as in staff knowledge and reactions. And they provide the ability to mitigate problems that may arise, then re-test to validate the effectiveness of the response and identify opportunities for further improvement.

Drive Testing Through Purple Team Operations

The best threat intelligence and automated testing platform may fail to live up to its potential if the corporate security team isn't testing defenses continuously and making adjustments to improve security performance. A purple team construct is the best way to maximize the security assessment process.

Purple teams bring together the threat focus of the red team and the defensive focus of the blue team to continuously test an organization's defenses against threats described by a common framework. They focus on the overarching threat landscape, they understand their security technologies, and they understand their organization and its operational attributes.

Purple teams ensure that organizations optimize their cybersecurity readiness continuously. The combination of the MITRE ATT&CK framework, an automated breach and attack simulation platform, and purple teaming as an operational construct helps deliver a threat-informed defense and cybersecurity readiness and effectiveness.

Establish an Overarching Assessment Program

An effective controls assessment program must incorporate the results of routine testing into a company-wide data lake that all the cyberdefenders in the organization can use as needed. This ensures that team members at every level of the security structure are focused on the same list of threats and have the same understanding of controls' performance. A purple team construct enables this unity of vision.

It is important, in the development of the new security program, to keep in mind that the security team cannot fix everything at once. By incorporating ongoing, regular attack simulations into day-to-day security operations, however, the organization can ensure that security staff will continue refining their detection capabilities and developing appropriate scenarios. You cannot have visibility without continuous testing. As a CISO at a global investment bank and financial services firm once said, "how do you have the visibility such that you know that you need to trigger a retest?" Continuous testing supports continuous improvement, which is what's needed to ensure readiness and mitigate threats.

> *"Continuous testing supports continuous improvement, which is what's needed to ensure readiness and mitigate threats."*
>
> ***–CISO,***
> *Global Investment Bank and Financial Services Firm*

Identify Underlying Organizational Issues

Continuous testing can reveal issues underpinning readiness that extend far beyond the tactical, day-to-day management of the security program. In one example from the healthcare sector, automated testing revealed a control failure that had its roots not in tactical errors but in personnel attrition stemming from non-competitive salaries. In hiring staff, human resources teams often aim to suppress salaries to preserve organizational resources, while the security leader wants to hire the best talent for the organization and, therefore, needs to offer a competitive package. In this example, continuous testing revealed a security control lapse due to high rate of staff turnover. Non-competitive salaries and attrition impacted readiness. This problem was only first revealed through security team-led continuous testing.

Testing and analysis can reveal a range of issues impacting readiness.[3] In another example, the U.S. Department of Defense expanded its understanding of operational readiness when it determined that deteriorating facilities and infrastructure, mismanagement of family housing, and supply chain issues were impacting mission performance — issues that were only revealed through continuous performance analysis. Corporate CISOs should take a similarly broad view within their organizations. On the basis of performance data results, CISOs can develop a data-driven approach to management that delves beyond control failures to look at root causes. This means (1) broadening the definitional scope of the term "readiness" and (2) maximizing the benefits of performance data.

By automating control testing, an organization can see not only how well its security program is performing overall, but also take a step back to see what is driving security failures. A routine testing regime reveals top-line program failures, such as technologies that aren't performing as advertised or staff who aren't responding fast enough. Leaders can then use performance data to analyze the reasons why — from salary suppression, to COVID rotations, to other exogenous stresses on the workforce.

Shift to a Threat-Informed Defense Mindset

The final step for CISOs to optimize cybersecurity readiness is to create the cultural change required to become a data-driven organization. Leaders need to advocate the benefits of data-driven effectiveness, supported by purple team operations. External statistics on security control failures support this shift: A full 82 percent of successful enterprise breaches should have been stopped by controls the organization had in place, but succeeded because the controls did not perform as expected.

Chief information security officers can explain how their organization's security infrastructure can be transformed with data at the center of all decision-making. Intelligence about specific TTPs from the MITRE ATT&CK framework provides a better understanding of expected adversary behaviors and visibility into the organization's control effectiveness. Shifting the team culture from red-versus-blue-team, adversarial approach to purple teaming is an opportunity to learn and improve — not a judgment where the wrong result will have negative consequences for whoever is responsible for the failed control.

[3] Congressional Research Service, "The Fundamentals of Military Readiness," October 2, 2020.

Chief information security officers can rally their teams around the true threats that imperil the organization, and they can use ROI analyses to clarify for senior management the efficiency benefits of testing automation. The benefits are increased visibility for everyone involved. Toyota's general manager of cybersecurity protection, Gabriel Lawrence, recently reflected on the benefits of purple team operations to cybersecurity effectiveness. He said, "Because you have that tight integration of the red skillsets and the blue skillsets working together at the same time, somewhere along the line, there's that point where someone says, 'That wasn't what I expected to see' or 'I didn't realize it worked that way. That's a huge benefit.'" The entire organization is stronger when every control's effectiveness has been validated and gaps are shared and resolved together.

> *"If we wait for a cyber Pearl Harbor to do something about cyber[security], it may never come. But we will, nonetheless, be losing huge amounts of valuable information to our competitors and to cybercriminals who cost our society billions of dollars a year."*
>
> ***–Richard A. Clarke,***
> *Former U.S. National Coordinator for Security, Infrastructure Protection, and Counterterrorism*

Conclusion: CISOs Steering in the Right Direction

There is no time to waste in the move to threat-informed defense. In 2008, former White House cybersecurity advisor Richard A. Clarke said, "Just because we haven't had the big attack doesn't mean that we should wait to act,"[4] adding, "If we wait for a cyber Pearl Harbor to do something about cyber[security], it may never come." Now, a decade and a half after this statement, organizations seem to be stuck in a holding pattern, and we have seen escalating cyberattacks on critical infrastructure, from the Russian government's supply-chain-enabled intrusion into U.S. government networks through SolarWinds to the criminal ransomware attack on Colonial Pipeline. Despite the clear risks, organizations have held back on making the necessary investments to ready their cyberdefenses.

Over the last two years, the COVID-19 pandemic has ratcheted up the frequency of cyberattacks, the pressure on CISOs to ensure that their assets remain secure, and the need to demonstrate controls' effectiveness to the executive management team. The goal of a security program cannot be simply a compliance mindset where questions about preparedness are answered with "we have X, Y, and Z technologies to combat that type of attack." Instead, the CISO needs to be able to answer readiness questions with clear statements like "we are prepared to detect and mitigate the threat behaviors that this adversary will use against us, and here is the proof."

[4] "Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor," Foreign Policy, April 2, 2008.

Chief information security officers need visibility into the total security program's effectiveness, clarity on what is required to stay ahead of threats, and control over security controls (composed of people, processes, and technologies). Absent continuous testing that generates clear performance data, achieving visibility into control effectiveness is close to impossible. Absent visibility, the team lacks control, and absent control, the adversary can easily slip past defenses. Incorporating automated adversary emulations of multi-stage attack campaigns into day-to-day security operations is vital for cybersecurity readiness, for a potential "cyber Pearl Harbor" or any other attack that may come.

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: How to achieve cybersecurity effectiveness
- Dummies Guide to Purple Teaming

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.