CSI

A Guide to Strengthening Your Institution's Cybersecurity Posture

INTRODUCTION

Advanced cyberattacks represent a credible threat to the network, data, users and devices of financial institutions of all sizes. Threats range widely in scope, including broad-based attacks on the network itself, focused attacks on individual accounts or employees and the exploitation of vulnerabilities in endpoint devices.

Now more than ever, financial institutions must continuously monitor IT systems and data access points to ensure that cybercriminals don't gain unauthorized entry. Much as a car thief moves through a parking lot looking for unlocked cars, many cybercriminals will target those networks and systems that are most vulnerable.

As cybercriminals continually evolve their tactics to gain access to systems and data, financial institutions must navigate the risks of increased vulnerabilities and stay vigilant against emerging cyber threats. It is no longer enough to think of cybersecurity as segmented pieces of a strategy. Institutions should embrace a layered, holistic approach to cybersecurity that includes cohesive strategies to defend the perimeter (both physical and virtual), protect internal systems and safeguard endpoint devices.

This white paper examines current cybersecurity threats in the financial services landscape and discusses strategies and managed cybersecurity solutions designed to mitigate risks while bolstering system hygiene and integrity.

EXPLORING CURRENT AND EVOLVING CYBER THREATS

According to CSI’s 2021 Banking Priorities Executive Report, bankers identified cybersecurity as the one issue that would most affect the financial industry in 2021. The industry survey responses clearly reflect a landscape altered by the COVID-19 pandemic during which most organizations were driven to remote work environments and digital services, largely increasing institutions’ vulnerability to cyber manipulation and exploitation.

Financial institutions across the country executed quick pivots to allow operations to continue during this unprecedented time. This abrupt shift to remote work and virtual processes served to accelerate technology adoption among employees and customers, from digital banking solutions to collaborative communication tools. However, this acceleration is a double-edged sword.

While the swift embrace of such technologies allowed institutions to meet the needs of customers, many found the accelerated adoption was not always executed in a secure way and presented hackers with ample opportunities for exploitation. Vulnerabilities are still being discovered by organizations and cybercriminals alike, with some exposing opportunities for malicious cyberattacks.

Current cyber threats to the financial services industry include:

Social Engineering: With social engineering, fraudsters attempt to manipulate individuals into exposing confidential information that may be used for malicious purposes. Considering that most successful breaches involve some form of social engineering, it's not surprising that it dominated the responses to this question in CSI's industry survey.

All it takes for a social engineering attack to be successful is one individual clicking a malicious link or opening an attachment, which gives a fraudster access to the system. Institutions should be concerned by the prevalence of this type of attack—and about what happens after a social engineering attack successfully infiltrates their systems.

Since financial institutions possess vast amounts of data and personal identifiable information related to their customers, hackers often use social engineering to carry out data theft. If hackers illicitly obtain valuable data, they can make the data available for purchase on the dark web or even try to sell it back to the institution.

Ransomware: Once installed, this type of malware locks out the authorized user and encrypts the available data to be held for ransom. By all accounts, ransomware attacks across industries are increasing and frequently making headlines. Since ransomware attacks pose little risk to the hacker while providing a speedy payout for criminals—and a low barrier to entry with ransomware kits readily available for purchase—fraudsters will likely continue to rely on ransomware attacks in the hopes of gaining hefty payouts.

Ransomware is not just a threat to larger institutions—banks and credit unions of all sizes must be on alert to thwart this type of attack. And victims of ransomware are forced to decide between paying the ransom or recovering their stolen data, a cost that can be as high as a ransom in some cases.

Ransomware is not just a threat to larger institutions—banks and credit unions of all sizes must be on alert to thwart this type of attack.

Increased Surface Area for Vulnerabilities: As hybrid workforces and cloud-based applications become more commonplace, an institution's surface area for vulnerabilities has significantly increased compared to years past. Attackers are targeting home networks—which typically do not have proper passwords in place and offer less robust security controls than in-office networks—to gain access to corporate data.

Endpoint devices, or any device that can be used to access an institution's network, are another area of interest for hackers, especially since many organizations made changes to the location of various endpoints when shifting to remote work. Other associated risks include varying levels of attention and protection for different types of endpoints, as well as failure to maintain up-to-date patches or protective software. Combined, these factors make endpoint devices an attractive target for hackers.

Brute Force Attacks: Cybercriminals are increasingly launching brute force password attacks in attempt to gain access to passwords or corporate data. In a brute force attack, a hacker repeatedly uses different usernames and passwords to find the correct credentials. Credential stuffing attacks, which are a type of brute force attack, consist of a hacker using data exposed in a breach to guess passwords and then login to an unrelated account, hoping that a victim reuses their passwords for multiple accounts. Both the SEC and FBI have issued warnings due to the increase in credential stuffing attacks related to the financial services industry.[1]

While brute force attacks require time, energy and a trial-and-error approach, the use of bots or other automated tools make it that much easier. These types of attacks are rising, particularly as the availability of leaked credentials surges on the dark web. And once a hacker obtains or cracks a user's credentials, they can perform an account takeover and launch any number of malicious attacks.

Supply Chain Attacks: This attack occurs when a bad actor targets a software vendor to deliver malicious code through seemingly legitimate products or updates. Supply chain attacks allow a fraudster to compromise distribution systems to potentially create an entryway into the networks of the supplier's customers.

According to the National Institute of Standards and Technology, not only can bad actors use the compromised software vendor to gain privileged access to a victim's network through hijacking updates or changing code, but also they can bypass perimeter security measures and often re-enter a network using the compromised vendor.[2]

The infamous SolarWinds and Kaseya breaches are examples of supply chain attacks, an increasingly popular method to distribute malware. The hackers perpetrating these attacks levied large-scale compromises with devastating effects to many organizations and garnered attention from the U.S. government.

For almost all attacks, hackers target those servers, networks or devices with the fewest number of security layers. By targeting an institution's weakest link, it is much more likely their malicious attack will be successful—making it imperative that institutions increase protections and embrace a layered approach to cybersecurity.

ENHANCING YOUR CYBERSECURITY DEFENSES

Embracing a layered approach to cybersecurity with comprehensive visibility and monitoring across networks, perimeters and endpoints will strengthen an institution's cybersecurity posture. With a layered security approach, each tool or strategy provides an additional defense against threats. If one layer fails, there are others to fall back on, which prevents an attack from immediate success. If a user—serving as the first layer of defense—clicks a malicious link, then a firewall or anti-virus software could prevent the attack from going any further.

Here are strategies that empower financial institutions to confront evolving cyber threats while strengthening cybersecurity monitoring and compliance efforts:

Back Up Data Regularly

When it comes to cyber threats such as ransomware, an institution's best ability to recover is through successful, complete backups. Since ransomware attacks thrive on holding data captive, attacks become less threatening if data has been duplicated and stored elsewhere. Think of responding to a ransomware attack in terms of disaster recovery: If you lost access to your primary data center due to a weather-related incident or power outage, how would you recover it?

Institutions should include provisions for segregated backups when reviewing backup strategy and controls. Segregated backups decrease the risk of a hacker seizing an entire backup. If an institution only has online network backups and hackers gain access to the network, it effectively renders them useless. Beyond performing regular backups, institutions should maintain good access controls, test backups and ensure successful restoration.

The following questions should be considered as institutions review their backup strategy:

- **Are backups being regularly performed and tested?**
- **What are the most critical assets to include in backups?**
- **What gaps currently exist in backups?**
- **Are backups located in one location or are they adequately segregated?**

Embrace a Cybersecurity-Centric Culture

Though an organization can outsource many aspects of cybersecurity, a security-focused culture is not among them. Cultivating and maintaining an organizational culture focused on the importance of cybersecurity is one of the most impactful strategies an institution can use to strengthen their defenses. Even with the most sophisticated cybersecurity monitoring tools, employees remain the first line of defense against cyber threats. Unfortunately, the "people factor" can also be an institution's weakest link, particularly as attacks grow in sophistication and frequency.

A security-focused culture is also critical if employees are working remotely, helping to defend that extended network. If institutions can instill a cybersecurity-focused mindset in their employees, that outlook is likely to carry over into their personal behavior and result in positive outcomes, including creating stronger passwords on personal devices and home routers. Continuous cybersecurity training and awareness campaigns that provide information on the latest threats are the best ways to keep employees on guard and up to date against prevalent social engineering schemes.

Continuous cybersecurity training and awareness campaigns that provide information on the latest threats are the best ways to keep employees on guard and up to date against prevalent social engineering schemes.

If employees continue to fail social engineering tests, it's time to rethink the strategy to explain the threat more effectively, identify the warning signs and provide incentives for employees to do their part. Consider assigning cybersecurity ambassadors to enhance cybersecurity training. By asking respected employees throughout an institution to act as the issue's ambassadors, other employees will have a resource, and this important issue will have vocal champions.

Adopt a Cybersecurity Framework

A cybersecurity framework helps financial institutions prevent, detect and mitigate cybersecurity events. Believe it or not, even small banks or credit unions can generate millions of security events per day, and it can be difficult to handle that amount of data. Adopting a robust framework with effective controls allows institutions to identify the signals inside all that noise.

While there are various existing frameworks to consider, the CIS Controls have a proven track record for holistic security, and are budget- and user-friendly. The CIS Controls are an FFIEC-recommended framework with a prioritized list of actions, providing a map for handling compliance initiatives and planning for IT spending. In fact, adopting the Basic CIS Controls decreases risk by up to 85%.[3]

An effective framework should act as a strategic guide to determine where risks exist and identify opportunities to strengthen their control structure. Cybersecurity frameworks also help institutions decide where to focus their budget and resources by looking holistically at the security of the entire organization. Examiners are also beginning to place greater emphasis on frameworks and expect institutions to have one in place. Organizations should view a framework as a tool to not only satisfy exam requirements, but also help improve overall cybersecurity.

DECREASE RISK UP TO **85%** **by adopting the Basic CIS Controls**

The CIS Controls are an FFIEC-recommended framework with a prioritized list of actions, providing a map for handling compliance initiatives and planning for IT spending.

Require Multi-Factor Authentication

One of the key technologies institutions should deploy to strengthen their cybersecurity posture is multi-factor authentication (MFA), which requires multiple credentials to verify a user's identity. According to Microsoft, leveraging MFA can block more than 99% of account compromise attacks since hackers cannot gain access by solely knowing or cracking a password.[4]

Many organizations use text messages or applications to send an authentication code, but landline phones, soft tokens or hard tokens are also options—especially for employees using personal devices for business purposes. While MFA does require an extra step for access, most employees are willing to add the software or get a text message with a code if it means increasing cybersecurity and avoiding being the user to cause a potentially harmful security event.

MORE THAN **99%** **of account compromise attacks can be blocked by leveraging MFA**

Monitor and Manage Threats in Real Time

If a threat makes it past prevention tools, threat monitoring and management become paramount. A Security Information and Event Management (SIEM) solution delivers insight and control of cybersecurity, providing incident response to any network threats or vulnerabilities in real time. A SIEM collects and holistically reviews event logs of devices throughout a technology environment, detecting and remediating any security events.

While a SIEM is a powerful tool to enhance defenses, this technology is expensive and requires the time and resources to configure, maintain and review the alerts produced. After purchasing SIEM solutions, many organizations never reach the point where they have the time or expertise to investigate the majority of alerts produced. And when alerts go unchecked, institutions risk the chance of a small incident becoming a major breach.

After purchasing SIEM solutions, many organizations never reach the point where they have the time or expertise to investigate the majority of alerts produced. And when alerts go unchecked, institutions risk the chance of a small incident becoming a major breach.

In 2013, Target experienced a major breach after failing to respond to warnings from their anti-intrusion software. Hackers were able to obtain names, credit card numbers and other information from millions of people, resulting in the company paying more than $200 million in legal fees and other costs associated with the breach.[5]

To help avoid such incidents, many institutions opt for a SIEM-as-a-Service (SIEMaaS) model to handle the burden of monitoring and reduce upfront costs. With SIEMaaS, a third party—such as a managed security service provider (MSSP)—collects all event logs and sends them to an outsourced SIEM. Alerts produced will go directly to the internal IT team or an outsourced security operations center for investigation and review.

An outsourced SIEM is fine-tuned and managed by a vendor's security operations center, significantly reducing the time burden on internal IT and turning the cost into an operational expense instead of a large upfront investment. MSSPs invest resources to configure their SIEM solutions to the point where truly valuable alerts are received, removing that task from institutions while allowing them to reap the benefits of advanced monitoring.

Additionally, it is important for organizations to consider how alerts will be received and ensure the proper processes are in place for reviewing and responding to alerts, especially on nights, weekends or holidays. SIEMaaS takes the burden of responding to alerts and remediating threats away from an institution, often providing around-the-clock support.

Deploy Endpoint Detection and Response

Endpoint detection and response (EDR) monitors specific endpoints, identifying anomalies and blocking malware using advanced threat intelligence. EDR stops the spread of malware in an infected system through detection, isolation and remediation. While technology like anti-virus software provides a basic level of monitoring, EDR goes a step further by leveraging artificial intelligence to learn baseline behaviors and patterns. EDR solutions also produce event logs that can be correlated and fed into a SIEM, offering enhanced insight.

Consider this example: *If a malware attack were taking place on a laptop or server, EDR would identify that as anomalous behavior, segregate it from the network and block the attack.*

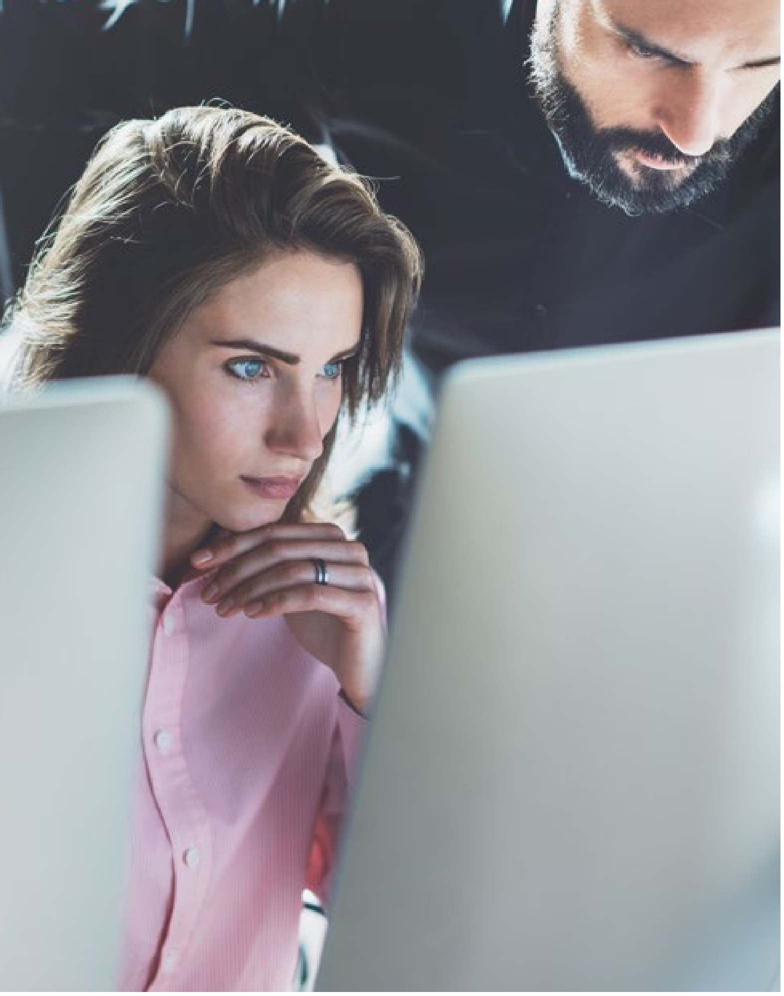
EDR solutions are also an effective strategy to protect against zero-day exploits, which are vulnerabilities with no available patches. Since EDR solutions do not rely on signatures to identify specific malware, these tools analyze behaviors to detect anomalous activity and defend against zero-day exploits. Any institution that implements an EDR system—or any similar technology—should have protocols in place to ensure the tools are working properly.

Prioritize Cloud Security

As more financial institutions turn to cloud-based technology to streamline and simplify operations, it is important to remember that protections must be extended beyond a traditional perimeter and include the cloud as well. Monitoring the entire perimeter—including the cloud—is critical to maximizing the benefits of the technology and building a strong cybersecurity posture.

Further, maintaining the proper security configurations will ensure the integrity of cloud-hosted systems and data. Cloud technology offers a variety of security advantages, but when a breach does occur, it is typically the result of a bad configuration. Institutions should also ensure they are quickly implementing security patches when available to avoid vulnerabilities being exploited.

Partnering with a cloud services provider or MSSP that understands the cybersecurity and regulatory requirements of financial institutions will help enhance the integrity of IT systems. Leverage their expertise and understand the controls they have in place to mitigate risks during and after a cloud migration. In addition, institutions should properly vet cloud service providers as part of vendor due diligence efforts.



Conduct Dark Web Monitoring

The dark web references a set of websites that are not publicly accessible and include online marketplaces for anonymous users to take part in illicit activities, such as buying and selling personal information that can be used to perpetrate identity theft. Once an institution has assessed its cybersecurity posture, identified the most pressing risks and implemented a robust framework, conducting dark web monitoring is an additional tool to strengthen cybersecurity and monitor for leaked credentials.

Before embarking on monitoring the dark web, consider partnering with a trusted third-party vendor or leveraging an existing relationship with an MSSP. But be aware that not all dark web searches are created equally. Research any potential partners to understand how they conduct their searches, how the information will be reported and if the data will be actionable. Will the vendor provide a simple report, or will it include recommendations based on the results?

Perform Penetration Testing and Vulnerability Scanning

By frequently testing security infrastructure against real-world tactics used by cybercriminals to exploit networks, institutions can detect and reinforce network vulnerabilities to strengthen security and compliance. Internal, external and wireless penetration testing empowers institutions with a holistic picture of their cybersecurity posture while fulfilling compliance requirements. These assessments will identify any weaknesses in points of entry—including firewalls or perimeter routes—as well as encryption and authentication methods.

Vulnerability assessments identify areas that need attention in both internal systems and external perimeter devices. But it’s not enough to simply conduct these assessments; institutions must review the results and remediate the findings to strengthen their cyber hygiene. As regulators continue focusing on cybersecurity compliance requirements, these tools will enhance cybersecurity posture and help avoid costly penalties.

> **Once an institution has assessed its cybersecurity posture, identified the most pressing risks and implemented a robust framework, conducting dark web monitoring is an additional tool to strengthen cybersecurity and monitor for leaked credentials.**

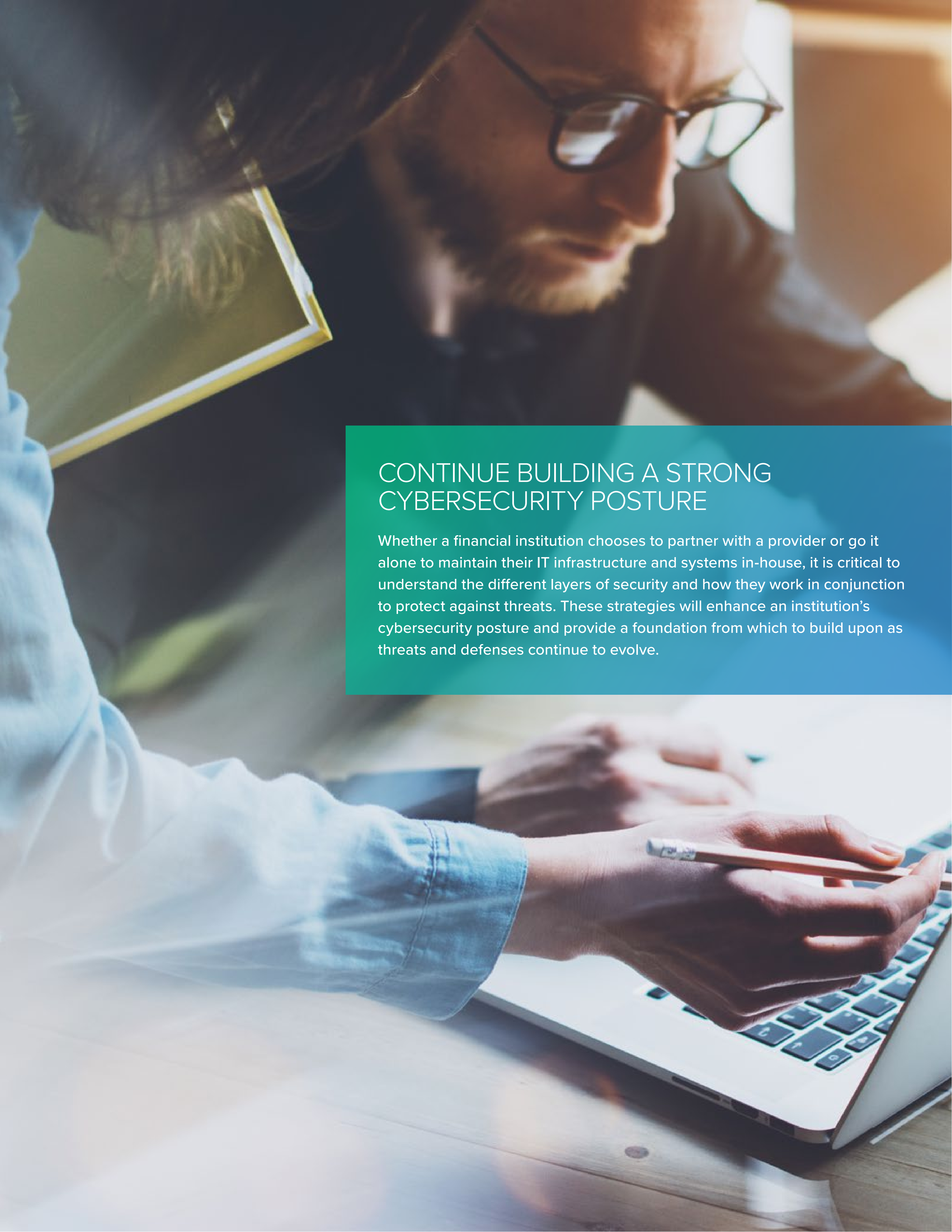
PARTNERING WITH A TRUSTED PROVIDER FOR MANAGED CYBERSECURITY

Managing these ongoing threats can be overwhelming for many IT leaders. The challenge lies in ensuring a comprehensive, layered approach to cybersecurity monitoring while keeping time, resources and cost burdens under control. Working with a trusted MSSP enables an institution to leverage a whole team of security guards, rather than relying on few internal staff to win the battle.

Partnering with an MSSP adds an additional layer to the security defenses already in place and allows an organization to take advantage of an MSSP's existing security controls and shared technologies, such as SIEMaaS or EDR. However, institutions should review and test security controls implemented by a third party as part of vendor due diligence efforts, including controls for software and hardware.

As cybersecurity compliance requirements continue to evolve, a trusted partner familiar with the complex regulatory requirements of the financial industry will help keep institutions up to date with the latest regulations while mitigating risk. An MSSP will also work with institutions to prepare for examinations and audits, further strengthening preparedness for cyber threats while meeting regulator expectations.

In today's world, cybersecurity monitoring, policies and procedures must transcend the boundaries of traditional physical perimeters and network connections to encompass every connection point an institution has with consumers and employees. And a financial institution that understands current threats, actively secures systems and mitigates risk by working with an industry-focused provider is likely more difficult to breach, which can encourage criminals to look elsewhere for a less prepared victim.



CONTINUE BUILDING A STRONG CYBERSECURITY POSTURE

Whether a financial institution chooses to partner with a provider or go it alone to maintain their IT infrastructure and systems in-house, it is critical to understand the different layers of security and how they work in conjunction to protect against threats. These strategies will enhance an institution's cybersecurity posture and provide a foundation from which to build upon as threats and defenses continue to evolve.

ABOUT COMPUTER SERVICES, INC.

Computer Services, Inc. (CSI) delivers core processing, digital banking, managed cybersecurity, cybersecurity compliance, payments processing, print and electronic document distribution, and regulatory compliance solutions to financial institutions and corporate customers, both foreign and domestic. Management believes exceptional service, dynamic solutions and superior results are the foundation of CSI's reputation and have resulted in the Company's inclusion in such top industry-wide rankings as IDC Financial Insights FinTech 100, Talkin' Cloud 100 and MSPmentor Top 501 Global Managed Service Providers lists. CSI has also been recognized by Aite Group, a leading industry research firm, as providing the "best user experience" in its 2019 AIM Evaluation: The Leading Providers of U.S. Core Banking Systems. In addition, CSI's record of increasing its dividend each year for 49 years has earned it a designation of one of the financial media's "Dividend Aristocrats." CSI's stock is traded on OTCQX under the symbol CSVI. For more information, visit csiweb.com.

RESOURCES

[1] What Banks Need to Know About Credential Stuffing and How to Stop It

[2] Defending Against Software Supply Chain Attacks

[3] CIS Controls v7.1

[4] One Simple Action You Can Take to Prevent 99.9 Percent of Attacks on Your Accounts

[5] Target to Pay $8.5 Million to 47 States in Security Breach Settlement