WHITEPAPER

SOC-as-a-Service for Financial Institutions

A Force Multiplier for Managing Cybersecurity Risk and Compliance

Information technology (IT) teams at financial institutions such as regional banks and credit unions are stretched thin. They're expected to meet compliance obligations while simultaneously taking care of cyberthreats. This is particularly true for mid-sized institutions without resources dedicated to security or compliance, putting them at risk.

What options do regional banks and credit unions such as these have? The emerging area of managed detection and response offers financial institutions the opportunity to augment their existing IT staffs and improve their security postures while at the same time simplifying compliance.

This paper provides an overview of the compliance and security challenges faced by mid-sized financial institutions and the value provided by managed detection and response (MDR) solutions. It also demonstrates how financial institutions can leverage MDR services to address every CIO's main concern: "Is my company safe and compliant?"

Financial Services Industry Challenges

Financial institutions face a combination of cybersecurity challenges and compliance mandates. While the overriding priority is mitigating risks to sensitive information and avoiding data breaches, financial institutions are also obligated to comply with relevant regulations. Regional banks and credit unions are particularly pressed by this combination as they often lack the resources available to larger financial institutions to successfully juggle these requirements.

Compliance Mandates

Regional banks, credit unions, and other mid-size financial institutions can face regulations from both national and state regulatory bodies. Governance, risk management and compliance frameworks, and security guidance developed by NIST, PCI DSS, the FFIEC and state bodies such as the New York Department of Financial Services all strive to assess risk and minimize security gaps. While such oversight provides useful recommendations for cyber risk management, applying and optimizing a cybersecurity strategy can overwhelm capable but short-handed IT and security staffs.

Gartner Highlights the Challenges

Gartner on Managed Detection and Response Adoption

By 2020, 15% of midsize and enterprise organizations will be using services like MDR, up from less than 5% today.

Source: Gartner "Market Guide for Managed Detection and Response Services" (11 June 2018)

Gartner on Cybersecurity Staffing

95% of technology leaders expect cybersecurity threats to grow—but only 65% have a cybersecurity expert on staff.

Source: Gartner 2018 CIO Agenda Survey (July 2018) https://www.gartner.com/newsroom/id/3882863

Not observing compliance mandates can prove costly, and not just from a monetary standpoint. Companies guilty of non-compliance end up spending more in the long run on fines and new resources needed to manage increased regulatory audit scrutiny. They also must endure negative media coverage resulting in customer churn when something goes wrong.

Dangers of Cyberthreats

Extremely sensitive and valuable data resides in the financial services sector—everything from personally identifiable information (PII), to check-routing data, to global stock and investment algorithms. The loss of this data and intellectual property has a major impact on a bank's brand reputation and customer loyalty. When consumers and business customers place their trust and their money in an institution, its reputation for information security is paramount.

Infrastructure at financial institutions is constantly evolving to support line-of-business initiatives. While traditionally this has focused on on-premises assets, cloud services in the form of software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) are becoming more commonplace as cloud providers address the security and compliance concerns of financial institutions. Still, the addition of cloud services increases a financial institution's "attack surface" and adds to their cybersecurity risk equation.

Cybersecurity Skills Shortage

Gartner found that, "Despite 95 percent of CIOs expecting cyberthreats to increase over the next three years, only 65 percent of their organizations currently have a cybersecurity expert."[1]

The shortage of people with security expertise is particularly acute in the financial services industry. Financial services firms are enhancing their on-premises infrastructure while also embracing the benefits of cloud computing. Such hybrid environments, where information resides both on-premises and in the cloud, require increasing technological sophistication and knowledge to secure.

Lack of 24/7 Coverage

Continuous monitoring is a security best practice and frequent compliance requirement for financial institutions. Such security monitoring demands building and maintaining a security operations center (SOC). A SOC is a combination of cybersecurity personnel, threat detection and incident response processes, as well as supporting security technologies that comprise an organization's security operations. In essence, a SOC combines the people, processes and technology needed to elevate and maintain an institution's security posture.

While a SOC is an industry best practice, smaller financial institutions typically do not have the budget for one. A Gartner report on security for midsized enterprises commented that, "A minimum of eight to 12 security analysts are needed for 24/7 monitoring—an unrealistic objective for most [midsized enterprises]."[2] Justifying the budget to hire a SOC team poses a challenge even for the most persuasive CIO. And locating, training and retaining the necessary security talent is a Sisyphean task for small and mid-sized financial institutions. Outsourcing the SOC function, however, provides a viable solution. SOC-as-a-service offerings, like the AWN CyberSOC™ service, enable companies to overcome the cybersecurity skills shortage and avoid the costs and difficulties that come with building, deploying, and maintaining an in-house SOC.

1. Gartner Press Release, "Gartner Survey Finds Only 65 Percent of Organizations Have a Cybersecurity Expert," 17 July, 2018, https://www.gartner.com/newsroom/id/3882863
2. Garter, "Cool Vendors in Security for Midsize Enterprises," 1 June 2018

Financial Services and Compliance: More Than Just Acronyms

Financial institutions of every size must comply with federal and state regulations. These regulations are designed to protect consumers, businesses and industry firms themselves. However, meeting these compliance obligations isn't easy. It takes dedicated staff and resources, and implementation of new processes and procedures to do so.

Below are some of the more common regulations that apply to many financial services firms.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) affects any financial institution handling payment cardholder data. PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor, by a firm-specific Internal Security Assessor for organizations handling large volumes of transactions, or by a Self-Assessment Questionnaire for companies handling smaller volumes.

FFIEC/NCUA

The Federal Financial Institutions Examination Council (FFIEC) is the inter-agency body of the United States government that prescribes uniform principles, standards and report forms for the federal examination of financial institutions. It is empowered by various entities, including the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CPFB).

NY DFS 23 NYCRR 500

The New York State Department of Financial Services (DFS) promulgated 23 NYCRR, also known by the name "Cybersecurity Requirements for Financial Services Companies," in 2017 to address concerns that financial firms face an escalating volume and sophistication of cyberthreats. 23 NYCRR 500 establishes minimum regulatory standards to promote the protection of customer information as well as the information technology systems of regulated entities that do business in the State of New York.

GLBA

The Gramm–Leach–Bliley Act (GLBA) became law in 1999. According to the FDIC, the "(GLBA) guidelines require each institution to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. While all parts of the institution are not required to implement a uniform set of policies, all elements of the information security program must be coordinated."

Targeted Attacks on Financial Institutions

While financial institutions of all sizes must comply with federal and state regulations that govern the industry, they face even greater risks and challenges from today's cyberthreats. A single data breach can cause irreparable harm to a bank, including damages that can never be overcome. Cybercriminals continue to devise new attack methods using increasingly sophisticated tools that have now gone "mainstream."

To follow are just a few examples of cyberattacks that banking and financial institutions have recently suffered.

Top Threat: Phishing

The National Bank of Blacksburg was compromised twice by hackers over a period of eight months. Cyberthieves stole a total of $2.4M. The second phishing attack in January 2017 used a booby-trapped Microsoft Word document that allowed thieves to gain a foothold in the bank. The latter breach caused $1.8M in losses and resulted in investigation, remediation and legal consultation costs of $453,000.[3][4]

Top Threat: Ransomware

Among the most notorious ransomware attacks from 2017 were the WannaCry, NotPetya and BadRabbit cryptoworms. The propagation of WannaCry, which infected 300,000 machines worldwide, depended on attackers exploiting Microsoft Windows vulnerabilities in the SMB protocol. In March 2018, the City of Atlanta was attacked using the SamSam ransomware strain, temporarily disrupting city operations. As of late April 2018, Atlanta had incurred approximately $2.7M in total incident response expenses as a consequence of this single attack.[5]

Top Threat: Brute-Force Login Attacks

Financial services firms are prime targets for brute-force login attacks in which threat actors systematically attempt various password or passphrase combinations. The goal is to eventually guess the right combination and access restricted resources protected by the password. Such attacks can target internal accounts for employee or contractor credentials or target consumer accounts for consumer credentials. One piece of banking malware identified in 2018 uses phishing to establish a beachhead followed by brute-force attacks to propagate internally.[6]

Addressing the Changed Landscape: Managed Detection and Response

Today, breaches are a given. Even companies with the most comprehensive cybersecurity protection can't stop all cyberattacks from invading their networks and wreaking havoc. That's why many companies are turning to managed detection and response services as a way to mitigate risk and enhance their security postures. This is a significant development as the cyberthreat landscape continues to evolve and is a critical consideration for companies in the financial services industry.

NIST Cybersecurity Framework and Managing Risk

The NIST Cybersecurity Framework is voluntary guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The framework helps financial institution management identify a cybersecurity and resilience posture that is commensurate with the institution's risk and complexity.

Regional banks and credit unions are somewhat unique in the financial services ecosystem in that they are typically strapped for resources compared to their larger brethren. MDR offerings provide an efficient and cost-effective approach to address the "detect" and "respond" portions of the NIST Cybersecurity Framework (see Figure 1).

3. Krebs on Security "Hackers Breached Virginia Bank Twice in Eight Months, Stole $2.4M", 24 July 2018 https://krebsonsecurity.com/2018/07/hackers-breached-virginia-bank-twice-in-eight-months-stole-2-4m/
4. SEC 10-K Annual Report for National Bankshares, Inc. for fiscal year ending 31 December 31 2017, https://www.sec.gov/Archives/edgar/data/796534/000143774918004594/nksh20171231_10k.htm
5. Pymts.com "Ransomware Attack Cost City Of Atlanta Over $2M", 24 April 2018, https://www.pymnts.com/fraud-attack/2018/ransomware-attack-cost-atlanta-over-2m/
6. ZDNet "Banking malware finds new life spreading data-stealing trojan", 19 July 2018, https://www.zdnet.com/article/banking-malware-finds-new-life-spreading-data-stealing-trojan/

NIST Cybersecurity Framework

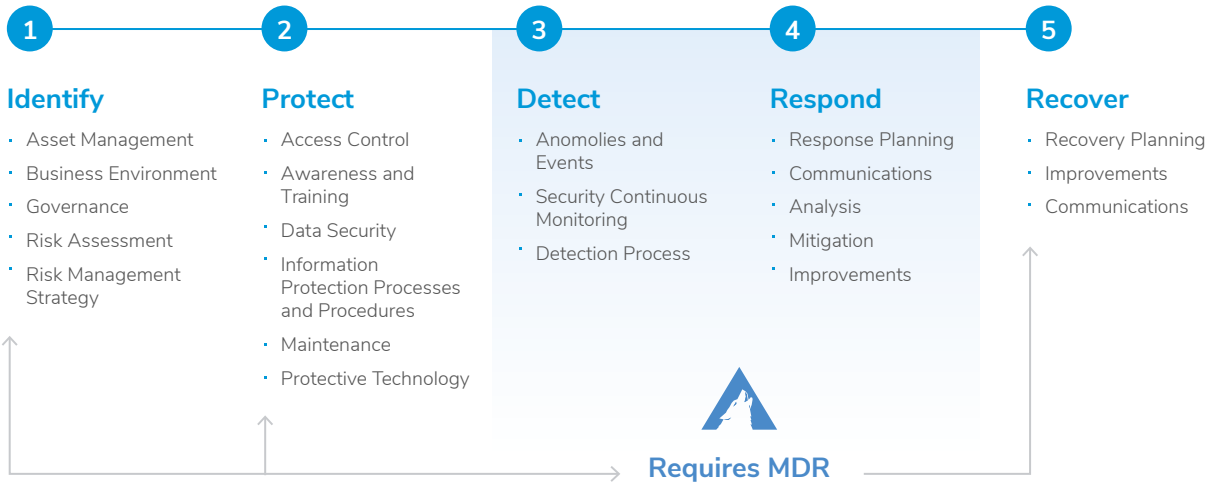

Figure 1: NIST Cybersecurity Framework

MDR: An IT Force Multiplier

SOC-as-a-service offerings illuminate the difference between responsibility and accountability. While a SOC-as-a-service solution is responsible for monitoring, detecting and responding to security events, the financial institution IT team is accountable for security and planning. As a recent Gartner blog mentions, "Gartner research again and again confirms that one cannot outsource planning or accountability for detection and response. Indeed, you can use services for almost everything, but planning (and adapting the plan as things change) requires internal resources."[7]

Managed detection and response services via SOC-as-a-service typically supplement rather than replace existing information technology and IT security staff. MDR services enable financial institution IT personnel to focus on projects that enhance an institution's competitive advantage while outsourcing the work of sifting through alerts and investigating security events.

MDR offerings through SOC-as-a-service providers have the added benefit of helping financial services firms build incident response plans. Responding to a security incident can be complex, costly, and involve multiple constituents including line-of-business, legal, and PR. Leveraging SOC-as-a-service frees up bandwidth to plan and respond to incidents and minimize the recovery costs.

Managed detection and response services via SOC-as-a-service typically supplement rather than replace existing information technology and IT security staff. MDR services enable financial institution IT personnel to focus on projects that enhance an institution's competitive advantage while outsourcing the work of sifting through alerts and investigating security events.

MDR offerings through SOC-as-a-service providers have the added benefit of helping financial services firms build incident response plans. Responding to a security incident can be complex, costly, and involve multiple constituents including line-of-business, legal, and PR teams. Leveraging SOC-as-a-service frees up bandwidth to plan and respond to incidents and minimize the recovery costs.

7. Anton Chuvakin/Gartner Blog, "New Paper Published: "How to Start Your Threat Detection and Response Practice"", 30 May 2018, https://blogs.gartner.com/anton-chuvakin/2018/05/30/new-paper-published-how-to-start-your-threat-detection-and-response-practice/

MDR and Compliance

Compliance regimes affecting financial institutions provide a framework for managing risk that includes common threads around monitoring, detection, and incident response. SOC-as-a-service providers offering MDR services provide an effective way to comply while also avoiding costs related to establishing and maintaining the infrastructure for security information and event management (SIEM) as well as other security tools.

For example, the FFIEC/NCUA guidance for financial institutions includes validating that a process exists to contact personnel who are responsible for analyzing and responding to an incident. SOC-as-a-service offerings monitor, detect and respond to security incidents to help fulfill the regulatory guidance, but rely on the financial institution to do the planning.

Arctic Wolf's AWN CyberSOC™ service helps financial institutions meet elements of a variety of compliance mandates, including FFIEC/NCUA guidance, the New York State Department of Financial Services NYCRR 500, PCI DSS, GLBA and SOX. (Visit Arctic Wolf's website for solution briefs that include specific mapping to rules and functionality.)

Summary

Financial services firms, particularly retail financial firms like regional banks and credit unions, are stretched thin as they manage cybersecurity risk and seek to maintain compliance in the face of budget constraints and a cybersecurity skills shortage. The maturing of managed detection and response offerings provides a way forward to solving both issues. SOC-as-a-service offerings like the AWN CyberSOC offer financial institutions the ability to improve their ability to monitor, detect and respond to cybersecurity threats while meeting their regulatory obligations around mitigating cybersecurity risk and ensuring resilience.

About Arctic Wolf

Arctic Wolf Networks provides SOC-as-a-service that is redefining the economics of security. The AWN CyberSOC service is anchored by Concierge Security™ teams and includes 24×7 monitoring, custom alerting and incident investigation and response. There is no hardware or software to purchase, and the end-to-end service includes a proprietary cloud-based SIEM, threat intelligence subscriptions and all the expertise and tools required. For more information about Arctic Wolf, visit https://www.arcticwolf.com.

ARCTIC WOLF Layer 7 Data Solutions

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com