Secureworks®

WHITE PAPER

More than Compliance— Improve Protections to Safeguard Your Data

Thinking Outside the Checkbox

The financial sector has long been targeted by cybercriminals who operate like digital bank robbers following the scent of money.

Because of its vulnerability the industry is highly regulated, and compliance-based security programs have helped to establish strong security controls and procedures at regional banks and credit unions as well as the largest global investment institutions. The need for strong security programs is not new to the financial services sector. So, what's changed, and how are firms more vulnerable today?

Compliance is Only One Dimension

Compliance-based security programs have been a driving force behind strong security controls and procedures at financial institutions. Regulations are increasing, requiring more time and energy from already overloaded IT staff. Banks, credit unions, lenders and other financial firms face added pressure as part of the Department of Homeland Security's (DHS) Critical Infrastructure sector. According to DHS, "large-scale power outages, recent natural disasters and an increase in the number and sophistication of cyberattacks demonstrate the wide range of potential risks facing the sector."[1]

Even with increased scrutiny and attention from regulatory bodies, the goal of total protection remains elusive, and one-size-fits-all compliance guidelines cannot totally quantify cyber risk in a way that banks, credit unions and other investment management firms can use to implement protection strategies effectively.

Compliance and IT risk frameworks developed by NIST, PCI, ISO, ISACA, GLBA and the FFIEC all strive to assess risk and identify gaps in preparedness. While they offer useful prescriptions for basic risk management, they act more like a reference checklist of best practices and leave the harder task of developing, applying and perfecting a cybersecurity strategy to an overwhelmed IT security staff. It's tempting to reverse-engineer a security program from a list of compliance mandates, but this is not a holistic strategy and the result can be gaps in coverage, inefficiencies or cost overruns when IT teams use their budgets to cobble together individual software packages as if from a buffet.

Even with a framework to follow, it can be difficult to set and adjust policy and security controls for your specific business needs, and to know where and how each framework intersects. New technological innovations in the financial services sector, like in-memory database technology and multi-tenant cloud computing add to the compliance burden as they must be assessed for risk and woven into the fabric of the existing information security program.

According to Ponemon Institute, the average cost of a data breach in 2018 increased by 6.4% to $3.9 million.[2]

An information security program assessment from an experienced and qualified partner can help financial institutions of all sizes define risk to new technologies, applications and systems, and help determine how to spend limited security dollars wisely in the ongoing cycle of compliance. These assessments can help fine-tune security charters and policies and design security metrics that are measurable and reportable for compliance requirements.

While compliance looms large for the financial sector, there's something even more important to your customers — trust.

Blocking and Prevention are Not Enough

Extremely sensitive and valuable data resides in all facets of the financial services sector — everything from personally identifiable information (PII) to check routing data to stock and investment data for corporations. The loss of this data has a major effect on brand reputation and customer loyalty. When consumers and business customers place their trust and money in your organization, your reputation for security is critical.

For the largest financial institutions, a serious security breach could result in the loss of major treasury functions should a trading partner leave with millions of dollars in fees or relationships. For stock brokerages and mutual fund management firms, a breach can result in data manipulation, loss of customer confidence and financial losses. For smaller regional banks and credit unions, the theft of data can divert significant IT resources to remediation while corporate governance must deal with multiple disclosure requirements — all while reputation suffers.

The idea that the global banking system is impenetrable has eroded over the past few years. In 2016, cybercriminals successfully infiltrated the global SWIFT messaging system for the second time to steal money from a bank. Up until now, the SWIFT network was thought to be the most secure financial messaging system in the world.

The sobering details of the second successful attack on Swift reveal a highly sophisticated threat that was not necessarily the result of weak security controls. According to *The New York Times:*

> ***"Somehow the thieves obtained a valid SWIFT credential that allowed them to 'create, approve and submit' messages on the network. Those messages— sent from PCs in the bank's back offices or from laptops—were then used to move money from one of the bank's accounts."***[3]

The stealthy techniques used in the SWIFT attack highlight a growing problem for IT security teams in the financial sector. Even though banks validate and review transactions to root out fraud, and even though sophisticated security controls are in place according to highly crafted risk assessment frameworks, the bad guys are finding a way in.

The sheer volume of network traffic and security alerts is providing cybercriminals with helpful cover for their attack techniques. In some ways, the financial sector has become a victim of its own success in applying protection technology. Today, the volume of security alerts is skyrocketing and IT security teams face exponentially more alerts than they can affectively monitor and analyze. This process is crucial to identify and separate the suspicious behavior from the general noise of modern network traffic.

With so many security alerts, the IT security team needs time and visibility to defend against cyberattacks. Speed of detection can make all the difference to financial organizations by reducing potential business disruption, protecting brand reputation and reducing remediation costs. Making the switch from reactionary measures to proactive ones by selecting advanced threat services that complement the existing security program will keep financial data secure without impeding business growth.

Advanced threat services rely on full-time security researchers who provide intelligence and visibility into cyber threats beyond the edges of the financial institution's network. This intelligence helps organizations resist targeted cyberattacks by reducing the time it takes to see and respond to them.

Security teams must have full visibility into the operations and security of their systems, networks and assets. Organizations must evaluate their current security architecture and consider recalibrating security policies to ensure that the right information is being collected and correlated to give security professionals a view of the "big picture" across networks, information and assets. Having visibility into what is happening behind your firewall is just as important as knowing what is trying to penetrate the firewall from the outside.

How to be Proactive about Credential Protection and Internal Threats

A variety of cybercriminals are targeting the financial sector, including unfriendly nation-states, hacktivists and organized crime groups. These threat actors conduct email and spear phishing to steal employee credentials that will give them access to the systems and data they seek. For this reason, many banks and financial institutions need to maintain strict separation of duties and systems access for their employees. They may also want to restrict the amount of information employees publish about their professional roles on social media platforms like LinkedIn. Criminals could use that information to target specific employees with spear phishing scams.

In addition to the cybercriminals trying to find their way inside the network, financial institutions are also combatting insidious insider threats. Malicious insiders know what valuable data is stored on their employer's networks and may have the credentials to gain legitimate access. When a trusted employee steals or manipulates financial data, it causes significant damage to a bank's reputation for information security.

Combatting insider threats requires real-time monitoring and visibility, as well as fast response capabilities. Financial institutions need the ability to monitor and identify suspicious network behavior from trusted insiders, including unusual log-on connections, transactions and requests. This also includes the ability to connect seemingly unrelated suspicious behavior.

It can be extremely helpful to engage qualified security experts that will emulate insiders using real techniques and evasion methods. Regular penetration testing should also include spear phishing techniques to identify employee weaknesses when it comes to security awareness and best practices.

Targeted threat hunting is another way to validate current security defenses against insider and other targeted threats. Targeted threat hunting proactively seeks out indications of compromise (IoCs), and also provides context and analysis of a breach to help prevent similar intrusions.

Targeted threat hunting relies on security professionals with highly specialized skills to effectively seek out and identify targeted and advanced adversaries. There are four essential capabilities required, including:

- Deep experience with advanced adversaries and varied tactics
- Broad visibility into threatened environments
- Access to ongoing, active research driven by field engagements
- The ability to correlate data from many vantage points and cohesively analyze it

Financial IT security teams know that completely eliminating the possibility of a breach is an unrealistic goal. Even layered security technology can no longer provide a complete defense. An effective security program accounts for eventual compromise and takes steps to rapidly identify, contain and eradicate threats inside the network. Malicious actors that remain undetected inside your network for longer periods of time can commit more fraud and more data theft, costing your organization more money and reputation damage.

Spear phishing is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers," but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.[4]

Conclusion

Preventing fraud and data theft are critical to the business operations, reputation and compliance efforts of financial institutions large and small. Threat actors from organized cybercriminals to malicious insiders have taken advantage of financial systems' technology to commit fraudulent transactions and steal data.

Meanwhile, pressure from regulatory bodies is increasing as more scrutiny is given to banks, credits unions, payment card processors, accounting firms and more—especially in the areas of penetration testing, vulnerability assessments, encryption, multi-factor authentication and monitoring.

Financial services firms know it's impossible to prevent all threats. But advances in security technology and services are making improvements in the ability to proactively detect and disrupt fraud before transactions are approved. Taking a combined approach that includes important compliance requirements, enhances visibility and threat monitoring capabilities and conducts targeted threat hunting will improve proactive security and protect your assets and financial reputation.

Sources:

[1] Department of Homeland Security -- Financial Services Sector; https://www. dhs.gov/financial-services-sector

[2] Ponemon Institute, "2018 Cost of Data Breach Study: Global Analysis", July 2018 , https://www.ibm.com/downloads/cas/861MNWN2 , accessed April 4, 2019.

[3] The New York Times; "Once Again, Thieves Enter Swift Financial Network and Steal;" May 12, 2016; http://www.nytimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html?_r=2

[4] Tech Target; Search Security; http://searchsecurity.techtarget.com/definition/spear-phishing

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States

1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France

8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany

Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom

One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates

Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan

Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp