WHITEPAPER

Network security assessment and patch management in the finance industry

GFI Software™

Table of Contents

Introduction

Financial institutions have to deal with a lot of regulations. Not only do they have to follow all financial guidelines as well as data protection protocols, but they have more malicious actors working to attack them than other industries.

When bad actors attempt a phishing scheme or ransomware attack, financial institutions are at the top of their priority list as the reward for a successful attack is exceptionally high. This means that in addition to the typical checks on compliance, financial institutions have criminals unceasingly attempting to gain access to their systems.

In fact, according to the Center for Strategic and International Studies (CSIS), financial institutions are the leading targets of cyberattacks. This sector is targeted not only for money, but also for "political and ideological leverage." Regulators are aware of these trends and are working towards creating more rules and guidelines for financial institutions.

Many of the laws followed aren't specifically aimed at cybersecurity in the financial sector, but the institutions must comply with all regulations directed both towards cybersecurity and data protection in general, as well as specific, financial industry-only rules.

With more focus in recent years placed on cybersecurity, regulators are looking at adding even more specific laws aimed at financial institutions' online presence, which can feel overwhelming with all the regulations that must be followed.

Let's look at some of the statistics to understand what banks and other financial institutions are dealing with. According to PWC's Global Economic Crime and Fraud Survey: Financial Services industry insights,

- 46% of respondents in the financial services industry reported being victims of economic crime in the last 24 months, with 16% of these suffering more than 100 incidents and 6% suffering more than 1,000 incidents.
- 50% had a regulatory inspection or experienced enforcement action in the last 24 months
- 1 in 5 banks have experienced enforcement actions by a regulator.

Cybercrime in the financial services industry is large and continuously growing, with regulators stepping up their inspections as consumers fight for more online protection.

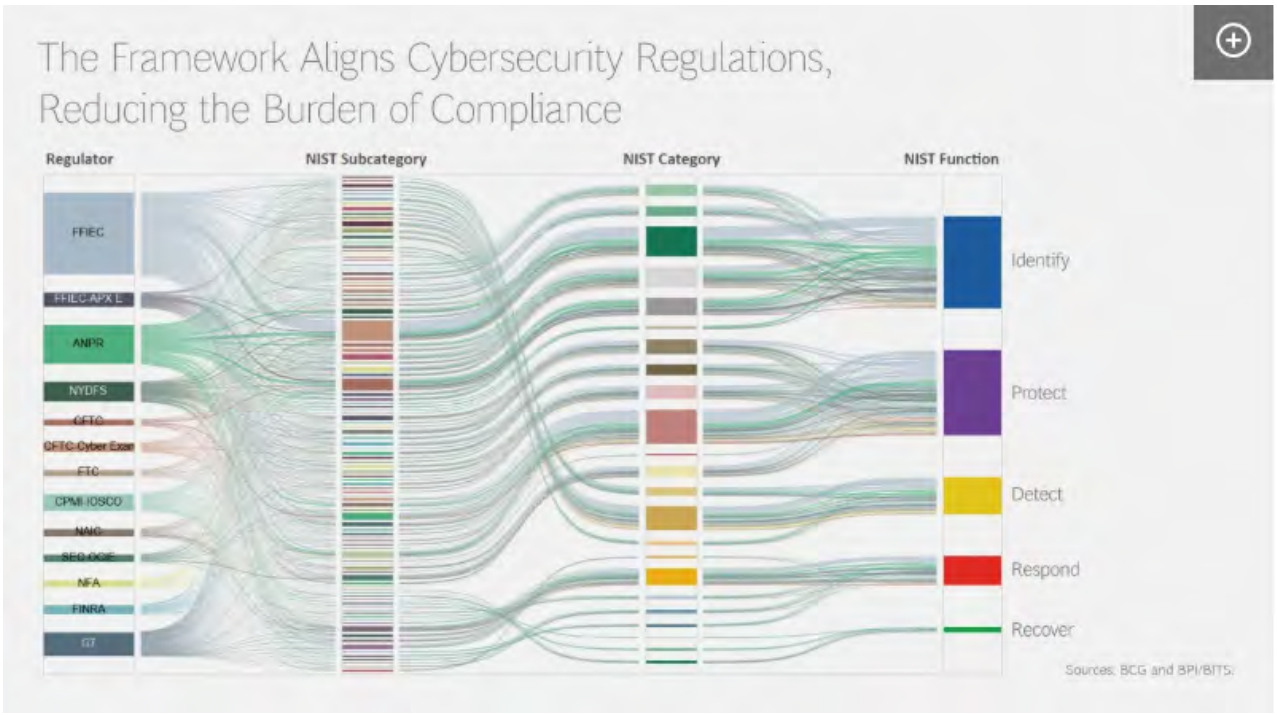
If we take a look at the top methods for detecting these financial crimes, it's clear to see that there needs to be an overhaul in how those in the financial industry perform security assessments. These methods were:

- Proactive fraud risk management 17%
- Suspicious transaction reporting 14%
- Frauds detected by accident 9%
- Proactive Internal audit 7%

Companies need to be more prepared in catching any potential openings for malicious actors with full, regular security assessments and a functional, automated patch management software.

How to stay compliant

With so many new and existing regulations along with cyberattacks coming at you from every angle, it can feel impossible to stay compliant. Over 30 new cybersecurity regulations have been released in the past five years alone in the USA.



Additionally, in 2017 “the Financial Stability Board announced that 72% of its 25 member jurisdictions were planning to issue further cybersecurity regulatory guidance.” Having to stay compliant with so many different regulatory boards is neither sustainable nor efficient, monetarily nor temporally.

While the regulations are in place to try to correct the problem, the overwhelming amount to manage may just end up contributing to it. In fact, “when surveyed two years ago, Chief Information Security Officers for financial services institutions reported that up to 40% of their time was spent on the compliance requirements of various regulatory frameworks, not cybersecurity.”

In order to simplify regulations, the The Financial Sector Coordinating Council (FSSCC) has published Financial Sector Cybersecurity Framework Profile. The Profile or FSP is a framework based on numerous guides, such as that of the National Institute of Standards and Technology in order to simplify how financial institutions can improve their cybersecurity as well as stay compliant.

By simplifying language and combining regulations that already overlapped, companies can focus more of their attention on the real purpose, cybersecurity.

The Profile is designed for all financial institutions, financial services companies, financial firms, and their third-party providers. Numerous organizations within the financial services industry, including banking, insurance, and more, designed the profile to function for the financial sector as a whole rather than a particular industry like banking.

According to the Profile, the numerous benefits of this approach are that it:

- Focuses senior executive and boardroom review of cybersecurity risks and budgeting;
- Brings plain language to benchmarking, risk management, audit, and in-house education;
- Offers compliance efficiencies that grow with a financial institution's complexity;
- Aids prioritization and focused use of resources;
- Eases collaboration with other financial institutions, third-parties, and innovative nonbank financial companies;
- Supports tailored supervision, examinations, and collaboration among state, federal, and international supervisors;
- Enhances understanding of systemic risk within the sector, across sectors, and among institutions and third-parties;
- Creates a common baseline security threshold; and
- Improves data collection and comparison.

The profile is supported by numerous players in the finance sector, such as by the FSSCC, financial institutions, and financial services trade associations representing financial institutions from each subsector.

Some trade associations that have given their support include The American Bankers Association (ABA) and The Global Financial Markets Association (GFMA). Additionally, it has the support of numerous U.S. federal regulators and agencies.

How to utilize the Profile

The Profile itself can be found on the National Institute of Standards and Technology's website and consists of four basic steps:

1. Complete the nine questions of the Impact Tiering Questionnaire to determine your Impact Tier
2. Based on the Impact Tier, assesses your company with the corresponding Diagnostic Statement questions
3. Identify any gaps or shortcomings in your cybersecurity plan
4. Develop and implement a plan to close gaps and address shortcomings to satisfy the cybersecurity expectations of its Impact Tier

Improve your cybersecurity

While the Profile has received ample amounts of praise for its assistance in increasing productivity and reducing redundancy when it comes to cybersecurity in the financial sector, IT employees must still have a thorough understanding of their network with network security assessments in order to even utilize step one of the Profile.

Additionally, after identifying the shortcomings in your compliance or cybersecurity plan, it can still be difficult to implement all of the necessary changes, particularly if your company is very large or your IT team is small.

For example, if financial institutions do not have a well-implemented patch management plan, malicious actors will quickly attack the vulnerability in your network, leaving you open for potential financial losses, large fines from regulators, and loss of public confidence in your institution.

Making sure you have a full overview of every machine inside of your system (including computers and mobile devices), software installed on these devices, every server that is running on your machines, and more, is vital. After gaining a detailed look at your system, it's absolutely crucial that you create a fully-formed patch management program.

Experts know that in order to not fall victim to simple human errors like missing an application when taking inventory, forgetting a patch update, or waiting for a pre-scheduled date to install a vital security patch, both the network security assessment and patch management should be automated.

In fact, not even taking potential human error into account, without a very large, full-time staff, it is seemingly impossible to follow the necessary best practices without the aid of software. Dedicated software like GFI LanGuard takes away the stress of staying compliant and protecting both your employees and customers.

GFI LanGuard eases the burden on banks or others in the finance industry by automating some of the most vital parts of your cybersecurity plan, such as:

- scanning computing and mobile devices for vulnerabilities
- automating patching for Windows®, Mac OS® and Linux®
- auditing all network and software in your system

1 Vulnerability Scanning

If your company doesn't already have a vulnerability assessment put in place, you can almost certainly assume that your users are already compromised. GFI LanGuard will not only help your financial institution discover all current vulnerabilities to help you begin to truly take cybersecurity seriously, but continues to do so even after the initial scan.

In fact, "more than 60,000 vulnerability assessments are carried out across your networks, including virtual environments, mobile and network devices." It carries out multiple scans of your operating systems, virtual environments and installed applications through numerous databases, such as OVAL and SANS Top 20. This way, you can protect yourself from a potential security breach before it is ever compromised, saving your company's reliability and data.

After identifying a vulnerability, it recommends a course of action and gives you the tools to solve the problem. Additionally, the graphic threat level indicator provides an "intuitive, weighted assessment of the vulnerability status of scanned devices."

2 Patch Management

Patch management is another essential component to ensuring your systems are fully protected in order to avoid any potential vulnerabilities that could lead to an attack.

Because network security breaches are most commonly caused by missing network patches, an automated patch management system is nonnegotiable for financial institutions that are barraged by both attacks and regulators. In order to detect network vulnerabilities before they are exposed, GFI LanGuard scans you machine regularly.

GFI LanGuard patch management is not only compatible with Microsoft®, Mac OS X® and Linux®, operating systems, but also with more than 60 third-party applications such as Apple QuickTime®, Adobe® Acrobat®, Adobe Flash® Player, Adobe Reader®, Java® Runtime and more, and multiple web browsers, including Microsoft Internet Explorer® Mozilla Firefox®, Google Chrome™ Apple Safari® and Opera™. It can deploy both security and non-security patches.

3 Network and Software Auditing

In addition to understanding any potential vulnerabilities within your network and making sure all patches are regularly installed, GFI LanGuard also performs network auditing to analyze your network centrally. Without a detailed analysis of the state of your network, it is impossible to create a fully functional security plan. With GFI LanGuard, you'll understand which applications or default configurations could pose a security risk as well as a full list of:

- Installed applications
- Hardware on your network
- Mobile devices that connect to the exchange servers
- The state of security applications (antivirus, anti-spam, firewalls, etc.)
- Open ports
- Any existing shares and services running on your machines.

Beyond this, GFI LanGuard is able to integrate with over 4,000 critical security applications, such as your antivirus or VPN client. You'll receive status reports and lists of instant messaging or peer-to-peer applications that are present within your network. It also "rectifies any issues that require attention such as triggering antivirus or anti-spyware updates."

4 Stay compliant

This application also helps you stay compliant by following PCI DSS regulations for all businesses handling cardholder data. While safeguarding your network, it helps to gauge the effectiveness of any PCI DSS, HIPAA, SOX, GLB/GLBA or PSN CoCo compliance programs.

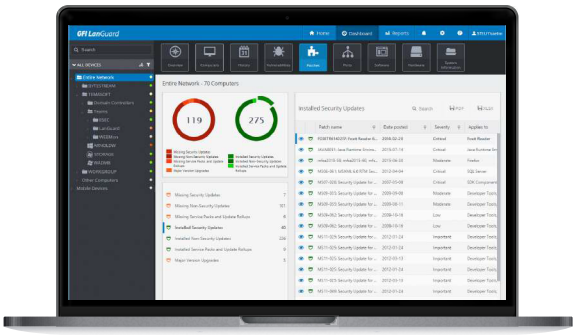
Additionally, the interactive dashboard offers a summary of all security audits with information about the network security status, relevant changes over time on your network, and more.

Staying compliant and secure isn't easy, particularly in the financial sector. However, with the assistance of software like GFI LanGuard, it's possible to complete a comprehensive plan for your financial institution's cybersecurity, automating the most important aspects of network security to make sure your clients stay safe and your company remains compliant.

Close the door on patch vulnerabilities

LanGuard

- ✓ Patch Management for Windows, Mac OS and Linux
- ✓ Network and software auditing
- ✓ Vulnerability scanning for computers and mobile devices



Get your FREE LanGuard trial!

GFI Software™