Meeting The Cybersecurity Challenge With NIST's Tool

cyber security ransomware

Summary: With 58% of C-suite and senior business leaders reporting that cyberattacks increased by 10% or more in 2021 vs. 2020, cybersecurity is increasingly vital. We review the top cybersecurity concerns from the 2021 CSBS National Survey of Community Banks and share an important tool to use in protecting your institution against surging cyber risks.

People in the world's Blue Zones — Greece, Japan, Costa Rica, and a few other places — tend to have longer, healthier lives than people in other parts of the world. When researchers investigated Blue Zone longevity, they found that diet, exercise, attitude, and community connection all played a role. The research provided a framework of knowledge designed to help people outside of these regions understand how to live longer lives.

Since there was only one US place in the Blue Zone (Loma Linda, CA), many of us could use this framework on life longevity. But, more immediately, a cybersecurity framework by the National Institute of Standards and Technology (NIST) can be used today to thwart the increasing number of cyberattacks that bankers are facing. We explore some of the cyber concerns of community financial institutions (CFIs) and review the NIST framework as a defensive tool.

Cyber incidents are on the rise

Fifty-eight percent of C-suite and senior business leaders said their organizations experienced at least 10% more attacks in 2021 than they had the previous year. The financial stakes are rising too. In the first half of 2021, there were $590MM of ransom-related transactions vs. $416MM for the entire year of 2020, according to the US Financial Crimes Enforcement Network.

CFI cybersecurity concerns

It is no wonder that the 2021 CSBS National Survey of Community Banks found that cybersecurity is the leading internal risk for community financial institutions (CFIs). It was a "very important" concern for the vast majority of participants, and twice as important as any other type of operational risk. Of particular concern were:

- **Data breaches.** The risk of a data breach is multi-pronged. In some cases, CFIs' most significant exposure may not be internal. It may stem from networks of retailers, suppliers, software vendors, and other companies that process or store customers' financial data. Last year, ethical hackers (those that test vulnerabilities so that the bad guys can't) were able to exploit vulnerabilities in 55 financial organizations' application programming interfaces, changing customer PINs and moving funds.
- **Social engineering incidents.** Armed with an understanding of human behavior, and detailed knowledge of their targets, bad actors may lead team members or customers to divulge confidential information, often without the team members or customers realizing what has happened. Social engineering scams are perpetrated through phishing and spear-phishing emails, calls, text messages, and other means. A Texas-based CFI reported nearly $1MM in fraud attempts during the first two weeks of February. Its customers

received text messages requesting validation of fictional wire transfers or debit card purchases. Those who responded were contacted by scammers who appeared to be calling from a financial institution's phone number.

- **Malware attacks.** Ransomware is malicious software that encrypts files and allows a perpetrator to hold files for ransom. Ransomware attacks have been on the rise at CFIs in recent years. Frequently, attackers also steal data and threaten to make it public. One way that CFIs and other businesses have reduced the potential damage of ransomware attacks is by backing up data.
  The ransomware business model has been evolving. In February, the FBI, along with other federal agencies, reported that bad actors are hiring independent services to "*negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cybercriminals.*"
- **Data manipulation.** Digitally stored data has become a target for cyberthieves, who have been accessing and modifying stored data. Cybercriminals are not always pursuing financial gain. Sometimes, the goal is to disrupt operations or pursue a political agenda.
  For example, a hacker might change credit rating scores to undermine confidence in financial systems or compromise data in other ways that facilitate fraud or generate misinformation or disinformation.

The NIST cybersecurity framework can be a valuable tool

As cyberthieves have multiple channels to target organizations, NIST has developed a cybersecurity framework to help businesses of all types understand, manage, respond to, and recover from cyber threats. Its "Framework for Improving Critical Infrastructure Cybersecurity" is a tool that can help CFIs understand and manage cyber threats, which could help reduce vulnerabilities and reputational risk. The NIST framework includes three primary components, the Core, Implementation Tiers, and the Profile.

1. **The Core** provides direction using a set of cybersecurity activities and outcomes, focusing on five primary functions. While CFIs are already following these five functions to some degree, it is good practice to review and refresh regularly.

- *Identify.* As the name implies, the process starts by improving understanding of cybersecurity risks within an organization so everyone is aware of and on the lookout for risks to systems, assets, data, and capabilities.
- *Protect.* Once potential threats have been identified, the next step is protecting against and limiting the impact of those threats. This function supports the identification, prioritization, and implementation of appropriate protections.
- *Detect.* Even with effective protection in place, cyberattacks will occur. This function supports effective monitoring and attack identification, so CFIs can respond effectively.
- *Respond.* Knowing how to respond when an attack occurs is critical. This function supports the implementation and evaluation of response plans. It also focuses on communicating and coordinating with internal and external stakeholders after an attack.
- *Recover.* In the aftermath of an attack, capabilities and services must be restored. The recover function supports the development, revision, and testing of recovery plans. It also focuses on learning from the event and adopting improvements to the overall system.

2. **The Implementation Tiers** focus on types of organizations and how their cybersecurity risk management practices align with the NIST framework. Knowing where your institution fits will provide areas of reflection on risk appetite, cybersecurity goals, and how much work your institution may need to do. There are four tiers.

- *Tier 1: Partial.* Tier 1 organizations tend to have reactive cybersecurity programs. They do not have integrated risk management programs and, typically, do not fully understand the risks accepted and

transmitted when interacting with business partners.

- *Tier 2: Risk informed.* Tier 2 organizations have defined risk management practices. However, these practices are not communicated and implemented as standard, organization-wide policies. These organizations are aware of the risks within business networks but may not act on them.
- *Tier 3: Repeatable.* Tier 3 organizations have defined risk management programs with documented policies, processes, and procedures that are implemented across the organization. The programs align with business requirements and are reviewed and updated regularly to meet ever-changing cyber threats. These organizations are aware of business network and supply chain risks and actively address them.
- *Tier 4: Adaptive.* Tier 4 organizations are resilient. They adapt cybersecurity programs based on experience and predictive factors. They continuously improve cybersecurity, and cybersecurity is part of leadership's organizational risk assessments. These organizations are aware of business network and supply chain risks and often rely on real-time information to track them.

3. **The Profile** is intended to help organizations identify and prioritize cybersecurity improvements. Profiles are diagnostic tools. They assess a CFIs "requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core."

The NIST framework offers guidance in easy-to-understand language that can help CFIs evaluate and modify current cybersecurity and risk management programs. Each component of the framework can facilitate discussion among leaders that improves the understanding of cybersecurity risk decisions and how these decisions are woven into the fabric of an institution.

Cybersecurity is an ongoing issue that CFIs must address fastidiously. Having the right tools to use is paramount in fighting cybercriminals. The NIST Framework is one of these tools and could help CFIs assess their cybersecurity readiness and prioritize the next steps.

TWO APPROACHES TO STRESS TEST YOUR LOANS

Now more than ever, it is important to stress test loans of all types from multiple perspectives. Choose your approach and get expert help, as needed. Learn more about credit stress testing today.

ECONOMY & RATES

Rates As Of: 03/18/2022 04:47AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.40	0.05	0.34
6M	0.81	0.12	0.62
1Y	1.25	0.26	0.87
2Y	1.93	0.51	1.20
5Y	2.14	0.43	0.88
10Y	2.16	0.33	0.65
30Y	2.44	0.28	0.54
FF Market	**FF Disc**		**IORB**
0.08	0.50		0.40
SOFR	**Prime**		**OBFR**
0.30	3.50		0.07