# Six Strategies to Bolster Your Cybersecurity

cyber security

**Summary:** According to the 2021 CSBS National Survey of Community Banks, cybersecurity risks remain the leading operational concern for community financial institutions. Here we look at six strategies institutions could deploy to contain the threat, protect their data and retain their customers' trust.

Spanning over 13K miles, the Great Wall of China was built as protection against nomadic populations and to protect the silk road trade. Building started as early as the 7th century BC, with the best-known sections built by the Ming Dynasty (1368-1644). A popular myth has it that the wall can be seen from the moon, although the apparent width of the wall from the moon would be equivalent to that of a human hair viewed from a distance of just under two miles!

These days it takes more than a wall to defend against the increasingly, sophisticated cyberthreats plaguing the financial services industry. We've previously discussed some of the cyber risk areas of greatest concern, including data breaches, social engineering incidents, malware attacks, data manipulation, romance scams, cryptocurrency fraud and tech-support fraud.

Without the resources that bigger financial institutions have to invest in cybersecurity and hire in-house professionals, community financial institutions (CFI) are at particular risk. They are often viewed as easier targets to cyber fraudsters. That said, there are many steps that your institution can take to reduce your chances of falling foul to cyber criminals. Here are six strategies to bolster your cybersecurity efforts.

1. **Nurture a cybersecurity culture.** In its latest data breach investigations report, Verizon found that human factors were involved in more than 85% of breaches — which is why building a cybersecurity culture is so important. As with any culture, this starts at the top, with C-suite executives making it clear that security plays a critical role in the organization's success. You should ensure there are clearly defined roles and responsibilities for security at all levels of your institution and that incident reporting processes are user friendly. Similarly, employees should receive regular training on the latest threats and how to spot them. Phishing tests will help you evaluate the success of your training. Above all, employees need to feel comfortable reporting suspicious behavior, so it's essential to avoid a culture of shame.

The executive director of cybersecurity at MIT Sloan says: "*We need a culture of cybersecurity because you can't tell everyone everything they need to do. You need them to understand that organizational safety is part of what they need to do in today's world.*"

2. **Use multifactor authentication.** According to Verizon, 61% of breaches are due to leveraged credentials. This primary means allows bad actors access to hack into an organization. Multifactor authentication is a powerful and cost-effective way of performing customer verification. Previously, we covered the issues at stake and the MFA options available for CFIs.

3. **Monitor your network 24/7.** With multiple systems in a typical CFI's IT infrastructure, security information and event management as-a-service (SIEMasS) is fast becoming a must-have, not the least because the FDIC mandates centralized log analysis to mitigate evolving risk. SIEMaaS can monitor and analyze data streams from across an institution's integrated systems to detect anomalies. This provides a holistic view of all possible

security risks for the institution to act upon. Your institution may want to consider outsourcing or partnering with a SIEM provider to help with any tech capability gaps.

A $450MM-asset Midwest CFI increased its network health by 20 points in two years after partnering with a SIEM provider. The CFI's network administrator says, "*The dashboard alerts have brought attention to areas that our IT teams can now address, which has helped reduce security and compliance threats within our networks.*"

4. **Protect your endpoints.** Endpoint devices — such as desktops, laptops, servers, routers and mobile devices — are vulnerable points of entry to any CFI's network and therefore primary targets for attackers. In fact, IDC estimates that 70% of breaches originate at these endpoints. As well as following best practices, your institution may want to consider selecting a partner to supply endpoint security. Gartner expects endpoint protection platforms to lead information security software spending in 2022, reaching $15.9B, and almost doubling by 2026.

5. **Evaluate third-party security.** Due to their size, CFIs often rely on third-party providers to offer the full range of services their customers expect, thereby exposing them to further cyber threats. For example, identity management firm, Okta, announced in March that it had suffered a data breach through subcontractor Sitel. Information from hundreds of its clients were compromised, but thankfully the scope of the hackers' access proved to be less than originally feared.

In November 2021, representatives of smaller financial institutions asked Congress to plug holes in the legislation that covered all entities that handle consumer financial information, including third-party technology providers, credit rating agencies and retailers. In the meantime, it's essential that your institution conducts its own due diligence to ensure that every entity your institution interacts with adheres to your security standards.

6. **Share information on platforms such as FS ISAC.** By joining platforms that share cybersecurity intelligence across the industry, your institution will be more able to stay abreast of new threats — and to stay safe.

The cybersecurity landscape is always shifting, so it's essential that your institution remains attuned to emerging risks – and that you continuously evaluate and strengthen your ability to detect and respond to cyber threats.

## START SMALL AND UPGRADE LATER WITH CECL FIT

We know that not every banker has the same needs. So CECL FIT® gives you options to custom-fit your portfolio. Start with a small package and you can still upgrade as you grow. Learn more about our CECL FIT solution.

## ECONOMY & RATES

Rates As Of: 06/06/2022 09:53AM (GMT-0800)

| Treasury | Yields | MTD Chg | YTD Chg |
|---|---|---|---|
| 3M | 1.21 | 0.05 | 1.15 |
| 6M | 1.68 | 0.04 | 1.49 |
| 1Y | 2.21 | 0.12 | 1.82 |
| 2Y | 2.73 | 0.17 | 2.00 |
| 5Y | 3.03 | 0.21 | 1.77 |

| | | | |
|---|---|---|---|
| 10Y | 3.03 | 0.19 | 1.52 |
| 30Y | 3.18 | 0.13 | 1.28 |
| **FF Market** | | **FF Disc** | **IORB** |
| 0.83 | | 1.00 | 0.90 |
| **SOFR** | | **Prime** | **OBFR** |
| 0.78 | | 4.00 | 0.82 |