**Independent Banker**

**January 2025**

**Portfolio**

**[tag] Checks & Balances**

**[hed] It’s time to bolster cybersecurity measures—now and forever**

[dek] As the costs of data breaches continue to rise, it’s essential for community banks to access and use available federal cybersecurity tools for combatting fraudsters and bad actors.

[byline] By Lance Noggle, ICBA

Cyberattacks are becoming more sophisticated, and banks face increasing regulatory pressure to strengthen their cybersecurity strategies. Meanwhile, the cost of a data breach is skyrocketing.

Last year, the average cost of a data breach in the U.S. was $4.88 million, up from $4.45 million the previous year. This represents a 10% spike in breaches—the highest increase since the global pandemic, according to IBM.

Community banks are feeling the effects of the changing regulatory landscape and growing customer data privacy concerns. As a result, ICBA members are prioritizing cybersecurity as a strategic imperative. They are improving security measures, providing additional employee training, and staying ahead of the latest threats and trends.

**[subhed] More than just due diligence**

As pillars of their communities, ICBA members must approach cybersecurity on an around-the-clock basis. After all, the bad actors never sleep; they’re constantly coming up with new ways to infiltrate systems, exploit them, steal their data and use it for nefarious purposes. Being forever vigilant is essential and can’t be overlooked; vigilance must become a part of your bank’s culture.

It's important to note that not every data breach or cyberattack is overly sophisticated. In fact, many of them can infiltrate through fairly innocent means. For example, the employee who doesn’t understand the danger of opening a phishing email from an unknown source can unwittingly wreak havoc on the bank’s systems, databases, and customer data. Banks can reinforce the importance of recognizing and avoiding phishing attempts by investing in regular cybersecurity awareness training.

For example, sending phishing email attempts to your own staff—something we know everyone hates, even though it’s extremely effective—is one way to keep everyone on their toes. After all, you’d rather have someone inadvertently click on a phishing email that was generated internally versus one that was sent by a cybercriminal, right?

Sending random phishing emails is just good practice. It also helps everyone understand and deal with the potential threat (e.g., do we just delete the message? Do we report it? Do we mark it and have the system quarantine it?). This serves as one more training tool that ensures staff members are properly following the bank’s policies and procedures.

**[subhed] Pack your cybersecurity toolkit**

Banks should also be stress-testing their systems regularly to help fortress them against both existing and emerging threats. The [Cybersecurity & Infrastructure Security Agency (CISA)](https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools) provides a free tool that community banks can use to ensure that their systems are up-to-date.

This “cyberhygiene tool” is one of the most accessible and free applications that community banks have available. It doesn’t impact a bank’s operations, nor does it involve a regulator, but it does provide weekly reports based on system scans for potential vulnerabilities. This makes it a no-brainer for banks that would otherwise have to establish their own internal systems for cyberhygiene monitoring and reporting.

Third-party systems are another potential entry point for cybercriminals and something that community banks should be aware of. The bottom line is that their vulnerability can easily become <i>*your<i>* vulnerability. We saw this as early as the massive data breach that Target suffered in 2013, when criminals exploited the systems of an HVAC contractor.

Developed by the Federal Reserve, the FDIC and the OCC, [*Third-Party Risk Management: A Guide for Community Banks*](https://www.fdic.gov/resources/bankers/third-party-relationships/third-party-risk-management-guide.pdf) provides a roadmap that banks can use to create and implement their own third-party risk-management practices. It includes scenarios that are specifically applicable to community banks, making it a good resource for ICBA members that want to improve their third-party vendor management practices in 2025.

Community banks using the Federal Financial Institutions Examination Council’s [Cybersecurity Assessment Tool (CAT)](https://www.ffiec.gov/cyberassessmenttool.htm) should be aware that the tool will be sunsetting in August, with no immediate replacement announced. This tool was developed in response to the increasing volume and sophistication of cyber threats. It helps institutions identify their risks and determine their cybersecurity preparedness.

Banks that rely on CAT should start exploring other options sooner rather than later. Not only will any new cyber-assessment tool take time and effort to identify, learn and adopt, but you also want to pick a platform that your regulator(s) are both comfortable with and supportive of.

ICBA has been working to ensure that the [Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022](https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia) doesn’t place undue burden on community banks that are already reporting cyber incidents to regulators. We’re not sure exactly where this issue is headed in 2025 (or beyond), but ICBA is working to ensure that the final rule matches as closely as possible to the reporting rules that are already in place.

***Lance Noggle*** *(*[*lance.noggle@icba.org*](mailto:lance.noggle@icba.org)*) is ICBA senior vice president, operations and senior regulatory counsel.*

[ends]

[big stats]

**$4.88M**

average cost of a U.S. data breach in 2024

**$4.45M**

average cost of a U.S. data breach in 2023

**+10%**

spike in breaches from 2023 to 2024—the highest since the COVID pandemic

*Source: IBM*

[pull quote]

Being forever vigilant [about cybersecurity] is essential and can’t be overlooked. Vigilance must become a part of your bank’s culture.