***Independent Banker***

**Portfolio: Innovation Station**

**October 2022**

[tag]

**Innovation Station**

[hed]

**Fighting cybercrime one innovation at a time**

[byline]

**By Charles Potts, ICBA**

[body]

ICBA surveys the industry and its members annually to identify their top concerns as part of its innovation strategy. Without fail, cybersecurity ranks among the top three, making it a clear priority for our organization.

Our bankers face both challenges and opportunities as they work to stay ahead of cybercriminals, paying attention to innovative solutions and partners to mitigate cyber risk. With cybercrime becoming increasingly complex and sophisticated, community banks must remain vigilant and monitor and manage their critical infrastructure.

To that end, ICBA invests heavily in cybersecurity partnerships and innovation through its ThinkTECH Accelerator program, Community Banker University, Preferred Service Providers and other available tools and resources. From the start, ICBA has worked to bring cutting-edge cybersecurity solutions to our members and the industry, and we continue to do so.

With cybercrime continually evolving, I’d like to remind our bankers about three key ways to help ensure the safety and soundness of their institutions.

**1. Network security monitoring**

Over the past couple of years, numerous reports have shown an uptick in cyber threats to the financial services industry*.* In a 2021 report, the New York Fed noted that financial services firms might experience up to 300 times more cyberattacks per year than other firms. Trends like this underscore the need for state-of-the-art network security monitoring. Adlumin, a ThinkTECH Accelerator participant that ICBA helped bring to market, offers premier services in this niche for community bankers.

**2. Training employees and customers**

With the explosion of digital solutions, community banks must train bank staff and customers on cybersecurity best practices. All too often, cybercriminals focus on the customer side of the equation. That's one reason ICBA selected Beauceron Security for one of its ThinkTECH cohorts. The company specializes in helping banks with cybercrime training for employees and customers. Companies like this help our members maintain a protected, safe environment.

**3. Governance**

Cyber risk assessments and tools are essential to the cybersecurity process. Managing and maintaining a consistent and efficient governance process is all too often a manual, laborious endeavor. Various solutions are available to help community banks analyze their institution's access, security controls and vulnerabilities and take the remedial steps necessary. Another of our ThinkTECH Accelerator participants, FINOSEC, offers a governance automation platform to save financial institutions time and enhance exam preparedness.

Furthermore, it is part of ICBA’s DNA to provide cybersecurity education through Community Banker University. We also maintain policy experts on staff who have the experience and expertise to address current and emerging cyberthreats and challenges. These tools work together to offer our bankers a comprehensive approach to cybersecurity.

**[Subhead] The time is now**

Community banks are at a critical juncture when it comes to cybersecurity. Many of the cybersecurity tools and resources we relied on in the past are no longer effective. That's why community banks should seek education, solutions and partners that specialize in addressing cybersecurity as it continues to evolve.

Finally, as you assess your cybersecurity strategies and plans, know that ICBA has extensive knowledge, expertise and education you can tap into to help you chart the path ahead. Visit ICBA.org to learn more about the cybersecurity tools and resources we offer to keep you and your customers safe.

**Charles Potts** (charles.potts@icba.org) is ICBA executive vice president and chief innovation officer.