Independent Banker
October 2023
Portfolio

[tag] Innovation Station

[hed] Put innovative thinking to work in risk mitigation

[byline] By Charles E. Potts

[body]

As we roll into October and Cybersecurity Awareness Month, I’d like to put forth a challenge: Think of risk mitigation not as a reminder of necessary defenses but as an opportunity to put innovative thinking to work.

At their core, risk mitigation and innovation are intricately tied. Neither is an individual project; they’re ways of doing business. With risk mitigation, as with innovation, the approach of “set and forget” doesn’t exist. Both need to be a part of the culture of the bank, and I find that the banks that take this to heart seek continuous improvement so that the new product or line of defense only gets better. That’s innovative thinking.

But looking at risk and innovation as two sides of the same coin begs the question, “How do you lead your organization to champion both?” Achieving that mindset comes down to three principles:

1. **Foster a culture of innovation—with risk mitigation in mind***.* Consider fraud, cyberattacks and other forms of risk as problems to be solved. Host brainstorming sessions. Assemble your organization and gain input. Create gamification tools, hackathons, innovation labs and more to build and test potential solutions. By encouraging this inventive, collaborative work, your organization will come out stronger. For instance, when [First Community Bank and Trust](https://www.independentbanker.org/article/2022/06/01/how-gamification-can-be-a-boon-for-community-banks) instituted Beauceron Security’s more gamified approach to cyber training, its phishing email click-through rates plummeted from 15% to 20% to under 1%.
2. **Train, practice and proceed.**Remain vigilant against emerging threats by training staff. Provide opportunities for formal education, such as sessions at Community Banker University (CBU). Join ICBA’s [upcoming cyber exercises](https://www.icba.org/solutions/operational-risk/cyber-and-data-security/exercises) (see sidebar). Share your experiences with your bank peer group. These efforts steer us to a stronger understanding of the landscape and a path toward thwarting threats.
3. **Lead by example.**Pursue positions in fraud and cyber groups. Consider new accreditations, including CBU’s Bank Security Certification. Identify technological solutions to support your bank’s needs. Demonstrate the role innovative thinking can play in risk mitigation.

You’ve heard the saying, “With great risk comes great reward.” While that may be true, in community banking, great risk mitigation—supported by innovative thinking—drives reward for our banks, our customers and our communities.

*Charles E. Potts is ICBA’s executive vice president and chief innovation officer.*

[ends]

[sidebar]

**ICBA cyber and data security exercises**

In these sessions, cybersecurity experts tailor training to the specific needs of community banks:

* CISA/ICBA Cyber Tabletop Exercise on Dec. 6 at 12 p.m. Eastern. Register online at <i>*icba.org/events*<i>
* Bank Supply Chain Breach (downloadable resource)
* Core Provider Supply Chain Breach (downloadable resource)

Visit [ICBA’s](https://www.icba.org/solutions/operational-risk/) online [Operational Risk Resource Center](https://www.icba.org/solutions/operational-risk/cyber-and-data-security/exercises) for more information.

[sidebar ends]