EXPERTS EXPLAIN

*5 Questions for UFS Experts, that answer trending community banking questions*

# Q. What is the top risk concern for community banks? A. Addressing cybersecurity.

What prevents a bank from improving their security posture? How could a bank's cybersecurity plan improve their operational efficiency? UFS Director of Risk Management Amy Radue was asked these trending questions in a recent interview.


Cybersecurity is clearly the top priority for community bankers when asked about their current risk concerns. Radue shared her observations regarding the heavy focus on cybersecurity as well as managing the pressures related to regulatory compliance.

### How are banks addressing cybersecurity both in the short term as well as the long term?

Radue indicated community banks are utilizing a number of strategies for a strong cybersecurity plan including: partnering with experts who understand cybersecurity, along with good cybersecurity insurance, as well as engaging in the different information sharing platforms that are out there such as: US-CERT, FS-ISAC and the ABA, among others. Radue also emphasized the value of sharing with a community of other bankers to collaborate on solutions that stay aware of the cybersecurity trends that are happening.

"Really great long term solutions for community banks look like establishing a place for cybersecurity in your strategic plan," said Radue while address solutions for community banks. She stressed the value in making sure the bank's board is constantly aware of the increasing cybersecurity challenges that the banks are facing, the resources that are needed to address cybersecurity plus maintaining a holistic view of cybersecurity to combat these concerns effectively.

### What prevents a community bank from improving their security posture?

"What's really challenging for banks when it comes to cybersecurity is just the resource constraints that cybersecurity causes, it could be anything from, a monetary resource constraint, internal personnel resource constraint, or even a knowledge resource constraint" said Radue. Perhaps the biggest question Radue asked was how do you know what you don't know?

"How do you make sure that the one IT person you have on staff is at the cutting edge, and in front of all these cybersecurity needs?" Radue asked hypothetically, addressing the real challenges and heavy weight felt by many community bankers when attempting to improve their security posture.

### What can a bank do that is concerned with their current cybersecurity plan?

For a community bank who is really looking to mature their cybersecurity plan, the best advice Radue offered is to find a partner that the bank trusts who is in the cybersecurity world day in, and day out, and willing to guide them through this journey. It is with that partner, they can build confidence for the bank in several areas, including how to address their incident response plan as well as making sure that the bank's cybersecurity plan adapts with the constantly changing cybersecurity landscape that all bankers are all facing.

### How could adapting your cybersecurity plan benefit and impact the bank's operational efficiency?

"If we take finding a cybersecurity partner as our number one step for a community bank when it comes to facing cybersecurity... what that does for your internal operational efficiency, is take that burden off the bank's internal staff to allow them to focus on other projects that need to be done," said Radue. She continued to emphasize that partnering

*...continued on back*

with a cybersecurity expert not only moves efficiency forward, but now the bank has the confidence that issues are tackled as they come or even before they happen by a team of experienced experts.

"Cybersecurity is scary, and cybersecurity is heavy, and it's something that needs to be part of our daily life as bankers, but it doesn't need to be those things... it doesn't need to be scary and it doesn't need to be heavy..." Radue said. She reiterated the value of finding the right partner, finding the right tools, utilizing the tools given to us through the FFIEC and with this guidance, banks have the ability to be prepared for a cybersecurity event. "This preparation really removes some of that burden, and so using all those different tools we have together, it doesn't have to be as scary as it sounds, on the day to day."

---

Amy Radue is the UFS Director of Risk Management and has been with UFS for 5 years. Prior to this, Amy spent the previous 10 years working for a community bank with responsibilities aligned to IT, compliance and risk management.

**To watch the video interview: Experts Explain, 5 Qs with Amy Radue, visit the UFS website video-blog: https://www.ufstech.com/10417-2/ or scan the QR Code:**

UFS

**BANK** TECHNOLOGY **OUTFITTER**

For more information, contact UFS at 262-376-3000 or email us at hello@ufstech.com
www.ufstech.com