Top Bank Risks

Cyber, third parties and regulatory changes continue to top the list.

BY JULIE KNUDSON

As 2017 passes into 2018, bankers are facing a risk landscape that is at once familiar and evolving. From concerns about third-party relationships to the challenges businesses face in workforce management, risks and their impacts are more interconnected than ever before. Each functional area has the potential to influence risks in the others.

To get a better handle on which risks should be on financial institutions' radars in the coming year, we consulted the experts.

Security and cyber risks remain at the top of most lists

Cybersecurity continues to be a primary risk focus for financial institutions of all sizes. Dennis Hild, managing director in risk consulting, specializing in financial services at Crowe Horwath, LLP, says part of the concerns going into 2018 revolve around the risk-threat lifecycle and the current stage of cyber in that evolution. "It's not very mature with regard to regulatory expectations and robust risk management," he explains.

Last year's massive Equifax breach—which affected more than 140 million Americans—was just one factor illustrating how banks handle security risks today. While past efforts looked primarily at how to mitigate vulnerabilities within the institution, the Equifax exposure broadened the risk profile for many organizations. It's the type of event that's likely to change what regulators expect in terms of cyber risk management and the use of self-assessments and other tools. "There are multi-layered issues, where you have involvement on the banking side internally but also significant reputational risk, third-party providers and other variable factors you may not have thought about," Hild says.

Rather than slowing as businesses ramp up their cybersecurity efforts, threat vectors such as ransomware have become more frequent and potent, affecting companies in nearly every sector and posing a significant risk to financial institutions. "Criminals continue to have a strong hand," says ABA SVP Ryan Rasske. "Banks devote massive resources to identify vulnerabilities that criminals might seek to exploit and to put controls in place."

As financial institutions continuously work to improve their technology infrastructure, Rasske says risks could arise as a result. "Banks have to reevaluate the process that they just modified to ensure the new process has adequate controls around it," he explains. With more technology upgrades and workflow changes to implement and monitor each year, banks must be vigilant to avoid creating new entry points for criminals.

Third-party risk a high priority

The banking industry has grappled for years with managing outside providers and the hazards those relationships may pose. "From a regulatory perspective, the key is

in 2018

> “Risks and their impacts are more interconnected than ever before. Each functional area has the potential to influence risks in the others.

that the regulators expect depository institutions to know who their third parties are,” says ABA VP Krista Shonk. But improving oversight of third-party risks—with banks striving to make their efforts not only more effective but also more efficient—is about more than keeping an inventory of vendors. “One thing we continually hear from regulators is that banks must have people on staff with adequate expertise to oversee their third parties,” Shonk says.

If institutions aren’t diligent in assigning employees with the expertise to conduct effective due diligence and risk analyses, liabilities may not be properly identified and mitigated. Shonk says that not only does her team routinely hear agencies mention shortcomings in documentation of risk and documentation for the rationale behind assigning various risk ratings, but also “weaknesses in the ability of community bank staff to analyze and put appropriate controls in place based on [statement of condition] reports.” This represents another area where institutions may consider improving their risk management strategy in 2018.

With banks’ increasing reliance on third parties, downstream risks are also becoming a larger issue. Not only does an institution need to vet their vendors, but the companies those third-party providers partner with are also coming under greater scrutiny. “I think we continue, as an industry, to move more toward offloading to third parties, but we don’t always know who they’re subcontracting with,” explains Joanne Campbell, CRCM, EVP for risk management at Camden National Bank in Camden, Maine.

Payroll processors may rely on a cloud service to transmit data, for example. Many service businesses use hosted email platforms. “We’re good at gathering information, but those controls aren’t within your realm,” Campbell says of the numerous touch points that come with vendor relationships. Third-party risks don’t stop with the primary partner, though institutions may find it difficult to follow the trail far enough to ensure that the proper security measures are in place through the entire chain. “You really can’t control it, other than within the contract and the service level agreement,” Campbell says. It’s part of the maturation of the third-party environment that continues to present risks within the banking industry.

Regulatory uncertainty is top of mind

A number of issues are looming on the near-term regulatory horizon, many of which banks may not have had to confront in years past. While much has been written about CECL’s looming implementation and its impact on risk, the prospect of regulatory relief should also be on bankers’ radars. For institutions anticipating relaxed rules, Will

Newcomer—VP of product and strategy, finance, risk and reporting in the Americas for Wolters Kluwer—says the view of regulators is, "Why would we ever go back?"

Whether and when relief comes to fruition, Newcomer says, "Regulators still have the right to say, 'Tell me you're in control.'" Rather than evaluating risk with an eye toward relaxed regulations and possibly being left behind, he instead encourages the use of stress tests and other tools to ensure the organization is in a good risk position no matter how the regulatory landscape may change in the future.

When it comes to the regulatory environment, Clifford Rossi, a professor and executive-in-residence at the University of Maryland's Robert H. Smith School of Business, says: "Generally speaking, banks will find 2018 to be a year of more uncertainty." Little is known about how new regulations may shape up, but changes in existing regulations will also be a focal point fraught with ambiguity.

After an acceleration in the growth of compliance officers and other professionals responsible for ensuring banks are in step with laws and regulations, Rossi says the Trump administration's financial regulatory appointees may take a closer look and perhaps soften some of those rules. "Banks will need to figure out what the administration really wants to do and how it will impact their processes. That will take some time." Potential regulatory reform could take many (and multiple) shapes, but until additional details are known, risk factors will center around what is still to be determined. "It could be complicated and expensive if banks need to rework things, so they'll have to keep an eye on it," Rossi says.

Talent management an ongoing challenge

Talent management is another area where experts see risks in the banking sector, particularly for community banks. Jason L. Painley, SVP and chief risk officer at Park National Bank in Newark, Ohio, believes organizations should consider how employee training could help them manage the various risks the bank may encounter. "Training in risk management and emerging risks needs to be ongoing for every position in the financial institution," he says.

Social engineering cyber attacks—to name one example—could (and have) hit at any segment of the reporting structure, and the scope of potential vulnerabilities is so broad that staff must act as the first line of defense. "You need to have everyone on all levels in tune to current risks and management strategies," Painley says. He adds that the threat environment tomorrow will be different than it is today. "Banks need to be looking forward and doing their best to identify risks before they become a reality. Continued spending on training—formal and informal—needs to be a priority."

Though Barbara Boccia, CRCM—senior director of U.S. advisory services at Wolters Kluwer—says that talent management has long been an important area of focus, she believes that changes happening with HR in the regulatory compliance arena may be shifting where human capital risks exist. "It really arises predominantly from the Wells Fargo case," she explains.

Though what Boccia calls "egregious practices around sales" was the primary trouble spot, she says that a disconnect between HR and compliance was identified after several whistleblowers' exit interviews. "How do you bring HR in and partner with them so they understand more about what compliance risks are, so HR can help identify those enterprise-wide risks that might be surfacing?" Boccia asks. It's a different role than HR has typically played in the past, but one that she says is critical to successful risk management going forward. "It's changing the risk profile a bit in terms of who the players are."

Lending risks on deck for renewed attention

With the industry now nearly a decade beyond the last financial crisis, Rossi sees real risk at the intersection of product and process. If the economy gets a boost from regulatory reforms and other actions, he says, "We could very well see an expansion in financial services where new products start to be developed." That's where the connection point between process, quality and product development becomes an important risk area. "As we saw in the last crisis, the infrastructure used to develop, originate and service those loans was, in many cases, not up to the task of controlling the risk that those assets had associated with them," Rossi explains.

Though other areas will continue to vie for banks' attention, Rossi says now is the time to invest in improving the infrastructure needed to manufacture and produce loans. "A lot happens when we're in an environment where business is starting to take off," he says. The effects of poor lending decisions may not come home to roost until years later, in the form of higher credit losses, but between streamlining processes and working through new technology deployments, Rossi says it's "very important to keep an eye out as the business cycle starts to go in an upward direction."

JULIE KNUDSON *is a frequent contributor to the* ABA Banking Journal.