

How Banks Can Improve Crisis Planning

By: Naomi Snyder, managing editor for Bank Director | SEPTEMBER 18TH, 2015

We discovered last month that cyber risk was the thing most directors worried about when we informally polled members of our bank services program. This month, we decided to poll experts on what banks could do to improve crisis planning. Not surprisingly, cyber risk planning came up often as an area that could use some improvement. Several of the people polled think banks could benefit from role playing exercises that would walk employees and the board through possible scenarios. The Federal Deposit Insurance Corp. has a few videos that help banks imagine some scenarios. Although planning documents are widely recommended, one consultant says they are pretty useless in a real emergency. Below are their responses.

How Could Banks Improve Crisis Planning?



Crisis planning is getting more attention these days because we are constantly reminded of events that could not only impact our business, but have significant impact on our reputations. **One data breach and we stand to lose faith in our ability to safeguard our clients' money.** While planning is expected, bankers could really get value from practice in two areas: 1) tabletop exercises and 2) media training. Tabletop exercises are role playing crisis scenarios whereby bank management gets on a conference call and develops responses, assigns roles, identifies tasks and develops timelines. Banks would benefit from doing this on a quarterly basis. Media training allows bank executives to learn how to look and respond appropriately to a tense situation only after they learn how to answer questions and the ground rules for working with the media. Turn on a video camera and see how well your team does. Crisis planning is better if treated as an ongoing discipline.

—**Scott Mills** is president of the William Mills Agency, a public relations and marketing firm specializing in financial services



Testing, testing and more testing! Banks typically have multiple plans that can be triggered in the event of a significant cyber-related "crisis," including, for example, a business continuity plan, incident response plan and crisis communication plan. Multiple groups within a bank likely have responsibility for these plans. And, the plans may not be aligned from a response standpoint with respect to significant cyber events. In the event of such a crisis, **it is critical for a bank to be able to respond in a uniform and effective way** at the enterprise level. Bringing a bank's various teams together to test or tabletop a significant cyber event can shed light on how the bank's various plans (and teams) will work together. This will also provide a valuable opportunity for refinement and alignment of the bank's related response plans.

—**Nathan Taylor** is an attorney and cybersecurity expert at Morrison Foerster LLP



Business continuity and disaster recovery considerations are an important component of a bank's business model. In addition to preparing for natural disasters and other physical threats, continuity also means preserving access to customer data and the integrity and security of that data in the face of cyberattacks. For this reason, the **FDIC encourages banks to practice responses to cyber risk as part of their regular disaster planning and business-continuity exercises.** They can use the FDIC's cyber challenge program, which is available on the [FDIC website](#). Cyber challenge was designed to encourage community bank directors to discuss operational risk issues and the potential impact of information technology disruptions.

—**Rae-Ann Miller** is associate director of the FDIC's Division of Risk Management Supervision



Banks can improve planning by **developing a crisis plan ahead of a data breach or cybersecurity issue**. These action plans should include:

1. Determining data to be protected along with the protection level required.
2. Classifying incidents or scenarios into categories.
3. Understanding threats the bank may face, starting with known threats, then creating on-going monitoring for emerging threats.
4. Determining the stakeholders and defining the incident response team.
5. Setting up a command center and appointing a command center leader.
6. Developing an incident plan, including a containment and investigation strategy.
7. Executing a communication plan to customers, media and agencies.
8. Testing and training end users in the application of the incident response plan.
9. Conducting a “lessons learned” session and updating [Incident Response Plan] procedures.

—**Jeff Sacks** is a principal in Risk Consulting for Crowe Horwath LLP, specializing in technology risk



Though banks understand the risk of cyberattacks, many are unprepared to act quickly and effectively to mitigate damage when faced with a serious cyber breach. To improve crisis planning, **banks should consider conducting simulated cybersecurity exercises involving key personnel**. Moving quickly following a cyber breach is critical to limiting unauthorized access to sensitive data and the resulting harm. Such exercises demonstrate why an effective cybersecurity program is more than a “tech issue,” and requires coordinated institutional mobilization across business segments, with oversight from senior management. Most banks will eventually find themselves in a hacker’s crosshairs no matter how advanced their defenses, and a coordinated, rapid response will not only limit short-term data loss and legal exposure, but will also help preserve a bank’s reputation and customer relationships.

—**Neil MacBride** is a partner at Davis Polk & Wardwell



Planning activities generate lots of documents, which are fascinating to auditors but useless in an emergency. You don’t have to give planning reports to your response team. Your phone is a perfect emergency communications console. **Social media, including Twitter, YouTube and even Facebook, are indispensable as communications tools**. You can monitor events as they unfold or push messages out to staff and public. Cyber is the new disaster. Compare today’s threat assessment with one from 2010. Notice that blizzards and hurricanes have dropped out of the top ten, replaced by data breaches and identity theft.

—**Steve Carroll** is a director with Cornerstone Advisors, a consulting firm specializing in bank management, strategy and technology advisory services



Naomi Snyder is the managing editor for Bank Director, an information resource for directors and officers of financial companies. You can follow her on Twitter at twitter.com/naomisnyder or get connected on [LinkedIn](#).