In more than 30 years of working for community banks as IT Director or as service provider, I have learned the technology risk with the greatest potential negative impact is the belief “that it could never happen to us.” The “it” may have changed over the years, but the danger has not.

The “IT” used to be the possibility of a disaster that called for the activation of a Bank’s business continuity plan. For years, many clients -- particularly the smaller ones -- were just not buying that something like that could affect them. Until 9/11. And Hurricane Katrina. And Hurricane Sandy. Those three previously unthinkable disasters woke the country up in a terrifying way – and caused many of the previous nay sayers within the community bank to re-think that belief and instead take business continuity planning and testing seriously.

Fast forward some years.

The “IT” in “It could never happen to us” has morphed; it is now the possibility of a systems breach or other security incident that threatens the information security, reputation and financial assets of an organization. “A breach is something a big company needs to be concerned about, but why in the world would we ever be the target.” Or so goes the thinking of many a $100 million or $200 million community bank.

The belief is often held, but not expressed, by individual members of senior management -- a dangerous enough scenario. More worrisome is when that unspoken belief is shared by the Information Security Officer and/or the head of Information Technology. In such cases, the bank’s technology security and compliance posture may be informed by arrogance, ignorance, or the defense that “we’re just a small community bank…” Such a belief, in my view, is dangerous, ill-informed and ill-advised and our experience with hundreds of community banks in the recent past supports that view.

In the last 2 years, I have seen the previously immune community bank be upended by scores of incidents involving ransomware, distributed denials of service, fraudulent wire attempts, and corporate account take overs to name but a few examples of what we have seen. Clients who thought it could never happen to them have been surprised by the incidents they faced, and even more surprised by how difficult it was to get to the bottom of what happened, and decide the appropriate course of action. It is these clients who are actively re-visiting their security incident response plans, actively strengthening their IT audit plans, and actively engaging with threat intelligence services and networks that improve the community bank’s cybersecurity posture for the future.

Such a shift in thinking is welcome – and one that the Banking regulators are trying to help promote. With their introduction of the FFIEC CAT tool (June 2015), as well as the FDIC’s introduction of the InTREx examination (June 2016), the examiners see Cybersecurity as a central technology risk for Banks of all sizes to properly address. A critical component emphasized is the focus on the Incident Response discipline which should be documented as though an incident were going to happen. The examiners are no longer taken by surprise by a sophisticated scam aimed at a smaller community bank; they see it as not only a possibility but a likelihood over time.

The right question to ask is not whether such an incident will occur, but rather when will it occur, and how effectively will the bank respond to the incident and protect the Bank’s reputation, brand and assets when it does?

At Accume Partners, we will help you ask the right questions, and help ensure that your answers are ones with which the Bank regulators, Board and owners would readily agree. Please mark your calendars on May 31st 1:00 pm EST for an Accume Webinar on Cybersecurity and Lessons Learned from Security Incidents.
Michael Barrack  
Managing Director, Technology and Cybersecurity Services

Department: Technology Compliance and Cybersecurity

As Managing Director of Risk Director and Cybersecurity Services, Michael Barrack provides IT security and risk and compliance consulting services for community financial institution clients across the United States. With more than 25 years of serving community Banks in Southern California, Michael brings a keen understanding of how our clients use technology to support the business, and what the regulators expect of Banks and Credit Unions as it relates to IT-related compliance.

Having been the accountable Executive in IT regulatory examinations as both a banker and service provider to Banks and Credit Unions, he has the experience and insight to know how best to prepare for and respond to such exams, which the Risk and Compliance team has incorporated in its offerings and consulting services.

Previously, Barrack served as Chief Executive Officer at iPay Technologies, LLC, a Kentucky-based bill payment processing company where he led the company through a period of explosive growth, tripling revenue and increasing profitability and the client base of community banks and credit unions substantially. A veteran to the banking industry, Barrack has led technology and compliance efforts at financial institutions over the course of his career including East West Bank, where he served as Director of Information Systems, and Community Bank, in which he led the Information Technology Group as Chief Information Officer.

Barrack resides in Henderson, Nevada and holds a Masters of Business Administration at University of California, Los Angeles. He received his undergraduate degree at Carleton College, graduating Magna Cum Laude.