Q&A: Michael Berman

According to the CEO of enterprise risk specialist Ncontracts, cybersecurity risk assessments aren't just an exercise in compliance. Besides the obvious benefits to data security, they can save your community bank time and money.

Interview by Molly Bennett

A risk assessment of any kind may feel like a dreary box-checking exercise, but a cybersecurity risk assessment can be an effective way to cut costs and minimize waste. We sat down with Michael Berman, CEO of enterprise risk and vendor management software provider Ncontracts, to find out more.

Why are cybersecurity risk assessments so important?
A data breach can shut down the entire institution if it is bad enough. You can buy insurance to help replenish your customers' losses and damages, but you can't really buy insurance to help you recover from the reputational damage and other long-term compliance risk. Those things are uninsurable. If you don't have the right controls and systems in place to protect your institution, you are creating a lot of risk.

Should community banks be using the FFIEC's Cybersecurity Assessment Tool?
Having a framework is helpful. I think all these tools are about the same, and they can provide insight into the need for additional resources. However, this type of assessment is a blunt instrument, because it is a one-size-fits-all approach. The government is in a tough spot trying to come up with uniform standards that apply to a $10 million-asset sized institution and a $10 billion-asset institution. They have made some compromises, so it's not a perfect tool by any stretch of the imagination, but it is a good starting point that will help make sure you are looking at the right things from a cybersecurity perspective. But nothing is better than an actual assessment by a professional to really understand what your threat factors are, what your controls are, and if they are being adequately addressed.

Can an assessment be done internally?
There are a couple of different aspects to an assessment, some of which by their very nature have to be done externally. There is the operational component, such as looking at whether your anti-malware software works or not. Then there is the internal risk assessment, based on management's review of whether the controls are working. And then we have an audit, which may be done by a third-party firm to confirm that the controls are working. Finally, the regulators come in behind all of that to be sure everything is working.

Where does the buck stop? The IT department? Management? The board?
The guidance has changed. The responsibility is ultimately with the board of directors and senior management, and both the FFIEC guidance and the primary federal guidance make the point of this. You are not offering a safe and sound institution if you have these types of risks, and you can't just blame that on IT and say, "Oh, we didn't really understand

"You can't really buy insurance to help you recover from the reputational damage and other long-term compliance risk [of a breach]."

—MICHAEL BERMAN, NCONTRACTS

what we were reading." They expect you to take the time to get answers to any questions you have, because ultimately it is your responsibility as a board member or a member of senior management to understand these risks and make sure the right resources are in place to mitigate these risks.

Beyond risk mitigation, what are the benefits of a risk assessment?
I think the biggest thing that most community banks don't realize is how the process of a risk assessment can affect the benefits. Is the process efficient? Is work being repeated that has already been done from another assessment? We're talking about enterprise risk, cybersecurity, business continuity planning and vendor management. All of those are exercises that help control risk, and too many institutions view them all as compliance activities, which means they are trying to check the box. This check-the-box process leads to the same work being repeated. A true risk assessment cuts across those areas, and you are able to get a holistic view of the organization. And it might affect multiple aspects of each of those topics, so you can look at it and know there is one team or person responsible for the control. That way, you are not spending resources unnecessarily, checking it four or five times with different personnel just because it happens to show up in four or five different places from a guidance perspective.

Which is why risk assessment tools can come in handy?
Exactly. You want to put in the data once and watch it go everywhere. The challenge is that a lot of times in community banks, this type of work is done in silos. They have a person who is involved in compliance, and another person is responsible for vendor management, and they have someone in IT who might be doing cybersecurity, and they have a different person in IT doing continuity planning. And it's no wonder that when you start looking at the results from the perspective of an examiner or an auditor, you see variance from the four people examining the same control. You are basically paying for a lot of work to be done multiple times. And that makes no sense from an efficiency standpoint, especially given how much pressure banks are under from a financial perspective.

> **"Most community banks don't realize how the process of a risk assessment can affect the benefits."**

So it's better to lay out a chunk of money now for a more comprehensive approach that may bring savings down the line?
Right. And not only that, it also deleverages you from personnel. There are so many times when a bank has a great cybersecurity person who gets hired by another bank. They are left with a manual system that was great when they had a great-caliber person around to operate it, but now that that person has left, they are left with a void. So, by having an application or some type of system in place that can guide the next person, it can make for a far more streamlined approach. The knowledge of what that original person did for cybersecurity really needs to run with your organization, not with your personnel. IB

Molly Bennett is executive editor of *Independent Banker*.