Information Security Risk Management

An Interview with Jason A. Witty,
Executive Vice-President and Chief Information Security Officer, U.S. Bank

EDITORS' NOTE *Prior to joining U.S. Bank, Jason Witty was the Senior Vice President and Cyberthreat Prevention Services Executive at Bank of America. Before his role at Bank of America, he was the First Vice-President of Security Services for LaSalle Bank N.A. He also led the internal Information Security team at The Options Clearing Corporation and served as Director of Global Security Architecture for Aon Corporation at its world-wide headquarters in Chicago. He has also had hands-on information security experience at Allstate Insurance, N.A.S.A. Langley, Siemens, and Jefferson Laboratories.*

Jason A. Witty

COMPANY BRIEF *Minneapolis-based U.S. Bancorp (usbank.com), with $428 billion in assets as of June 30, 2016, is the parent company of U.S. Bank National Association, the fifth largest commercial bank in the United States. The Company operates 3,122 banking offices in 25 states and 4,923 ATMs and provides a comprehensive line of banking, investment, mortgage, trust, and payment services products to consumers, businesses, and institutions.*

How do you define the role of Chief Information Security Officer (CISO)?

The CISO position used to be IT-focused where we were trying to deploy the latest firewall, get the latest intrusion detection system, or executing other technology-centric strategies. This is still important but, increasingly, it's become a business executive role with a focus on information security risk management, not just on technology. Certainly for U.S. Bancorp, it's a business first management type of role that has a high degree of technology dependence, but it's first and foremost a business role.

There is so much focus today around cyber but much of it is around how to address problems when they occur and mitigating damage. Is there enough focus on prevention?

There needs to be a framework that is comprehensive and that takes into account deterrent, protective, detective, response, and recovery type activities.

There is a lot of focus from the various government agencies on having a good response plan and I feel it's very prudent to assume it's going to be when not if, and to conduct regular exercises. One can look at some of the breaches that happened in 2015/2016 and it was very obvious that some of them hadn't done exercises prior to the event. They didn't know to engage PR before the CEO spoke to someone, or to ensure that their legal counsel or forensic provider was brought in through an external counsel, not directly by the company, so that information would be privileged. This allows the company to handle their risk management process better.

Talking points were created as the event occurred as opposed to having gone through a situational awareness process with the right level of governance people around the table thinking through how they would react, and creating a rational process should an event happen.

Controls need to be there to prevent intrusion. However, there is a very active threat environment that dictates that we can't stop everything, so we have to be prepared in case those controls miss something and to ensure it's not left to fester for too long.

You deal with classified information. How critical is it that the line be more open when it comes to intel sharing and is the proper dialogue taking place to address the critical role that sharing plays?

In 1999, the financial services industry made a decision that we don't compete on safety and soundness, and that threat or attack information needs to be shared between financial institutions. This decision was based on a directive from the Clinton Administration that said that information sharing analysis organizations needed to be created. The FS-ISAC was created in 1999 in response to this and, almost immediately, banks started sharing attack information with each other.

Please note that none of this has anything to do with customer data, customer transactions, or anything else that would impact people's privacy. The sharing is all about malware hashes and URLs and the subjects of phishing e-mails – cyber threat information.

This is now a 17-year-old process for us and it's working very effectively in financial services to the point where, a few years ago, there was so much sharing going on that we had to automate it. It had become too voluminous for an actual human being to deal with.

The industry has moved toward a series of threat automation protocols where computers can tell other computers what the threat looks like. Analysts still need to be involved, but it's come quite a long way since we started this process.

We see many other sectors that don't have this same process. There isn't the same level of collaboration in other areas that one might expect.

How do you come to a common understanding with the board when you are on the tech side of things?

When a CISO is in the boardroom, they have to be talking in plain-English business terms about risk management. Although cybersecurity risk is nuanced, it is really just a subset of broader risk management principles - we can't be using the latest techie jargon to describe the problem.

It's important to outline the risk and the outcome if it's realized, as well as the probability of something happening. Boards are there to fulfill a risk management function, so they understand risk well. To the extent that we can put the issues we face in risk terms and use proper business lingo, it makes for a much easier conversation.

How important has it been for you to have a seat at the table and to develop an understanding that your role is much broader than technology?

Any of the successful CISOs who have been able to create a robust program share a lot of common traits in that while they may still report in to IT, the issue of information security has transcended from just being an IT problem. It is focused on getting all employees to own a little piece of information security and on getting the board educated enough about it to provide the right level of credible challenge. CISOs have to be able to think like a business leader and understand that the entire function of information security exists purely to protect revenue, and boards get that.

The technology is really the how not the what.

Are you able to implement metrics to make sure what you're doing is having the right impact?

Definitely. There are many different philosophies on metrics. We like to have performance indicators and risk indicators. We try to address leading indicators as well as lagging indicators. There are certain things you can't measure until after they have happened, so they are lagging indicators. Other things you can reasonably predict – for example, being able to create a culture that documents risk well allows you to then be able to ask how long the risk has been around and whether it has increased or decreased. If it has increased beyond the tolerance level, the board should be informed. ●