Q&A with Thomas J. Ridge

— by JAMES M. DEITCH —

An interview with former Pennsylvania Governor Tom Ridge that covers cybersecurity threats and how to guard against them.

This interview with Thomas J. Ridge, chief executive officer (CEO) of Ridge Global LLC, Washington, D.C., first secretary of the U.S. Department of Homeland Security and 43rd governor of the Commonwealth of Pennsylvania, took place originally at the Mortgage Bankers Association's (MBA's) technology conference earlier this year. The cybersecurity topics he discusses are even more relevant today as the headlines are filled with news of security breaches and the need for heightened information security.

Q: *You've called cyberattacks a global scourge. Could you share examples of items that are publicly disclosable that are good illustrations of what happens to companies that don't have appropriate security?*

A: Let's take a look at Home Depot, Target and Anthem, and I'll throw in a fourth for another reason. At some of these companies, there was nobody strictly accountable for cybersecurity. Target had three people in charge, which means nobody was in charge. Others had old IT [information technology], and there was public information out there about their vulnerability but they never patched it. A couple of them had internal process failures. They had some capability to identify the malware but it was ignored or lost.

The more important lesson was Sony. That was the second time they had been hit. Hackers went after PlayStation® in 2012 or 2013. You know that lesson—if the horse kicks you once, it's the horse's fault. But if it kicks you a second time, it's your own fault.

Q: *You mentioned Anthem and a fourth example.*

A: The big organizations that have the resources need to have an enterprisewide security strategy, and a lot of them don't. And independent mortgage banks often do not have the resources, I suspect, so let's talk about the big boys first.

"[O]ne of the biggest threats that any enterprise has are the people inside—the employees."

Cybersecurity is not just the CIO's [chief information officer's] problem. HR [Human Resources] must be involved, the fiscal side of the house, IT and operations all must be involved. With our friends at PWC [PricewaterhouseCoopers], we recently did a joint cybersecurity exercise at a very large, publicly traded company, and it was successful—but there were still silos within the organization. They did not have an enterprisewide type of security approach to building a culture of resiliency internally. It was amazing to me that a publicly traded company would be thinking very narrowly.

Sony had silos and everybody was trying to deal with their own IT and security concerns, and obviously not enterprisewide, and the CEO and CTO [chief technology officer] paid for this. Ensuring cybersecurity is more than just ensuring one's job security; it's about brand, reputation, loss of earnings—the whole nine yards.

Q: *The federal government is not immune from the global scourge. There are many examples that show most breaches are not brute-force attacks on the network perimeter. How do bad actors gain entry and, once in, what do they typically do?*

A: There is enough literature out there that one of the biggest threats that any enterprise has are the people inside—the employees. And it is not that they're malicious; sometimes they are

just careless. Sometimes a phishing exercise is very attractive on the Internet, and before you know it, somebody has access to your system. Or there's a candy drop—you might get a thumb drive with a note on it, with something attractive to you, and you plug it into your system . . . or denial of service. The greatest vulnerability is insiders—employees and former employees, vendors and former vendors.

Vendors are a big challenge. How many companies have security protocols or requirements for third parties doing business with them? When they do a risk assessment, do they find out what vendors are doing with their information? Do they limit access to your data and network? Our natural inclination is to trust people. That is a real challenge. But a lot of it has to come down to employee security awareness.

"The digital sun is never going to set—it is only going to get hotter because the complexity and the sophistication of hackers is growing. "

We are becoming more and more dependent on the digital infrastructure, and there is a lot of promise associated with it. The digital sun is never going to set—it is only going to get hotter because the complexity and the sophistication of hackers is growing. The malware changes every single day. And historically, if you were pinging the system, you might be able to match what you discover against millions and millions of pieces of malware and know someone is trying to penetrate your system. But now there are increasingly sophisticated attacks; there may be one code that they may work at for months, if not years, for a particular incursion.

It is important for all of us in business to understand that it is not a technology problem, it is a huge business risk. We cannot eliminate it. But we need to develop an enterprisewide strategy to manage it.

Q: *Mortgage bankers will close $1.5 trillion of consumer mortgages for families in the U.S. this year. If you were a CEO of an entity engaged in lending, what would you be asking of your CIO about security?*

A: First of all, do you have a CIO? Because a lot of enterprises don't. But I like your question because it is assuming the CEO is embracing the responsibility of overseeing the network. I would ask, not necessarily in this order: What are the risks in our sector? What are the risks that you are seeing to our enterprise? And what have you done about it?

I'd ask the CIO: Do you rely only on yourself to assess these risks or do you get another set of eyes to take a look at these risks and get some advice? I'd ask the CIO: Are you making sure that you are developing strategies for security enterprisewide?

We worked with a company that had significant relationships between their operational technology people and their information technology people, and when we recommended they sit down and hold more in-depth meetings to really make sure that their respective areas of the company are integrated in terms of cybersecurity, they asked, "Why would we want to do that?" So, you really want to break down those silos.

I'd say to the CIO: We're probably going to be breached—do you have an incident-response plan? Who do you call to deal with the breach from the technical side? How are we going to deal with regulators? How are we going to deal with the public? Do we have a communications plan? You have to assume there is going to be a breach.

One of the interesting things is taking a look at Target, because they went out and brought somebody in but they never got a handle on how severe the breach had been. It went from 40 million accounts to 60 million, and a couple of weeks later it was 70 million. If they had been able to go out to all their endpoints simultaneously, they would have had the correct information right away.

Their PR response was flawed because they did not have the ability to get a handle on how severe the breach was in the first place. So I think every organization, whether it has a CIO or not, has to anticipate a breach and be prepared to deal with it. They need to have an incident-response plan, and hope they never have to use it. It's like property and casualty insurance plans. You hope you never have to use them, but you have to have them nonetheless.

Q: *We talked about $1.5 trillion in mortgages this year, and each of those mortgage applications has thousands of elements of data—most of them with personally identifiable information that is confidential. Lenders have loan officers in the field with laptops. While loan origination systems [LOS] have good security, what about all of the systems and nodes residing next to SaaS [software as a service] or enterprise LOS systems? What particular risks do you see with this and what should we as an industry be doing to protect both the confidentiality of consumer information and the reputation of companies?*

A: Well, you have a lot of endpoints and you have to make sure that they're secure. You have to make sure that you limit access to your network, and you have to encrypt the information in transit and once it is stationary.

Banks are a target-rich environment. I don't know if the nation states are particularly interested in this information, but organized crime would love to have it. They can create faux people and faux families. Billions and billions of dollars are lost because people get access to this information. It's more than just the credit card information; that's easy. They get into accounts and copy data and create false identities with that information . . . until they get caught, and then they move on. They infiltrate a couple of hundred thousand packages of information about individuals and they use it at their will. We have watches and they have time. It is a real challenge.

It is a huge challenge for financial services companies, and particularly mortgage bankers, given the aggregation of information that they have about people and families. If I were a CEO or CIO, what would keep me up at night is thinking about what happens if somebody exfiltrates the data. What happens if it's done and I find out about it months later because I don't have any monitoring systems? Your worst nightmare is if you get a call from somebody in Europe or Asia or South America, and they let you know that your data was exfiltrated months ago and it's been used all over the marketplace.

Q: *How do these criminal enterprises target a particular company? Could you give us a profile and describe the types of risks that you think are existential that are facing lenders today? Who are these people? Can you name them?*

A: Usually it's organized crime that uses the information. Some of these actors just ping your system on a regular basis to try to get through your perimeter, and if all you have is a perimeter

fence, you're in big trouble. Sometimes they'll try to get inside the system to see if there is any vulnerability they can exploit.

I would argue that the small and medium-sized businesses may be more vulnerable than the large enterprises because of limited resources. They don't have a big IT staff, and they are not spending millions and millions of dollars on cybersecurity.

These hackers will take a look at the market and figure out how much you are spending and they know you have a target-rich environment. They'll take their time and ping the system and try to find vulnerability. They'll try phishing exercises, and if that doesn't work they'll try denial of service and see how quickly you respond. They'll go down that chain and find some way to get into your system. Again, we have watches; they have time.

Q: *How long do some of these threats lurk, such as in the case of Sony and Anthem, before they are discovered? And how much data is exfiltrated before it is known?*

A: I can only tell you what I've read. I've read information that says that some of the breaches have been in the system for six months to a year before they exfiltrate. They are working their way through the system. But we do have diagnostic tools that can help monitor that and tell you how long they've been in your system. The literature says that it is typically many months before they start taking data.

Q: *The MBA has some great economic data about how much it costs to produce a loan and how much those costs have changed in the last three to four years. The numbers seem to indicate that 20 percent to 25 percent of the cost of a loan is now compliance-related, and what you're suggesting is to layer on top of that a different type of cost—the risk management costs of cybersecurity. What is the message that a CIO or CTO takes back to his/her company and CEO? What are the things that need to be communicated to the CEO, the board and the ownership of a company, and how does one go about that?*

A: I know CIOs are reluctant to tell the CEO what to do. One of the recommendations to the CEO is to support your IT staff, give them the cybersecurity tools and resources they need upon request. I think the CIO is always looking for resources, and that is understandable. Small companies have limited resources so the conversation with the CEO has to be around certain basic security capabilities that they need. The CEO has to develop an enterprisewide mindset.

Ultimately the responsibility and leadership of the digital network is not really with the CIO. It is the CEO who needs to understand that it is not a technology program; it is about people, process and technology. The relationship between the CIO and CEO is critical, but the tone is set not by the CIO—it is set by the CEO. And believe it or not, there are some people who throw all that responsibility to the men and women in charge of IT, and it is not fair. It is a shared responsibility and enterprisewide. We call it a culture of digital resiliency. He or she, the CIO, is going to be an agent in that process but it has to come down from the CEO and the board. **MB**

James M. Deitch, CMB, is president and chief executive officer of Teraverde Management Advisors in Lancaster, Pennsylvania. He is a certified public accountant (CPA); has served as chief executive officer of four national banks, including two *de novo* banks; and has served on the Mortgage Bankers Association's (MBA's) Residential Board of Governors (RESBOG) for three terms representing a community bank lender. He can be reached at jdeitch@teraverde.com.