BUFFALO
BUSINESS FIRST

FOCUS: BUSINESS OF LAW: CYBER

HOW I...

Shared my expertise in Albany

DOPKINS & CO. CYBER EXPERT TESTIFIED ABOUT PROPOSED REGULATIONS

It was about eight years ago that businesses began to take notice of cyber security, especially in fields such as health care where clients needed their information protected, said William Prohn. These days, the focus has further increased.

JIM COURTNEY

When the state Assembly's Standing Committee on Banks conducted a hearing on cyber security regulations proposed in New York that will affect the banking and financial service industries and their vendors, Western New York's William Prohn was one of nine individuals to testify. Prohn, director of information technology at Dopkins & Co. LLP, joined the accounting and consulting firm 30 years ago and has gone from being a computer systems specialist to helping to secure IT. He also consults and educates clients on cyber threats. His duties gradually changed to meet client needs.

He was invited by the office of Assemblywoman Crystal Peoples-Stokes to testify Dec. 19 in Albany at a hearing to explore the needs of banks and financial institutions, as well as review state laws and regulations designed to protect against cyber threats. The legislation, which is intended to protect consumers, requires that banks examine their cyber risk and put in controls that correspond to that risk.

WILLIAM PROHN

Company: Dopkins & Co. LLP

Joined firm in: 1997

Residence: Tonawanda

Certifications: Risk and Information Systems Control (CRISC); Governance of Enterprise Information Technology (CGEIT); Information Systems Security Professional (CISSP); Information Systems Auditor (CISA)

Teaches: Accounting and information systems courses at Canisius College and University of Rochester

I was on a panel about cyber security and Assembly Member Crystal Peoples-Stokes was in the audience when somebody asked a question about legislation. Some of the other panelists said this is going to make it a lot easier and I argued that it is going to make it a lot harder. Unless there is some basic legislation that applies to everyone, how do I know what I'm supposed to do? It breeds confusion. She came up to me afterward and told me that the concept struck her. I met her staff and talked to them about cyber security. She chairs the Assembly's Standing Committee on Operations so the cyber security of state agencies falls under her. When this hearing came up, her office wanted to see someone from Western New York there and thought my take on it as a broader approach to security than just legislation would be interesting.

My argument to the committee was that there should be a universal base set of rules that everyone – individuals, nonprofits, hospitals and banks, for instance – has to adhere to. And if there is something that a bank needs to do more than that, then legislate that part. It might be different then what a hospital has to do but at least we are all doing the basics.

My complaint is that this only applies to banks. I got some pushback from a senator-elect who is on the committee. He said, "Do you think we're going to legislate everybody?" I said, "Well, you legislate traffic laws for everybody." The argument made by mortgage bankers was that they were too small so how can they do this? My argument to that was, "Maybe you don't need to do all of this but you should be subject to the same basic security that everyone else is."And I think that's where this law goes awry. Another complaint is that they'll have to spend money to comply with this in New York, but in a state like Pennsylvania you don't have to spend the money to comply. My response was: "but you're safer and you can sell your safety and demand a premium for that."

The committee was mostly concerned with protecting the consumer, even though the consumer may not know they need protecting or even want protecting. They were concerned on a much broader scale about how cyber banking affects the consumer. For example, if I'm a senior citizen in an apartment, do I know that I don't have to go out in the winter to cash my check (and instead can bank online)? Some of the questions asked of some of the banks were: What are you doing to educate the consumer about the availability of this stuff? In a roundabout way, it's worthwhile because if more people are aware of it and know the security risks, they'll pay more attention to it.

When I talk to clients and prospects about cyber security, everybody knows what it is and is worried about it but they think it doesn't apply to them. They think the Russians aren't after them so why worry? What people are surprised to find out is that the overwhelming majority of problems are actually mistakes perpetrated by employees who don't know what they're supposed to be doing.

There is so much that a business can do but isn't quite implemented, but once there is an awareness, they can go forward from there. After we meet with clients, they come away with the feeling that it's not as painful and complicated and they can make progress. They see value in it.

– Michael Petro