Long Island BusinessNEWS
JANUARY 20-26, 2017 | VOL. 64 | NO. 3 | $2.00 | LIBN.COM

EXECUTIVEPROFILE

THE CYBER DEFENDER

As the chair of Uniondale-based Ruskin Moscou Faltischek's two-year-old cybersecurity and data privacy practice group, John Cooney says cyber-attack prevention is now the normal course of business for organizations large and small.

Photo by Judy Walker

How did this practice group start? We had been doing a lot of this work with the health law group because of HIPAA and the breaches that started. We saw breaches happen across all industries – including those at Target and Home Depot. Everyone was at risk – all the state and federal agencies [began] promulgating law much the way HIPAA did. We needed to have a group of dedicated attorneys that could provide the same services, compliance, regulatory response and breach investigations across all industries.

What did you determine? We found regulations, law and preventative measures are very similar across the industries. The difference is on what data has to be protected. In healthcare, it's PHI, Personal Health Information, and now across other industries it's PII, Personal Identifiable Information. So for instance, with credit cards, [it's a person's name, address, CVV code]. All this information is at risk regardless of what industry you're in.

What's happening now? There's a big push in financial services by the New York Department of Financial Services for new regulations to protect consumers, coming under a lot of regulations. Consumers are a big target of criminals and hackers – it's a treasure trove of information.

Are some industries more vulnerable than others? I have clients across all industries. I haven't seen an industry that is safe. Everyone is at risk to some extent. It doesn't matter if it's criminals or other individuals who take information for profit. They don't care about the size of the company. They care about how fast they can access the information in order to steal or profit from it in some way. Thousands of small to mid-size companies were part of a concerted attack in New York and Long Island from overseas in the last year. Instead of [targeting] one company, they got 100,000 records. It's still being pursued by authorities.

What about risks for individuals? [Even on a] home computer, privacy right now and where information is stored now has to become part of everyone's daily concern and review. [If you have a] new service at a company or at home, you have to review that software agreement…you really have to look and see how the information is being used.…

What should organizations do? A company needs to assess and deal with cyber risk the same way they deal with other risks. Now, it's the cost of doing business. The major banks and retailers are pushing back on small partners and vendors to have procedures and protections in place, or those companies will not do business with them, whether it's a vendor or partner, you have to prove you're on top of cyber risks and have protections in place. Otherwise doing business with you is too risky.

What can small and mid-size businesses expect from larger clients? If you have an existing relationship with a larger company, it's the new requirement of business going forward. Or if it's a new relationship in contract…major companies will bring it to the forefront [to determine] if they can do business. Medium to small businesses should be requiring the same from their vendors, from their smaller partners, anywhere that information is exchanged.

Are organizations in denial that their companies are vulnerable? There has been a lot more awareness in last six to nine months to get ahead of these issues. There was a lot denial two years ago. Companies have moved towards a posture to help deal with this.

What are the new challenges for small businesses? A lot of tech companies are professing to install this software and everything will be all right. But you have to make sure solutions can deliver and mitigate your legal liability. We caution companies that a software solution is one piece of the puzzle. A piece of software might only be mitigating 10 percent of the risk on the tech side and the legal side. There's no silver bullet and then your company is protected. You need a formal risk assessment of your vulnerabilities and then work towards remediating [any risks] and deal with issues on an ongoing basis.

What else should companies do? They should review contractual obligations…. It's all encompassing for a business and not an easy subject. It's difficult to find people from a legal perspective who can help protect a business. It's called an integrated solution, with a technical and legal and internal team working together on these things, not piecemeal. [Otherwise, it's] disjointed, inefficient and very costly.

How do cyberattacks impact business? There are immediate risks. While a company has to deal with keeping a business running [they also must] fix systems, and protect from future litigation. After a company reports a breach, class action law suits by affected individuals [could be filed] a day or two later… [claiming] you did wrong to expose their information. We come in as attorneys with a technology team to shield any findings of a company's negligence or lack of security controls that can be used in a future claim or action against the company.

Do small businesses that don't have an IT budget have their own particular set of vulnerabilities? There are a number of different firms that you can outsource to. There are cloud service provider companies that specialize in managed services, and provide that to you to manage offsite, [with] network upgrades, software patches, and take responsibility for it…. Make sure it's a reputable business, and have contractual protections.

Are companies attacked without realizing it? Yes. An attack [could have] gone on for months without detection. Usually that's traceable to a company not monitoring its systems or a lack of controls where they would have noticed it much sooner… A lot of the attacks come from internally – an internal employee downloading records or selling it to somebody. Controls have to be in place, and implemented properly. If they had looked in the right place or had the right controls, they would have seen it much sooner.

Is the threat likely to change? Overall, the threat will only continue to increase – there's too much money to be made by individuals attacking the companies. It does change literally on a three-month basis – a new attack or method becomes more prevalent than another. We saw a number of attacks called 'business email compromise attacks,' with the hacker pretending to be company executives or vendors trying to get money transferred to a new bank account. Eighteen months ago it was unheard of, six months later it's prevalent.

Is there enough talent to meet demand? Right now there is not enough talent to meet the demand. I know some of universities and colleges on Long Island that are starting up programs to develop young people's skills. From a legal standpoint, law schools are starting to recognize this growing field. Not many schools offer this concentration. I think that will change very quickly.

– ADINA GENN