Ruskin Moscou Faltischek P.C.: Providing an integrated suite of cybersecurity services

After accumulating a great deal of experience dealing with HIPPA breaches in the health care industry, attorneys from Ruskin Moscou Faltischek P.C. recently found themselves assisting clients in other industries with internal and external breaches of protected information. In fact, as breaches and cyberattacks became more common and costly, touching every industry, the firm decided to create a multi-disciplinary team to better serve its clients' needs.

In January, Ruskin Moscou Faltischek started a dedicated Cybersecurity and Data Privacy Practice group, comprised of eight attorneys with extensive experience in cyber and privacy law and diverse concentrations in areas of law such as corporate, health, financial services, intellectual property, litigation, and white-collar crime and investigations.

"We felt this was necessary given the accelerated pace of federal and state regulatory actions, investigations, fines and penalties across every industry—financial services, retail, health care, government contractors," said John Cooney, head of the firm's Cybersecurity practice. "There is no federal data security standard. Different states have different rules; it is very confusing and a huge burden on businesses." For example, many executives are unaware that regardless of where their business is physically or operationally, if the business stores the personal information of any Massachusetts resident, the company is subject to the Massachusetts data privacy law, he said.

Ruskin Moscou Faltischek provides its clients with an integrated suite of services from start to finish, including compliance and prevention, breach investigations and responses, as well as regulatory and litigation defense work. "I don't believe any other firm has a model like the one that we have developed," Cooney said. "Whether it is compliance or in response to a breach, we have a group of trusted technology partners and other professionals who we bring together to analyze cybersecurity matters and mitigate an organization's exposure to the greatest extent possible." By hiring the data security and forensic professionals directly, Ruskin Moscou Faltischek can mitigate an organization's exposure, including future litigation and enforcement actions, by shielding the findings and work under the attorney-client privilege and work-production doctrine. This is especially important given the increased litigation associated with data breaches. For instance, 12 hours after a breach that affected 80 million customers in February 2015, Anthem Inc. found itself the target of a class action suit alleging breach of contract and negligence.

While litigation experience is important, attorneys with a great deal of technology knowledge are essential in this area of the law, as well. Before he became a lawyer, Cooney was a software engineer on Wall Street and at Fortune 500 companies. His fluency in tech matters is critical when speaking with businesses and the firm's departments and clients.

When a cyberattack happens, a business needs a robust team comprised of the most tech-savvy individuals who understand what needs to be done and can translate it, Cooney said. Recently, a large Long Island-based company contacted the firm as the victim of wire fraud. A hacker hacked into one of its vendor's email accounts and sent a message with new bank account instructions for wiring funds. "Based on the hacker's emails, it wasn't clear if our client or the vendor had been hacked," he said. After conducting a forensic investigation, Ruskin Moscou Faltischek attorneys were able to determine the hacker did not penetrate their client's systems, which enabled it to file a criminal complaint as a precursor to recover funds from two international banks. "Time was of the essence," Cooney said, noting the investigation had to move quickly. "Once funds are wired, they can disappear very quickly. Because we moved quickly, we were able to recover the bulk of the wired funds."

Members of the firm's Cybersecurity Practice Group from left to right partner Douglas M. Nadjari, Esq.,chair John J. Cooney, Esq. and Andrew T. Garbarino, Esq.

The wire fraud case highlights the importance for organizations to not only safeguard their own information, but to vet business partners and vendors they do business with, as well. "It's a chain," Cooney said. "We've already seen agency enforcement actions against companies for not taking responsibility for their vendor's data security standards."

The New York Department of Financial Services recently issued guidance that it would be conducting cybersecurity preparedness assessments of third-party vendors of banks, including law firms and accounting firms. "This is going to become the new normal," Cooney said. "The government, as well as businesses, want to be assured before doing business with you that your organization has a plan and technology in place to prevent [cyberattacks] from occurring. This will affect everyone—all businesses in all industries."

Board of directors and executives are not immune from responsibility either. They are facing increased scrutiny and liability from the courts and the government, Cooney said. "They can't say, 'I left that up to my IT department so I can't be held accountable.'" Rather, board members and executives have a responsibility to understand the threats their organization faces, he said. "It's important executives get up to speed in this area. They can be held accountable for breach of fiduciary duty or gross mismanagement."

John J. Cooney, Esq. (L), chair of the firm's Cybersecurity Practice Group and founding partner Melvyn B. Ruskin, Esq. (R)

One of the biggest challenges with clients, Cooney said, is demystifying the belief that they have to scrap their entire technology infrastructure and spend thousands, even millions, of dollars on new technology.

The first step is identifying an organization's current strengths and weaknesses, he said. While one company may need additional software, another may already have state-of-the-art technology but lack employee training. "You have to figure out what the current standards are in the context of your industry," Cooney said. "What will mitigate your liability?"

In January, New York State Attorney General Eric Schneiderman proposed legislation that will broaden the type of information that has to be protected. The legislation will offer a safe harbor for organizations that meet the highest safeguarding standards, Cooney said. Companies need to understand what they're investing in, he said. "This is a great example of the point that a business needs to invest in the tools, technology or processes that will mitigate liability and, in this case, result in protection for your organization from the state."

Ruskin Moscou Faltischek encourages all organizations to conduct a vulnerability assessment, which involves looking at strengths and weaknesses, from a technology standpoint, as well as physical and administrative safeguards. Although recent headlines about major breaches concentrate on external cyberattacks, more than 50 percent of breaches are the result of employee negligence or theft of computer files and paper records, Cooney said.

The firm generally implements a Written Information Security Program (WISP) for its clients to implement policies and procedures to limit threats. "We've seen agencies bring enforcement actions and private litigation against an organization because it had no password security policy or out-of-date antivirus software," he said. "These are easy things an organization can do."

The government requires reasonable and appropriate security measures, Cooney said, noting companies need to have technological, administrative and physical safeguards in place. "If they can start working toward these safeguards, and make it part of their culture, it will prevent many of the breaches today and assure business partners that it is serious about safeguarding protected information," he said.

"We are a globally connected world," Cooney said. "Everyone is connected to the internet." And, thus, everyone is vulnerable to a cyberattack or data breach of some kind.