ROCHESTER BUSINESS JOURNAL
RBJ
VOLUME 31, NUMBER 43 WWW.RBJDAILY.COM JANUARY 22, 2016

Enact security policy to avoid legal woes after a breach

Complicated rules and regulations currently vary from state to state

by LISA MARIA RICKMAN

Photo by Kimberly McKinzie

"Regardless of whether you think you're a target, it's important and it makes good business sense to deal with these issues upfront," said Paul Greene, head of the privacy and data security group at Harter Secrest and Emery LLP.

Addressing company cybersecurity calls for more than just better passwords and education. Legal concerns also come with data security, especially when that security fails.

One of the difficulties companies face right now is the patchwork of federal and state legal and regulatory schemes that control the kinds of information that companies collect. Forty-seven state schemes regulate data breach response, some of which have substantive requirements for security. Some states require encryption of personally identifiable information, but some don't, emphasizing the need for companies to look at the specific requirements for the states in which they do business.

"For example, if you accept credit cards, there's a separate security standard to live up to," says Paul Greene, head of the privacy and data security group at Harter Secrest and Emery LLP. "There's really a wide array of legal and other risks that companies have in relation to protected information."

New York does not hold companies to the same level as Massachusetts, which has a set of requirements for both the technical and physical protection of information. Kate Martinez, an associate on Nixon Peabody's privacy and data protection team, says there is a proposal in New York to have very similar types of requirements on both data security and cyber protection. The New York Department of Financial Services recently proposed these cyber requirements to the financial sector; though it is not the law as of yet, the proposal opens up the discussion.

"So, if a company doing business in New York or anywhere else suffers a breach, there is quite an investigation that needs to be done on top of seeing what has happened, to see who has been impacted, because that will really determine the obligations of any company that has suffered a security incident," says Martinez. "And, on top of civil liability, the state's attorneys now from across the country have taken a keen eye in understanding how data breaches impact consumers, so the company may have to look at not only potential civil liability but also enforcement and penalties."

With the laws evolving seemingly daily, it can be a challenge to keep up with the expanding data security rules. Things like biometric data and website login information are protected in some states but not in others.

"The move is toward more protection under the state laws, rather than less," says Greene. "With 47 different states out there, you can imagine there's a great potential for change."

While many may look to protect only company and credit card information, the latest danger is with health care information.

"A couple of years ago, credit card data was a big thing," says Charlie Wood, executive vice president of the Enterprise Risk Management Division at the Bonadio Group. "You can actually look online to see … what credit cards are being sold for on the black market. Now, they have been so inundated, it is a simple issue of supply and demand."

Wood says most of the attacks he has seen in the past year are targeting health care information, a much greater gold mine of personal information than a credit card.

"In a health care record, you are getting names, Social Security numbers, dates of birth, addresses. Everything you need to steal somebody's identity," says Wood. "Last year, statistically, was one of the worst leaked years of all time—112 million health care records were breached and that accounts for just under, I think, 35

Reprinted with permission of the Rochester Business Journal.

percent of the U.S. population."

In relation to health care information, health care providers, self-funded group health plans or even health care savings accounts are entities that may be covered under HIPAA, the set of federal rules governing protected health information. Recently HIPAA has been expanded to push liability down to nearly anyone who's handling the protected health information.

"They're called business associates. If you have companies that process this information for you, HIPAA now imposes certain obligations on those business associates," says Greene. "The move is toward more protection and more regulation."

So what can businesses do to protect themselves? It is important for a business of any size to consider having a written information security protocol to protect itself from litigation when something does happen, because every company is at risk.

"Regardless of whether you think you're a target, it's important and it makes good business sense to deal with these issues upfront," Greene says. "In relation to protection, it's important for a business to have all the relevant policies in place. For example, an information technology usage policy, that's key. A security policy for your network, that's key. That helps protect you.

"One of the best things to have in place is a written data breach response plan, and that helps you set out in advance what the responsibilities are, if and when you find a problem, how to react to it. It helps you manage the risk and avoid some of the confusion that happens when a breach occurs."

Experts agree that making data security part of everyday operations is the best way for a company to protect itself from breach and the legal risks associated. When it comes to cybersecurity as a necessity, Greene draws an analogy to pre-Sept. 11 disaster recovery plans.

"Before 9/11, disaster recovery was out there, but it was really something for the bigger companies, really something for the critical infrastructure industries; now any business worth its salt makes disaster recovery part of its planning because it's just another reality that's out there," Greene says. "Data security may be scary and a big unknown for companies who are just starting to think about it, but just like disaster recovery, it's something that can be tamed, can be overcome and dealt with through dealing with the right professionals."

Lisa Maria Rickman is a Rochester-area freelancer.

Reprinted with permission of the Rochester Business Journal.