RBJ RBJ.NET ROCHESTER BUSINESS JOURNAL
VOLUME 37 NUMBER 17 Part of the BridgeTower Media network SEPTEMBER 24, 2021

Cybersecurity: It's not just your business you're protecting

Protecting against cybercrime for law firms and other legal organizations is particularly acute because it is not just legal professionals' data and confidential information at stake, says Cheryl Nelan, the owner and president of CMIT Solutions of Monroe."One of the first things we say to law firms is it's not just your business, it's other people's businesses on the line," Nelan says.


Cheryl Nelan

Nelan notes that if law firms fail an information technology audit then their more sophisticated, larger clients will take their business elsewhere.

"It means business to law firms to make sure they are protecting data," Nelan says.

Sitima Fowler, co-founder and vice president of marketing for Iconic IT, says that law firms are increasingly being targeted by cybercrime.

"In May 2020, it was reported that targeted cyberattacks were rapidly becoming a security nightmare for many law firms of all sizes," according to a chapter Fowler recently authored for the publication, "Outsourcing of Core Legal Service Functions: How to Capitalize on Opportunities for Law Firms." "In the span of five months, seven legal practices were victims of ransomware. All these attacks were carried out by two highly organized cybercriminal groups, one known as REvil and the other calling itself Maze."

Anna Mercardo Clark, a partner at Phillips Lytle and leader of the firm's data security and privacy team, says that the 2020 Legal Technology Survey Report from the American Bar Association reported that the number of law firms reporting a security breach increased from 26 percent in 2019 to 29 percent in 2020.

Fowler notes that cybercriminals don't even need to develop their own hacking technology and can buy it. "There is an entire industry focused on supplying cybercriminals with the tools they need to build their own malware," Fowler wrote in "Outsourcing of Core Legal Service Functions: How to Capitalize on Opportunities for Law Firms."

"Called Malware as a Service (MaaS) or sometimes Cybercrime as a Service (CaaS), this software and hardware is leased to individuals for the sole purpose of carrying out cyberattacks. As unbelievable as it sounds, MaaS websites offer full services; a botnet to distribute the malware, a personal account used to launch the attack, and even technical support come with these malware packages. MaaS suppliers organize their services like a typical business model, working nine to five when employees are most typically at their desks and networks are the most vulnerable."

Nelan says that even if businesses do not have data that can be sold on the Internet's black market for money that they can face having their data ransomed and having their business crippled.

"A lot of folks think I'm just a small business, 'Who is going to care about me?'" Nelan says. "'My employees, they're never going to click things.' It's large businesses. It's small businesses. Everyone is at risk of being hacked."

Clark, who has achieved multiple certifications from the International Association of Privacy Professionals, says that cybersecurity is one of the professional responsibilities that lawyers have to their clients.

For every business, "you want to maintain your data securely because you have a responsibility to your clients and your customers and you have concerns that a breach might affect your reputation and your sales and perhaps even your stock price," Clark says. "With law firms we share a lot of the same concerns, but there are additional layers on top of those other concerns."

Clark says that at least 39 states have adopted some version of an American Bar Association Model Rule of Professional Conduct suggesting that part of a lawyer's professional duty of competence is keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

New York's specific rule of professional conduct requiring competent representation of clients requires that lawyers "keep abreast of the benefits and risk associated with technology the lawyer uses to provide services to clients and or to store or transmit confidential information."

Clark notes that cybersecurity for legal organizations also requires that it is a lawyer's professional duty to keep clients' information confidential and to supervise non-lawyer vendors that assist the lawyer in rendering legal services to clients.


Sitima Fowler, VP of Marketing, Iconic IT

Law firms also have to protect confidential information of parties that are not their clients because of discovery obtained during the course of litigation, Clark says.

Clark also notes that companies in New York state must abide by the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which imposed more data security requirements.

"It's putting basic security in place to protect your data to make sure you're not breached," Nelan says. "There's several things to that."

Nelan says that law firms also need to make sure they are meeting the level of security required for their clients based upon their industry. For example, health care clients need to abide by Health Insurance Portability and Accountability Act (HIPAA), or finance clients need to abide by Financial Industry Regulatory Authority (FNRA) standards.

So how do law firms protect their clients' data and their own data from cyberattacks?

Clark, Fowler and Nelan all say security training for employees is imperative, including how to avoid phishing and other dangers.


Anna Mercardo Clark

All three also say that multifactor authentication for logging into firms' computer systems is essential.

Nelan says that law firms need to have a strong plan for backing up their data. Sometimes clients think they know where all of their critical data is backed up but, say, their accounting data is on Quickbooks and backed up somewhere else, Nelan says.

Part of cybersecurity is ensuring critical data is backed up and knowing exactly where it is located and knowing how long it will take to recover that data, Nelan says.

The rise of employees working from home has also raised cybersecurity implications for law firms, local experts say.

Fowler says that one important step is to ensure that any hardware that is taken to the home or courtroom needs to be encrypted so that if it gets stolen or lost the data on that device won't be compromised.

Fowler also says that good security measures for employees working from home include having personal firewalls set up, having employees access their office computers through a virtual personal network or using a secure cloud computing system like Microsoft 365.

Clark, Fowler and Nelan all recommend law firms obtain cybersecurity insurance, but they all note that the market for obtaining insurance has become more difficult due to the rise in frequency of the attacks.

Fowler recalls that insurance companies were once almost giving cybersecurity insurance policies away for free because of the lack of interest from companies.

Now, it has changed 180 degrees due to the rise of ransomware and other cyberattacks, she says.

"Insurance companies are also paying closer attention to these ransomware attacks," Clark says. "This kind of insurance space is relatively young in comparison to other general commercial coverage, and I think it'll be interesting to see how the products and pricing develop in the coming months."

Amaris Elliott-Engel is a Rochester-area freelance writer..