ROCHESTER BUSINESS JOURNAL
RBJ
VOLUME 35, NUMBER 30 WWW.RBJ.NET OCTOBER 25, 2019

Corporate spending on cybersecurity continues to increase

By ANDREA DECKERT

Companies will continue to spend more money on cybersecurity measures, industry data shows.

Worldwide spending on information security products and services exceeded $114 billion in 2018, an increase of 12.4 percent from 2017, according to Gartner Inc., a global research and advisory firm. For 2019, they forecast the market to grow to $124 billion, and $170.4 billion in 2022.

In the 2019 Global Cyber Risk Perception Survey, 79 percent of respondents ranked cyber risk as a top five concern for their organization, up from 62 percent in 2017. The survey was conducted in partnership with Microsoft Corp. and Marsh, a global professional services firm.

There are a number of ways companies can use their cybersecurity budgets to keep hackers at bay, local experts say.

Those well versed in the cybersecurity arena agree employee training is key.

"If employees know what to look for, they can think twice before they click," says Paul Greene, a partner with Harter Secrest & Emery LLP, adding that companies must be vigilant when it comes to cybersecurity. "Attackers are organized, well-funded and motivated."

Greene chairs the firm's Privacy and Data Security practice group. In his role, Greene advises clients on aspects of pre-breach preparation and risk management.

Jenny Holmes, an associate at Nixon Peabody LLP, also stresses the importance of employee training, adding people on the job are often the best defense against a cybersecurity attack.

"It's really a cost-effective way to combat against data breaches," she says.

Holmes is a member of the firm's Privacy & Data Protection team, developing and implementing systemwide privacy and security plans for numerous companies of various sizes, including the creation of response plans.

Breaches can be extremely costly for companies, Holmes notes, from customer notifications to credit reporting, so having policies in place can help reduce, or eliminate, those costs.

Both Holmes and Greene say now is an ideal time to review a company's policies and procedures related to cybersecurity since New York will be implementing the Stop Hacks and Improve Electronic Data Security Act in March.

The SHIELD Act requires companies to have comprehensive programming enacted to prevent breaches, have training programs in place and regularly monitor their controls for effectiveness.

Now is the time when companies can see where their information security programs stand and in what areas they can invest to make improvements, while complying with the SHIELD Act, the local attorneys say.

While it takes time and effort to help make a business cybersafe, Greene says companies are doing the legwork.

"Companies are paying more attention," he says.

Many businesses contract with outside firms that specialize in information technology management and cybersecurity in an effort to keep on top of technological advances in the fight against cybercrime and make sure they are protected.

Sitima Fowler, co-CEO of Capstone IT, says it is essential to have policies in place, as well as systems up and running, that can help prevent attacks.

It is also important for businesses to conduct drills on their systems regularly to see where they are still most vulnerable and make adjustments accordingly.

With changing technologies and more sophisticated hackers, businesses must stay on top of their cybersecurity health, Fowler says.

"A lot of times businesses don't think about it until it happens, and then it's too late," she says.

Andrea Deckert is a Rochester-area freelance writer.