RBJ RBJ.NET ROCHESTER BUSINESS JOURNAL
RBJ GUIDE TO WEALTH MANAGEMENT | Part of the BridgeTower Media network | JULY 5, 2024

It can happen to you: Experts weigh in on cybersecurity, cybercrime

By ANDREA DECKERT

Reg Harnish believes that small businesses have unique challenges when it comes to cybersecurity.

That's because most cybersecurity efforts are focused on mid-size or large organizations, explained Harnish, CEO of OrbitalFire, adding that in the Rochester region, nearly all of the businesses are micro- or small-sized operations.


Harnish

Since the focus is not on the smaller firms — and they are just as likely to experience a cyberbreach as any other sized firm — they often must divert their attention from the day-to-day operations of the business to focus on cybersecurity matters, from cyber insurance applications and customer expectations to federal and state regulations and cyber-crime.

"Cybercrime is 1,000 percent getting in the way of business," he said, adding that cybersecurity will also continue to be an increasing requirement for small businesses.

Harnish offered some strategies for small business to use when it comes to cybersecurity. They included holding someone at the organization accountable, making an inventory of a company's assets, focusing on defensibility and resilience and finding a provider that can help.

Such steps can have a major impact on a firm.

"Your commitment and ability to show accountability demonstrates continuous improvement," he said.

Harnish noted that it's hard for small business to tackle cybersecurity on their own, especially since it's a moving target, and added that cybersecurity is not an IT function.

"Most cybersecurity has nothing to do with IT," he said.

Harnish made his comments at last week's cybersecurity virtual panel discussion presented by the RBJ and Daily Record.

He was part of a panel of local experts who discussed the latest cybersecurity trends to make sure you and your company are as protected as possible.

The Virtual Panel Discussion was sponsored by Harter Secrest and Emery LLP, Just Solutions, OrbitalFire and Phillips Lytle LLP.


Greene


Staszkiw


Wolf

The other panelists were:

- F. Paul Greene, partner, Harter Secrest and Emery LLP
- Michael R. Staszkiw, senior associate, Phillips Lytle LLP, and
- David Wolf, vice president, Just Solutions

Greene spoke about the National Institute of Standards & Technology's Cybersecurity Framework, which puts forth a set of recommendations and standards that enable organizations to be better prepared in identifying and detecting cyber-attacks.

It also provides guidelines on how to identify, protect, detect, respond, recover and govern when it comes to cyber incidents.

The framework helps companies "get their house in order and protect their data," he said, adding that staying on top of security and privacy matters can make a business more competitive.

Companies should adopt a teamwork approach when it comes to cybersecurity efforts, led by management, legal and technical personnel, Greene said.

The top complaint regulators have when a breach occurs is a lack of governance, which includes areas such as risk management and oversight.

Green noted that cybersecurity is another area business leaders must be responsible for and can be approached similarly to other areas of the business.

"You know how to govern already, just apply those same skills in the cyber realm," Greene said. "Slowing down, and slimming down, when it comes to data will help you in your governance efforts."

Wolf spoke about the regulations, frameworks and compliance around cybersecurity.

He recommended business leaders work with someone in the cybersecurity field to determine what regulations apply to their businesses and make sure they are compliant with those regulations.

They should next choose a corresponding security framework, which is a collection of well-documented standards, policies, procedures and best practices intended to strengthen an organization's security posture and reduce risk.

Following the above steps, Wolf said, can determine if a business survives or it doesn't.

"Don't be fooled," Wolf said. "It can happen to you."

He also noted seven ways to improve a company's security posture, including security awareness training and multifactor authentication.

Wolf said it's essential for businesses to incorporate all seven steps.

"If not, you really are at risk," he said.

Staszkiw, who works with clients on data and privacy issues, spoke about the rising incidents of tracking technology litigation, which centers on web tools - like pixel systems, chatbots and session replay software - which are used by company websites to collect and analyze user activity.

In technology tracking litigation, plaintiffs have alleged that personal data was collected, shared with third parties and monetized for targeted advertising, allegedly all without user consent, he explained.

When it comes to questions related to cybersecurity litigation, Staszkiw said businesses should consider consulting with an attorney who can help them navigate the cybersecurity legal landscape.

"Being aware of these types of lawsuits is key and will help you along the way," he said.

adeckert@bridgetowermedia.com / (585) 653-4021