ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
JUNE 30, 2025

Cybersecurity experts share practical advice for small businesses

■ ANDREA DECKERT

The rise of the internet has unlocked significant growth opportunities for small businesses, but it has also created new vulnerabilities, according to a local cybersecurity expert.

"There are a lot of advantages but there's also a lot of risk," said Reg Harnish, CEO of OrbitalFire. "Connectedness is a vulnerability."


Reg Harnish

Harnish was one of the local experts who participated in the recent RBJ/Daily Record's cybersecurity virtual panel discussion, which focused on the latest cybersecurity trends to make sure one's business is as protected as possible.

The virtual panel discussion was sponsored by OrbitalFire, Phillips Lytle LLP and Just Solutions.

Other participants were Paula Plaza, an attorney with Phillips Lytle, who focuses her practice on antitrust litigation and data security and David Wolf, vice president of Just Solutions.

Harnish, whose firm has seen a dramatic increase in the number of small businesses affected by cyberattacks, offered modern tips for small businesses and gave five reasons businesses should invest in cybersecurity.


Paula Plaza

They include being compliant with regulatory requirements, protecting their money and intellectual property, for insurability and reputation.

Harnish said staying on top of cybersecurity efforts can help businesses create a competitive advantage.

He advises businesses to take some basic, necessary steps when it comes to cybersecurity, focusing on managing risk without jeopardizing one's business mission.

Businesses should understand their obligations, including those to their customers who likely have cybersecurity language built into their contracts, he explained.

Companies should also be prepared to respond to a cyberattack, which could include financial fraud or a business email compromise.

Cybersecurity extends beyond one's information technology department, he noted, adding it includes a range of departments,

from human resources and legal to finance and crisis communications.

Harnish also advises a business make someone the point person who is accountable for cybersecurity measures at the firm. An ideal candidate would be someone who understands the business and is good at getting things done.

"Accountability is everything in cybersecurity," he said.

Plaza spoke about cybersecurity laws and enforcement actions companies should be aware of, as well as compliance strategies.

She noted there are various regulations around cybersecurity for businesses, and civil penalties – sometimes hefty ones – may be imposed if firms are not in compliance.

Plaza advises that businesses use care when dealing with data and information, such as when it comes to customers, and take extra precautions.

She noted that regulators look at a range of factors when assessing compliance, including a company's size, number of employees and the amount of data it handles.

"It's often done on a case-by-case basis," she said.

Plaza also recommends businesses put one person in charge of cybersecurity efforts who oversees companywide policies and procedures, as well as retaining and developing relationships with cybersecurity experts.

She suggests companies undergo a cybersecurity simulation to assess their preparedness and determine areas where they can improve.

Additionally, Plaza said companies should not overlook third parties and can mitigate risk through written contracts, insurance and periodic risk assessments.

Wolf spoke about how businesses can use Artificial Intelligence safely and to their advantage.


David Wolf

Wolf noted that AI tools such as ChatGPT, co-pilot and Gemini are powerful tools and must be used responsibly, suggesting companies view each AI interaction like posting on a public website.

Having proper policies and procedures for AI is key, he added.

To help reduce a traceable data footprint while using AI tools, he said companies may want to turn off chat storage/history when possible and use private modes if available.

Wolf also recommends firms choose business versions, when possible, which include enterprise tools that offer enhanced privacy tools and prevents a company's data from being used to train AI models.

Companies should also avoid entering personal or client data when using AI tools.

While it is important to apply safety protocols, Wolf said companies should not shy away from incorporating AI tools into their operations, noting it can help companies be more productive and competitive.

"AI isn't going away, and companies need to know how to drive it and how regulate it," he said.