

Cybersecurity requires strategy, culture and vigilance, local experts advise

■ ANDREA DECKERT

For many small and mid-sized businesses, cybersecurity challenges stem less from indifference and more from uncertainty about where to begin.

“Small businesses aren’t really ignoring cybersecurity,” said Chris Sirianni, president and founder of IT Insights. “Many are really just overwhelmed and don’t know what to do next.”

Sirianni’s remarks came during a June 25 cybersecurity virtual panel hosted by the Rochester Business Journal and The Daily Record and sponsored by Brite, IT Insights, OrbitalFire Cybersecurity and Phillips Lytle LLP.

Joining Sirianni on the panel were Anna Mercado Clark, partner at Phillips Lytle LLP; Reg Harnish, CEO of OrbitalFire Cybersecurity, and Trevor Smith, president of Brite, who all discussed the latest cybersecurity trends and practical steps businesses can take to better protect themselves.

Sirianni outlined several foundational cybersecurity measures for smaller companies, including implementing multifactor authentication, using password managers, providing security awareness training and partnering with managed service providers.

He also encouraged businesses to adopt managed detection and response platforms and evaluate compliance requirements.

Most importantly, he said, cybersecurity should be woven into an organization’s culture rather than treated as a set of isolated rules.

“Don’t think of cybersecurity as just a bunch of rules and policies that exist,” Sirianni said. “Really build it into your culture.”



Chris Sirianni



Trevor Smith



Reg Harnish



Anna Mercado Clark

Artificial intelligence was another central topic of the discussion.

“There’s no question that AI has significantly impacted the cybersecurity landscape,” Smith said, noting that cybercriminals are increasingly using AI to make attacks more sophisticated and difficult to detect.

As businesses adopt AI technologies, Smith recommended creating a secure AI strategy that begins with understanding what data an organization possesses and who has access to it. Organizations should also establish policies governing AI usage, implement oversight and governance structures, and consider the financial implications of AI investments.

“Apply AI where it drives measurable outcomes and tangible business value,” Smith said.

Harnish challenged the notion that cybersecurity is inherently expensive and overly complex, arguing that a well-executed security program can deliver meaningful returns on investment.

Among the potential benefits, he cited competitive advantages, lower operating costs, streamlined business development processes, improved reputations, business process enhancements and reduced cyber insurance premiums.

Achieving those benefits, however, requires a shift in perspective.

“Don’t think of cybersecurity as something you are forced to do, but instead what can you accomplish and what are the new opportunities,” Harnish said. “Identify your objectives and then do the work.”

Mercado Clark focused on the growing legal risks associated with technology and data privacy. She pointed to a rise in privacy and security class-action lawsuits, many of which target small and mid-sized businesses that may lack the resources of larger organizations.

She cautioned companies against assuming that widely accepted industry practices automatically shield them from liability.

“Just because it’s commonly being done in the industry, that doesn’t necessarily protect you from litigation,” Mercado Clark said.

To mitigate those risks, she recommended conducting periodic risk assessments with the help of legal and cybersecurity experts and carefully evaluating what information third parties can access.

“We are seeing a significant rise in this type of litigation,” she said.