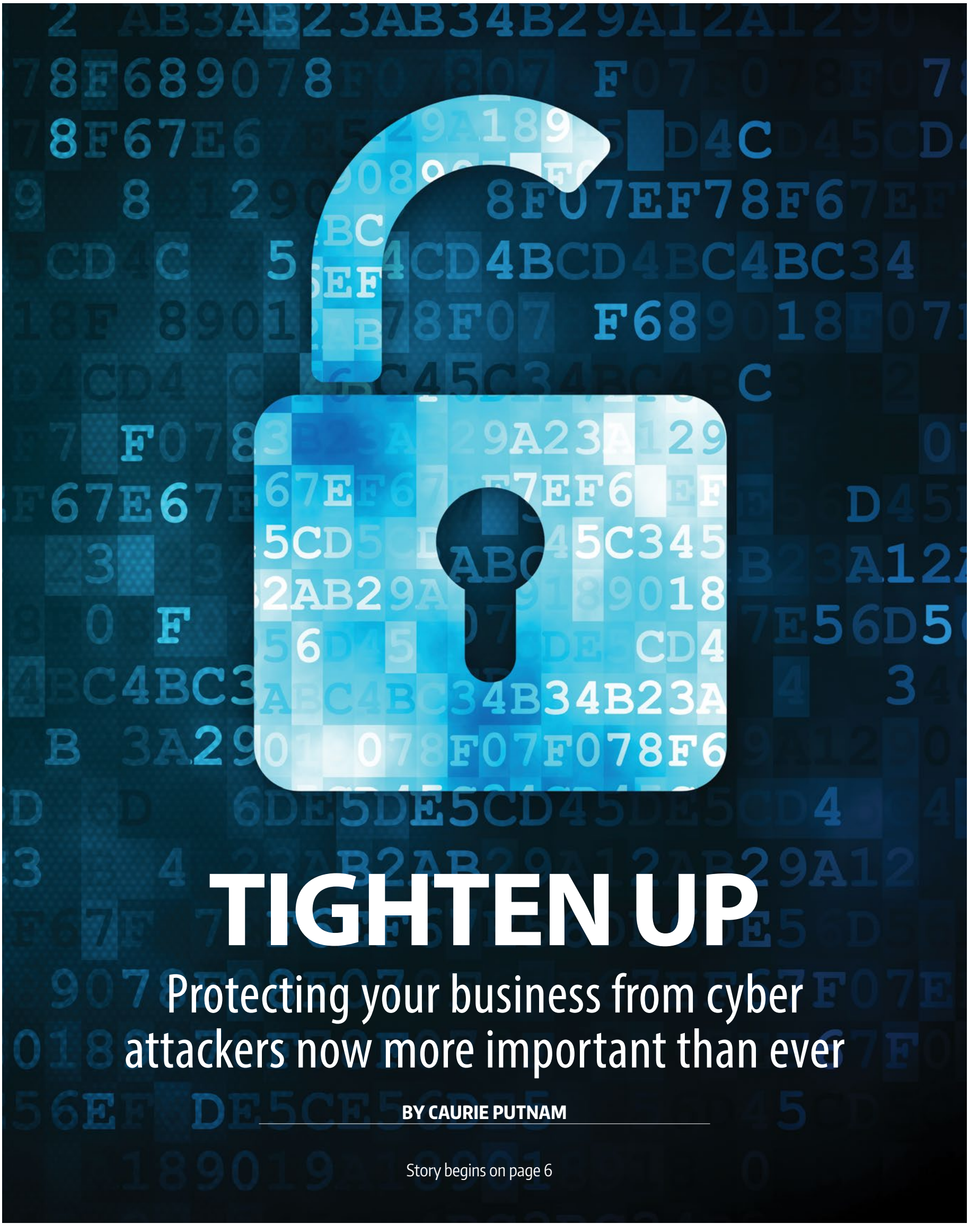
ROCHESTER BUSINESS JOURNAL
FEBRUARY 10, 2023

SPECIALREPORT
Cybersecurity



TIGHTEN UP

Protecting your business from cyber attackers now more important than ever

BY CAURIE PUTNAM

Story begins on page 6

Cybercrime on the rise: How to protect your business

By CAURIE PUTNAM

Although it's a new year, there's no end in sight when it comes to cybercrime. According to Cybersecurity Ventures' 2022 Official Cybercrime Report sponsored by eSentire, the global cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.

We talked to four professionals in the field to find out what significant shifts they saw in cybersecurity last year, what businesses should be on the lookout for in 2023 and how they can protect themselves today.

OrbitalFire: Be prepared for cyber insurance challenges.

Reg Harnish, is the CEO of OrbitalFire, a leading cybersecurity services provider focused on simplifying, automating, and ultimately solving security challenges for small businesses.

Harnish has worked in the cybersecurity industry since the early 2000s and is a fellow of the National Cybersecurity Institute and a member of the Forbes Technology Council.

And yet, Harnish still considers himself to be a "newbie" in the field because cybercrime constantly changes and evolves its levels of deviance and impact.


Harnish

"Cybercrime is increasing in severity, complexity, and damages," said Harnish, whose firm is located in the Capital Region, but has small-business clients in ten states and quite a few in the Rochester region.

He believes only about 1% of the nation's approximate 33.2 million small businesses handle cybersecurity risk in a meaningful way due to hurdles such as fears of expense, a false feeling of invulnerability, a belief that cybersecurity is too complex, and challenges with cybersecurity insurance.

"Cyber insurance has become a contact sport," said Harnish, who is concerned about small businesses increasingly having their cybersecurity policies canceled, coverage decreased, or rates dramatically increased. This has been a problem for about two years, he said, and will be a continued major hurdle for small businesses in the year ahead.

The OrbitalFire team works with clients to find good partners in the cyber insurance space and to work as a go-between to establish and verify that the protection tools the broker wants to see not only exist but are working well.

CMIT Solutions of Monroe: Incorporate employee education.

Cheryl Nelan has long had an affinity for small businesses and a desire to help them protect their technologies. Twelve years ago, she started CMIT Solutions in Rochester where she serves as president and CEO.

Most of her clients are small to mid-size businesses from various industries in Rochester, but she also has clients across the country. One of the most significant cybersecurity shifts Nelan has seen in the past few years is a plethora of new, creative attacks aimed at employees.


Nelan

"The pandemic changed the types of attacks we're seeing," Nelan said. "Today, education is one of the top things we do to protect our clients."

She has seen an increasing number of smaller companies realize the concept of zero trust applies to them too, not just to larger enterprises. Zero trust, a term that was coined by Stephen Paul Marsh in 1994 and popularized by John Kindervag in 2010, is defined by IBM as "a framework that assumes a complex network's security is always at risk to external and internal threats."

"We start at the ground up," said Nelan about how her team helps protect a business from threats by educating everyone within the business. "Ninety percent of IT problems originate from users, but with awareness, most people will work really hard to protect the business they're working it."

Nelan tells small businesses that it's no longer enough to put an anti-virus on a computer and hope for the best. In 2023, a multi-tier strategy for cybersecurity that is created, monitored, and continually improved by professionals is critically important.

ProArch: Add proactive eyes to your team.


WIlcox

Ben Wilcox is the chief technology officer for ProArch Technologies, Inc., a global IT consulting and services organization headquartered in Atlanta with offices around the globe, including Fairport. He has worked in the cybersecurity space for over a decade.

Among the cybersecurity trends he sees happening now are increased interest and delivery in managed detection and response services (MDR).

Per ProArch's website, "MDR services drastically shrink threat detection and response time by monitoring threats across an organization's IT landscape 24/7/365, analyzing alerts, hunting for threats, and responding to security incidents."

Wilcox describes MDR as "pro-active eyes that look at threats from a behavioral standpoint" and "a really quick win for customers." Some of the incentives for using MDR are a potential reduction in cyber insurance rates and an automatically increased level of security.

One cybersecurity trend Wilcox said died in 2022 is traditional anti-virus detection, which is increasingly being replaced with endpoint detection and response (EDR). EDR is an integrated endpoint security solution that continuously monitors end-user devices to find and respond to cyber threats like malware and ransomware.

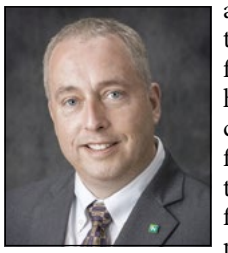
On the topic of ransomware, Wilcox doesn't see this threat easing up anytime soon – instead, it is becoming more of a problem as cybercriminals get more creative and personalized in their attacks.

IBM reported in their global Cost of a Data Breach 2022 that the share of breaches caused by ransomware grew 41% from 2021 to 2022 with the average cost of a ransomware attack being $4.5 million (not including the cost of the ransom itself).

Wilcox also says that, in 2023, businesses should anticipate a continued threat of third-party threats and more of a collaborative effort around cybersecurity from all members of a business, not just the IT professionals.

"The human element of cybersecurity is the one area we can't put a technical control in place," Wilcox said. "There are always going to be human interactions and people are always going to make mistakes."

Northwest Bank: Be cognizant of your third-party vendors.


Spencer

Lance Spencer, senior vice president and chief information security officer for Northwest Bank, has worked in the cybersecurity field for two decades. In the past few years — fueled in part by the pandemic, global unrest, and economic challenges — he's seen "a lot happen in a relatively short period of time" when it comes to cyberattacks.

One of the key cybersecurity shifts he saw in 2022 and anticipates will be even more of a problem in 2023 was third-party vendor supply chain risk. What this means is, businesses don't just need to be proactive with their cybersecurity, but aware of the cybersecurity of their vendors and other entities they work closely with, including their bank.

When choosing a bank, Spencer says businesses should take into account the bank's customer service and responsiveness (both of which will be critically important should a cyberattack occur) and that the bank is adhering to cybersecurity best practices, including secure platforms and fraud protection.

Some of the services Northwest Bank provides to customers in the cybersecurity realm are email blasts with critical security alerts, educational social media posts, and a security center.

Caurie Putnam is a Rochester-area freelance writer.

Shore up the human firewall against creative cyber attacks

By PATTI SINGER

The email to the chief financial officer seemed to come from the CEO.

The message said the CEO was visiting a vendor. He needed them to release a shipment right away and would the CFO transfer the necessary money. The vendor had recently changed banks, so the message included the new routing and account numbers.

"The email looked perfectly legit," said Mark Lucas, executive vice president of Entre Computer Services.

The details matched what the recipient knew: The boss was traveling and had planned to visit vendors.

"So, he made the transfer, only to discover that there was a fraudulent email,"


Lucas

Lucas said of the incident that happened to an acquaintance. "Someone had hacked into the CEO's email."

The email may have been a spoof, but the bottom line was that the bank information didn't belong to the vendor and the company wound up out tens of thousands of dollars.

Unlike big companies, businesses with 100 or fewer employees may not think they have the resources to hire professional cybersecurity firms and beef up protection — or need to.

"Over the last five years I've sat across the desk from multiple CEOs of small businesses when I've told them, 'we need to get you protected, we need to get tools installed, we need to make sure that you don't get attacked,' their answer to me has been, 'I'm not too worried about it. I've never been attacked,' " Lucas said. "The guys that were saying that are the very same people that are calling me up because they just got attacked and they're saying, 'Help, I never thought it would happen to me.' "

The statistics on breaches can be scary. According to Global Cyber Alliance, one in two small businesses have already experienced an attack, that more than 70% of attacks target small business and that 60% of small business that suffered a data breach were forced into bankruptcy.

IT and cyber security professionals said that in response to claims over the past few years, insurance companies are demanding small businesses protect their data and networks in order to get coverage.

Fred Brumm, co-owner of CETech,


Brumm

said he has a list of 120 requirements from various insurers in order to write a policy. Items include multifactor authorization, a written information security policy, email spam filtering and having a third-party test the IT controls.

Continued on page 47