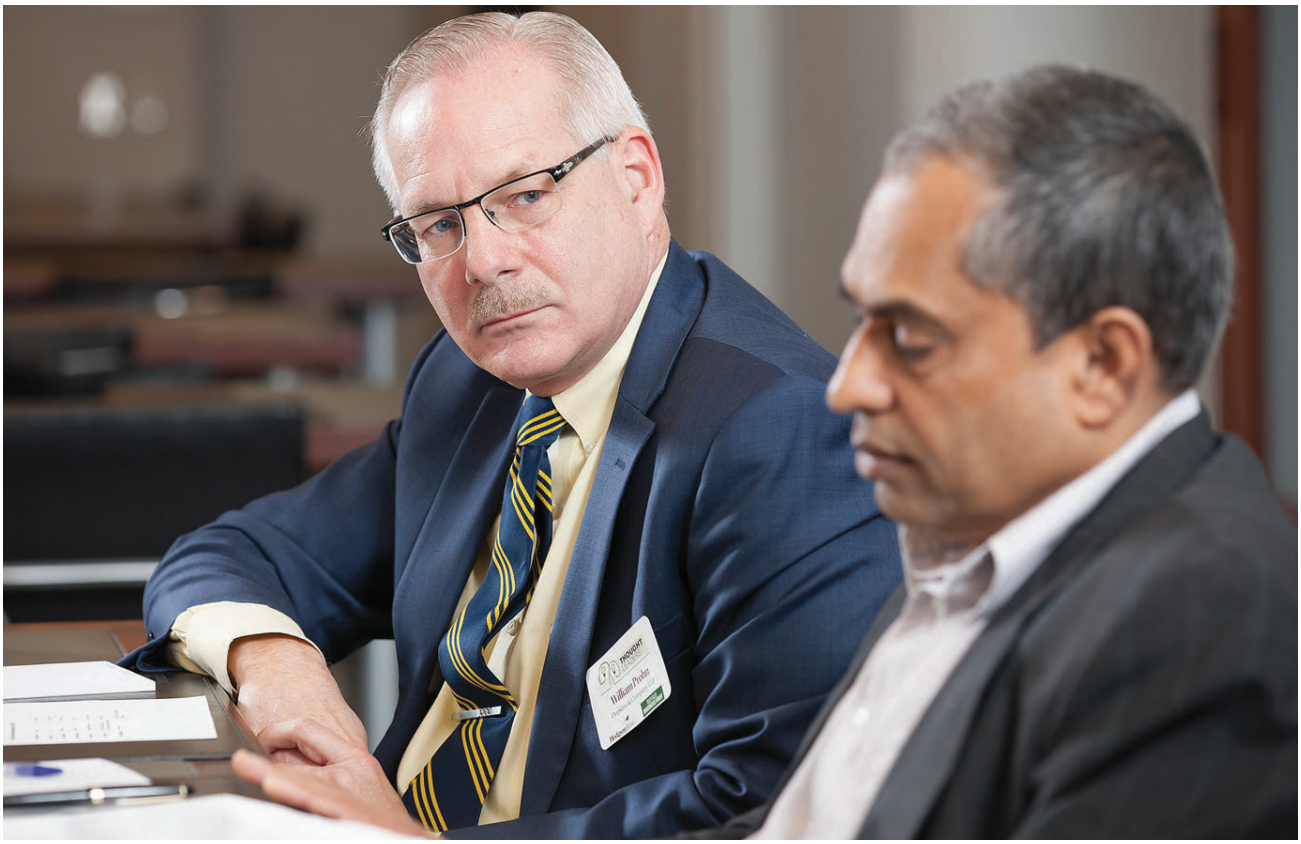
THOUGHT LEADERS

CYBER RISKS

Many business leaders still aren't doing enough to combat attacks



BOTH PHOTOS: JIM COURTNEY

Dopkins & Company partner William Prohn, left, and University at Buffalo professor Shambhu Upadhyaya shared their insights on the state of cyber security at a roundtable discussion last week. Below is panelist Michael McCartney, president of Avalon Cyber.

BY ALLISSA KLINE
akline@bizjournals.com

Many business owners and leaders still aren't doing enough to shield their operations from cyber threats. Why not?

It usually comes down to money. But there's another less-tangible factor and that's the notion that something like a data breach will never happen to them.

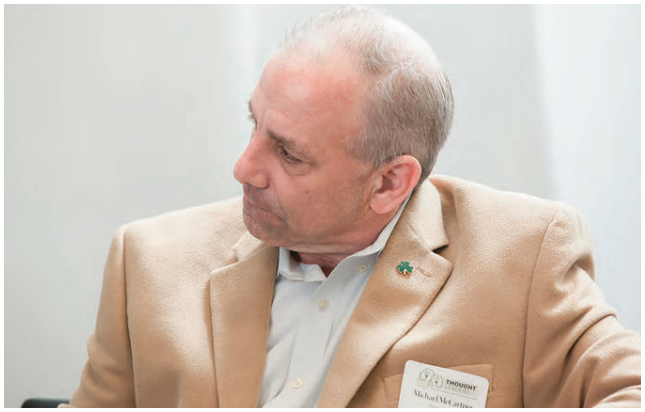
"Any increase in your IT spend stinks, and it's really hard to get your arms around the (return on investment) other than to say, 'Well, the alternative is that 60 percent of small to midsized companies that get breached go out of business in six months," said Michael McCartney.

He is president of Avalon Cyber, the digital forensics unit of Avalon Document Services in Syracuse.

"So companies ask themselves: 'What is my risk of going out of business?' and a lot of industries that aren't regulated are still kicking the can," he said.

The state of cyber security was the topic of discussion March 15 at a Business First "Thought Leaders" discussion sponsored by Hodgson Russ LLP in Buffalo.

The list of panelists included Wil-



with REG HARNISH, MICHAEL McCARTNEY, WILLIAM PROHN *and* SHAMBHU UPADHYAYA

"As long as there are vulnerabilities, there will be people who want to exploit those vulnerabilities for gain."

REG HARNISH, CEO, GreyCastle Security

"In my opinion, there's a real difference between information technology and information security."

MICHAEL MCCARTNEY, president, Avalon Cyber

"You need to put cyber security on the list of risks and consider it and address it just like you would with any other risk."

WILLIAM PROHN, IT director, Dopkins & Company

"Training alone will not solve the problem. So you have to work with tools and techniques, and policies have to be enforceable."

SHAMBHU UPADHYAYA, professor, UB

"All you can do is nip at the edges and try to change the calculus of the probability ... through training and policies."

GARY SCHOBER, partner; data breach and cyber security practice leader, Hodgson Russ LLP

"The first thing (to tell startups) is that you will get hacked. After that, it's a risk assessment."

JONATHAN JASINSKI, associate, Hodgson Russ LLP

"It's a cat-and-mouse game. No matter what you do, there will still be the risk of a bad actor."

JESSICA COPELAND, partner, Hodgson Russ LLP

liam Prohn, IT director at Dopkins & Company; Shambhu Upadhyaya, University at Buffalo professor in the department of computer science and engineering; Reg Harnish, CEO of GreyCastle Security; and three Hodgson Russ attorneys: Gary Schober, Jessica Copeland and Jonathan Jasinski.

They agreed that all businesses – big and small, public and private – are at risk of experiencing some sort of cyber event.

And those events can be costly. According to the Ponemon Institute, which conducts research on privacy, data protection and information security policy, the total cost per data breach in 2016 averaged $4 million. The average cost per stolen or lost record was $158.

Last year, Harnish's firm led the recovery effort at Erie County Medical Center after the 583-bed hospital became the victim of ransomware. The attack forced ECMC to shut down the computer systems and rebuild them over several weeks.

No ransom money was exchanged.

Upadhyaya wants to see more training and more policies that can be enforced. But Harnish said business owners aren't likely to take cyber security seriously unless there's an element of motivation.

"Human behavior can only be addressed by motivation, not training," he said. "And the reason this isn't changing is that we haven't motivated folks."

There are no general regulations by which businesses must abide when it comes to cyber security. But in New York, banks, insurance companies and other state-regulated financial services organizations must comply with a set of cyber security rules that took effect last year.

They include adopting written cyber security policies, appointing a chief information security officer and notifying the state Department of Financial Services of a cyber event within days of the discovery.

Harnish and Schober said they have seen an uptick in inquiries from clients who want to know how to comply with the regulations. But with the rules comes more confusion and something else to pay attention to.

"Instead of the security risk, now (clients) have to deal with the compliance risks," Harnish said. "'Am I more concerned now with hackers or auditors?'"

The group said it's much more difficult to make cyber security-related improvements at established businesses. But how should startup companies prepare?

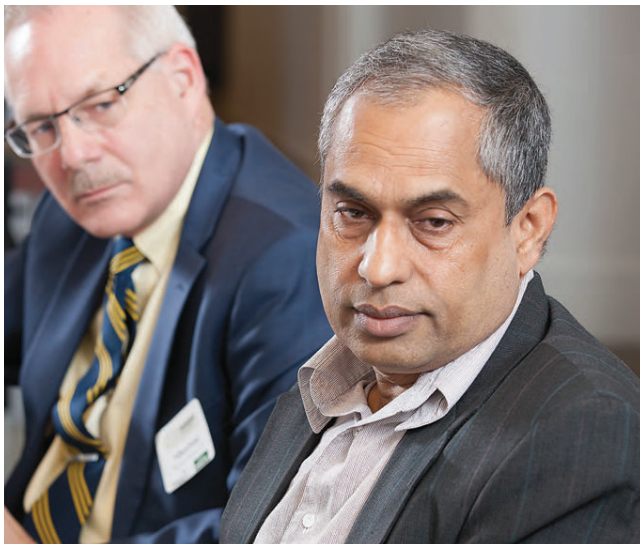
Harnish said: "Smile and tell them not to waste money on cyber security."

Other panelists disagreed.

"My first question would be: 'What is your business?' I need to know what they want to protect," Copeland said. "The bare minimum capital investment at that startup fledgling time is probably what's appropriate. Then you can rightsize it as the company grows."

The bottom line: There is no silver bullet that's going to eliminate the likelihood of attacks, McCartney said.

"But there are things we can do to manage and mitigate the risk and limit exposure," he said. "We need to limit the time between incident and exposure."



JIM COURTNEY

Panelist Shambhu Upadhyaya, right, termed the state of data security "grim" but expressed confidence the trend will improve.

▸ CLOSER LOOK AT THE THOUGHT LEADERS

The Thought Leaders is a yearlong series of discussions with Western New York business leaders and attorneys at Hodgson Russ LLP.

Each month, leaders in diverse industries meet for a roundtable discussion moderated by Business First journalists. Excerpts from the conversation are published after the roundtable.

The next one will feature decision-makers involved in the home health care industry.

Discussions are held in the law firm's Pearl Street offices in Buffalo.