PROVIDENCE BUSINESS NEWS

PBN SUMMIT CYBERSECURITY

CROWNE PLAZA | 10 | 31 | 2017

GAME CHANGER: Matt Cullina, right, CyberScout CEO, says call volume spiked at the company following the cybersecurity breach at Equifax, which he called "a game changer," during the PBN Cybersecurity Summit at the Crowne Plaza Providence-Warwick on Oct. 31.
PBN PHOTO/MICHAEL SKORSKI

14 PANEL: PROTECT DATA BEFORE IT IS TOO LATE

19 CAN YOU DETECT A BREACH?

Panel: Protect data before it is too late

BY MARY LHOWE | Contributing Writer

THE cybersecurity breach of Equifax this past spring, which unloosed the personal financial and identity information of 145 million Americans, "was a game changer," said Matt Cullina, CEO of CyberScout, at the third annual Providence Business News Cybersecurity Summit on Oct. 31.

"After Equifax hit the news, our call volume spiked," he said. "Normally when people call, they are fearful or concerned. These callers were angry."

Much of the summit's panel discussion at the **Crowne Plaza Providence-Warwick** covered ways to protect individuals and businesses from cybercrime. Tactics range from training of employees to alerting them to ways that criminals can slip into computer systems.

Easy tip: Never access sensitive information for work via public Wi-Fi, such as at a Starbucks. And always encrypt sensitive information before sending it out via email.

Weak spots in internet-connected systems, including software and people, where cybercriminals can penetrate computer systems are called the "attack surface."

Mike Steinmetz, state cybersecurity officer, told attendees that this surface is getting bigger all the time. He cited the addition of consumer products that communicate with your iPhone or with each other, such as so-called smart-heating systems, or even appliances such as refrigerators.

All of these things can be hacked, and the hacker can then go sideways into other systems. "Ten years ago, savvy hackers had to go to the dark corners of the internet" to find the technology and means to enter legitimate systems, Steinmetz added. Now, almost anyone can find these tools on the dark web.

Asked to name the major trends in fraud and cyberthreats, John Alfred, a captain with the **R.I. State Police** and head of the state's Joint Cyber Task Force, first named spear phishing. That's when a hacker poses as a legitimate person, say, as your boss or a co-worker contacting you by email.

To defend against spear phishing, Alfred said, make sure the person on the email is who he claims to be. That can be as easy as making a phone call on the spot.

Jeff Ziplow, cybersecurity risk assessment partner with regional accounting firm BlumShapiro, agreed. "You might think you are talking (via email) to your CEO, but you are really talking with an attacker," he said. "Pick up the phone." Another basic rule is to never send money in response to any email communication. Also, inoculate your system with firewalls.

Second on Alfred's list of trends was ransomware, when a bad actor locks up your system until you pay ransom to have it unlocked.

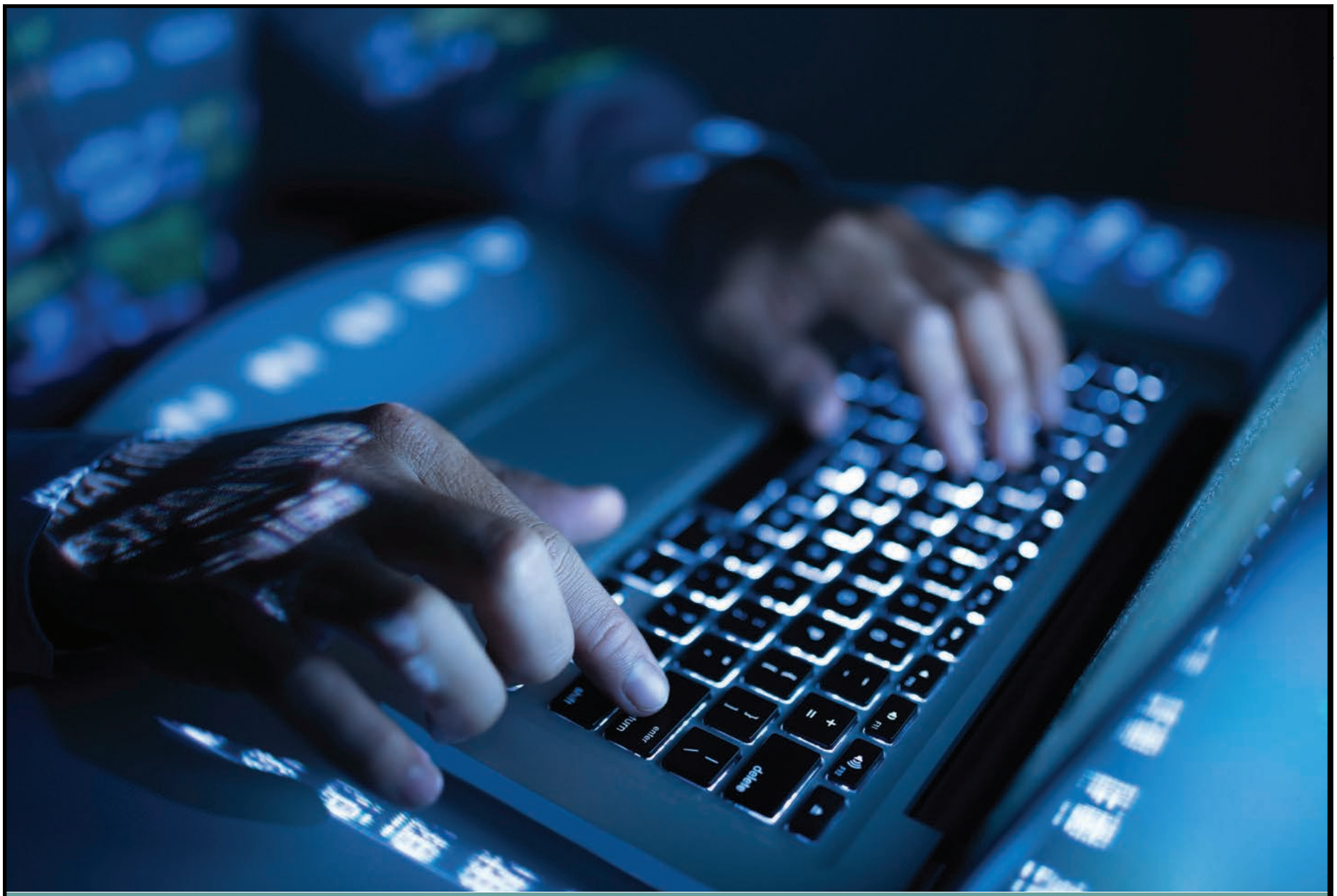
Linn Foster Freedman, a partner with Connecticut-based Robinson+Cole, who practices data privacy and security law, noted ruefully that cybercriminals are often sophisticated, even offering customer service, such as a link for buying Bitcoins. The defense from ransom attacks is to back up your information somewhere off your network.

Mobile phones also are a highway to your data, Alfred said. Androids are an open-source program, which makes it easy for hackers to write software applications that contain malware. Download a malware-infected app and you could let the enemy in. More recently, hackers are inserting malware in any phone – Android or iOS – via attachments to

CONTINUES ON PAGE 16

'You don't want to become that low-hanging fruit. **Clean up your online presence.**'

FRANCESCA SPIDALIERI, Salve Regina University Pell Center senior fellow



Cybersecurity Expertise

Risk & Vulnerability Assessments
Process & Technology Evaluations
Employee Awareness Training
Network Monitoring

BlumShapiro

Accounting | Tax | Business Consulting

Rhode Island | Massachusetts | Connecticut

401.272.5600
blumshapiro.com

CONTINUED FROM PAGE 14

text messages, Alfred said. Defenses are to install antivirus software on your phone, and to never open a suspicious attachment received via text.

More than once, panelists noted the grim expressions on faces in the audience. Steinmetz assured people they have to face up to the reality of cybercrime and get ready for it. "There is no dialing back the clock on this. You need to listen and think seriously about how you are going to become more digital. Avail yourself of the information that is out there."

Businesses, especially small business, also may be threatened by complacency. "A false sense of security puts people in great danger," said Francesca Spidalieri, a senior fellow for cyber leadership at the Pell Center for International Relations and Public Policy at **Salve Regina University**. "You don't want to become that low-hanging fruit. Clean up your online presence. You might be surprised what you put out every day through social media, such as when you are going on vacation, where your kids are."

Scrutinize contracts with vendors – from insurance brokers to Cloud access – to make sure their systems are secure, panelists urged.

"When buying services from vendors, demand solid systems of security and privacy, said Cullina, whose Arizona-based company has a Providence office. "We must say to vendors, 'Here is what I expect if I am going to do business with you.' Businesses handling data badly will

CYBER SOLUTIONS: Linn Foster Freedman, right, a partner with Robinson+Cole, looks on as Jeff Ziplow, center, cybersecurity risk assessment officer with BlumShapiro, answers a question during the PBN Cybersecurity Summit at the Crowne Plaza Providence-Warwick on Oct. 31.
PBN PHOTO/MICHAEL SKORSKI

be called to task."

Many defense tactics are more complicated than simply training. These include buying cyber insurance, with careful vetting of the policy; knowing the ins and outs of rules in other states and countries; and working with legal specialists if you need to report and ameliorate a real security breach.

Cyber liability insurance is relatively new, and many companies still don't have sufficient defenses on this front. "Cyber insurance is tricky," said Foster Freedman, whose firm has a Providence office. "It is not a one-size-fits-all situation. Work with an insurance broker that has experience in this area."

The insurance industry itself is ramping up to understand and respond to cybercrime. "There are eight to 10 different parts of this coverage; the insurance industry is still trying to figure out the standards," Cullina said.

Jerry Alderman, president of New England region property & casualty for New York-based Marsh & McLennan Agency LLC, noted that, for instance, just five years ago, cyber liability insurance did not include phishing. And, he said, homeowners insurance now may include cyber liability.

Another important protection may be business-interruption insurance. In case of a serious data breach, a company or part of it can go dark while data banks are locked up, or during the process of reporting and handling requirements of notification and compensation.

> 'Give [employees] the chance to **be responsible for your information.**'
>
> **LINN FOSTER FREEDMAN, Robinson+Cole partner**

Getting properly insured is one piece of a company's cyber program. Another is having a crisis-management team and response plan in place well before a criminal breach occurs.

"The day a breach happens, you are not going to get crisis-management professionals at a reasonable price," said Alderman, whose firm has a Providence office.

Foster Freedman, who has worked closely with companies to respond to and manage cyberattacks, said the response team should include people from the C-suite, finance, HR, communications and the company's privacy officer. A whole panoply of actions unfolds after a breach, including legally required reporting to governments (in Rhode Island, the attorney general) and to affected individuals, restoration of system operations or data, public information and fines.

How should a company respond to a criminal breach?

The first rule Foster Freedman emphasized was to not call an incident a criminal "breach" – a legally technical term – until it is determined to be so, in contrast to a simple, possibly in-house, accident or misdirection.

"You don't have a breach until I say you have a breach," she declared. "Call it an 'incident.' And don't send email to each other except to say, 'Meet me in the conference room.'" Next, she said, "get your lawyer involved," keeping the conversation, at the start, under attorney-client privilege.

Foster Freedman and Cullina said companies should not respond to an apparent cyberattack by trying to do their own forensics. Call in the specialists.

"We have handled 4,500 breaches," said Cullina. "By the time the company calls us, they have already done stuff. They could be messing up the evidence trying to do [forensics] on their own. It can end up snowballing into something worse."

Panelists said there are 48 different state laws about cyberattacks in the United States, with variations among them. Rhode Island's Identity Theft Protection Act of 2015 requires that a cybersecurity breach be reported to the state attorney general within 45 days of its discovery by the victim.

Alfred said victims should report the incident to his Joint Cyber Task Force, partly because the police may know how your attack might fit into other cybercrime on their radar.

Hovering over the discussion, of course, is the Cloud. Is your data safe in the Cloud? Is its safety your responsibility?

"We assume that Cloud vendors are safe and that they have secure protocols in place," said Ziplow, whose company has a Cranston office. "The reality is, we don't know. Ask your vendor about procedures. Evaluate various Cloud vendors."

Foster Freedman added, "The data are still yours."

Other advice includes always encrypting personal data; changing passwords and using phrases for passwords; getting rid of personal data your business doesn't need to have, thus reducing your exposure; maintain privacy, such as confining a notification that you will be out of the office to internal networks.

Finally, bring employees up to speed with knowledge and sensitivity to the dangers. "Give them the chance to be responsible for your information," said Foster Freedman. "No one wants to be the dumb one who clicked on the Chinese website." ■

Panelists Linn Foster Freedman, Robinson+Cole; Francesca Spidalieri, Salve Regina University's Pell Center; Matt Cullina, CyberScout, and Jerry Alderman, Marsh & McLennan

PBN's 3rd Annual Cybersecurity Summit drew a large crowd at the Crowne Plaza on Oct. 31

Kevin Tracy, Bank of America, with Cindy Lepore, Kelli Viera and Ken LeGendre, Marsh & McLennan, Partner Sponsor

Panelists Francesca Spidalieri, Captain John Alfred and Jeff Ziplow

Panelist Mike Steinmetz, RI State Cybersecurity Officer and Principal Advisor, RI Homeland Security

Panelist Jerry Alderman, Marsh & McLennan

Captain John Alfred from the R.I. State Police discussed the R.I. Cyber Task Force

Salve Regina University's Exhibitor Table

PROVIDENCE BUSINESS NEWS
PBN SUMMIT
CYBERSECURITY

Partner Sponsor Secure Future Tech Solutions' Tim Waugh with Lisa and Eric Shorr

Audience members listen intently to the panel discussion

Panelists Jeff Ziplow, Linn Foster Freedman and Matt Cullina answer an attendee's question

Bryant University Executive Development Center's Paul Dacey and Mike Bennett

Ross Nelson, Cox Business, Partner Sponsor

Jennifer Hogencamp, Jessie Kanter, AnnMarie Fillion and Panelist Jeff Ziplow, BlumShapiro, Presenting Sponsor

PBN's Editor Mark Murphy moderated the panel discussion

Panelist Matt Cullina, CEO, CyberScout

GUEST COLUMN | RAY GANDY

Can you detect a breach?

THE EQUIFAX HACK GENERATED headlines because it was huge – compromising vital personal information of potentially 145 million Americans – and forcing the retirement of the company's chairman and CEO. You might think your company is an unlikely cyberattack target because it isn't a corporate giant. Not so. Sixty-one percent of the companies hacked in 2016 had fewer than 1,000 employees, according to the latest Verizon Data Breach Investigations Report.

The growing frequency of data and information security breaches means that information security is no longer solely an information technology concern.

Here are some questions to answer to begin to evaluate your cybersecurity preparedness.

Do you have a security strategy robust enough to protect your high-value information?

Management and IT should regularly evaluate your organization's risk profile – your industry, the types of information you collect and the systems in place to protect data. Ongoing cybersecurity risk assessments are critical because the risk environment is ever-changing.

What gives you confidence in your data security?

Unauthorized users have gone after a range of data types: operational, financial, customer, personal and strategic information, such as intellectual property or trade secrets. What controls are in place to protect the various data points and how do you know they are working? How often are internal controls reviewed? Have the controls ever been tested by a third-party, such as through a penetration or simulated attack?

Would your organization be able to detect a breach?

Your internal controls – including monitoring logs and network access – should be able to detect a breach. All affected parties need to be notified and management should review the underlying cause of the incident and put a recovery plan in place to minimize the risk of repeat attacks.

When was the last time your organization had a security assessment against a standard framework?

The National Institute of Standards and Technology has a framework that can be applied to all types of organizations. Critical security controls, or CIS, are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most frequent and dangerous attacks.

Some industries have unique requirements. Financial-services organizations should be familiar with the Federal Financial Institutions Examination Council recommendations, health care organizations have breach notification and other obligations under the 1996 federal Health Insurance Portability and Accountability Act, and retailers have the payment card industry data security standard.

When was the last time you reviewed the data-security risks posed by your vendors and partners?

Your organization should periodically review which outside parties have access to your systems and the controls in place to protect that access.

Establish minimum cybersecurity practices for each vendor and regularly evaluate how well each meets the requirements. You should also be part of your vendors' notification chain should they experience a breach or cybersecurity incident.

What investments are you making in your employees' cybersecurity practices?

Many new-hire orientation programs include information about cybersecurity policies, but then the subject is never dealt with again. Your company should clearly communicate to all employees on a regular basis information they need to know about their role in cybersecurity. ■

Ray Gandy is a director and leader of CBIZ Tofias' IT risk and security practice in New England, with offices in Providence and Boston.

Risk assessments are critical because the risk environment is ever changing.

Protection for your business and your peace of mind.

DDoS Mitigation Services DDoS attacks are evolving. They're now so common, it's not a question of if an attack will occur, but when. With new and trickier ways to undermine your site, it's crucial you have a partner who can keep up on trends and changes attackers are making to evade detection. Your business needs the expertise of Cox Business DDoS Protection.

Steps For Successful DDoS Mitigation

1 MITIGATE

When an attack occurs, we'll immediately begin to mitigate it for you. Our Security Operations Center is staffed with experts who understand the internet landscape and how to assess potential threats.

2 COMMUNICATE

We'll immediately let you know when we detect a potential threat, what we see and how we plan to resolve the situation. You will be informed during the entire process, so you can keep your team continually updated.

3 PREPARE

Our experts are always keeping fresh with the latest information. We conduct drills regularly to ensure we're prepared for new and ever-changing attacks.

Data Services

Cox Business offers DDoS protection for all of your internet services, so you'll be protected from any size incident. We can automatically detect and monitor DDoS attacks for you.

Security Operations Center

Our team of seasoned, effective pros is the perfect complement to our advanced technology in helping prevent attacks. Our team monitors analyzes data in real-time, 24/7, to detect potential threats and mitigate when necessary.

To Learn More Visit:
www.coxbusiness.com

Cox Business®