the EdgeRoom®

October 22, 2019

Five Technology Experts Weigh in on Today's Cybersecurity Challenges

By Melanie Brenneman

Try catching a mosquito from the bed of a pickup truck that's bumping over soccer ball-size rocks. To many, nailing this is easier than addressing today's cybersecurity challenges.

Law firms and accounting firms are target-rich environments for cybercriminals. A firm's systems can provide everything from Social Security numbers to privileged corporate data – all items that can fetch big dollars on the black market.

How can organizations defend against or even stave off digital threats?

In honor of National Cybersecurity Awareness Month, I (virtually) sat down with the following five technology experts:

- Matthew Brothers-McGrew, CISO and EVP of technology of Reveal Data
- Randy Johnston, EVP of K2 Enterprises and chairman and CEO of Network Management Group, Inc.
- Mike Paul, CTO of Innovative Computing Systems, Inc.
- Steve Salkin, managing editor of ALM's Cybersecurity Law & Strategy
- Tomas Suros, chief solutions architect at AbacusNext

Together, they shared the following advice on how best to protect organizations.

Bolster your strongest lines of defense

Firms have a built-in line of protection from digital threats: their employees. But to activate that level of vigilance, they should concentrate on security education and awareness.

"No matter the type of technology deployed, the users share responsibility for securing the system," said Mike Paul, CTO of Innovative Computing Systems, Inc. "It is not only IT's job to handle security. The end user is key in helping keep threats at bay, and security education should be an ongoing quarterly/annual process."

Steve Salkin, the managing editor of ALM's Cybersecurity Law & Strategy and a legal technology veteran for more than 20 years, echoed this sentiment in the context of current threats.

"One of the biggest cybersecurity challenges facing law firms is from within with attorneys and support staff falling for phishing schemes," Salkin explained. "Let's face it, many attorneys and law firm staff are still not very tech-savvy, and a well-constructed email asking them to update account information or change a password can elicit a response. I think progress is being made here. Firms are issuing warnings, telling lawyers and staff to contact IT before responding to emails asking for such information and conducting tests to see who within the organization responds to phishing emails. But the old saying about leading a horse to water applies. I think that the best way to combat this threat – and many firms are now doing so – is to send phishing tests and follow up with a training session."

Takeaway: Invest in security awareness training so that users on the front line can identify trouble before it starts. Likewise, ensure that users know where to turn to in case they spot potential threats.

"Next-generation phishers are taking the time to research their targets – monitoring company news, identifying employees and gathering the information that will help them craft convincing, custom phishing campaigns. Criminals may pose as a company administrator or business partner and make requests like the ones you receive every day," said Tomas Suros, chief solutions architect at AbacusNext. "When in doubt, contact your company or business partner's support line to find out if the email is legitimate."

Embrace agility

"It's not a matter of if you'll be attacked, but when. Even if your internal or external IT team does everything correctly, you can still be attacked," said Randy Johnston, executive vice president of K2 Enterprises, a leading technology CPE provider to CPA professionals, and chairman and CEO of Network Management Group, Inc., a managed IT consulting and services company. "While firms are spending time, money and effort to address cybersecurity, they are not advancing as fast as the attackers. For bad actors, breaking into systems is a full-time job. For most system administrators, cybersecurity is only part of the job."

Always evolving cyberthreats demand accelerated responsiveness from firms.

"Security is never set it and forget it," said Paul. "Threats are constantly evolving and require a nimble company to navigate the changes."

While the pace of cyberattacks may seem relentless, the innovation of the threats may be lacking – which is good news for firms and IT professionals.

"There is nothing terribly novel about cybersecurity threat actors as they are in many ways just con men, criminals and tyrants of yore with updated tactics," said Matthew Brothers-McGrew, CISO and EVP of technology, Reveal Data, who began work in the security industry as a testifying expert focused on cases that intersected with complex computer science, software, breaches and cybersecurity issues.

“With each new year, I read a lot of ‘emerging threat’ lists, and lately these have all been new takes on old cons. This is good news because it means many of the basic tools of a strong risk-based security program remain surprisingly relevant and effective even in this world of emerging threats.”

Takeaway: Johnston said a straightforward act could help protect your organization.

“Backup is the most important part of cybersecurity preparation with user training being second,” he comments. “In 2019, I’ve seen about two attacks per week. Both a CPA firm and law firm in New York City wound up paying $1 million ransoms because they were attacked with crypto-viruses and didn’t have sufficient backup.”

Brothers-McGrew endorsed revisiting security tools.

“Security teams must constantly tweak these basic tools to match the adversary’s evolving tactics. These tweaks are akin to moving to hybrid cars from traditional fuel cars. Nobody who drove a ’70s Impala is totally flummoxed when getting behind the wheel of a Prius.”

Establish holistic security programs

Sometimes, weaknesses result from incomplete visions and plans or measures that have engrained themselves into processes over time.

Suros cautioned against settings that provide convenience at the expense of security. “The default [of some firms] is to give everyone access to everything. Access to sensitive information and software tools should be limited to protect client information and company information.”

Paul agreed and stated: “The biggest challenge [organizations] face relates to an evolution of their current processes and practices as it pertains to security. A company may have had a certain way to carry out adding new users, securing the desktop/server or evaluating a vendor. However, this may have been set up several years ago, or ad hoc, with little consideration given to security.”

Firms should also avoid ranking compliance over security.

“Most firms struggle with implementing meaningful security programs rather than merely being compliant in this environment of ever-increasing regulatory regimes and breach litigation. In my experience, many law firms are naturally focused on compliance as a means to security rather than implementing a security program with a strong foundation that is built on the fundamentals,” explained Brothers-McGrew. “To understand why security and compliance are not always in alignment, one must accept that regulation is often created as a means to shift liability away from a regulating body onto their members. I’m not saying that regulations are inherently bad, but that the goals of regulation can be at odds with a security professional’s primary mission to manage and reduce real, recognized risk for their organization. I have seen firsthand the devastating consequences when companies that hold multiple compliance certificates are breached because they were prescriptive and focused on compliance.”

Takeaway: Revisit the firm’s security program and processes to enforce a holistic approach.

“The most successful security professionals are steering the conversation away from a compliance-first mentality with its endless regulation, questionnaires and auditor checklists,” said Brothers-McGrew. “With the right strategy, it can have an effective security program while being compliant by building a culture that is focused on security first.”

Many thanks to the experts that contributed their time and expertise to this article!

About the Author

Melanie joined Edge Marketing in 2010 after an in-house career focused on marketing, public relations, and communications for private and publicly traded technology companies. Since then, she’s helped close to 50 technology companies make lasting and beneficial impressions in the legal and accounting communities. Her guiding mantra: “It’s not about results. It’s about the RIGHT results.”

As senior account manager for Edge, she creates cohesive PR and marketing plans formulated to help businesses reach their goals. A typical day includes anything from strategic planning, brainstorming and writing content, and delivering new ways to engage the media and target markets.

Known for her “helium hand” (but she likes to call it leadership), Melanie is a past president of the Austin chapter of the American Marketing Association (AMA) and a former board member for the Houston chapters of AMA and the Public Relations Society of America. She lives in Austin, Texas, and actively spoils her two dogs every day.

Originally published October 22, 2019 by www.theedgeroom.com