Protecting Your Systems

Virginia Society of Certified Public Accountants

VSCPA, K2 Talk Security at Tech-Know Summit

The VSCPA held the newly renamed Tech-Know Summit at the Richmond CPA Center on Oct. 25–26, and a lot of the key takeaways had to do with security and stopping bad actors from gaining access to your systems. Read on to learn more about the latest technology and security tools from K2 Enterprises, the VSCPA's partner for the event.

twitter.com/VSCPANews facebook.com/VSCPA instagram.com/VSCPA

Security: A Practical Guide

In his session with the same name as this recap, K2 partner Val Steed said that thinking about things logically can help a great deal in keeping your business secure.

Would-be data thieves, Steed said, can do a lot of damage with physical or remote access. That means securing our systems has to be a top priority because of the sensitive client data those systems contain.

"The bad actors figured us out as accountants many years ago," Steed said. "For years, we flew under the radar. Then six or seven years ago, they realized that CPAs, especially those of us in public practice, have a lot of client data, and as a profession, we haven't been that tech-savvy with security."

Val Steed

Of course, that's not unique to the accounting profession. Steed offered sympathy for "underfunded and understaffed" health-care professionals who have to deal with Health Insurance Portability and Accountability Act (HIPAA) standards. And he also singled out one financial-services company for its backwards password policies.

"For years, Charles Schwab wouldn't even allow you special characters in passwords," Steed said. "Now, they're allowing you to use dual-factor identification. The financial groups are getting a lot smarter."

Dual-factor authentication is just one of the security tools available to companies and individuals in this day and age, but a lot of the advances have come on the physical, rather than virtual, side. Ocular and face scanning technologies are proliferating in addition to the now-standard ID cards and key fobs.

That's because physical access can allow bad actors to get to sensitive data even more efficiently if they can pull it off. Scammers who can gain access can find an unused machine and get access to reams of sensitive data. One way of getting in is by "tailgating" real employees, perhaps holding coffee in each hand to provide an excuse for not pulling out an ID card.

"I tell my employees that it's hard, but they have to be tough on the tailgaters," Steed said. "You have to card yourself in, because bad actors are going to try to prey on the kindness of others and an uncomfortable situation."

For all the talk about physical access, cybersecurity remains just as big of a concern, in part because it's often so easy to breach. Most data breaches are accomplished in a matter of minutes, while only a lucky few companies are able to stop them as quickly as they're initiated. Typically, discovery time is measured in months.

The fallout of security breaches can be devastating ▶

in several ways. Downtime to get back into compromised systems leads to lost productivity. Confidential information is almost always compromised, particularly concerning for businesses with fiduciary responsibility. And that leads to a loss of reputation, which is now less of an issue for a very concerning reason: Virtually everyone has been compromised.

"The ones that are really scary are the ones who aren't going to announce they're there," Steed said. "When I fell in love with accounting technology years ago, I never thought we'd be using so many of our resources to fend off people who are bored or angry.

"People have always tried to steal, but I never dreamed it would be this big of a deal. We've evolved from silly little computer viruses that were intended to mess up somebody's day."

Humans remain the weak link in the cybersecurity chain — breaches and security failures are almost always human-caused, rather than technology-caused. The most common reasons for breaches, Steed said, are ransomware, social engineering, unencrypted data, poor authentication controls, poor patch management, exposure through trading partners, Bring Your Own Device (BYOD) policies and the Internet of Things (IoT).

The last two are particularly scary because they arrive hand-in-hand with technologies that purport to increase productivity and make our lives easier. BYOD allows employees to find the devices that work best for them, and the IoT offers connectivity and remote access to facets of our homes we never dreamed possible. ▶

Your Best Defense

How can you protect your home and business from cybersecurity breaches? K2 experts speaking at the Tech-Know Summit offered the following advice:

Judge writing ability harshly. "If you get an email and they can't spell words or they have bad grammar, that's a really good hint. 'This come with Benefits.'" (Val Steed)

Healthy skepticism. "These shortened links, whether it's Google or TinyURL, how do you know where they're taking you? How do you know it's not taking you to some malicious website? Always be skeptical of shortened links." (Tommy Stephens)

A good Outlook. "The preview pane in Outlook, which has worked the same way for 15 years, is your gift. Microsoft shuts down all pictures and all scripts in the email. What would be a risk is if I actually opened up the email. That could activate a script if there was a script attached." (VS)

Encrypt, encrypt, encrypt. "We want you to have encryption everywhere. We want you to have it on the hard drives of laptops and desktops and USB sticks and servers, and we're doing it because of security breach law compliance." (Randy Johnston)

Skew your security answers. "Do you know the security questions where they say where did you go to high school, who is your best friend, where were you born? Ninety-nine percent of that is on social media. I knew one person who answers those questions as if she was her mother. They have to make the leap that it's not the high school where I graduated, but the one where my mom graduated." (VS)

Be careful where you connect. "When you connect to unencrypted WiFi, anyone else on that network can see everything that you're doing." (TS)

Know the limitations of IT. "One of the issues with internal IT teams is that they don't know what they don't know. They support the apps that they know, but they don't know other software." (RJ)

Put yourself in position to succeed. "Remember, most of your team members want to do the right thing. They just need to know what that is." (VS)

Steed recommended that anyone thinking about implementing BYOD or dipping a toe in IoT do so carefully, with intense research, and to think hard about who you're doing business with and who you're inviting into your home or company.

"Pick big-time, brand-name devices if you're going to use Internet of Things devices," he said. "If something goes wrong with Nest [thermostats], we're going to hear about it. We're going to know, and it won't be a month later. Ring [doorbells], we'll hear about it right away. My little irrigation tool… eh." ■

Inside Your Firm's Technology Controls

Steed's K2 colleague, Tommy Stephens, expanded on the issue of internal controls at his session, "Evaluating Technology Controls." Internal controls, Stephens said, are largely a matter of resource allocation, and he says most organizations aren't allocating theirs as well as they could be.

"We dump almost 100 percent of our internal control resources into preventive efforts, and every internal control is going to fail at some point," he said. "We're only human. A person is going to have a five-step process and only do steps 2–4. If we are dumping 100 percent of our resources into preventive efforts, what happens when the preventive control fails?"

Stephens covered the difference between general controls and application controls within the area of information technology. The former are implemented at the organization level, while the latter can be applied in a much more granular matter. And the ultimate aims of both are often misunderstood.

"Let me throw some cold water out there," Stephens said. "People walk around with the idea that internal controls are intended to eliminate risk. They're not. They're intended to reduce risk to a prudently acceptable level as defined by cost-benefit analysis."

Tommy Stephens

Stephens identified login and access control as the single biggest impact area for technology controls. He cited a statistic from Atlanta-based accounting firm Warren Averett that 40 percent of deficiencies identified in a study are associated with login systems. That means that's where designers of internal controls can get the most bang for their buck.

Access control is an example of a general control, or an organization's first line of defense. General controls are applied across an organization's systems and provide reasonable assurance with respect to security, stability and reliability of IT infrastructure. Password policies are another major part of general controls, and it's one that organizations shouldn't hesitate to outsource to technology.

"I think as human beings, we can't comply with password policies today," Stephens said. "If you have not taken a look at some of the password management software that's out there, you need to take a look. All of the password management tools are so good that ▶

General vs. Application Controls

Examples of IT general controls:

- Control Environment
- Change management procedures
- Source code/document version procedures
- Logical access policies, standards and applications
- Incident management policies and procedures
- Problem management policies and procedures
- Technical support policies and procedures
- Hardware/software configurations, installation, testing and management
- Disaster recovery/business continuity
- Physical security

Examples of IT application controls:

- Usernames/passwords to access applications
- Specific rights granted within business applications
- Edits on field to ensure the proper type of data is being entered
- Audit trail reports
- Preventing price overrides on bills or invoices

it's hard to go wrong."

IT application controls, meanwhile, are applied on a user, application or business-process level. General controls might allow a user to sign into an organization's network, but a separate login allowing specific users into an accounting application is an application control.

The common thread in both general and application controls is employee ownership of data policies. It's important to stress the negative effects of a data breach to impress upon employees the importance of following policies and best practices.

"Your team members have a vested interest in your company," Stephens said. "They want raises and promotions. And what do they not get when you have a data breach?"

Acceptable-use policies for the Internet are crucial, but it's also important to keep them reasonable. It's not realistic to expect employees to stay on task 100 percent of the time, but it's important to make sure they're not shirking their jobs or jeopardizing security.

"I view the Internet as today's version of the phone," Stephens said. "There's still the quality of usage — porn, gambling sites, things like that. But if they're getting their jobs done, that's what's important.

"If they're spending 15 minutes a day planning a vacation, that's fine. If they're spending 15 hours a week, we have a problem." ■

How to Filter the World

Stephens wants you to know this key point: Nobody's perfect. Everybody makes mistakes. That's why technological safeguards are so important in dealing with bad actors and heading off potential data breaches.

"Everybody in this room is going to make a mistake at some point. This is the biggest problem with security," he said. "So what I want you to think about is levels of redundancy. Unless you're perfect, and I know I'm not, there needs to be redundancy in place."

Stephens likes to use Outlook rules to help with his own organization's data security. Any email from outside the K2 domain from a user he doesn't know that contains a link or attachment is routed to a specific folder for further analysis.

He also makes use of the spam protection contained in Outlook and notes that any email provider will provide some level of protection. But he stressed the importance of paying attention to the emails that get caught and those that get through to make sure the controls are working properly.

"You're going to have to define what false positive rate works for you and continue to turn the knobs so you're not blocking too many good messages," he said.

Those protections are particularly important because of the volume of malicious actions against companies. The average employee in the United States receives 14 phishing emails per day. New phishing websites and malicious programs are cropping up at incredible rates — 400,000 a month of the former and 390,000 a month for the latter. And just one slip-up can have devastating consequences.

"If I ignore 99 percent of those emails but fail to ignore the 1 percent, I've just potentially infected the whole company," Stephens said.

The major techniques in phishing emails are well-known, but worth going over. Links and attachments are potential attack vectors, and the emails will often be presented as the answer to a question you never asked. Sometimes a problem will be identified and your information needs to be verified at a link provided in the email. And there's a sense of urgency if you fail to act immediately.

The scary part is that users are providing ammunition to scammers in the form of information readily provided on social media. Stephens' own mother got a call from her "grandson" saying that his friends were arrested for possession of illegal drugs and he needed money to get them out. The only tipoff to the scam was that the caller called his "grandmother" by the wrong nickname.

"How would somebody have known who my son's grandmother was? Social media," Stephens said. "Think about all the stuff we're putting out on Facebook. The crooks are intelligent. They realize that we're putting information out there that makes it easier for them to commit these fraud schemes. Be careful what you're putting out there."

Spam protection and common sense are just one element of a strong cybersecurity protection plan. ▶

Antivirus software is still a big deal, but it's not the same software you were running in 2000, because the cybersecurity game has changed so greatly, with approximately 1,000 new strains of ransomware popping up each day in 2017.

Back then, it was important to download the new virus definitions as often as possible, so the software could identify and block files that resembled those definitions. Today's antivirus software is based on heuristics and logic — "Johnny is attempting to run a program on his computer that we've never seen before."

"What are the odds that I'm going to run a program that the people at Trend Micro or Symantec have never seen before? They're near zero," Stephens said. "So they block it. It's a much more intelligent way of stopping malware. A blacklist might have worked 25 years ago, but it could never work in today's environment."

Outbound filters are just as important in protecting the release of sensitive data. Data loss prevention (DLP) tools often operate by looking for specific patterns in emails, such as this one: Four numbers, followed by a hyphen, followed by four numbers, followed by a hyphen, followed by four numbers, followed by a hyphen, followed by four numbers. That's a credit card number, and you can apply similar logic to look for Social Security numbers, phone numbers, etc.

"When it finds that there's content that meets the patterns that you prescribe, it won't allow you to send the outbound email message, either in the message or the attachment," Stephens said. ■

"You have policies in place that say 'Thou shalt not do this,' but people violate policies. If we want to make sure people aren't sending unencrypted tax returns, we can use a DLP tool to block that outbound transmission."

Spotted at A&A

Attendees at the A&A conferences had the chance to network at receptions in Roanoke and Falls Church (pictured).

VSCPA members Tres Brackens, CPA (left), and his father, Jim Brackens, CPA (right) catch up with "TaterBot" in Roanoke.

VSCPA President & CEO Stephanie Peters, CAE, introduces member Joe McNamara, CPA, a candidate for the Virginia House of Delegates, at the Roanoke networking reception.

VSCPA members (from left) Diane Dickson, CPA; Joan Renner, CPA; John Renner, CPA; Bill Young, CPA; and Lynn Almond, CPA, catch up at the Falls Church networking reception.