BPM's David Trepp Quoted in Accounting Today About Cybersecurity Services

05.29.19

This article originally appeared on May 29, 2019 in Accounting Today. To view the original article, click here.

On Monday, May 6, accountants around the United States woke up to start their workweek only to discover that their CCH products — a suite of tax and other solutions offered by Wolters Kluwer Tax & Accounting — were down. Confusion turned to panic, which then turned to anger pretty soon after customers were informed the company had been the victim of a cyberattack.

Social media forums began to light up with questions, discussion, conjecture and rumors. The few hours between the products going offline and the first set of communications the software provider sent its customers were enough to cause a frenzy, especially as the May 15 tax deadline for tax-exempt clients loomed around the corner. Wolters Kluwer's communication was sparse, but over the next few days the company announced that the CCH product suite had been the subject of a malware attack, that the products had been taken offline to protect customer data as soon as the breach was discovered, and that they would remain offline until the situation was deemed safe.

Sure, CCH customers — not just in the U.S. but around the world — were mad. But Wolters Kluwer's response was swift and what cybersecurity experts deem prudent.

Cybersecurity expert Wesley McGrew, director of cyber operations for Horne Cyber, said that it's almost impossible to know how such a breach really starts. Releasing information only when it is known for certain is the best way for a company to respond, as opposed to making statements that it may have to edit and retract later.

"The investigation requires bringing in incident responders and security specialists to figure out how the [cybercriminals] got in in the first place," he said. "Bringing the systems offline was done out of prudence — you can't have people uploading files without knowing exactly what the situation is."

"Every indication is that [Wolters Kluwer Tax & Accounting] is doing what they should be doing," said McGrew, whose company is a subsidiary of Top 100 Firm Horne, which uses CCH products and was affected by the outage. "Responding and investigating, and they seem to be staging back online in a measured fashion, which is probably smart. The worst you can do is rush to get back online, still have an infection, and leak even more data."

It took about 24 hours for the media, including Accounting Today, to pick up the CCH story, mainly because information was limited. But as soon as coverage began, the mood both among accountants engaging on social media and Accounting Today's readers settled down to calmness. A week after the outage, Wolters Kluwer negotiated with the Internal Revenue Service to offer extensions to nonprofit organizations and others whose accountants had been affected by the outage.

"I understand details are slim," a user of news aggregation and discussion website Reddit posted. "Do what ya can, when ya can. — Cooling Boots over here in Virginia."

Real-world ripples

The reaction to a breach in any industry typically follows a pattern: confusion, panic, anger, then some version of surrender. In some ways, this very human way of dealing with a cyber crisis is appropriate, given that the fault for many of them doesn't lie with technology, but with people.

The thing is, the very same qualities that make an excellent employee — good client service, empathetic, compassionate — also make them a prime target for hackers, because the easiest way to gain access to systems and data is not through microchips or code-breaking, but by simply asking. Socially engineered hacking remains the biggest security concern in the accounting profession today. That includes methods like phishing, a tactic by which cybercriminals send probing emails posing as a client or other known entity, fishing for sensitive data, access to accounts, or just money. So the fastest path for bad actors? The human touch.

"For most of your readers, phishing is probably the No. 1 threat," said David Ross, principal and cybersecurity practice leader at Top 100 Firm Baker Tilly. "There's been a huge uptick in the last few months in spear-phishing attempts, which are very specifically targeted to an individual. Prevention is a twofold approach. On the technical side, you implement systems to filter and catch as many of these emails [as you can] so they don't get to the end recipient; the other is personnel training."

One of the ways security consultancies help their clients establish a robust security posture is through penetration testing, also known as pen testing. As well as the penetration of computer systems, probing for weak spots, consultancies will sometimes physically show up at a client's office and start covertly testing staff for vulnerabilities.

"Helpful people are a real target," said David Trepp, IT assurance partner at BPM, a Top 100 Firm in California that also provides pen testing and other security services. "It's an intractable problem for service firms in general that hire people who have a service mindset. The only way to overcome that is through vigilant training, and providing good controls and systems that don't allow them to get in trouble."

Helpful staff will more readily respond to a stranger who appeals to their willingness to be of service, Trepp explained. For instance, he may pose as an IT person who just needs to take a "quick look" at an accountant's laptop to "get his boss off his back" and get a fix done quickly.

"All we need is about three seconds with an unblocked, unattended computer, or an employee willing to believe we're tech support, or a live network jack somewhere where nothing is plugged into — and we're in," Trepp explained.

It's these in-person tests, and gamification of the training process, that are most successful in making staff as immune as possible to hackers. Videos and lectures are not as effective as basically running a con, as they don't have the real-world effect of actually duping a trainee, Trepp explained.

"Statistics suggest the average human being falls for a social engineering attack about four times — with training — before they become 'inoculated' against that type of attack," Trepp said.

Three seconds. Four successful attacks. The odds seem stacked against the good guys.

The cybercriminals are winning

"I'm our firm's audit manager, and people can call me a dinosaur, but I will never allow our financial statement processes to be dependent on a cloud system, especially after this ordeal," another Reddit user said following the CCH outage. "We don't store any of our tax data on the cloud either."

This statement is emblematic of one of the biggest problems in cybersecurity today, and that is that accountants — and lawyers, bankers, doctors and small-business owners — are not technology experts; they're experts in their own fields. Which means the career cybercriminals, as tech experts using the same technological advances the rest of the world has access to, will always be one step (or more) ahead of the curve.

This Reddit user's comment is based not on a clear and full understanding of how cloud technology works — in many cases, cloud computing is more secure than on-premise software for a range of reasons — but rather on fear. And fear could prevent the accounting profession from moving forward quickly to adopt new technologies like artificial intelligence and blockchain, allowing cybercriminals to forge ahead with faster and smarter ways to gain access to company information, while the profession lags behind in preventative measures.

"This is a truism, and I hate to admit it, but we're always behind," said Jon Murphy, vice president of cybersecurity for RGCybersecurity, an Alliantgroup company. "Bad guys have no unions, labor laws, regulatory requirements, have unlimited terms, can work wherever — it's a mindset. They love figuring out and breaking things. They're always finding flaws and exploits before we can fix them."

Murphy, who also advised Presidents Bill Clinton and George W. Bush on cybersecurity strategies, said a military concept called "defense in depth" is the way to go for accounting firms of any size. Just as a castle will have many layers of protection, from a moat, to a drawbridge, to battlements, boiling oil, and soldiers, so too should a security system have multiple methods of prevention built in.

"We now have blockchain and deep learning to help us," Murphy said. "Blockchain came from the dark side to hide ill-gotten gains, but we're starting to use it for good. But prevention is not just a tech thing — it has to be a holistic programmatic approach: people, process, data, technology."

Norm Comstock, managing director for UHY Advisors, a Top 100 Firm that also provides technology consulting services, advises small firms to allocate their cyber budget wisely between prevention, detection and recovery.

"If you're cumulatively spending $1 million on cybersecurity, where's that $1 million being deployed? All on prevention? If nothing is being spent on detection, you create a false sense of assurance," he explained. "In very recent history, someone as large as Marriott Starwood actually suffered from a significant breach over a five-year period. Prevention methods were in place, but detection tools were not being leveraged, maintained or manned so that they could actually disrupt a large breach from happening."

The breach Comstock is referring to was discovered by Marriott in 2018, and affected the records of up to 500 million customers. The hotel chain later disclosed that hackers had had access to their system since 2014.

Comstock advises accountants to pay close attention to “mixed environments,” such as the use of personal cell phones for business in a BYOD (bring your own device) office environment. By mixing consumer applications and enterprise applications on a single device, sharing memory and other resources, a user may download malware by accident during personal usage that can then easily infect enterprise data.

Small firms can look to resources such as the National Institute of Standards, which provides a Cybersecurity Framework, and to industry associations like the American Institute of CPAs (see the AICPA’s Cybersecurity Resource Center on www.aicpa.org) to help build a cybersecurity posture that protects their clients and fits into their budget.

It can seem an insurmountable task to face down cybercriminals and come out on top. Sometimes it feels like a breach is inevitable, and it’s only a question of when. But professional services firms are growing a network of advisors, software and resources to build out cybersecurity and strengthen their security posture. The first step is to take cyber seriously, because all it takes to wipe away a lifetime of client goodwill and data is three seconds.