ROCHESTER BUSINESS JOURNAL
RBJ
VOLUME 32, NUMBER 46 WWW.RBJDAILY.COM FEBRUARY 10, 2017

IRS, experts warn firms of all sizes about scams

Federal agency issues warning of recent fraud involving W-2s

By ANNE SAUNDERS

Sometimes the first clue comes when an employee, chatting with a colleague, mentions she filed her taxes and got a puzzling message from the Internal Revenue Service that she already had filed. If the colleague says, "hey, that happened to me too!" that could signal a company has suffered a data breach.

"Tax return fraud is a multibillion-dollar issue every year in the U.S.," said Paul Greene, a lawyer at Harter Secrest & Emery LLP who specializes in working with companies dealing with data breaches.

Last year at this time, the IRS said there were 1,026 reports of phishing or malware schemes in January, up from 254 the prior year. The increase in reported incidents continued into February, nearly doubling the reported incidents from the same time in 2015.

This year, the IRS is warning these attacks are hitting ever-smaller organizations.

"The W-2 scam, which first appeared last year, is circulating earlier in the tax season and to a broader cross-section of organizations, including school districts, tribal casinos, chain restaurants, temporary staffing agencies, health care and shipping and freight," the IRS warned in a Feb. 2 memo.

"It's not just national chains anymore," Greene said, who has assisted many Rochester area businesses dealing with this problem though he would not identify them by name.

Typically, the issue is not a high-tech cybersecurity lapse, but a staff member who fell victim to a sophisticated spoof via email.

These email messages typically come from someone who appears to be a legitimate higher-up asking for information. The email might state: "I'm getting on a plane, and I need all our employee W-2s to review when I land in Los Angeles."

A diligent employee in human resources fulfills the request, unaware the information is going to a hacker far away who can use the data to file fraudulent tax returns or put it up for sale to other criminals.

The reason a scam like this is often successful, Greene said, is because hackers got into a company's email system long before the attack, getting copies of the messages to and from the leaders, learning who does what, how they communicate by email—even when someone is actually getting on a plane to travel.

"This happens locally quite often," he said. "For example, they'll set up auto-forwarding."

This enables hackers to read everything sent to a company executive whose email they have hacked. Then fake instructions can be sent convincingly to an employee who has data of value to the hackers.

"They're relying on our reliance on email. They're relying on the fact that everything happens at a moment's notice in today's business world. And the fact that people want to be helpful," he said.

With scams continually evolving, staying ahead of the game is essentially impossible, Greene said.

"You're not going to stay ahead of their efforts or creativity. The hackers do this full time and it's very lucrative," he said.

The way to respond is to educate personnel about these risks, and encourage them to double check with their leaders when a request for sensitive information or money comes via email.

"Regardless of your size, you need to start with your people and empower (them) to ask questions, to think twice when there's a request for a wire transfer, any kind of information. And allow that HR person to say to that CEO, did you send this email to me, do you really want this information?" Greene said. "You get that kind of culture in place and you can stop a lot of this risk."

Another smart move is to hire a company that can look into a computer system and identify if it has been hacked, he said.

"Any company with any level of risk concerning data, and if you have employees, you have risk, should take efforts to assess the security of their systems and determine if they've been compromised," he said.

Excellus BlueCross BlueShield is one local company that undertook such a search after other BlueCross BlueShield companies had data stolen, he noted. When a company similar to your own experiences a breach, that is another risk factor, since attacks often target a swath of similar systems, Greene said.

"It used to be very lonely being a data breach lawyer in Western New York," he said.

Not so much anymore.

"My practice morphed from commercial litigation with a data security focus to being primarily data security," he said.

As such, he recommends anyone who suspects a breach to get legal help in dealing with the problem. There are a multitude of different state laws that may apply, and a lawyer can help coordinate a breach response that encompasses regulators, law enforcement and forensic investigators.

Prevention, however, is a bit more straightforward, he noted.

"If you had to choose one thing to do, it would be to educate and empower your people, to make clear that security is everyone's job," he said.

asaunders@rbj.net / 585-546-8303