4 questions small firms need to ask about cybersecurity

By CHRIS GAETANO
Trusted Professional Staff

Just because you're a small firm, don't assume that cybercriminals won't notice you. **Yigal Rechtman,** an expert in IT audits, said this all-too-common mindset amounts to nothing more than "security by obscurity," which really isn't that secure at all.

Speaking at the NYSSCPA's Business and Industry Conference last October, Rechtman warned his audience that professionals such as doctors, lawyers and, yes, CPAs, are "ripe targets" for cybercriminals. All too often, said Rechtman, small practitioners believe, "We're too small—no one is going to attack us." However, he noted that cyberattacks on small entities have become a rising trend. So, even if you run a small, local firm, "we no longer have this privilege" of ignoring the proper management of cybersecurity risks. There have already been breaches reported by firms with as few as two professionals, and Rechtman believes there will be many more in the future.

Smaller firms are increasingly becoming targets for several reasons, according to Rechtman. For one thing, even the smallest firms can hold a wealth of valuable information that can fetch high prices for those who can access it. Think of a two-person CPA firm: Even they have bank information, Social Security numbers, billing information, legal documents, tax returns, maybe even a proprietary document or two, "making all professional networks a high-impact and high-magnitude target, which translates to high risk."

Another reason is that cybercriminals will often follow the path of least resistance, and larger firms, with more resources, have been able to set up and maintain strong defenses, leading to a situation where "phishing and scamming and data mining is all happening on a secondary industry level, and that's what we have here." Basically, smaller firms are easier targets, he said.

What exactly is a small firm supposed to do? Broadly, according to Rechtman, there are four different ways a firm can act in response to cybersecurity risk:

1) Don't leave your firm exposed. For example, he said, people often keep company data on their phones, which can be hacked or even physically stolen.

"I know some of you are hyperventilating at the thought," Rechtman told his audience, "but the point is that's the way to avoid risk, so your data, the company's data, is not on your phone and you are not subject to the company data. You think, 'Well, what do I have—I just send emails,' but what if there's an attachment with some proprietary information?"

2) Reduce risk. This is the world of creating and implementing security policies, which is "nice to do if we can," though Rechtman felt that a lot of firms can have gaping blind spots when it comes to their own security. For example, even if a firm gets the strongest, most sophisticated cybersecurity system in the world, it's worth nothing if threats can simply piggyback onto their vendors and practically walk right through the front door.

"If you take nothing else from this presentation, I would say take vendor management to heart. Vendor management *is* cybersecurity today," he said, adding that "most cyberattacks today are done through some sort of vendor or subvendor or sub-subvendor."

"By a show of hands, anyone here been in love?" he asked. "What happens? You forget what you're supposed to do. You get a phone call and someone says, 'How would you like to send flowers to someone you love,' and you think that's a great idea, and they tell you to go to this website and enter your information, and you can get flowers for free!"

3) Share the risk. One should do this either to mitigate its effects or to share the responsibility for its prevention. One way to do it is through purchasing cybersecurity insurance, though Rechtman warned that this can be tricky because, sometimes, insurers will insert a lot of clauses that, if broken, mean reduced or even the elimination of coverage.

Firms can also share risk with their auditors through a Service Organization Control (SOC) 2 report. While the SOC 1 report is meant for reporting on controls in general, SOC 2 is geared more toward reporting on security controls in particular. Regulators, insurance companies and even insurers have increasingly begun to insist on SOC 2 reports as a way to demonstrate compliance on cybersecurity protocols, according to Rechtman.

"This is a way to share risk: Who are we sharing risk with? The auditor who wrote the report and gave us an unqualified opinion. One way companies are increasingly sharing risk on, for example, security or confidentiality or even availability and process integrity is by using a SOC 2," he said.

Another trend in how people have started sharing risk is through indemnification clauses on third-party breaches, as well as by putting indemnification clauses in service letters. Companies are also increasingly putting "right to audit" clauses into contracts, which allow you to conduct your own security audit in order to make sure whoever a firm deals with isn't going to come tracking in malware from outside.

4) Accept the risk. Rechtman said this is the "lowest of the low," but noted there are companies that say they'll just accept the risk and move on. This, he said, is a terrible mistake.

"My answer to them as an auditor, as someone who comes into the audit—and I specialize in IT and look at IT risk in particular—I ask them, 'Really?' Because many times, they don't think through what it means as far as impact, and by the time [a major breach happens], it's too late for that to be considered."

Regardless of what a firm does, Rechtman impressed upon his audience the importance of doing *something*. If you don't, the CPA's role as a trusted professional—one who has access to all sorts of valuable client information—goes from asset to liability.

cgaetano@nysscpa.org