CPA
Practice Advisor

the cloud model suggests that all types of companies ask: “Who's really operating your systems?” And “What is the cybersecurity risk associated with working with vendors?”

Dec. 28, 2016

The ever-present risk of cyber attacks and the growing reliance on vendors due to the cloud model suggests that all types of companies ask: “Who’s really operating your systems?" And "What is the cybersecurity risk associated with working with

giving employees and vendors access to data and IT systems; and should help reduce the risk that third-parties and your employees can cause, whether intentionally or by accident.

The Threat to the Accounting Professional and their Clients

A survey by the Association of Chartered Certified Accountants (ACCA) of their members regarding cybersecurity awareness and preparedness showed that 57 percent said their systems were hardened against attack. Yet 32 percent said they had no idea what their company policy was on encrypted data. Forty-three percent of auditors felt their companies followed COBIT 5 or other formal standards. Security experts said this shows there is growing awareness of the risk. But they say the survey also highlighted what they call "contradictory" practices.

The Tax Advisor Reports that in 2016, 59 percent of accountants reported that at least one of their clients were victims of identity theft. That could be the fault of the accountant in some cases.

The Risk Inherent in the API Economy

In what has been called the API economy, businesses today outsource many key functions to third-party SaaS (Software as a Service) companies and use managed services. That has been shown to be best practice among many businesses, including CPA firms and with accounting teams. However, that model introduces vendors into the company's IT network. And hackers tend to exploit the weakest link, which could be these vendors. For example, when hackers stole 350 million credit cards from the retail giant Target, the attack vector was the company that maintained their refrigerators. Their system was connected to the presumably more secure Target network.

The Need for Identity Management and Third-Party Vendor Monitoring

data using their credentials. And after the attack, monitoring tools can help with forensics and identify weak spots.

The Accountant's Checklist

That said, here is a checklist of some of the best practices that accountants can follow:

- Find a security managed services firm that can be your forensics partner when disaster strikes.
- No system is 100 percent free from hacking. Hackers can seemingly attack whatever they want. So work from this defensive posture and plan accordingly. That is, write a communication and risk management plan with instructions on how to handle a data breach with customers, regulators, vendors, etc.
- Monitor and record all third-party actions. Set alerts for logins, databases and other activities that don't match the vendor's tasks.
- Set limits on vendors' access times, location, and application access as well as put in place some formal procedures for granting access.
- Use two-factor authentication. For example, a cell phone is needed to receive a code to login to systems. Most systems will support that and if not consider switching to one that does. Passwords can be stolen. But the hacker is unlikely to have stolen the cell phone too.
- Publish some rules for your vendors that they must adhere to when they connect their systems to yours. For example, require each of their employees to show they have taken security awareness training. And repeat that each year.
- Don't forget that mobile devices are a risk. You could use mobile device management (MDM) applications that can push security rules onto employee's phones and tablets.
- Train employees not to click on links in phishing emails.

Just as in life, the proverbial phrase that there's two things of which you can be

having an incident occur and putting your very business at risk.

———

***Isaac Kohen** is the founder and CEO of Teramind (https://www.teramind.co/), an employee monitoring and insider threat prevention platform that detects, records, and prevents, malicious user behavior. Isaac can be reached at ikohen@teramind.co.*

Firm Management