wise to the ways of cybercriminals. They're proactively partnering with IT and business leaders to take preventative action, mitigate risk and avoid costly breaches.

Jodi Chavez • Mar. 19, 2021

Almost from the outset of the pandemic, financial services organizations found themselves near the top of hackers' hit lists. And, at least in a few crucial respects, it's not so hard to see why. Reams of personal and financial data. Intimate institutional connections, often to much larger fish in the ecosystem. Comparatively immature IT infrastructures. Limited overall threat awareness. From the other end of the periscope, we must have looked like sitting ducks.

The good news is the extent to which that narrative is no longer true. The range of responses from financial services companies of all kinds, and the swiftness with

which many have made changes to bolster both IT and accounting practices in the

Just how *bad* is the situation with cybersecurity right now? What are the latest numbers in the context of financial services organizations generally, and CPA practices specifically?

Let's start with the numbers.

- Data breaches at CPA firms have risen by more than 80 percent in recent years — and they've also changed in kind. For example, more than 40 percent of those breaches now represent attacks involving ransomware and/or extortion.

- Small to medium-sized accounting firms have been identified as particularly compelling targets for cybercriminals. Why? They have access to sensitive client data, they often serve as connectors or gateways to larger, more prominent organizations and they seldom have the advanced IT infrastructure of banks and larger firms. It's a combination that has global cybercriminals licking their chops.

- Despite the clear and present danger, not to mention the increasing frequency of cyber attacks, however, it is the exception to the rule for cybercrime to result in arrest and prosecution. In the context of identity theft, for example, only one identity thief is convicted for every 20,750 victims, according to analysts.

Why the seeming leniency on the part of law enforcement? The fact is, many of these criminals are based overseas. While the U.S. has extradition treaties with many countries, there are almost an equally large number — more than 76 countries, including China and Russia — with which we do not. Put two and two together and the baseline obstacles to successful prosecution aren't difficult to spot.

None of which in any way lets organizations off the hook, of course. (If anything, the effect is just the opposite.) Given that reality, however inconsistent it may seem to

potential industry targets, what can financial services firms do to shore up their

Yet, while the need for such skilled professionals is clearly quite pronounced, as we have just discussed, where are hiring managers to find them? They aren't exactly out there in droves, a point which brings me to two recommendations.

First, in the interim, close collaboration between these two departments — finance and IT — is going to remain essential for best-in-class risk and threat mitigation practices today. Organizationally, this should be a focus area.

Second, there are exciting opportunities for seasoned finance professionals to start evolving these capabilities on their own, and CPA-specific training programs are one route to get there. The American Institute of Certified Public Accountants (AICPA) already offers several, for example.

What can you do with this sort of training? What does it look like in practice?

- Audit and assess the end-to-end state of an organization's existing cybersecurity risk management program, identifying any gaps and probing for weaknesses.
- Build out more robust controls across the finance function.
- Develop and implement advanced training to increase the organization's overall cybersecurity readiness.
- Create threat detection and response protocols, thereby empowering key stakeholders to take action and mitigate losses in the event of a potential breach.
- Work consultatively with other business heads, providing advisory services and ensuring strategic alignment across all areas of the organization.

And that's just the tip of the iceberg. As these training programs continue to evolve and become more sophisticated, I'm excited to see how CPA practices and other

financial services organizations grow and change in turn.

to demonstrate advanced technical capabilities as part of their core accounting function should stand to gain a distinct competitive advantage — in fact, it could position them head and shoulders above the rest.

==========

With more than 22 years' experience in the staffing industry, Jodi oversees the field organization and provides direction for Tatum. Jodi is responsible for continuing to transform Tatum into a data-driven organizational search and consulting firm helping clients select the key financial talent they need to execute their business strategies.

Advisory • Firm Management • Security • Staffing

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.