CPA
Practice Advisor

FIRM MANAGEMENT

Now in Hackers' Crosshairs: Accounting and Finance Firms

Why the escalating cybersecurity threats for finance and accounting firms? For one, you likely have sensitive customer data, in addition to key information about their employees, vendors and customers.

Greg Dyer • Nov. 02, 2020

This has been a year unlike any other in almost every respect, and cybersecurity is no exception. Here's why the changing threat landscape could give a scare to accounting

and finance firms — and what they can do about it.

Why Hackers Have a Bead on Accounting and Finance Firms

We've been seeing a dramatic increase in malicious activity since the onset of COVID-19, with the FBI recently announcing that they're fielding as many as 4,000 cybersecurity-related complaints per day, a 400 percent increase on pre-COVID-19 levels. Also new: the extent to which firms in the finance and accounting space are being targeted. Just ask Canadian firm MNP, for example. A ransomware attack crippled the firm last spring, forcing it to cease operating for an entire week. Coming on top of broad-based pandemic-related disruption, that's way too much time for any business to be offline.

Why the escalating cybersecurity threats for finance and accounting firms? For one, you likely have sensitive customer data, in addition to key information about their employees, vendors and customers. In the eyes of a malicious actor, that looks like a "master-key" that could unlock many doors.

Keep in mind, smaller organizations of all kinds, from hardware stores to hospitals, are being targeted. Wherever less-evolved IT security practices and sensitive data come together, hackers are on notice. And with good reason, too — in 40 percent of ransomware attacks, after all, the victims ultimately pay the ransom.

The High Cost of Inaction

It's hard to overestimate the potential negative impacts of cybersecurity threats downstream. Losing sensitive financial records, tax documentation and more to malicious actors is going to cost you clients, of course, but the true costs cut deeper. For example, research shows that for companies with unfavorable reputations, hiring and retaining talent comes with an estimated $7.6 million in additional financial outlays *annually*.

To better protect your business — and your clients' data — a few simple best practices can go a long way:

- **Educate your teams:** Given that "lack of cybersecurity training" is consistently cited as among the leading causes of successful ransomware attacks, educating staff members is a key first step toward thwarting malicious actors.
- **Conduct risk assessments:** Regularly auditing the client information your firm collects and stores is especially critical if you're considering making any changes, which could open new loopholes for cyber risks.

- **Send for backup:** Retaining several different generations of backups should be sufficient to ensure business continuity in case of a breach: say, one backup for each week of the month, extending back in time for one year. Just make sure these backups are physically removed from your network — otherwise, in the event of a malware infection, your backup could be compromised.

Finally, I recommend checking out these case studies to see how digitally advanced partners can help your organization adopt best-in-class IT practices, evolve your tech infrastructure and generally stay a step ahead.

Next Steps for Accounting and Finance Firms

The good news is that organizations across the board right now are spending slightly more than one tenth of their IT budgets on cybersecurity, a strong indicator that safeguarding digital infrastructure is emerging as an increasingly clear business priority. All told, in fact, net spending in this area has increased by more than 23 percent since 2017. That's certainly an encouraging trend.

But forward-thinking, cyber-resilient accounting and finance practices must follow suit in the near term, too. Evolving your capabilities, building more advanced infrastructure, better educating teams — think of these as essential next steps in order to more effectively inoculate yourself against threats in our ever-changing cyber-risk landscape.

========

Greg Dyer leads Randstad's inhouse services concept and enterprise strategic accounts team, where he is responsible for strategic commercial sales, client delivery and account management for many of Randstad's largest clients. Greg oversees a team of strategic account directors and inhouse leaders and has a proven track record of establishing solid go-to-market strategies, setting and communicating clear vision and goals and delivering outstanding results. Under Greg's leadership, Randstad has significantly improved strategic delivery and fulfillment in many client staffing programs.

sponsor of continuing professional education on the National Registry of CPE Sponsors.