CPA
Practice Advisor

tax season captures their time and attention. Here are three cybersecurity trends that CPAs and accounting firms must address this tax season.

Jan. 31, 2022

By Isaac Kohen.

As tax professionals brace themselves for a busy tax season complicated by an ongoing pandemic, novel tax credits, and shifting workplace arrangements, they must also take action to defend against a cadre of new cyber threats.

Threat actors increasingly target accounting and tax firms. According to one analysis, reported data breaches at CPA firms have increased by 80 percent since 2014 as threat actors look to steal customer data, extract financial payments, or wreak

havoc. The costs and consequences have similarly soared. Data breaches can cost

platforms, put a data disaster just a click away. These attacks, which exploit people's ignorance, uncertainty, and familiarity, can provide threat actors with front-door access to company networks and customer data.

It's estimated that three billion phishing emails are sent each day, while phishing messages sent through SMS, frequently called "Smishing" attacks, increased 700 percent in just six months. According to Cisco's most recent three trends report, 86 percent of organizations report having at least one employee who clicked on a phishing message.

Fortunately, training works. CPA and accounting firms need to invest in comprehensive phishing scam awareness training, ensuring that their teams are prepared to identify and defend against phishing scams this tax season.

#2 Accidental and Malicious Insiders Put Data at Risk

While organizations frequently direct their cybersecurity budgets to target external threats, company insiders put data and network integrity at risk without recourse. Insider threats, including employees who accidentally misuse sensitive information and those who maliciously compromise critical data, pose a significant threat to data privacy and cybersecurity.

For example, 85 percent of data breaches involve a human element, and human error plays a signifincant role in a company's cybersecurity capacity.

To combat insider threats, CPA and accounting firms can teach and enforce cybersecurity best practices, including data management standards, personal and professional device distinctions, and digital hygiene fundamentals.

Of course, some insiders will compromise company or customer data on purpose. Often motivated by money, these malicious insiders use their privileged network

access to steal and distribute sensitive information for profit.

rely on compromised login credentials, software vulnerabilities, or malicious insiders to access company networks and encrypt critical files, can have enormous financial repercussions.

The average ransomware payment rose from $7,000 in 2018 to more than $200,000 by 2020, an unfathomable increase that should keep every organization alert and ready to respond. Meanwhile, new developments, like ransomware-as-a-service operations only heightened the concern.

Looking to maximize their victims' liability, ransomware groups frequently target organizations during peak productivity cycles. For CPA and accounting firms, this means they should be prepared for threat actors to attack their operations during tax season.

Even simple cybersecurity protocols, like regularly updating passwords and requiring two-factor authentication, can thwart threat actors. This tax season, getting the basics right can make all the difference.

Account for Cybersecurity in 2022

This is bound to be a uniquely challenging tax season even without the unique obstacles posed by a shifting cybersecurity landscape. While the threat is significant, CPAs and accountants can act not to strengthen their people, processes, and procedures to ensure that cybersecurity doesn't become an impediment to an incredible customer experience this tax season.

=========

Isaac Kohen is VP of R&D at Teramind, a leading global provider of employee monitoring, data loss prevention ("DLP") and workplace productivity solutions. Isaac is a published thought leader and recently authored the e-book "Measuring

Employee Productivity In Today's Workforce". Follow on Twitter: @teramindco and