

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

**ACCOUNTING & AUDIT**

# 2022 Digital Security and Cybercrime Update

In 2021, cybercrime cost U.S. businesses more almost \$7 billion, yet today, only 50% of U.S. businesses having a cybersecurity plan in place.

Mary Girsch-Bock • Sep. 30, 2022



In 2021, cybercrime cost U.S. businesses more almost \$7 billion, yet today, only 50% of U.S. businesses having a cybersecurity plan in place.

**ThoughtLab**, a leadership and economic research firm recently conducted a cybersecurity benchmarking study. The study, [Cybersecurity Solutions for a Riskier World](#) analyzed cybersecurity strategies, with 1,200 large organizations in 16 countries participating in the study.

According to the study, material breaches rose 20.5% from 2020 to 2021, with cybersecurity budgets rising as a direct result of those breaches. But increased budgets do not necessarily equate with preparedness, with 29% of CEOs and 40% of chief security officers admitting that their organizations remain unprepared for a large-scale cyberattack. Their reasons varied:

- 44% cited supply chain issues
- 41% cited the fast pace of digital innovation
- 28% cited inadequate cybersecurity budgets and lack of executive support
- 24% cited a shortage of talent versed in cybersecurity

How do these facts impact your firm? Keep in mind that in some states, CPA firms are held liable for any data breaches that impact their client's personal data. But even if you're not legally responsible, a cybercrime committed against your firm will directly impact your current client list as well as those looking to contract with your firm for services.

Though cybercrime threats vary, today, ransomware and phishing are considered the two top threats to businesses nationwide. If you're not exactly sure what ransomware and phishing are and the impact they can have on your business, read on.

## **Ransomware and Malware**

Ransomware is a type of malware that is used most often, infiltrating your computer system and encrypting the files so that you're unable to access the system unless a ransom is paid. If the ransom is paid, the company receives an encryption key that will allow them to access their files once again.

In many cases, businesses have resorted to paying ransom to gain access to their files. Unfortunately, paying the ransom is no guarantee that the hackers will give you access to your files.

## **Phishing**

In years past, phishing attempts were clumsy and fairly easy to detect. That's not the case today, with counterfeit communications difficult to identify. Today, there are over 150 million phishing emails sent daily.

Phishing typically lures victims in by email, with the request made to look like communication from a trusted institution such as a bank or government agency. A link is always included in the initial contact email or text, which takes you not to the site indicated, but to the hacker's site, where your personal information can be easily compromised. Because of the level of sophistication available to hackers, it can be difficult to determine the legitimacy of an email or text.

One way to check for the legitimacy of a link is to place your mouse over the link itself. This will display the hyperlink and allow you to see exactly where the link will take you.

Of course, the best way to prevent phishing is to not click on any link sent to you until you've verified it. It's also important to never respond to an email or text that requests personal information or asks for a password.

Whether your firm is small or you have offices around the world, you're vulnerable to cyberattacks. Taking the proper precautions will help keep your firm and your client data safe.

Accounting & Audit • Backup & Security • Firm Management • Technology •  
Internal Revenue Service (IRS) • Intuit • Article • cybercrime • Data Security •  
Firm Management

CPAPA 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.

© 2023 Firmworks, LLC. All rights reserved