hackers. But the threats that are most likely to affect the firm are also the ones that the firm has the most power to prevent.

Aug. 28, 2018

When thinking of cyber risks, most accounting firm leaders think about threats from hackers. But the threats that are most likely to affect the firm are also the ones that the firm has the most power to prevent.

In its annual review of cyber liability trends and losses among public accounting

Incidents involving employee action or error comprised nearly 100 percent of those incidents. "In other words, nearly all were preventable," Thompson says.

This data mirrors an April 2018 report from the Ponemon Institute and ObserveIT, showing that incidents involving negligent employees or contractors are costing companies an average of $283,281. This is based on interviews with more than 700 IT practitioners globally. The average number of incidents per company has increased from 10.5 to 13.4 since 2016.

Why are employees or insiders usually the root problem of data breaches? The top security culprits tend to be insufficient password protection, users clicking on suspicious links, lack of updated anti-virus and malware protections across all devices and use of unsecure networks, according to the Ponemon Institute. Also, threats are becoming more sophisticated with techniques to access devices and networks — and avoid detection longer. So-called fileless attacks use the device's own approved applications such as Microsoft Office applications to infiltrate network data. Still, such attacks usually require the approved user to click on a link to launch the malicious program.

In its 2018 Cost of Data Breach Study, the cost of a data breach is up 6.4 percent globally from a year ago and the average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year from $141 to $148.

What are the top tips for reducing cyber threats and liability at accounting firms? According to Kari Stern, senior claims manager with NAS Insurance in California, a partner with CPA Mutual, firms should consider:

- Having users change their secure passwords at least quarterly to access firm data;

- Ensuring that anti-virus and malware protections are active and updated on every

- more easily monitor and end access at any time; and,
- Explore end point protections through your IT vendor to defend against user errors that allow malware or ransomware through.

Accounting firms should also review their cyber liability policies to understand exactly what is covered and what is not. Some policies don't cover breaches that are due to errors by vendors or approved third parties. "The best approach is a strong defense," Thompson says. "Working on risk management on the front end will help firms catch and eliminate many more threats before a loss or claim is necessary."

Firm Management

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.