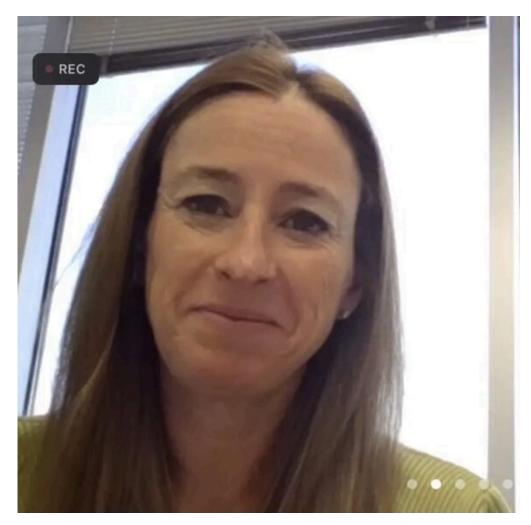# Small businesses stand in danger of cyberattacks, and here's how to keep them safer

Sandra J. Pennecke / The Virginian-Pilot
Nicole Harrell, data privacy and security chair for Kaufman & Canoles

By **SANDRA J. PENNECKE** | sandra.pennecke@pilotonline.com | Staff writer
UPDATED: April 29, 2021 at 11:34 AM EDT

"The cost of data breaches is astronomical. It is an extraordinarily expensive factor in our economy and to each of your businesses."

Nicole Harrell, data privacy and security chair for Kaufman & Canoles, laid it on the line as the featured speaker for a free webinar hosted by the Retail Alliance on April 27.

She said the average cost of a data breach in the retail industry is just over $2 million, and she shared statistics that estimate the global cost of data breaches at about $2 trillion a year.

"I think the issue here that is most surprising is the average time it takes to identify and contain a data breach is 280 days," Harrell said. "Most of the time the perpetrator is in the system for a very long period of time, going unnoticed and waiting for a particular event to occur, before they launch their attack, so to speak."

In her role, Harrell helps clients understand their risks and plan against cyberattacks. She also analyzes cyber incidents and coordinates mitigation and response plans.

During the hour-long virtual event, Harrell discussed the landscape of cyber threats and ways for small businesses to protect themselves.

"As you can imagine, the threats are constantly changing," Harrell said. "If you think of the way each of you works to evolve your business over time, the individuals who are perpetrators here are also doing the same with respect to their 'business,' albeit it is extraordinarily damaging in nature."

She said 61% of cyberattacks and data breaches target small and medium-size businesses, with 48% of these being a result of phishing or social engineering, she said.

Small and medium-size businesses are particularly vulnerable because they tend to not budget for security-type issues, Harrell said.

And that's quite alarming, since the attacks against them have become more targeted, sophisticated and severe.

"Sixty percent of small businesses go out of business within six months after a cyberattack," Harrell said. "That is a very unfortunate statistic, and I can say that we have certainly seen that over the course of time."

So, what can business owners do to protect their livelihoods?

Harrell shared the following 10 tips for small businesses:

Train employees in security principles

Protect information, computers and networks

Provide firewall security

Create a mobile device plan

Backup business data and information

Control physical access to computers

Secure Wi-Fi networks

Use best practices on payment cards

Limit employee access to data and information

Employ a password and authentication policy

"The most important thing on this list is the one at the top," Harrell said. "Training your employees is critical and absolute here when it comes to protection for small businesses."

With many employees working remotely during the pandemic, Harrell stressed the added importance of having them well-versed in risks and security best practices.

"Train them to be proactive and to not be hesitant to say 'This looks suspicious, let's look at it before we actually click or do anything with respect to it,' " she said.

Sandra J. Pennecke, 757-652-5836, sandra.pennecke@insidebiz.com

Originally Published: April 29, 2021 at 6:58 AM EDT