Small Companies Are Least Prepared for Cyberattacks

Companies with less than $10 million in annual revenue are less likely than their larger counter- parts to be prepared to deal with all kinds of cyberattacks, ransomware, malware, denial of service, credential theft, attacks on third parties and the supply chain, and more-according to the self-assessments of cybersecurity leaders at enterprises of various sizes surveyed by WSJ Pro Research.

Smaller businesses also are less likely to have cyber insurance that could help cushion the blow of an attack.

Still, smaller companies might take some comfort from the fact that only about a quarter of those surveyed said they had been the victim of a cyberattack in the previous 12 months, compared with about half of companies with more than $1 billion in revenue.

Cybersecurity experts say small businesses generally may be a less attractive target to cybercriminals because there just isn't as much to steal from them as there is from big companies.

However, the experts also say that the level of self-reported cyberattacks comes with a big caveat; many small businesses simply don't know that they've been the victim of a cyberattack, because they don't have the tools to identify one.

James Drever, a regional director in the Wyoming Small Business Development Center Network, says he frequently gets calls from small businesses that think they might have been hacked but don't know who to contact.

Mr. Drever says the vast majority of attacks he's seen against small businesses are easily preventable. About 90% of the calls he gets from hacked businesses can be traced to weak password practices, such as reusing passwords and not implementing lock- out policies, which prevent criminals from running code that endlessly guesses credentials until they get into an account.

These attacks can be simple for cybercriminals to pull *off* and they can be devastating for small businesses, says Ryan Olson, vice president of threat intelligence at Palo Alto Networks Inc.

In an increasingly common type of attack called business email compromise, cybercriminals typically get access to an executive's email account and use it to instruct a subordinate to wire money to a bank account that the criminals own. Business email- compromise scams cost companies in the U.S. $1.77 billion last year, according to data the Federal Bureau of Investigation collected from cybercrime complaints.

Written by Adam Janofsky