Ransomware attacks make dealership cyber insurance more expensive, complicated

Escalating ransomware claims are a primary factor behind cost increases and increased cybersecurity requirements this year, experts say.

December 10, 2021 09:52 AM

LINDSAY VANHULLE

AUTOMOTIVE NEWS ILLUSTRATION

Insurance carriers have tightened requirements for coverage, such as demanding dealerships use multifactor authentication.

In October, as Smith Automotive Group was in the process of renewing its cyber insurance policy, the group's controller got an email from CFO Karen Kulinich asking her to wire $190,000 from a specific account.

The invoice and the wording of the email looked legitimate, like something Kulinich would have written. Only Kulinich didn't send the email. She was at a lunch meeting and had communicated that she would be unavailable for a couple of hours. When Kulinich later checked her phone, she said, "that's when both of us just froze."

"She was one click away from sending $190,000," Kulinich said.

The incident prompted the four-store Nissan group in Georgia to talk about adopting multifactor authentication.

ABOUT CYBER INSURANCE

What it does: Generally covers the expense of responding to a cyberattack, such as a ransomware attack, and includes the restoration of data and the costs of a forensic assessment. Also covers business interruption losses and a ransom payment, if made, as well as credit monitoring for clients if data is compromised.

What's happening: Increased ransomware claims are leading to higher premiums and tighter requirements for cybersecurity controls, such as multifactor authentication.

What should dealerships do? Before an insurance renewal period, understand what providers require and adopt new or additional security measures to avoid implementation delays or loss of coverage.

Source: Automotive News research

Days later, Kulinich said, Smith's cyber insurance provider said the group would be required to have such authentication in place to obtain coverage. It was the first time the carrier had required that particular cybersecurity protocol, she said. The renewed policy, with a $1 million coverage limit per claim, also is more expensive — Smith's $4,900 annual premium rose to $12,000 for the same coverage amount.

The dealership group's experience isn't unique. Insurance carriers during the past year have tightened requirements that companies — across industries, not only dealerships — adopt new and additional security steps, people who specialize in cyber insurance told *Automotive News*. And even companies that have invested to lock down their systems are shouldering higher costs for coverage.

That's primarily because claims from ransomware incidents have escalated, said Brian Alva, senior vice president of cyber underwriting for Corvus, a commercial insurance provider that writes cyber policies for customers including dealerships.

Both the size of hackers' ransom demands and the frequency of such claims are climbing, Alva said, which has caused insurers to take a closer look at how to better assess risk and reduce the frequency of claims. That's driving many of the price increases and new security requirements, he said, including demands for multifactor authentication.

"Depending on the size and complexity of the risks, you're going to get a lot of insurance carriers, Corvus included, starting to look at kind of even more in-depth controls beyond just multifactor authentication," he said. "What type of endpoint protection are they using? What does their backup strategy look like? Is it resilient enough to withstand a ransomware attack?"

Alva: Controls “more in-depth”

Companies struggling to obtain coverage in the current market generally fall into two buckets: those that have experienced multiple cyber incidents and haven't taken steps to prevent future events, and those that haven't experienced a security breach but also haven't invested in "the new baseline controls that the market's requiring," Alva said.

RELATED ARTICLE

How cyberattacks disrupt the auto supply chain

Service backlogs

Demand for upgrades of dealership systems to meet insurers' requirements has created a backlog of requests from existing and prospective customers for security consultants who work with dealerships.

"We're backlogged well into '22," Proton Technologies CEO Brad Holton said. His company received three calls in one week after Proton's name was mentioned by a dealer during a peer group discussion about ransomware, he said.

A retailer with 35 to 40 stores hired Proton in August because it was unable to obtain cyber insurance, Holton said. Proton worked with the insurance provider to demonstrate that additional protocols would be in place within weeks and months while noting that the group needed coverage sooner.

"Even then, it was an elevated premium," Holton said. "It's just totally different. Two years ago, it was no problem for anyone to get cyber insurance."