

SPECIAL FOCUS ON THE HIGH NET WORTH MARKET PAGE 8

Modern Ransomware Operations Take Corporate Approach to Extortion

Incident Response Plans, Vendor Management Critical to Cyber Security Preparedness

MIDDLETOWN, R.I. — Insurance agencies and other small businesses face increasing threats from cyber criminals that can disrupt operations, compromise sensitive information, cause reputational damage with clients and result in significant financial harm. Two cyber security professionals provided insights into what happens during and after a

cyber event and what small businesses can do to best prepare for increasingly sophisticated ransomware attacks.

In 2025, more than 3,600 ransomware incidents were reported to the FBI's Internet Crime Complaint Center, the central hub for reporting cyber crime. Health care was the most targeted sector

with 460 attacks and 182 data breaches reported. More than one million cyber security complaints were filed overall — a 26% increase from 2024 — with total reported losses in excess of \$20 billion.

Sixty-three new ransomware variants emerged in 2025 alone.

“In the ransomware landscape, where we used to see maybe a dozen ransomware operators, we’re seeing that number blow up,” said Chris Loehr, executive vice president and cofounder of Cyrenity Cyber. “It seems like almost every week to two weeks, there’s a new ransomware group that comes up with a creative name.”

Taking a Corporate Approach to Extortion

Today’s top ransomware groups have evolved from lone actors into highly organized syndicates by taking a corporate approach to cyber crime.

Spencer Pollock, CIPP/US, CIPM, data privacy and cyber security attorney at McDonald Hopkins, explained that there are three different levels of ransomware groups: mother ships, affiliates and nonaffiliates.



Chris Loehr (left), EVP and cofounder of Cyrenity Cyber, and Spencer Pollock (right), data privacy and cyber security attorney at McDonald Hopkins, gave a cyber presentation at the Independent Insurance Agents of R.I. InsureCon 2026.

The mother ships name themselves, create a ransomware virus and set up a corporate-style structure. “They have CEOs, COOs, CTOs, help desks and HR, and they go out and do recruitment,” said Pollock.

The mother ships recruit affiliates who are interested in distributing the virus. When someone shows interest, that person provides credentials, including references, so the crime syndicate can have a degree of certainty of competency and that its rules will be followed. For example, the deal could be that if the cyber criminal infects a company with ransomware and gets paid by the victim, the mother ship would receive 20% of the ransomware payment. The cyber criminal might have to agree that if the victim pays the ransomware, he will provide a key to unlock the data, not share the data on the dark web and will delete any stolen data.

The last group is nonaffiliates, which Pollock noted are becoming increasingly popular. These rogue actors use open-source digital tools to construct a virus. They differ from mother ships in that there is no accountability to anyone for their actions — and they are more difficult to stop.

“You might take down the group, but then [someone] in the group spins off and uses the virus to continue attacks under a new name,” said Pollock.

Loehr added that the FBI will stop a group’s ability to perform its work, but typically the crime syndicate will keep a low profile for a few months, rebrand themselves and start over again.

“It’s really difficult for law enforcement to actually find the individuals behind these groups and bring them to justice. A lot of them right now are in Russia, and there’s not a chance in hell that Russia is going to give up anybody to us,” said Loehr.

Case in point, Conti was a major Russian-linked ransomware group that was active from 2019 to 2022. It operated like a corporation and extorted over \$180 million in 2021 alone. It dissolved in 2022 following internal leaks, but its members dispersed into other cybercriminal operations.

“Think of Conti like IBM. Everybody in the tech world has some kind of line back to IBM. The same thing goes with Conti. They were the masterminds behind this, and they’re the ones that monetized it at scale. A lot of people are still affiliated with them directly or indirectly or are spin-offs, but most of them are using lessons, tools and techniques that they learned from Conti,” said Loehr.

A Small-Business Ransomware Attack

When a small business experiences a ransomware attack, there is typically no warning. The owner or employees find out something is wrong with the computers when they receive a note about how to communicate with the hacker.

In the ransomware landscape, where we used to see maybe a dozen ransomware operators, we’re seeing that number blow up. It seems like almost every week to two weeks, there’s a new ransomware group.

— Chris Loehr,
Cyrenity Cyber

Most small companies use third-party IT providers — called a managed service provider (MSP) — and that would typically be their first call. Sometimes MSPs know what to do, but not always, noted Loehr.

If the small business has cyber insurance, they will call into a hotline manned either by a law firm or an incident response firm. Then legal counsel will be brought in.

“Five to seven years ago, not every incident needed legal help, but with the regulatory and litigation environment that we live in now, we want to make sure every [communication] is privileged,” said Pollock.

While all data breaches begin as data incidents, not all incidents develop into a full-blown breach, which is an important legal distinction based on whether sensitive information was accessed or obtained, noted Pollock.

If data was accessed, it could lead to individual and regulator notifications.

“The very worst-case scenario is that it leads to litigation, class-action litigation

or regulatory investigation,” said Pollock. “I bring this up with a client within the first five minutes because they need to understand, and I need them to shift their mentality because we all need to operate in anticipation of litigation. When we do that, I can retain an expert on the client’s behalf and direct the investigation.”

All of the calls and email communication would then be considered privileged and protected if there is class-action litigation or a regulatory investigation.

“A lot of SMEs [small- and medium-sized enterprises] think they aren’t going to get sued because they aren’t a big company and a regulator isn’t going to care about them. This is not the truth anymore. We’re getting class-action litigation for 100 or 1,400 people [being affected],” said Pollock. “These are conversations to have with your clients, especially if you’re helping place insurance policies for cyber.”

With the average data breach costing more than \$4.2 million, cyber insurance is an important way to help defray costs and connect insureds with the proper cyber security professionals.

In addition, insureds can meet with cyber security experts before they have an incident.

“You need to trust our guidance, and that’s hard to establish when you’re in crisis mode. So, doing everything beforehand and understanding who you’re going to work with is very important,” said Pollock.

Building a Risk Strategy

Having the right advisors in place is part of having an effective risk management plan that includes frequent password changes and multifactor authentication.

Historically, the number one failure on the part of organizations has been their inability to properly secure identities (usernames and passwords). People did a “terrible job” of setting strong passwords and implementing multifactor authentication, noted Loehr.

Recently, there has been a shift to system vulnerabilities as the number one cause of breaches. The vulnerabili-

ty could be a computer but is more typically a firewall issue.

“It could be something on the cloud that the bad guys know about — and they know about it ahead of you. So they exploit those vulnerabilities to gain access to your network, or it could be something that you actually knew about, but didn’t do anything about, which happens a lot, too,” said Loehr.

In addition, it is important to have digital file backups to help protect against data loss; however, it has to be an “immutable backup,” that is completely separate from the rest of the network. Ransomware criminals look to delete backups, so it is critical that they are not

connected to the same network.

“We were working with someone who had backups separated, but they used the same username and password as the regular network, so that defeated the purpose,” said Loehr.

Pollock noted that incident response plans should be practiced, so it is clear who should be involved both internally and externally.

Vendor management is essential as well. As businesses become more dependent on third-party vendors, cyber security risks increase. Vendors often have access to sensitive information or have shared access into certain systems.

“While it’s great for everyday use and practicality, it’s horrible for security because now you not only have to look at your own security controls, you have to make sure your vendor is taking care of those security controls as well,” said Pollock.

He noted that the 2014 breach of Target started with a small HVAC vendor’s payment portal.

While few people remember the name of the HVAC company, everyone knows who Target is, added Pollock. “Your clients, employees and stakeholders don’t care who your vendors are. They care what you’re doing to ensure your vendors are taking those proper precautions.” ■

Reprinted by permission of Standard Publishing Corp. © 2026.

To subscribe to *The Standard* and stay up-to-date on what's happening in New England insurance, please go to www.spcpub.com or call 617-457-0600.