CYBER SECURITY

RANSOMWARE ESCALATES: PHYSICAL THREATS AGAINST CEOS

A NEW SURVEY has found that in 40% of ransomware incidents in the U.S., CEOs or other executives were physically threatened if their organizations did not pay the ransom demanded by hackers.

The findings in Semperis' "2025 Ransomware Risk Report" highlight other pressure tactics, such as ransomware criminals threatening to file regulatory complaints to force payment. The study's findings emphasize the need for businesses to remain vigilant against ransomware threats that can completely shut down their networks and websites until they pay ransom.

Ransomware threat growing

- 78% of firms reported being targeted within the past 12 months.
- 55% of those that paid a ransom did so more than once, with 29% paying three or more times.
- 15% of firms that paid never received usable decryption keys, or received corrupted ones.
- 23% recovered within a day, while 18% needed up to a month.

Source: Semperis' "2025 Ransomware Risk Report"

New tactics

Physical threats – Ransomware actors are resorting to extreme measures to pressure victims into paying, including threats of physical harm to business executives. In the past 12 months, 40% of incidents involved physical threats against executives, according to the Semperis report.

Threats of reporting to regulators – In 47% of attacks, ransomware criminals threatened to file regulatory complaints against victim companies if they refused to pay.

Other tactics – In early 2025, Cisco Talos reported that the Chaos ransomware group threatened additional damage by launching DDoS attacks and spreading news of the breach to competitors and clients if payment was withheld.

What businesses can do

- Address vulnerabilities and strengthen defenses to improve the ability to recover if an attack occurs.
- Regularly back up your data to an offline or secure location.
- Train staff to spot e-mails that may contain ransomware and avoid opening attachments or clicking on links from unknown or suspicious senders.
- Ensure your organization has well-documented, clearly communicated crisis response and recovery processes, and practice them in test scenarios that mirror real-world conditions.
- Hold vendors and partners with system access accountable to the same security and recovery standards you require internally.
- Install updates to your operating system, web browsers and other software as soon as they become available.

The takeaway

Even companies with solid defenses are penetrated. Consider purchasing cyber insurance, which can help your organization recover from a ransomware hit or other cyberattack. In some cases, the insurer can help you avoid paying the ransom without compromising your ability to continue operating.

If you have questions about cyber insurance, give us a call.

Continued from page 1

CT Claims Are Spreading from Southern California

The Rating Bureau found in a recent report that post-termination CT claims were initially less costly, but the longer they stay open, the more quickly costs accelerate.

That's compared to regular CT claims filed by workers who are still working for their employer, which start off more expensive but tend to develop more slowly over time.

The takeaway

While these claims have long been a persistent problem in Southern California, they are spreading to other parts of the state, including the Bay Area and Sacramento, Katherine Antonello, CEO of Employers Holdings, said during the company's earnings call in August 2025.

They've become such a burden on the system that California Insurance Commissioner Ricardo Lara acknowledged the rising frequency of these claims when approving a recent workers' comp benchmark rate increase.

Employers should strive to reduce the risk of repetitive motion and cumulative injuries as part of good safety practice. At the same time, it's important to document all injuries and near misses.

If a CT claim is filed, employers should conduct thorough investigations, meticulously document workplace hazards and training, and assess possible links between the injury and work.

Also check with your insurer to ensure the claim was filed within the state's statute of limitations, which is one year. For post-termination claims, the clock starts on the worker's last day of employment.

For claims by active employees, the statute of limitations has not yet begun.