Ransomware Fallout

Firms That Pay Ransom Often Hit Again

A NEW REPORT found that one-third of companies who are hit with ransomware and pay the hackers to unlock their systems, are often likely to be targeted a second time.

And after they pay, they are often faced with significant consequences, including system rebuilding costs, their data still being leaked and financial consequences, according to the "2022 Cyber Readiness Report" by Hiscox. The eye-opening results of the study come as the number of businesses hit by cyber attacks continues growing.

Considering the potential damage to your organization if your systems are compromised in the aftermath of a ransomware attack, even if you have cyber insurance to pay recovery costs, it's best to take steps to thwart attacks in the first place.

More than ransom

It's clear that paying a ransom often doesn't mean the recovery for an affected business will be smooth, according to the report, which covers the poll results of 5,000 organizations.

Paid Ransom; Problems Persist

- 36% of organizations that paid the ransom were hit again within 12 months.
- 41% of companies that paid the ransom and received the recovery key ended up with incomplete databases and were still forced to rebuild their systems.
- 29% of firms that paid the ransom demand still had data leaked.
- 26% of businesses paid a ransom in the hope of recovering their data because they did not have any back-ups.
- 26% of businesses hit by ransomware said the attack had threatened the solvency and viability of their operation.

The risk

Nearly half (47%) of firms reported that they had been hit by a cyber attack during the past 12 months, up from 40% in 2021. Of those who were attacked, 17% were ransomware victims.

The median cost of an attack has risen 29% to just under $17,000.

Small firms can no longer expect to fly under the radar as the criminals increasingly have them in their sights.

What you can do

Some firms have little exposure to a cyber attack, particularly if they don't handle customer data or are not tech-driven operations. Each firm has a different exposure level.

For companies that have cyber exposure, protecting their organization requires a multi-pronged approach that includes cyber insurance and strong data security protocols.

Cyber insurance may cover the cost of a paid ransom as well as recovery and rebuilding costs. If your organization has exposure, please give us a call to review your risk and see if cyber insurance is right for your business.

Besides that, Hiscox recommends taking a number of steps to protect against an attack and be able to recover from one faster:

- Keep all of your software up to date to include the installation of all the latest security patches.
- Frequently back up your data on a server that is not hooked up to the cloud.
- Train workers on how to recognize and avoid common social engineering attacks that criminals use to trick them into revealing sensitive information about themselves or their company.
- Teach your staff how to detect potentially dangerous e-mails that try to get them to click on a malicious link that can unleash ransomware or other malware. ❖