The Cost of a Ransomware Goes Beyond the Ransom Paid

One of the fastest growing cyber threats to businesses is ransomware, which hackers use to shut down an organization's computer system until the victim pays a ransom to unlock it.

While most organizations focus on the cost of the ransom, which can easily run into the tens of thousands of dollars, the costlier damage is to the company's operations, which can be hampered or completely shut down after their systems are rendered unusable.

Ransomware is one of the fastest-growing cyber threats and attacks are expected to grow 240% in 2022 from the 2021, making it vital for your organization to have in place systems to reduce the chances of becoming victimized.

Ransomware typically enters a company's systems after an employee clicks on a link in a rogue e-mail, which allows the malicious code to infect the company's systems and eventually shut them down, locking out all users and making all or some of the data inaccessible. After it has frozen the systems, it will demand a ransom to unlock it.

According to a survey by Hiscox, the bulk of ransomware attacks lead to business interruption losses:

- Corporate loss of business income or services: 36%
- Corporate loss of digital assets: 16%
- Corporate loss of financial assets: 3%
- Breach of personally identifiable information: 25%
- Breach of personal financial identity: 17%
- Breach of personal health information: 3%

But, experts believe that a significant portion of ransomware attacks go unreported, making it difficult to get a grasp on the full effects.

And while most states have laws requiring organizations to report privacy breaches, that's not true for ransomware attacks.

The full damage

In the 2021 the average ransomware payment was a record $570,000, which compares to $312,000 in 2020, according to figures released by the Unit 42 security consulting group.

But the ransom is only part of the story, as most businesses also have to contend with:

- The cost of lost productivity
- Lost profits
- Harm to business reputation
- The cost of reconstructing data

Ransomware typically targets your most important data, but sometimes it just makes your entire system unusable. It may also lock down your marketing materials, payroll data, intellectual property, financial transactions and health records.

Some companies try to beat the hackers by hiring outside professionals to decrypt all of the information that the ransomware perpetrators have frozen.

But that's a risky proposition because it often leads to incomplete data recovery. Full recovery is usually only possible with the decryption key.

Ransomware criminals who are not paid will often destroy the key, leaving affected companies in a more serious bind.

If you're lucky, a ransomware attack may only be confined to one server or computer. But if it hits the right servers, it can spread throughout your organization to all users and, if you are connected with vendors or partners, it can even spread to their systems.

There are a number of tactics that ransomware criminals use, such as:

- Holding the data hostage
- Threatening to disclose confidential or proprietary information
- Threatening to sell or auction confidential or proprietary information

Controlling risk

CFO magazine recommends that you do the following to reduce the risk of being hit by ransomware:

- Train and educate personnel on an ongoing basis.
- Specifically address and plan for ransomware in your disaster recovery and business continuity plans, including testing of those plans.
- Ensure that all anti-virus and other security software is properly updated. This software will detect and eliminate many forms of ransomware.
- Engage a third-party expert security vendor to assess your organization's systems and procedures.

If you suffer a ransomware attack, you should:

- Identify and isolate infected and potentially infected systems.
- Disable shared network drives connected to the infected systems.
- Consider suspending regular backups of those systems to prevent the virus from spreading further.
- Engage an information security consulting firm that specializes in assessing and mitigating these sorts of attacks.
- Send out a memo to all your staff warning them of the infiltration and to not open e-mail and attachments from suspicious sources.

Insurance

Cyber insurance can help pay for the effects of a ransomware attack. Depending on the insurer, some policies will pay the ransom, while others expressly exclude it, citing the "moral hazard" of such coverage.

If you are concerned about the damage a ransomware attack could inflict on your organization, call us to discuss your cyber insurance options.

###