CYBERSAFE SOLUTIONS

The Cost of a Ransomware Attack

A ransomware attack is similar to a digital hostage situation. Cybercriminals leverage malware to encrypt or lock users out of their computer network and withhold data. They only regain access when a payment is made, usually by a deadline—but even then, many victims never receive their restored data at all.

Ransomware By The Numbers

- The average global cost of a data breach was **$4.54 million** in 2022, according to IBM's 2022 "Cost of a Data Breach" report.
- Ransomware-caused breaches have spiked by **41%** in the past year alone, IBM continues.
- Most companies take **nearly six months** to detect a data breach, even major ones.
- **Nearly a third (31%)** of businesses fail after falling victim to ransomware, according to freemium VPN service Atlas VPN.
- The human element plays a significant role in **82%** of breaches, finds Verizon's 2022 Data Breach Investigation Report (DBIR)—making active prevention not only possible, but crucial.

The Cost & Recovery of a Ransomware Attack

- In the United States, the cost of a data breach is **$9.44 million**—an astounding $5.09 million more than the global average, IBM continues.
- The file decryption process can take **days to complete**, and must be done by experts.
- **75%** of businesses are without their files for two or more days, and **30%** are without them for five days or more.
- This sacrifices **weeks of productivity** as the business recovers.

Steps to Prevent A Ransomware Attack

Below are some best practices organizations can follow:

- Always consult your trusted IT advisor and cybersecurity specialist.
- Test your back-up system to ensure a quick recovery, but do not rely on back-ups alone.
- Conduct a thorough risk assessment.
- Develop security policies.
- Enhance employee security posture with SOL Security Awareness Training and Simulated Phishing Tests.
- Implement 24/7/356 continuous cybersecurity monitoring—the most critical step.

The Repercussions May Not End There

An emerging risk is making recovery even more expensive for businesses. Cybercriminals have begun downloading copies of victims' files and threatening to publicly release them if the ransom is not paid. This creates new potential for third-party claims and other complications from the data breach—making active prevention the best defense against ransomware.

Benefits of Continuous Monitoring

Costs of a Cyber Attack	Benefits of Continuous Monitoring
Sacrificed Productivity	Real-Time Alerts
Financial Losses	Proactive Prevention
Legal Fees	24/7/365 Threat Intelligence
Damaged Customer Trust	360-Degree Visibility
Potential for Repeat Attacks	No Log Review Delay

About Cybersafe Solutions

Cybersafe Solutions is an industry-leading Security Operations Center-as-a-Service (SOCaaS) provider offering unmatched threat detection, response, and containment for your network, endpoint, and cloud environments. With 20 years of experience in the online threat landscape, Cybersafe leverages top-tier threat intelligence and cutting-edge technology to protect your most important assets.

www.cybersafesolutions.com | 1-800-897-CYBER (2923)