Understanding Ransomware: The Costly Threat and How to Combat It

WHAT IS RANSOMWARE?

Ransomware is malicious software that encrypts data and demands a ransom to restore access. It can target individuals and organizations and is often spread via phishing emails or compromised websites.

FREQUENCY

In 2023, a new organization falls victim to ransomware every

10 SECONDS

GLOBAL RANSOMWARE COSTS

Expected to surpass **$30 billion in 2023**, up from **$20 billion in 2022**. Projections indicate damages could reach **$265 billion by 2031**

KEY STATISTICS

37%

AVERAGE RANSOM DEMAND

In 2023, the average demand surged to **$5.3 million, a 37% increase from 2022.**

DATA RECOVERY

Only **59%** of organizations **fully recovered** their data after paying a ransom, despite **78% making payments.**

ATTACK VECTORS

PHISHING

90%

of ransomware attacks in 2023 began with phishing emails

ENCRYPTION & DATA EXFILTRATION

In **84%**

of attacks, data is both encrypted and exfiltrated.

SECTORS AFFECTED

HEALTHCARE

34%

of ransomware attacks in 2023 targeted healthcare, causing life-threatening delays.

SMEs

43%

of attacks targeted small and medium-sized enterprises, often unprepared to handle such threats

SIGNS OF RANSOMWARE INFECTION

UNUSUAL SYSTEM BEHAVIOR

Files become inaccessible or display strange extensions like ".locked" or ".crypt."

STRANGE NETWORK ACTIVITY

Take immediate action if alerted by antivirus software

ANTIVIRUS ALERTS

Unusual outbound traffic could indicate communication with a ransomware server.

RANSOMWARE DEFENSE STRATEGIES

RECOGNIZE PHISHING ATTEMPTS

Verify email senders and avoid downloading suspicious attachments.
Example: An employee noticing a slight error in a sender's email address avoided downloading malicious attachments.

USE STRONG PASSWORDS AND MFA

A retail company avoided an attack by implementing Multi-Factor Authentication (MFA), preventing access even after credentials were stolen.

REGULAR BACKUPS

69% of organizations successfully restored data through backups, highlighting the importance of regular backup practices.

AVOID PUBLIC WI-FI

Use a Virtual Private Network (VPN) to protect sensitive data when outside the office.

CYBERSECURITY SPENDING AND TALENT SHORTAGE

$219B IN 2024

Global cybersecurity spending is projected to reach $219 billion in 2024.

3.4 million PROFESSIONALS

A global shortage of 3.4 million cybersecurity professionals by 2024 poses a challenge to defending against ransomware attacks.

CONCLUSION

To mitigate ransomware risks, organizations must implement robust email security, use MFA, ensure regular backups, and maintain up-to-date cybersecurity practices. Cyber insurance can also provide a safety net, with 77% of ransomware incidents covered by policies in 2023.

Talk to your Paramount representative or email
Marketing@paramountassure.com