U.S. Risk, LLC

SPOTLIGHT ON RANSOMWARE

Ransomware has become increasingly sophisticated, specialized and often incredibly difficult to prevent. This form of cybercrime involves hackers breaking into computer networks and locking up digital information until the victim pays for its release. Larger companies have been the primary target assumably because they have deeper pockets, but cybercriminals are increasingly attacking smaller organizations because they typically have less security in place. While ransomware is on the rise, there are ways to dramatically reduce if not eliminate the threat.

RANSOMWARE TRENDS

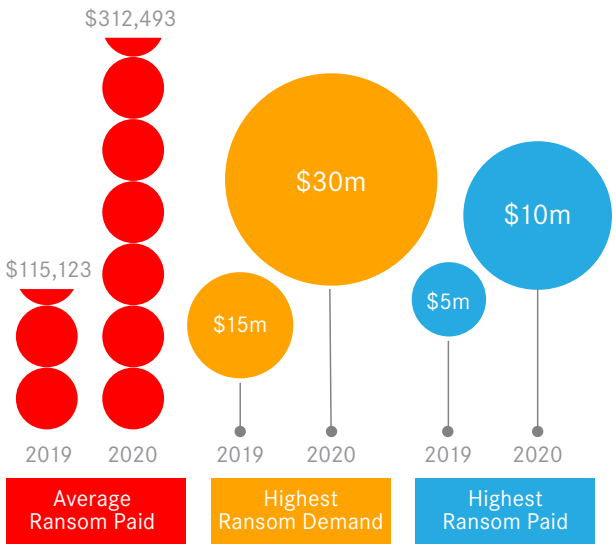
- Payments are soaring. The average ransomware payment nearly tripled last year as compared to two years prior.
- Paying a ransom doesn't guarantee data recovery. One survey found ransom was paid in about one-third of cases. However, only a tiny percentage got all their data back, and nearly a third couldn't recover more than half the encrypted data.
- There is a rise in double extortion. This is when an attacker seizes data and demands payment. If payment isn't made, the attackers will publish the data in an attempt to damage or embarrass the victim. In an increasing number of cases, it seems the demand for payment is really in return for not leaking stolen information online.
- Cost of ransomware recovery has doubled, with the average total cost of recovery estimated to be ten times the average ransom payment.
- Lawsuits being filed over small incidents are growing: more cases are seeking early settlements.

› Proliferation of Ransomware

Experts predict there will be a ransomware attack every 11 seconds in 2021 and that the global cost associated with ransomware recovery will exceed $20 billion. By 2025, organizations will invest more than $1 trillion in their cybersecurity.

› Ways to Reduce Your Risk

The most basic approach should include developing a companywide focus on security, an incident response plan and a separate backup system for data. In every ransomware event to date, it appears at least one (or more) of the following causes was to blame: no endpoint detection and response (EDR) strategy, ineffective backup solution/implementation, and open remote desktop protocol.



- Implement Social Engineering/Phishing training to all employees, at least annually
- Implement email filtering solutions
- Implement Multi Factor Authentication (MFA) in the following areas:
  - ◊ Privileged User Accounts
  - ◊ Remote Access to Computer Systems by Employees
  - ◊ Remote access to Computer Systems by Vendors and Independent Contractors
- Implement Endpoint Detection & Response (EDR)
- Implement a Patch Management Program
- Implement Daily Backups and Encrypt Backups
- Implement Network Segmentation both physically and virtually
- Disable all Remote Desktop Protocol ports (RDP) and Remote Desktop Gateways (RDG)
- Implement Use of Net Generation Antivirus Software (NGAV)
- Implement External Penetration Testing, at least annually

› The Final Safety Net

While cyber insurance cannot act as a replacement for the security measures all companies should be implementing, it can help organizations with a financial safety net as well as proactive risk mitigation and management resources.

SPOTLIGHT ON RANSOMWARE

TOP 10 CYBER INSURANCE TRENDS

1. Cyber claims are growing in number and complexity
2. External attacks are causing the most expensive losses, but internal accidents are occurring more frequently
3. Business interruption is becoming the main cost driver behind claims
4. Remote work and COVID-19 have heightened exposures
5. Ransomware incidents are becoming more frequent and financially damaging
6. Business compromise email attacks are surging
7. Regulatory exposure is increasing around the globe
8. Class action litigation is rising
9. M&As are introducing cyber risk
10. Nation state-sponsored attacks are increasing

GLOSSARY OF TERMS

Multi Factor Authentication (MFA)

An electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. MFA protects the user from an unknown person trying to access their data such as personal ID details or financial assets.

Endpoint Detection & Response (EDR)

Also known as endpoint threat detection and response (ETDR), EDR is a cyber technology that continually monitors and responds to mitigate cyber threats.

Patch Management Program

Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (“vulnerabilities” or “bugs”) in the software.

Network Segmentation (physical and virtual)

Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network.

Remote Desktop Protocol (RDP) or Gateway (RDG)

A Windows server role that provides a secure encrypted connection to the server via RDP. It enhances control by removing all remote user access to the system and replaces it with a point-to-point remote desktop connection.

Next Generation Antivirus Software (NGAV)

Detects, responds to and prevents all kinds of cyberattack tactics, techniques and procedures (TTPs).

External Penetration Testing

External penetration testing is a security assessment of the perimeter systems. External penetration testing usually tests from the perspective of an attacker with no prior access to your systems or networks.

THE BOTTOM LINE

Preparation is key when it comes to cybercrime prevention and loss controls. A trusted insurance expert highly experienced in all the various forms of cybercrime and how to insure them needs to be brought into the process as early as possible to ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.