Ransomware: a call for enhanced resiliency

Ransomware is a dynamically evolving risk, impacting organizations around the world with rapidly increasing loss frequency and severity. AIG's insights are intended to focus conversations around loss preparation and risk management, and help guide well-informed cybersecurity investments.

Cybercrime, and specifically ransomware, is growing exponentially.

By 2025, Global cybercrime damage costs expected to reach $10.5 trillion. A ransomware attack on businesses predicted, by 2021.

Ransomware is rapidly evolving, fueled by the rise of:

- Ransomware as a Service (RaaS)
- data exfiltration prior to encryption
- deeper, more invasive attacks

Sophisticated cyber resilience is imperative, and companies need to continuously adapt in this changed threat environment.

Network outages and business interruption are lasting longer. AIG observed a typical outage length of 7-10 days from global ransom & extortion claims.

The demand and cost for forensics, recovery, legal counsel and other response services is at an all-time high given the volume of attacks.
Ransomware claims have increased significantly in frequency and severity in recent years and continue to evolve.

**150% Increase in frequency**

AIG has seen an increase of more than 150% in frequency of ransom and extortion claims notifications since 2018.

All sizes of company are impacted by ransomware, across all types of industries.

Ransom and extortion claims accounted for 1 in every 5 cyber claims in 2020, up from 1 in every 10 cyber claims in 2018.

**Demand values can be in the tens of millions of dollars with payments varying depending on the characteristics of the attack.**

When data was exfiltrated prior to encryption, ransom and extortion claims costs were 2x higher.

**Losses may impact multiple coverage sections: extortion, event management, network interruption, security & privacy.**

Data sourced from AIG cyber claims analysis, Q3 2020

---

Ransomware victims have similar deficiencies in controls for managing ransomware risk.

**Key controls:**

- Use strong authentication controls for all administrative access where possible, and deploy compensating controls where it’s not
- Deploy modern endpoint controls and timely remediate vulnerabilities
- Enable appropriate active directory controls and understand / verify your attack surface

We encourage you to visit www.cisa.gov/ransomware for additional actions and resources available to your organization to address ransomware.

AIG, as a global cyber insurance market leader, is committed to helping clients improve their resilience against ransomware and other cyber threats. Contact your local AIG cyber team member to learn how.