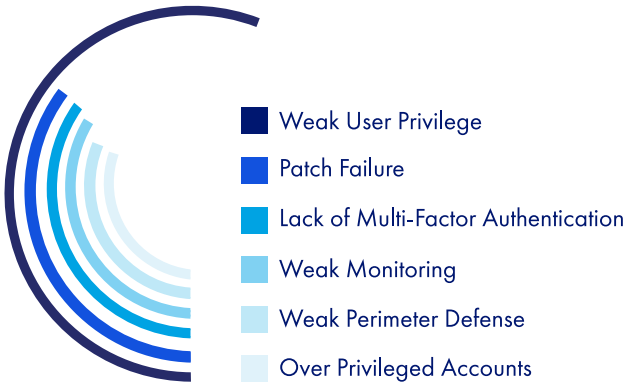
2024 Ransomware Threat Insights

AIG has provided cyber risk insurance since 1999 and, over its two-plus decades of experience, has accumulated invaluable insights into the ever-evolving ways cyber criminals launch attacks, gain access to, and interrupt organizations. In today's ever-evolving claims environment, we share these insights to help our clients and brokers better understand and manage their exposures.

Vulnerabilities Leading to Incidents

More than 60% of ransomware incidents are linked to Weak User Privilege, which is when organizations fail to appropriately protect privileged accounts.

Leading Causes of Incidents



Key Takeaway

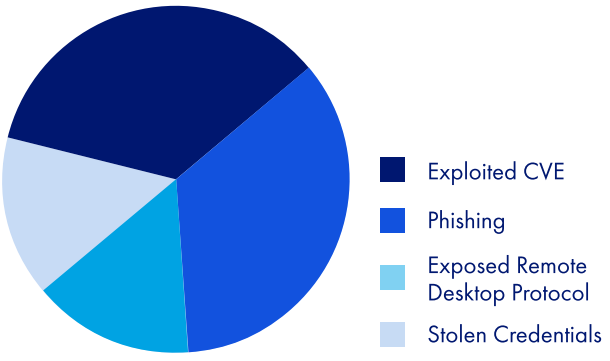
Organizations need to understand and correctly manage privileged accounts by regularly auditing user privileges and following the principle of least privilege. Each account is given the minimum level of access or permissions needed to perform their job function.

How Cyber Criminals Are Getting In

Phishing and Common Vulnerabilities and Exposures (CVE) are the leading ways cyber criminals are launching attacks.

45% of organizations reported exploitation of CVEs as the initial attack vector in 2023, a 26% increase from 2020.

Leading Attack Vectors



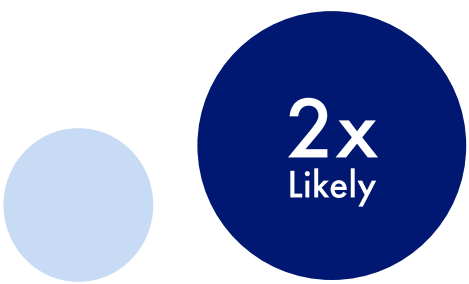
Key Takeaway

With a focus on exploitation of vulnerabilities by threat actors, organizations must develop their capability to prioritize critical CVEs and improve their maturity in conducting risk-based vulnerability management to ensure that the most critical vulnerabilities are promptly patched and remediated.

Managing Cost and Business Interruption

When an organization's backup data is affected during a ransomware incident, the average critical business interruption loss of hours increases by 65%.

Likelihood of an Organization to Pay a Ransom



Unaffected Backups

Affected Backups

Key Takeaway

A strong ransomware protection strategy that includes securing backup data via redundancy, different media storage, and offline storage is critical to outcomes in a ransomware attack, both in terms of cost of business interruption as well as ransom payment. Organizations should also employ incident response protocols that define roles and responsibilities in an event and hone those capabilities through tabletop exercises.

METHODOLOGY

These observations are based on aggregated AIG's Root Cause Analyses and Incident Dialogue data, comprising of both AIG clients as well as non-AIG clients, collected from Jan 2021 to Dec 2023. The total number of organizations sampled were 344. Approximately, 75% of the sampled organizations had an annual revenue >$100M. The dataset consists of global data and is limited to ransomware incidents.

To learn more about AIG's cyber solutions, contact your local AIG Financial Lines Underwriter or visit www.aig.com/cyber.