



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.



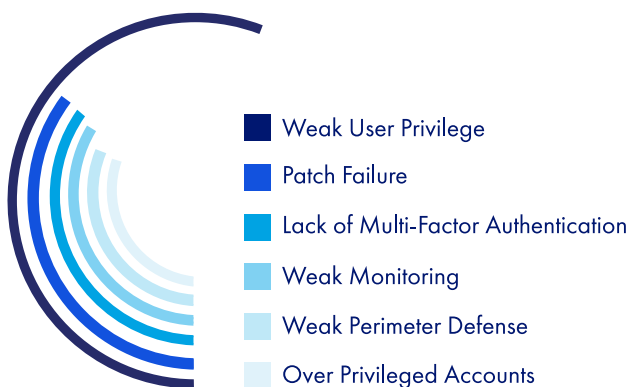
How Cyber Criminals Are Getting In



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.

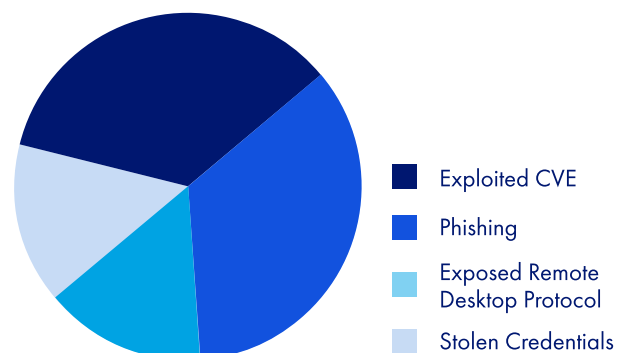
Leading Causes of Incidents



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.

Leading Attack Vectors



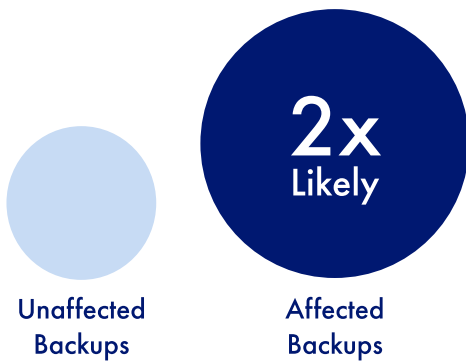
Key Takeaway

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



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.

Copyright ©2024 American International Group, Inc. All rights reserved.

This document is provided for information purposes only and has no regard to the specific situation or particular needs of any specific person or entity. It is not intended to be a complete statement or summary of the matters or developments referred to herein. You should not regard this document or the contents herein as a substitute for the exercise of your own judgement. All information is current as of the date of this document and is subject to change without notice. AIG is under no obligation to update or keep such information current. No representation or warranty, express or implied, is made as to the accuracy, reliability, usefulness or completeness of the information.

American International Group, Inc. (NYSE: AIG) is a leading global insurance organization. AIG provides insurance solutions that help businesses and individuals in approximately 190 countries and jurisdictions protect their assets and manage risks through AIG operations and network partners.

AIG is the marketing name for the worldwide property-casualty and general insurance operations of American International Group, Inc. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions, and coverage is subject to underwriting requirements and actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.