Brown & Brown

PROPERTY & CASUALTY

MOVEit and More Critical Vulnerabilities

A Matter of When, Not If

Aggregate Risk in the Cyber Insurance Market

Major supply chain attacks such as SolarWinds, Microsoft Exchange, Log4Shell and, most recently, MOVEit, have shifted how cyber insurers examine aggregated risk. These risks raise concern around aggregation-type losses and have consistently increased over the past 12-24 months. As technology and threat actor capabilities evolve, the cyber insurance market and those seeking cyber coverage must continue to be diligent.

The scope of a supply chain attack could be significant. A single attack vector, such as a critical vulnerability exposure on a server, can compromise an entire customer base hosted on or interacting with that server. For insurance carriers, the consequences of exposure to such a widespread vulnerability could be fatal. If a breach impacts a large number of their insureds, an insurer's entire portfolio could be liable to pay hundreds of millions of dollars in claims overnight. Given the potential risk, the insurance market has taken extensive preventative measures by implementing mitigation strategies, modifying policy language, scrutinizing more specific areas of concern and sometimes tightening their underwriting requirements.

As insurance carriers rush to adapt and find equilibrium in the ever-changing threat landscape, customers seeking to purchase or renew cyber coverage should work closely with their broker to solidify their controls and help ensure market interest. Proactively communicating with a broker about areas of underwriter concern, having a comprehensive overview of patch management and typical timeframe, and staying up to date on and applying the latest critical vulnerability patches are imperative for a seamless renewal process.

The MOVEit Vulnerability: A Case Study on Cybersecurity Risks and Implications

MOVEit Transfer is a widely used file transfer application developed by Progress Software. It facilitates secure and efficient data exchange between parties. In May 2023, security experts identified a critical vulnerability in the MOVEit Transfer web application front end, enabling administrative access and SQL injection attacks.

The CI0P ransomware group, a criminal organization that operates for financial gain, was identified as the responsible party for the MOVEit attack. Since emerging in 2019, the CI0P ransomware group has extorted many companies by monetizing stolen data. This particular group has exploited the MOVEit vulnerability, issued threats to various affected organizations worldwide and also impacted government agencies.

More than one hundred organizations worldwide reported data breaches due to the vulnerability. The compromised

data included sensitive company files (Material Nonpublic Information - MNPI), personal identifiable information – such as employees' names, emails and home addresses – dates of birth, insurance numbers and bank details.

The first signs of the exploitation spree occurred on May 27. Four days later, MOVEit provided an update and patched the vulnerability. Security researchers and the U.S. government flagged the vulnerability on June 1, prompting the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to urge all MOVEit customers to examine their networks for signs of unauthorized access within the past 30 days. Additionally, CISA recommended downloading and installing the software patch released by MOVEit to address the security issue.

The MOVEit vulnerability has several implications for cyber insurance policyholders. They should assess if their policy covers incidents arising from third-party software vulnerabilities. In the event of a data breach, policyholders may have coverage for expenses related to investigations, mitigations and customer notifications. Business interruption coverage may apply for financial losses caused by the breach. Additionally, all organizations should review their zero-day vulnerability response capabilities and execute internal process improvements as needed to enhance their security posture.

The MOVEit vulnerability has compelled organizations to prioritize cybersecurity and adopt proactive measures to help protect sensitive data. Valuable lessons learned include the importance of timely patching, implementing robust security measures, having a well-defined incident response plan and obtaining comprehensive cyber insurance coverage. These lessons aim to strengthen organizations' security posture and mitigate similar risks in the future. Overall, organizations should understand the implications of this event to enhance their cybersecurity practices and help ensure the protection of their data, business operations and stakeholders.

How to Prepare

Insureds should start by attempting to identify "sources of aggregation" that, if exploited or disrupted, can negatively impact many organizations, endpoint devices or individual persons. Sources of aggregation often rely on technologies, services, companies and/or the paths of interconnectivity between them. Insureds should also be prepared to answer specific questions from insurance carriers by:

- Staying current and applying the latest zero-day vulnerability patches and minimizing your typical patch time frame for zero-day vulnerabilities.
- Having a comprehensive understanding of patch management and a clear overview of the patch landscape so these are readily available for a smooth renewal process.
- In the event of an exposure to a zero-day vulnerability, determine:
  - How have you been affected?
  - Who needs to be notified?
  - What is covered under my insurance policy?

How to Respond

During a breach like the MOVEit vulnerability or other cyber breaches, it is crucial to have a practical strategy in place to help prevent or minimize impact. Organizations typically rely on applying patches to protect their systems. However, this process takes time, which is precisely what cybercriminals exploit. Therefore, a trade-off needs to be considered. Organizations can either temporarily block the affected service, causing downtime, or attempt to apply the patches while hoping that sensitive information will not be compromised during that time. It is a decision that must be carefully assessed to achieve a balance between mitigating the breach and maintaining operational continuity.

Contact the Brown & Brown Risk Solutions team to see how we can help you prepare for Cyber threats.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving cyber insurance program.

Brown & Brown

Find Your Solution at BBrown.com