Cyber Risks & Liabilities

Second Quarter 2021

The Importance of a Standalone Cyber Insurance Policy

Over the course of the past decade, many organizations have relied on standard property and liability coverage rather than a standalone cyber insurance policy to provide protection for cyber incidents. In fact, a recent survey from the Insurance Information Institute found that over half (59%) of organizations don't possess dedicated cyber coverage.

However, as digital threats continue to advance—contributing to a significant surge in both the cost and frequency of cyberattacks across industry lines—neglecting to purchase a standalone cyber insurance policy has become an increasingly high-risk practice. After all, organizations' elevated cyber exposures have motivated the vast majority of traditional property and liability insurance carriers to revise their policy terms as it pertains to protection for such exposures.

Specifically, many standard insurance carriers have begun implementing additional policy restrictions and more stringent coverage conditions related to cyber incidents in an effort to prevent unexpected (and costly) underwriting losses. Some carriers have even updated their policy wording to explicitly exclude coverage for cyber-related losses altogether.

That being said, a growing number of organizations that aren't equipped with standalone cyber policies are encountering coverage gaps within their commercial insurance programs. In the event of a cyberattack, these organizations would either receive only partial reimbursement for the resulting losses from their traditional property and liability insurance, or no assistance whatsoever. Especially in the midst of soaring cyberattack intensity, such a lack of coverage could lead to lasting financial hardships, delayed recovery capabilities and severe reputational damages.

With this in mind, it's crucial for your organization to ensure a clear understanding of the extent of coverage that your standard property and liability insurance provides for cyber-related losses. If this coverage is insufficient for the degree of cyber exposures that your organization is facing, securing a standalone cyber policy might be necessary to maintain adequate protection.

In any case, remember that every organization's cyber risks are different. Be sure to consult a trusted and experienced insurance professional to determine your organization's unique cyber exposures and subsequent coverage needs. For further guidance and insurance solutions, contact us today.

Provided by MST Insurance Solutions, Inc.

MST INSURANCE SOLUTIONS

Limiting Ransomware Exposures From Remote Desk Protocol

Remote desk protocol (RDP)—which is a network communications protocol developed by Microsoft—consists of a digital interface that allows users to connect remotely to other servers or devices.

Unfortunately, RDP ports are frequently being leveraged for launching ransomware attacks. In fact, a recent report from Kaspersky found that nearly 1.3 million RDP-based cyberattacks occur each day, with RDP reigning as the top attack vector for ransomware incidents.

Don't let RDP cause a ransomware incident at your organization. Review these tips for minimizing the likelihood of such an incident:

- **Close your port**. RDP-based ransomware attacks usually stem from organizations leaving their RDP ports exposed to the internet. As such, always keep your RDP port closed to the internet.
- **Establish a virtual private network (VPN).** A VPN will allow employees to securely access your RDP port, while also making the port harder for cybercriminals to locate online.
- **Bolster your software.** Ensure all workplace technology is equipped with top-rated security software to help deter attempted attacks.
- **Restrict access.** Be sure to uphold the principle of least privilege by only providing employees with RDP port access if they absolutely need it to conduct their work tasks.
- **Have a plan.** Lastly, make sure your organization has an effective cyber incident response plan in place that addresses RDP-based ransomware attack scenarios.

For more risk management tips, contact us today.

Handling the First 24 Hours After a Cyberattack

When a cyberattack occurs, how your organization responds can make all the difference in mitigating the damages. In particular, time is of the essence. That's why it's vital for your organization to have an effective cyber incident response plan in place that specifically addresses key actions to implement within the first 24 hours following an attack.

During these initial hours, your organization's response can help foster business continuity, protect stakeholders, limit legal repercussions and ultimately put a stop to the incident as fast as possible. What's more, taking steps to quickly contain the attack can provide significant financial benefits. According to a recent report from the Ponemon Institute, organizations that were able to resolve a cyberattack in less than 30 days saved over $1 million in resulting costs when compared to organizations that took more than 30 days to do so.

In order to minimize the lasting damages that can often accompany a cyberattack, here's an overview of important tasks to complete during the first 24 hours after an attack is discovered at your organization:

- **Start documenting the incident.** As soon as you find out that a cyberattack is taking place, begin documenting what you know. This should include when and how the attack was discovered, the technology or data impacted by the attack and any other supporting evidence regarding the event. Keep updating this documentation as you learn more about the incident.
- **Alert important personnel.** Be sure to gather the members of your organization's cyber incident response team and alert them of the attack. This may include IT leaders, crisis communication experts and legal advisors. These individuals should then begin carrying out their designated roles and responsibilities as outlined in the cyber incident response plan. Inform additional employees about the attack on a need-to-know basis.
- **Secure all workplace technology.** Do what you can to secure all organizational servers and devices, as well as stop further data loss or destruction. Take any impacted technology offline, but don't turn it off, as it could offer important evidence during the attack investigation. Launch any backup systems or data required to perform key operations and ensure business continuity (if applicable).
- **Seek further assistance.** Consult your organization's forensic team and—depending on the severity of the incident—local law enforcement to start conducting an in-depth investigation of the attack and help identify the perpetrators. Reach out to your insurance company to kickstart the claim process and receive further assistance.
- **Inform the appropriate parties.** Based on guidance provided by your crisis communication experts and legal advisors, develop a plan for effectively sharing the key details of the attack with organizational stakeholders, shareholders and government agencies (if necessary).

For additional loss control resources, contact us today.