NAVIGATING THE CYBER INSURANCE CLAIMS PROCESS

Presented by Hilb Group

Cyber incidents—including data breaches, ransomware attacks, and social engineering scams—have become increasingly prevalent over the past decade, impacting organizations of all sizes and industries. These incidents are only expected to become more damaging and devastating in the years ahead, making it difficult for organizations to recover. In fact, global cyber economy researcher and publisher Cybersecurity Ventures projected that the cost of cybercrime could surge to $10.5 trillion by the end of 2025—more than tripling from $3 trillion in 2015. Considering these findings, it's vital for employers to secure sufficient cyber insurance. Also known as cyber liability insurance, such coverage can help pay for a range of first- and third-party expenses (e.g., incident response and data recovery services, legal fees, lost income, reputational damage, and regulatory defense costs) that may result from cyber incidents, thus mitigating the risk of large-scale financial losses when these events occur.

When a cyber incident strikes, it's important for employers to know how to navigate the claims process and understand what their insurance may cover. In doing so, organizations can ensure a timely and cost-effective recovery, keeping related damage to a minimum. Although no two claims are the same, and specific response measures may vary based on the nature of an incident and its associated losses, this article outlines four general steps for organizations to take amid the cyber insurance claims process.

Step #1: Notify important parties

As soon as an organization identifies a potential cyber incident, whether it's via threat detection software or an employee report, it should carefully assess the situation to determine the validity of the incident. Upon validation, the employer should swiftly execute their cyber incident response plan by contacting necessary parties (i.e., the local authorities, the cyber insurer, and the broker) to kickstart the investigation and insurance claims process.

Notifying these parties is crucial for several reasons. Not only does it allow the organization to receive prompt assistance when a cyber incident occurs, but it may also be required to ensure coverage for the related losses. In particular, many cyber insurers mandate their policyholders to contact them immediately upon discovering an incident, typically before taking any other steps or incurring any additional costs to maintain coverage. As such, failure to notify the insurer in a timely manner can expose the organization to possible complications in the claims process or even a denial of coverage. That's why the employer should carefully review their policy to understand specific provisions regarding the discovery of a cyber incident and the required timeline for notification.

When it comes to notifying necessary parties, the organization should be prepared to provide in-depth information and resources regarding the overall scope and severity of the cyber incident. This will help the local authorities understand how to move forward with their investigation and give the cyber insurer and broker the details needed to streamline the claims process. Key information and resources may include a current narrative of events, documented proof of the incident, and a calculation of associated losses. Because such information and resources can change as the incident develops, the organization should continue collecting details in real-time and update necessary parties as needed.

Step #2: Coordinate with vendors

After the employer notifies the necessary parties about the cyber incident, they should coordinate with various vendors to help remediate the situation and minimize related damage. Depending on the organization's cyber insurance policy and particular preferences, it may select these vendors independently (as outlined in its cyber incident response plan) or obtain referrals from the insurer and broker. Therefore, the employer should be sure to communicate with the insurer and broker before moving forward with any vendors. In some cases, insurers may even require policyholders to receive explicit consent regarding vendor selections to prevent possible coverage exclusions. This is because some insurers have pre-negotiated rates with certain vendors, which can help minimize the costs incurred during claims. There are multiple vendors for the employer to consider, each playing a different role in handling the incident. Key vendors include the following:

- **Legal counsel** – An attorney who specializes in cybersecurity, also called a breach coach, can assist an organization in determining applicable data compliance standards for recording and reporting the loss or exposure of sensitive information. This attorney may also help the organization coordinate with other vendors and set up any necessary services (e.g., credit monitoring applications and call centers) for stakeholders or other individuals affected by the cyber incident.

- **Forensic investigators** – In addition to working with the local authorities, the employer can consult forensic investigators to look into the cyber incident further, identify the perpetrators, and assist with data recovery. These investigators can also help the employer prepare and uphold the integrity of any digital evidence associated with the incident. Such evidence may be particularly useful amid any legal proceedings involving the incident.

- **System recovery professionals** – While forensic investigators can help the organization recuperate data impacted by the cyber incident, system recovery professionals can support the organization's IT department as it works to restore any compromised networks, servers, and technology. In turn, these professionals can ensure the organization resumes normal operations as quickly as possible, therefore reducing downtime and limiting lost income.

- **Crisis communication experts** – The employer can utilize crisis communication experts to adopt a plan for handling any public relations concerns related to the cyber incident. In other words, these experts can work with the organization to deliver appropriate post-incident communications to regulators, affected parties, and the general public, thus helping the organization meet applicable breach notification requirements and minimize the risk of widespread reputational damage.

Step #3: Mitigate the incident and document associated expenses

Upon coordinating with its selected vendors to fully mitigate the cyber incident, the organization should work closely with its broker and the insurer's key representatives, namely the claims adjuster, to calculate the total expenses incurred amid the event and determine coverage capabilities. This entails keeping detailed records of all associated damage and restoration costs. Here are some important expense-related records for the organization to hold on to:

- **Vendor invoices and statements of work (SOWs)** – The employer should ask every vendor they coordinate with to provide detailed invoices and SOWs that summarize the work being performed, highlight daily progress on this work, and break down each component of the final bill. Further, the employer should clearly distinguish which aspects of every bill pertain to restoration costs versus improvement expenses. This is a crucial step, as most cyber insurers will only offer coverage for restoring systems and operations to the status they were in prior to a cyber incident rather than enhancing these elements beyond their original state. Moreover, neglecting to separate such costs could cause difficulties and delays during the claims process, extending the overall recovery timeline and prolonging the final payout from the insurer.

- **IT receipts** – In addition to keeping vendor invoices and SOWs, the organization should maintain any documentation of IT purchases made throughout the recovery process. This may include the cost of repairing damaged systems or replacing hardware that couldn't be recovered with comparable solutions. Receipts should be separated based on the nature of each purchase; those related to system restoration will likely receive coverage, whereas those associated with upgrades to the IT landscape (e.g., enhanced security software) may not. Additionally, the organization may find it useful to distinguish between purchases that provided permanent IT solutions (e.g., the replacement of corrupted devices) versus temporary fixes (e.g., the interim use of alternative technology to reduce operational downtime).

- **Business interruption calculations** – Depending on the specific details and severity of the cyber incident, the organization may incur minor or major business interruption expenses throughout the recovery process, especially relating to lost income. Because most organizations affected by cyber incidents are usually able to reinstate their key operations within a matter of days, cyber insurers often heavily scrutinize business interruption calculations and related expenses. In some cases, cyber insurers may even leverage forensic accountants to review these expenses further. As a result, it's critical for the employer to consult their sales and operations teams to ensure accurate calculations and foster open communication with the insurer's representatives to reach a positive outcome. The most valuable business interruption expenses for the organization to document include diminished production capabilities, operational inefficiencies caused by temporary workarounds, lost or canceled orders, permanent contract losses, and prolonged downtime that allowed customers or clients to purchase products and services from competitors.

- **Other recorded expenses** – The employer should record all remaining expenses incurred amid the cyber incident, such as temporarily elevated production and labor costs that helped make up for downtime. In the event that the incident prompted a lawsuit or attention from regulators, any additional legal fees (e.g., defense costs) and penalties should also be documented.

Altogether, keeping detailed documentation of all expenses related to the cyber incident can help the organization promote amore seamless claims process and confirm that the insurer's representatives have the necessary resources to provide an accurate payout.

Step #4: Resolve the claim and determine key takeaways

Finally, the employer should provide any additional information the insurer requests to help resolve the claim as quickly as possible. Upon receiving the final payout, the employer can review the cyber incident as a whole and identify key takeaways. This typically involves conducting a post-incident analysis. Such an analysis should focus on where the cyber incident originated, how it was detected, how effective the incident response plan was in handling this event, and the different technical, operational, and financial impacts of the incident. Depending on the cyber incident's origin and associated losses, it may also be worthwhile to evaluate whether any organizational failures or shortcomings played a role in the event.

The results of the post-incident analysis will guide the organization's identification of cybersecurity weaknesses and its effort to fill possible gaps with bolstered defenses. Doing so is critical to help prevent future cyber incidents and minimize related expenses. Necessary adjustments may include modifying the cyber incident response plan, updating or introducing new software, and implementing stricter security policies. Based on the outcome of the claim, the employer may also want to consult their broker to determine whether any coverage adjustments are necessary to ensure ample protection for cyber incidents going forward.

Conclusion

By having a deeper understanding of the cyber insurance claims process, organizations can navigate potential incidents with ease and keep related losses under control.

Contact us today for more risk management guidance and insurance solutions.

hilbgroup.com

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers shouldcontact legal counsel or an insurance professional for appropriate advice.
© 2024 Zywave, Inc. All rights reserved.