JS|HELD

PERSPECTIVES

Strategies to Avoid Cyber Insurance Claim Challenges: Part I

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Cyber risk is now a normal part of our personal and professional lives. When companies suffer a cyber incident, they often look to their insurance policy for coverage to help mitigate the financial exposure. Additional external resources, such as incident response firms, also help the insured get back to normal operations.

A common scenario we encounter is when a policyholder does not fully understand the scope and limit of their coverage. Although we do not interpret insurance coverage, let's examine some noteworthy challenges we see policyholders face when navigating through an insurance claim.

This is a two-part series. Part I poses a series of questions to assist insureds or policyholders in thinking through the common issues and in identifying the potential challenges of not addressing these concerns. In Part II, we present some strategies to help organizations further reduce their risk posture.

In this piece, we cover five themes the policyholder should understand:

1. The policy language
2. Actual coverage
3. Quantifying impact
4. Aligning policy to incident response plans
5. Managing policies that are not always tailored to unique business needs.

The Policy Language

Unlike other types of insurance coverage (e.g., property, commercial general liability), cyber insurance changes quickly due to fast-changing threats, and as the industry evolves and adapts. Therefore, when reviewing policy language, some questions to consider are as follows:

- Does the cyber policy liability coverage fit your organization's unique needs and risk posture?
- What are the limits of coverage, both dollar-wise and areas of afforded coverage?
- What exclusions could impact the claim? Be extremely mindful if you are operating in multiple regions domestically and throughout the world. You could be impacted by more external events than you realize.
- How does the policy define the recovery and restoration periods?
- What do "restored operations" look like? Does the insurance policy cover the necessary costs to get your operations to the same pre-incident state?
- What defines an upgrade? Do you have coverage for upgrades? And how do end-of-life and end-of-service considerations impact the claim?
- Does your policy cover the latest threats?
- What endorsements should be added to help with the recovery after a cyber incident?
- Have you discussed the resources covered under the policy? For example, are you required to use specific vendors for response activities, or do you have latitude for whom to pick?

It is important for the insured to have an understanding of the policy and consult with professionals such as brokers, counsel, and insurers for any questions regarding the interpretation of the insurance policy.

Actual Coverage

If insurance purchasers lack a good grasp of what is covered, have a professional assist with determining what policy and limits fit the organization's needs.

If a company purchases a policy and assumes reimbursements for all their damages up to the coverage limit, a significant pitfall may be lurking. Furthermore, even when you think you have the proper policy, errors and omission (E&O) policy may be a worthwhile investment to consider. Some additional considerations:

- Is the existing coverage for directors and officers (D&O) appropriate?
- Do any other types of insurance apply or help to fill gaps? For example, does your property policy have any cyber coverage or is there an exclusion?
- What defines reputational harm and how is that calculated?
- Is there coverage for an extended period of indemnity?
- What defines a waiting period? Would losses begin after a defined waiting period or at the date of the incident?

- What defines extra expense? Is it an expense to reduce loss or pure extra expense? What timeframe (e.g., period of restoration) is the extra expense covered for?

Additionally, with the increased use of information technology (IT) in operational technology (OT) environments – especially in select industries – an incident that originates as a cyber event could very well end up causing physical damage. This means property insurance could come into play. However, there is typically an exclusion or lower policy limits under an insured's property policy.

Quantifying Impact

When a claim or proof of loss is submitted to an insurer, a numerical value will always be attached. But can that claim amount be validated as an insurable loss? Quantifying financial impact post-incident requires supporting documentation and some sound thinking and development, including:

- Can claim calculations be independently verified by outside professionals, such as forensic accountants?
- Can claim activities be validated as necessary and reasonable by outside professionals, such as technical experts?
- Does a mechanism exist to track expenses post-incident in real, or near-real, time? If not, reconstructing expenses, with supporting evidence, can slow down the claims process.
- Has the organization performed a pre-incident business impact analysis? If yes, when was the last time it was updated and were financial changes over time considered?
- Has the company performed a cyber-related disaster recovery exercise?
- Can the financial impacts be categorized? For example, lost earnings, lost customers, lost production, reputation impacted, etc.
- Have sales been delayed or lost? What is the actual loss sustained?
- Did the organization incur extra expenses and / or did variable expenses decrease during the interruption period?

Also remember that period of indemnity – the period of time for which indemnity is payable under a business interruption policy – will impact quantifying damages, making it one of the most critical components of quantifying the business interruption loss. Some questions to ask are:

- What systems were affected?
- What were the specific functions of those systems?
- How do those functions impact the business and its ability to generate sales / net income?
- What was done to mitigate the downtime or impact to the business during remediation?
- Are there technical alternatives to expedite recovery?
- What issues may have transpired during the recovery?
- What date was the remediation complete?

Aligning Policy to Incident Response Plan

If there is a misalignment here, there may be challenges during the claims process. The greatest misalignment is having no incident response plan at all. But assuming one exists, ask the following questions:

- What does an incident response plan look like at your organization?
- Are the appropriate stakeholders, roles, and responsibilities identified? Here is a teaser response: if the plan calls for an external public relations or crisis communications firm, the policy may cover those costs.
- Does the policy include any technical or notification requirements that need to be conducted to ensure coverage remains in effect?
- Have you considered what you would do if you were restricted from accessing financial and similarly important critical data? Think offline and cold storage immutable backups here.
- What is the recovery plan to minimize financial exposure?
- Are technical and business teams able to work together to perform damage analysis?

Managing Policies That Are Not Always Tailored to Unique Business Needs

For even the most prepared, a risk always exists that something falls through the cracks. The first step to forestall this risk is avoiding the "one size fits all" coverage: specifically for policy coverage limits and premium payments. Some issues to keep in mind:

- Are industry-specific considerations accounted for?
- Does coverage and language align to your business needs, risk profile, customer profiles, and data you use and hold?
- Does your industry earn revenue by fixed fee contracts? Would this lost revenue just be a delay in sales? When do you earn and record revenue? Is this outside the period of restoration?

Understanding the business and how it aligns with your insurance policy is critical in calculating your losses.

This may be stating the obvious, but insurance coverage by sector (e.g., manufacturing, retail, healthcare, etc.) all differ based on industry norms and requirements, which is why it is vitally important to understand how the policy meets the organization's unique needs.

CONCLUSION

Cyber risks are changing, and cyber insurance is evolving with the changing landscape. In turn, businesses also need to stay informed about these changes to mitigate losses, prevent losses from occurring, and ensure adequate coverage for their specific risks.

To overcome challenges, organizations need to be proactive and not reactionary. It is important to plan and document all claimed costs. Partnering with professionals who have experience in the pre- and post- incident phases can tailor the policy and premium payments for your organization. These professionals could include risk managers, brokers, insurance, breach coaches, counsel, incident responders, forensic accountants, and digital forensic experts are just a few.

Part I was designed to pose questions to consider when reviewing cyber insurance policies. Moreover, these questions are meant to help policyholders understand what could delay the claims process.

In Part II, we will offer examples of real-life challenges experienced during the cyber claim process and how an insured may avoid these experiences.

ACKNOWLEDGMENTS

We would like to thank our colleagues Jessica Eldridge and George Platsis for insights and expertise that greatly assisted this research.

MORE ABOUT J.S. HELD'S CONTRIBUTORS

Jessica Eldridge is a Senior Vice President in J.S. Held's Forensic Accounting -- Insurance Services practice. She has over 19 years of investigative and forensic accounting experience in measuring financial damages involving business interruption, cyber, extra expense, stock, builder's risk, employee dishonesty / fidelity, personal injury, subrogation, and litigation support services. She also has extensive experience with the administration of common fee funds and the oversite of property damage claims for large construction projects.

Jessica can be reached at jeldridge@jsheld.com or +1 857 219 5720.

George Platsis is a Senior Director providing Digital Investigations & Discovery services in J.S. Held's Global Investigations practice. Mr. Platsis is a business professional, author, educator, and public speaker, with an entrepreneurial history and upbringing of over 20 years. He has designed and delivered solutions, and led teams, to improve breach readiness, enterprise-wide and business-unit specific incident response programs, and estate hardening for a series of Fortune 100 clients in healthcare, media, financial services, manufacturing, defense, and commercial electronics industries, including support of clients in the small and medium business space. Additionally, he brings complex investigation

and emergency management experience to businesses and individuals seeking to reduce their risk posture. George is a Certified Chief Information Security Officer.

George can be reached at george.platsis@jsheld.com or +1 321 346 6441.