JS|HELD

PERSPECTIVES

Strategies to Avoid Cyber Insurance Claim Challenges: Part II

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

INTRODUCTION

In Part I of this series, we posed a series of questions to consider when purchasing cyber insurance. Our approach was deliberate: the *right* questions help get you the *right* insurance to address cyber risks facing your organization. Remember, seek the ***right coverage for you***, not just *any* coverage.

Part I focused on:

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

Now to follow up in the second piece of this series, we identify not only ***how*** to answer some of the questions we posed, but also, ***what value*** those answers bring. Moreover, we identify some of the |common gaps and how to address them.

HOW TO MINIMIZE RISK OF "GREY ZONE" LANGUAGE

You don't know what you don't know. Precision in language matters. Even the "ANDs" and "ORs" could significantly impact expectations and the claims process. It is incumbent on the policyholder to ask questions about definitions and qualifiers. Furthermore, do not be shy to ask scenario-specific questions either. Doing so will allow an organization to:

- Define what cyber liability insurance is and is not,
- Determine how much cyber insurance is needed,
- Identify which exclusions or limitations apply,
- Prepare for how to analyze a potential loss,
- Understand loss and policy provisions, including applicable deductibles,
- Maintain appropriate records, artifacts, and related documentation to support claims, and
- Calculate a business interruption and extra expense claim in the event of a cyber incident.

Having thought through these issues, and having answers or even best estimates ready, will help an organization right-size the cyber insurance policy for their business. Moreover, having discussions with a forensic accountant, alongside a cyber security professional, prior to a cyber event allows an organization to better prepare answers to many of the anticipated questions, well in advance. What is the net result? The organization is better positioned to manage incidents and their impacts, and the organization has established the necessary protocols in place to support its claim.

INSUFFICIENCY OF BUSINESS INTERRUPTION CYBER COVERAGE

Many organizations underestimate the financial impacts of a cyber event. Business Interruption and Extra Expense policies may provide some coverage (e.g., loss of business income, overtime, travel expenses, and expedited deliveries to meet customer demands) but an organization may determine that additional coverage is needed to bridge gaps. The way to stay ahead of the curve is to reasonably calculate the potential loss of business income and extra expenses that may be incurred during an interruption, such as:

- **Dependent Business Interruption, sometimes called Contingent Business Income**. This coverage can assist during an interruption caused by a third-party service program, such as a failed software patch, human error, or cyberattack.
- **Reputational Harm.** Not all cyber policies include coverage that protects an organization's reputation. Even when this type of coverage is available, there are limitations, such as duration and scope and even what exactly defines reputational harm.

CALCULATING LOSSES

Given the complexity and uncertainties related to cyberattacks, impacts, and third-party dependencies,

there is no clear-cut science to estimate losses. But an organization can begin to estimate their losses by having a better understanding of how their revenue streams may be impacted by a cyberattack. Here are some categories to look at:

- **Fixed Fee Contracts**. Understand when revenue is earned, recorded, and how that relates to the period of indemnity.
- **Pay Type**s. Know ahead of time if unproductive hours for salaried employees are considered in the policy. This scenario will impact a business interruption calculation and may direct funds to certain coverage types (e.g., extra expense versus saved expense).
- **Extra Expense**s. Get a better sense of what constitutes an "extra expense" or "expense to reduce loss." Also, make sure to be mindful of the period of indemnity.
- **Paid Bonuses**. Understand how bonuses may be considered. Are they required by contract, or can they be a business decision? This makes a difference in your calculations.
- **Make Up or Delayed Sales**. Understand how make up or delayed sales are factored into the business Interruption calculation (e.g., if a manufacturer was not able to produce its product for two days, had inventory on hand, production was made-up once their system was back online, and they were not at full capacity prior to the loss, there may not be a business interruption loss).
- **Location Site and Type**. Understand the actual impact of the incident (e.g., if the incident is concentrated in a specific site, region, or revenue segment). It is important to understand how the cyber incident affected sales, especially if the business has multiple locations or generates sales through both online and at a physical store(s). Sales and expenses may need to be evaluated at more than just the impacted locations.

MINIMIZING THE BLAST RADIUS AND ACHIEVING POLICY ALIGNMENT

Understanding how the business interacts with technology is essential to good planning. Specifically, mapping dependencies not only gives planners insights about how the business operates, but also gives them a glimpse into how a future incident may unfold. Effectively, the pain points are being identified ahead of time, and, in the case of an incident, one can see how the cascading issues play out. One way to think of dependencies is using these examples:

- Technologies to technologies, e.g., applications to databases
- Processes to technologies, e.g., customer service to applications
- Processes to processes, e.g., sales to accounting.

By going through this exercise, an organization is better suited to identify what types of gaps exist, see where external support is needed, and even identify potential risk areas both before and after an incident, including those that require follow-up work (e.g., lawsuits, reputational damage, exposures to greater expense, etc.).

Once identified, a final mapping exercise against the insurance policy should be performed. In essence, an organization that goes through this exercise is "exchanging business cards before the incident" and "pre-positioning assets." Part of this "pre-positioning" or formalized planning can include identifying the forensics, response, legal, and public relations firms, and determining if they are an approved vendor. These third parties could be written into the insurance policy as approved vendors. This approach may even allow an organization to negotiate vendor hourly rates prior to an incident.

CONCLUSION: AVOIDING COMMON PAIN POINTS

The purpose of this two-part series was to help organizations identify likely trouble areas that could arise during the claims process. If the organization has suffered an attack, proactively managing these issues helps an organization navigate a smoother claims process.

In closing, here are some of the biggest challenges we have seen when the proactive steps have not been taken, along with some quick fixes to them:

- **Poor initial communication with impacted stakeholders, including with carriers and vendors**. Prior to a cyberattack, have discussions with incident response vendors and claims experts to have a plan and methodology in place.
- **Poor understanding of the policy and exclusions**. Ask tough questions during the purchase and renewal process, not after the incident. See the section above on how to clear the "grey zone" during purchase.
- **Inability to respond to information requests**. Be prepared to respond to requests for information to support a claim, post-incident. Knowing what the common types of requests are, and maintaining the ability to answer these requests, will make the claims process much smoother and expedited. Be ready to tell that story such that it addresses your coverage and be able to provide the evidence to support it.
- **Defining the Period of Restoration**. The lines can become blurred between response, restoration, and recovery. The sooner the timeframe can be defined, the easier the claims process will be.
- **Waiting Period**. Determine how the waiting period is calculated (e.g., business hours, clock hours, etc.). A waiting period can impact loss calculations and thresholds for reimbursement of the claim.
- **Attributing lost revenue to a cyber event**. A change in revenue does not necessarily mean the loss is attributed to the event as other factors can impact sales. That is why there needs to be a correlation between the cyber incident and the financial impacts, supported by the necessary documentation.
- **Generic Policy**. Avoid the one-size-fits-all policy, get addendums, and ask questions. The organization should get a policy that is suited to its business, operations, industry, and unique risks.

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.