

Checklist for Mitigating and Quantifying a Cyber BI Loss

“There are only two types of companies: those that have been hacked, and those that will be.”
~ Robert Mueller, FBI Director, 2012

Introduction:

Quality documentation and forensic analysis is the cornerstone to effectuate a positive result on a cyber claim. Most cyber risk policies include coverage for business interruption or loss of income and extra expenses associated with a breach, which typically can make-up some of the more significant costs. When a cyber business interruption loss occurs, it is the responsibility of the Risk Manager or Policyholder to lead the development and presentation of losses caused by the event. Immediately after a loss, significant attention, leadership and data analysis are required to fully document a claim.

Keep in mind that a complex loss will be evaluated for insurance purposes or for a general audit; therefore it is essential to quickly establish a claim validation and presentation process to capture and document all loss-related costs.

Initial Steps should include:

- ✓ Reporting the loss promptly through your insurance broker or risk manager.
- ✓ Taking all reasonable measures to mitigate the impact of the breach.
- ✓ Immediately review all insurance policies that may provide coverage.
- ✓ Identifying timeline of events, determine (as exact as possible) the time of the breach for each of the impacted systems, locations, etc.
- ✓ Confirming if/when the breach has ended, been stabilized or still on going for each of the impacted systems, locations, etc.
- ✓ Establishing a separate account number or charge code in your cost accounting system for each of the impacted systems, locations, etc. under which all cyber breach related costs will be captured.
- ✓ Determining the stage at which the breach occurred and corresponding loss in production/sales/access began.
- ✓ Securing production/sales budgets/forecasts that can be used to project production/sales had there not been a breach.
- ✓ Identify any seasonality affect to production/sales or similar periodic fluctuations.

- ✓ Creating schedules to track all costs and expenses potentially associated with the breach including but not limited to attorney fees, crisis management fees, public relations expenses and claim preparation fees.
- ✓ Establishing a protocol for the claim presentation and audit by creating a timeline with targeted milestones. This will create a clear path for all parties involved and set expectations for the adjustment process.
- ✓ As soon as practical, developing a Rough Order of Magnitude (ROM) that outlines all areas of projected loss amounts by coverage category. Where estimates are difficult to complete early on, be sure to include the amount of loss in a potential coverage category as “to be determined” (TBD). This document will be useful for your team to understand the overall potential impact and for the adjuster as the loss reserve is set.
- ✓ Consider potential loss to reputation/brand and loss of trust by customers or business partners.

Differences to consider in Business Interruption Claims Dynamics

	Physical Cause of Loss	Cyber Cause of Loss
Location of the loss	Single geographic area or location	Wherever the network or application is used
Identification of Period of Interruption	Well - defined	Ambiguous, uncertain start and/or end date
Length of Period of Interruption	Weeks, Months, Longer	Minutes, Hours, Days
Policy Waiting Period	0 - 72 Hours	7-12 Hours
Non-continuing Expenses	Often applied as part of BI claim calculation	May not be relevant if short BI downtime
Cost Distribution	Rebuild and Revenue Loss	Extra expense and response costs
Additional Expenses	Standard Extra Expenses; fuel, new location, temp staff, etc	Forensics, information recovery, technology business continuity

Costs often covered in a Cyber policy

- Reconstruction or replacement of compromised property, such as servers or other IT equipment,
- Reconstruction of data and programming,
- Cost of rebuilding networks, programs and data,
- Cost for notifying customers impacted by the breach (including the cost of credit-monitoring services for a predetermined period of time),
- Employee lost productivity costs,
- Crisis management expenses, rapid response security professionals,
- Forensic investigators and accountants.

Cyber losses may have a significantly greater proportion of extra expenses than more traditional business interruption losses because of the shorter duration of a cyber-outage and the immediate need to spend to implement back-up plans, hire outside expertise and replace systems components and software.

During an interruption, insurance may cover some extra expenses such as:

- Costs associated with setting up a warm or hot site to take over processing while the main data centers are not operating;
- Costs for outside forensic services to identify the nature of the breach, close down the intrusion and repair the system in order for the breach not to reoccur; and
- Overtime pay for IT employees who are required work additional time due to the implementation of a breach response plan.

It is essential that risk managers understand their organization's cyber risk financial, contractual and reputational exposures pre-breach, work with brokers and underwriters to explain the organization's cyber liability exposures and associated controls, carefully review coverage options in all policies, and properly manage the post-breach claims documentation process to necessitate an expedited insurance recovery.

About Us:

The Procor team has managed more than \$10 billion of insurance claims. Ranging from the largest man-made and natural disasters and losses in history to more common and frequent business interruption losses, our experts have intimate claim knowledge in virtually every industry including: hospitality, casinos, retail, manufacturing, chemical plants, healthcare, senior care and assisted living, financial institutions, oil & gas, transportation, distributors, technology, pharmaceuticals and others. Our experts are respected by both policyholders and insurance companies alike because we prepare comprehensive, logical and well-documented claims that result in fair and timely insurance claim settlements.

For more information please visit www.procorllc.com