LOCKTON® | JS|HELD

Cyber Business Interruption Playbook

A GUIDE TO RESPONSE & RECOVERY

Table of contents

01

Introduction

Over the past 20 years, technology has changed the way we communicate, conduct business, and live. It is rare to walk down a city street and not see a person using some type of technology. It has become an integral and indispensable part of our everyday lives.

The important role technology plays in business cannot be understated. Businesses worldwide rely on digital interconnectivity for growth. Organizations rely on the internet, videoconferencing, accounting, and project management apps to stay connected. Technology is the key to efficiency for most businesses, helping to streamline processes, maintain data flow, and reduce operational expenses.

This reliance on technology, however, does not come without risks. Companies that rely on digital interconnectivity are targets for cybercriminals. These threat actors have found ways to disrupt the digital environment and wreak havoc on businesses across the world.

For example, companies that rely on interconnected digital systems for their supply chains are susceptible if those digital systems are compromised. A cyber event affecting any part of such a network can cause widespread disruption, delaying product deliveries and leading to penalties, lost contracts, or damage to business relationships and reputations. Companies need to understand that the consequences of a cyber event can be far-reaching, impacting not just their financial health but also their long-term viability and competitiveness.

> **This Cyber Business Interruption (BI) Playbook is intended to help companies navigate the unique complexities they face in preparing for cyber business interruption events. The Cyber BI Playbook provides insights on how to take a proactive approach to business interruption, which includes risk assessment, insurance coverage, incident response, and recovery planning.**

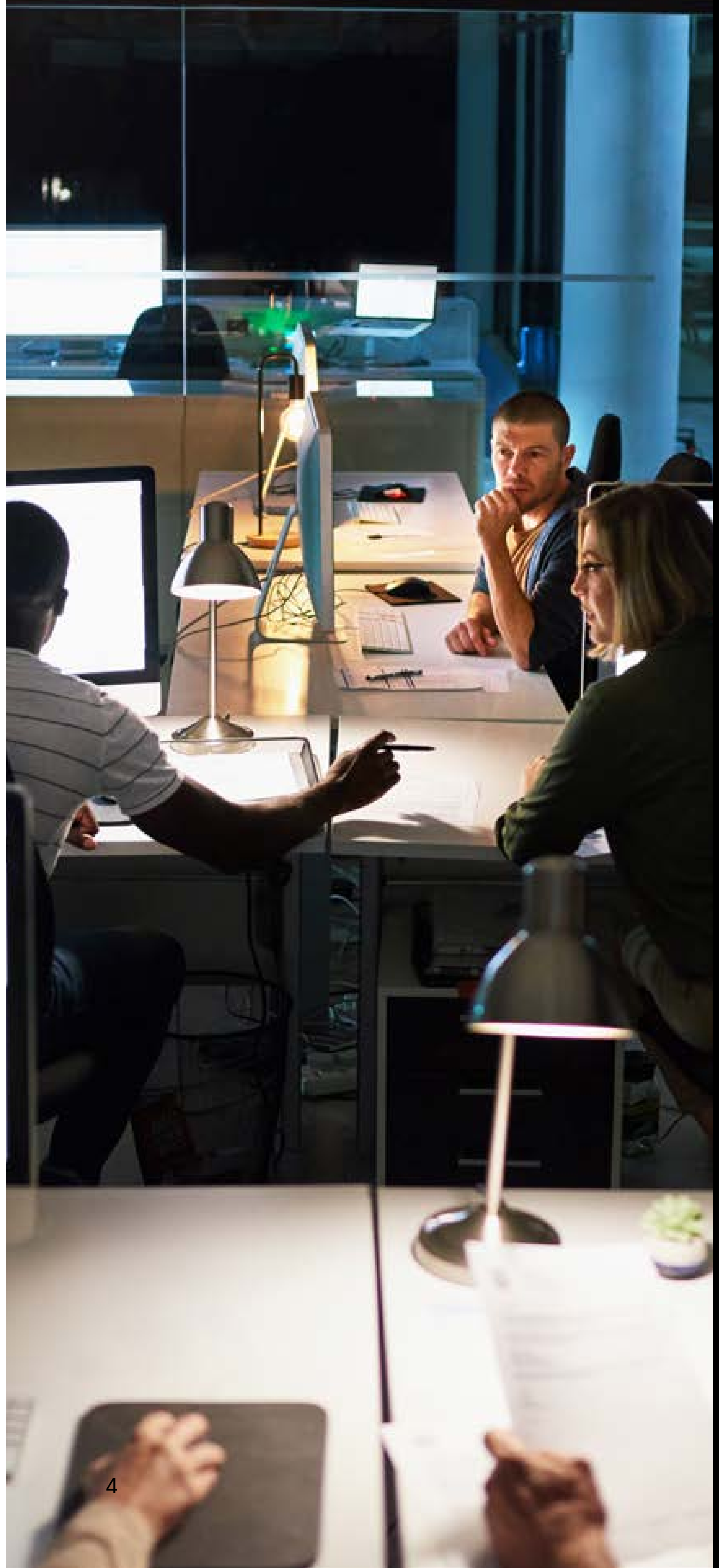
02

Preparing for business interruption

Most organizations recognize that unplanned events can disrupt operations. Resilient organizations make the investment in time, money, and other resources to plan how they will minimize and react to disruptions.

Planning for business disruption typically involves the development of an incident response plan, disaster recovery plans, and business continuity plans. Although these plans all deal with how an organization should act in the face of an event, there are distinct differences that warrant developing each option. In some cases, for example, organizations will consider implementing incident response and continuity of operations programs to oversee resilience and response activities across the enterprise, with separate plans for various parts of the business (for example, cybersecurity or environmental).

Incident response plans focus on how an organization detects, responds to, and recovers from incidents. Disaster recovery plans are typically specific to a system (for example, an application server), are developed by the system owner, and are outside the scope of this document. Business continuity plans focus on how an organization will maintain critical operations, possibly in a reduced capacity, during a disruptive event. Ideally, all three of these plans will be developed in collaboration and will complement each other.



Why should organizations prepare for business interruption?

Although preventing all disruptions to a business is not possible, an organization can significantly reduce the costs related to a disruption and, in some cases, enable it to survive a crisis.

For example, assume a small tire manufacturer uses a third-party software and machine to track lot numbers and stamp finished tires with traceability numbers (such as lot or serial numbers). If this supplier goes down due to its own event (for example, ransomware), the tire manufacturer can no longer ship tires. If the tire manufacturer is responsible for supplying tires to a major OEM auto manufacturer, it could be looking at penalties and may not survive days, let alone weeks, absent effective planning.

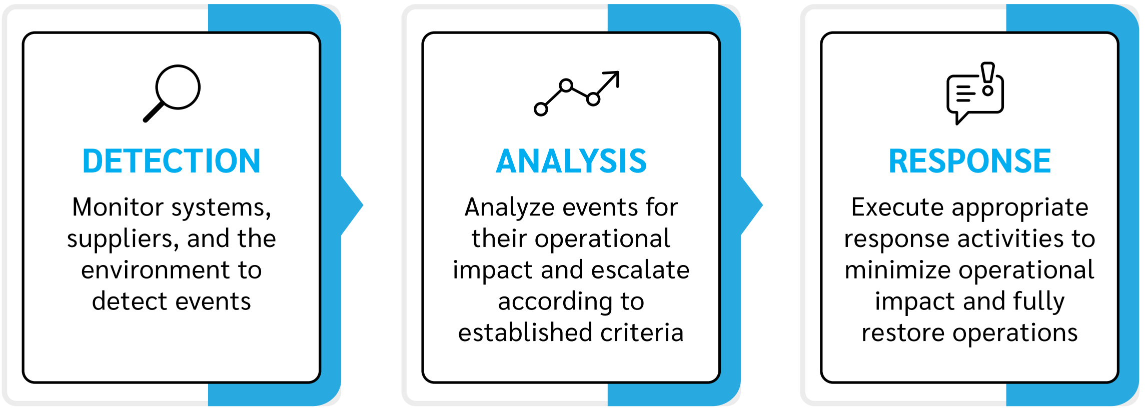
If this tire manufacturer conducted planning for business disruptions before the disruption to its supplier, it would likely have identified lot traceability as a key aspect of production. It could have identified a secondary supplier or developed a manual process for keeping the manufacturing process going while an alternative could be found.

Steps to developing an incident response plan

Developing an effective incident response plan is a time-consuming task. It requires a solid understanding of an organization's business, its operating environment, its staff and resources available, and the types of events that might affect it. Purchasing a complete plan or template and adopting it without customization is not advised.

Although an organization can hire experts in the field of incident response to help develop an incident response plan, these plans are best developed with the involvement of key stakeholders from across an organization. This will ensure relevancy of the plan and help speed up its adoption.

Most incident response plans include three major components, which follow the sequence of how an organization will react to events. These include detecting events, analyzing events, and responding to events.



DETECTION
Monitor systems, suppliers, and the environment to detect events

ANALYSIS
Analyze events for their operational impact and escalate according to established criteria

RESPONSE
Execute appropriate response activities to minimize operational impact and fully restore operations

Before an organization can respond to a cyber incident, it must first be able to detect when a cyber event occurs. A cyber event can be any computer activity that affects the organization or its assets — for example, a user logging in to their email, a website outage, or the opening of a sensitive area after hours. Organizations typically identify events through monitoring of their systems; subscribing to third-party information sources, such as the critical vulnerability alerts published by the Cybersecurity and Infrastructure Security Agency (CISA) or industry-specific advisories; communicating with key clients and suppliers; and other means.

It is not uncommon for a company to learn from an external entity, such as law enforcement, that it has a malware infection it was previously unaware of. Establishing relationships with local and federal law enforcement and CISA representatives is always a good idea.

IDEALLY, AN INCIDENT RESPONSE PLAN WILL DOCUMENT HOW AN ORGANIZATION WILL:

- ✓ Detect events;
- ✓ Rank information sources that may conflict with each other; and
- ✓ Log and track events.

Once an organization can regularly detect most events, it must have a mechanism for analyzing and reacting to those events. No organization has the time, money, and resources to treat every event the same. Incident response plans should document the criteria for classifying events and determining what is an incident versus a crisis — in other words, the difference between an event that requires a response and one that may threaten the survival of the business.

The process of developing this criteria must consider an organization's operations, finances, obligations — for example, to provide a critical service to subscribers — and similar factors. Criteria should be developed with leadership's involvement and approved by the company's executive management team. This will be one of the standards used to determine when executive leadership needs to be notified of incidents.

Often, incident response plans will define various criteria and then provide a table of example events to help staff better understand how to categorize events (see Figure 1). In some cases, organizations may create separate tables for employee, operational, and financial impacts. Criteria should be regularly reviewed and updated to ensure alignment with the business.

FIGURE 1: Identifying examples can help incident response teams better categorize events when they occur.

	CRITICAL (CRISIS)	HIGH	MEDIUM (INCIDENT)	LOW (EVENT)
Severity	Events in this category have the potential to significantly impact employees and the organization's ability to conduct operations, or result in financial damages.	These events may not directly threaten the organization's survivability but will have an operational or financial impact, and could grow into a crisis if not immediately addressed.	These events will not require an organizationwide response. But if they are not dealt with in a timely manner, they can grow into a high-severity incident or crisis. Often, IT and security teams deal with these events daily.	This category is where most events fall. It includes both expected and unexpected events such as a user login attempt or an interruption of VPN services. Many events, in this category will be classified and quickly forgotten, while others may warrant continued monitoring.
Operational impact	• Loss of employee life or serious injury • Operational disruption of greater than 72 hours	• Injury of one or more employees • Operational disruption of greater than 24 hours • Outage of key system lasting more than 4 hours	• Operational disruption of greater than 4 hours • Key system outage lasting more than 1 hour • Repeated unauthorized login attempts	• User activities (e.g., login attempts) • Privilege escalations • Changes in network configurations

Once an incident or crisis is declared, an organization needs to respond. This section of the incident response plan will identify roles and responsibilities, recovery timelines, checklists, and other tools the organization will use in response to an event. Incident response will often trigger data backup procedures, crisis communications, assumption of alternate duties for affected employees and, in some cases, ceasing noncritical operations until an incident is contained.

Best practice is to routinely review and iterate incident response plans to better align them with the business and further reduce the impact of any incident. Many companies conduct after-action reviews following all incidents and crises to capture findings while they are still fresh.

KEY ROLES & RESPONSIBILITIES THAT EVERY INCIDENT RESPONSE PLAN SHOULD COVER INCLUDE:

- EXECUTIVE LEADERSHIP AND BOARD: Provide executive-level support for the incident response plan and program, contribute and approve escalation and notification criteria, and handle executive-level decisions (for example, ransom payments).
- CORPORATE COUNSEL: Ensure the organization response is appropriate from a legal and regulatory perspective, minimize legal risk, and protect company interests.
- CORPORATE COMMUNICATIONS: Manage the flow of information to both internal and external stakeholders, maintain company reputation, and ensure transparent and consistent communication.
- FINANCE: Focus on financial risk and impacts, budget allocation for response, accurate and compliant reporting, insurance claims management, cash flow monitoring, vendor and contract management, and regulatory reporting.
- RISK MANAGEMENT: Ensure response activities align with the organization’s risk management framework, coordinate across functions, and initiate contingency and business continuity plans.
- OPERATIONS: Maintain operational continuity, oversee event escalation, coordinate transitions between reduced and normal operations, and ensure employee safety and awareness.
- INFORMATION TECHNOLOGY: Identify and mitigate technology-related risks, ensure continuous monitoring, maintain situational awareness of threat environment, contribute to root cause analysis, and oversee vulnerability identification and patching, system recovery, and technology backups.
- CYBERSECURITY: Detect and monitor threats, manage incident triage and prioritization, contain and isolate affected systems, eradicate identified threats, contribute to root cause analysis, and conduct employee awareness training.
- FACILITIES: Ensure employee safety and compliance with health and safety regulations, secure physical premises, oversee surveillance monitoring, manage backup services (for example, generators and porta-potties), and prepare alternate sites.

Common third parties involved in incident response

- Breach counsel
- Forensic accountants
- Digital forensics (DFIR) experts
- Public relations
- Restoration and remediation consultants
- Cyber extortion experts
- Notification/credit monitoring services
- Insurance brokers
- Insurers
- Law enforcement

Steps to developing a business continuity plan

As with incident response plans, it is imperative that organizations take the time to develop custom business continuity plans that are tailored to their unique operations. Even two companies in the same industry will have different ways of operating. Organizations can consult with third-party experts but should not expect them to be able to develop comprehensive business continuity plans without significant internal stakeholder engagement.

Business continuity plans are aimed at maintaining critical operations in the face of an event. Organizations must therefore first identify their critical operations, key dependencies, obligations, and other aspects of their business.

Organizations must then prioritize these aspects to determine those most important to the businesses' survival and success. This can be done through business impact analyses, quantification workshops to better understand the financial impacts of potential event scenarios, and risk assessments to determine which lines of business are most at risk.

Once analysis and prioritization are complete, organizations can develop mitigation strategies and plans regarding how they will keep critical operations running during disruption. Strategies may include finding alternate vendors for key resources, leasing and equipping alternate sites, eliminating the use of vulnerable technologies, or reducing operations for a period of time.

These processes must be captured in written documents, and their effectiveness should be tested during periodic exercises. Training should also reinforce what employees should do during disruptions.

Cyber insurance & business interruption coverage

Cyber insurance is designed to cover financial losses resulting from cyber events, such as data breaches and ransomware attacks. Policies typically include a collection of coverages, such as:

- Third-party liability (claims by others);
- Forensic investigation and data recovery expenses;
- Breach notification costs;
- Cyber extortion losses (including the reimbursement of ransoms paid); and
- Business interruption.

While all these coverages are important parts of a well-rounded cyber insurance program, our focus here is the business interruption coverage available in almost every cyber policy.

The purpose of business interruption insurance is to return the insured entity to the position it would have been in had the triggering event not occurred, subject to certain limitations and exclusions. For many, business interruption coverage is the most important and yet least understood component of a cyber insurance program.

The business interruption loss in most cyber insurance forms is calculated as the sum of the net profits lost because of a computer system outage or disruption and the expenses that must continue during the interruption.[1] Regardless of the specific language of the policy, the goal should be to cover the organization for the actual loss sustained.[2]

These days, most organizations rely on computer systems to function; an extended outage of these systems is likely to lead to significant income losses and/or expenses. It is important for organizations to quantify their potential losses from different types of cyber events to determine the amount of cyber business interruption coverage — if any — they require.

The scope of business interruption coverage in cyber policy forms has expanded since they were first introduced about 20 years ago. Where coverage was first made available principally for the outage of a policyholder's computer system caused by a malicious attack, coverage is now routinely available for outages that are not the result of an outside attack — often called "system failure" coverage. Coverage is also now available for a policyholder's business interruption caused by the outage of computer systems controlled by outsourced IT service providers and possibly many others.

Business interruption insurance: From property to cyber

More than 200 years ago, the insurance industry recognized that the loss of tangible property could have financial consequences well beyond the actual value of any damaged or destroyed property. Indeed, a disruption to business operations, regardless of cause, can be devastating to an enterprise.

Over time, business interruption became an essential component in commercial property insurance policies. With the recognition of the risks posed by cyber threats — and the need for insurance products to address those risks — business interruption coverage has been adapted to cyber risks and is now an essential component of a cyber insurance policy.

NOTE: Where a cyber event causes property damage that results in business interruption, a property policy may respond if a cyber policy does not provide coverage.

[1] Alternatively, the loss may be calculated by determining the business's lost earning during the disruption and subtracting the variable costs saved when the business was not operating. The first approach is often referred to as the "gross profit" method; the approach described in this footnote is the "gross earnings" method.

[2] For example, with partial disruptions, continuing expenses are offset against actual revenues earned during the loss period.

Important components of cyber business interruption coverage

Business interruption insurance is complex. Terminology varies among carriers, and terms can vary between policy forms.

Beyond the business income calculation formula itself, limits of liability purchased, and self-insured retentions, the following terms can affect the scope of coverage provided and the amount of recoverable loss:

a. TRIGGERING EVENTS: Does the policy specify that it will only respond in the event of malicious attacks ("security events"), or are nonmalicious "system failures" also covered? Coverage for security events is the core of cyber coverage, but most stand-alone cyber policies also cover, or provide an option to cover, nonmalicious system failures. Some forms carve out or limit coverage for certain types of nonmalicious outages, such as those that might affect several unrelated organizations.

b. DEPENDENT BUSINESS INTERRUPTION (DBI): Also called contingent business interruption and outsource provider coverage, DBI provides coverage for computer outages (network security events or system failures) of other organizations that have a disruptive impact on the policyholder's business. Where provided, the scope of the coverage can vary. Is it only for information technology providers? Can coverage be obtained for outages of those providing business outsourced services or other nontechnology products and services? Limits, retentions, and waiting periods may be different for different types of events.

c. WAITING PERIOD: This is the amount of time an outage must last before business interruption coverage is triggered. Waiting periods from eight to 48 hours are typical in cyber policies, although they may vary depending on the type of event or affected system. It is important to understand whether or not the waiting period is a monetary deductible.

d. EXPENSE COVERAGE: What is the scope of expenses covered outside of the business income calculation? Minimally, expenses incurred for the purpose of reducing the business income loss should be covered, but coverage for other categories of expenses incurred because of an event may also be available. In recent years, cyber policies have included the costs incurred to prove a business interruption loss has occurred — for example, the fees and expenses of a forensic accountant.

e. PERIOD OF INDEMNIFICATION (POI): This is the period during which income loss is recoverable under the policy. How POI is defined can vary among policy forms. It may be limited to the time a computer system was not functional, or it may be defined as the time that business operations were interrupted. It may also be measured by a set number of days or include a set number of days after a system is restored or business operations return to normal — sometimes referred to as an extended period of indemnification (EPOI).

Exclusions should also be noted. Cyber business interruption coverage is generally not available for an event that involves physical property damage or is caused by a natural peril; business interruption coverage may be available for these events in a property policy. Cyber policies also typically exclude coverage for events caused by failure of infrastructure (water, power, internet) and by government actions. Some expenses, such as the costs to defend lawsuits, are often excluded from cyber business interruption insurance but might be covered under a different part of a cyber policy or another insurance policy.

When a cyber event happens

Once it becomes clear that a cyber event has occurred, it is important to act immediately. If an organization has an incident response plan, it should be triggered and followed by the incident response team. If your organization must respond to a cyber event, you should:

- Contact your broker and insurer to discuss rights and requirements under your insurance policy. Most cyber policies require insurer consent before vendors can be retained.
- Retain breach counsel, with carrier consent, to ensure all legal obligations in connection with the breach are met and that your rights are protected. Counsel should retain, on your behalf and with your insurer's consent, a forensic firm and/or other cyber technical experts to investigate, evaluate, and remediate the event. In connection with a business interruption claim, these vendors will help you:
    a. Confirm the cause of the event or loss, so carriers can determine whether a covered event occurred.
    b. Identify specific affected systems and impact to the business.
    c. Determine the proper corrective action and most efficient recovery timeline.
    d. Identify any technology upgrades that may have been completed concurrently with the event that may impact the period of recovery.
- Consider the steps needed to continue conducting business as normally as possible during the event and/or to return to operations as quickly as possible.
- Keep track of all expenses that would not have been incurred but for the cyber event. Policy language may differ, but it is better to maintain records for all expenses and determine whether there is coverage later. Include records for temporary employees hired or additional hours worked by regular hourly employees.
- Gather the documentation necessary to prove business income loss (see Appendix B) and hire forensic accountants to review with your financial team.
- Consider income loss while computers were not functioning and after computer systems return to the state they were in prior to the event. Did it take additional time for business operations to return to normal? How quickly did customers return? Did you actually lose income, or was it deferred until after business operations returned to normal?
- Discuss with your broker, forensic accountant, and the insurer's forensic accountant the methodology to calculate the BI loss before the proof of loss is submitted to the carrier.

It is important to remember that responding to a cyber event, and submitting a BI claim, is a process. Rely on the experts you have retained, especially your broker and forensic accountant, to guide you. BI claim resolution may take months, depending on the complexity of the claim. Communication is key to making this process more efficient.

Business interruption in healthcare

A large hospital is the victim of a ransomware attack, which encrypts multiple servers, including the hospital's backups. The hospital must divert its emergency room patients to other hospitals. Imaging machines and other devices are down. Appointments and surgeries are rescheduled or canceled. Additional staffing is required as all medical charts must be filled out manually. And sensitive patient information is compromised and exfiltrated. It takes the hospital more than a month to become fully operational again, even after paying a ransom.

The restoration costs, income loss, and extra expenses are well over $60 million. This amount does not include the ransom payment of $10 million and the costs for breach counsel, forensic investigations, notification to patients, regulatory investigations, and third-party class action defense and settlement.

These costs add up quickly. It is imperative that a business conduct due diligence before an event to make sure it has adequate insurance coverage.

Conclusion

As technology continues to improve, businesses will utilize it for efficiency, productivity, and growth, thus remaining vulnerable to technology-related disruptions. How organizations respond to a disruption will determine, in some instances, whether they will continue to thrive, or even survive.

Cyber insurance, and in particular BI coverage, can help businesses mitigate this risk. Businesses, however, do not have to navigate these risks alone.

Cyber risk consultants can help your organization assess its exposure to cyber threats, non-data breach privacy issues, and other forms of cybercrime. These specialists can also help you determine the potential financial impacts of cyber events and develop strategies to mitigate them.

Your broker can help navigate the complexities of cyber insurance policies, ensuring that a business is adequately protected against evolving cyber threats while optimizing insurance coverage. An experienced and knowledgeable broker can help you select the right policies and appropriate coverage limits and act as an intermediary between you and your insurer during the claims process.

A forensic accountant, as part of your incident response team, is also key to this process. Forensic accountants can project future losses and evaluate the effectiveness of your business continuity plans. During the claims process, a forensic accountant can help you quantify your financial impact and any lost revenue due to an event. Post-incident, forensic accountants can assist preparing detailed reports, such as a proof of loss, to submit to your insurer in compliance with your policy.[3]

Staying ahead of cyber threat actors may seem like a full-time job, but relying on experts to put you in the best financial place for recovery is crucial. Do not wait until a cyber event happens to fully understand the impact this may have on your business — start planning today to be ready for a cyber event tomorrow.

[3] Most cyber insurance policies with business interruption coverage provide a sublimit for preparation of proof of loss costs, which would include forensic accounting costs.

Appendix A: Post-breach documentation — request for information (RFI)

Preliminary questions for the insured

1. What date and time were the claimed location(s) impacted by the cyber event?
2. What date and time was the cyber event discovered?
3. What date and time did the claimed location(s) resume normal business operations after the cyber event?
4. What are the normal business hours for the claimed location(s)?
5. How were various business segments impacted by the cyber event?
6. Were any operations completely shut down?
7. Were any operations partially shut down?
8. How did the shutdown affect revenue streams and expenses? How does the business generate its various revenue streams?
    a. How did the cyber event prevent the business from generating revenue?
    b. Were clients/customers turned away due to the cyber event?
    c. Was revenue/production able to be made up?
9. Does the organization have any fixed fee or time and material contracts?
10. Was payroll impacted by the cyber event?
11. Are employees salaried, hourly, or both?
12. What work did employees perform during the period of restoration?
13. Was overtime paid to employees due to the cyber event? If so, when and how is it tied to the cyber event?
14. Are any employees’ hours billable? If so, how does the organization track their normal billable hours?
15. How were operating expenses impacted by the cyber event?
16. Did the business incur any additional expenses due to the cyber event?

Appendix B: Potential documentation requests

These requests will normally be made to include preloss, loss, and postloss periods to enable the projection of operating results (trending), the actual activity during the loss compared to the projections, and the postloss operations to identify any potential makeup. Periods and records requested will vary by the answers to questions listed in Appendix A.

1. Business interruption/extra expense claim schedules in Excel to include all supporting documents.
2. Detailed monthly profit and loss statements, by location, if applicable.
3. Monthly/weekly/daily revenue reports, by location, if applicable.
4. Invoices/receipts for major extra expenses incurred.
5. Federal income tax returns, including all supporting schedules (not always necessary).
6. Monthly/weekly/daily production records.
7. Monthly/weekly/daily timekeeper reports, by hours worked, total hours billed, and total dollars billed.
8. Weekly payroll registers (sometimes by employee, other times by department).
9. Listing of any lost clients/projects as a direct result of the cyber event.
10. Staff utilization reports for professional services firms.
11. Inventory records for production/manufacturing entities.

LOCKTON®

UNCOMMONLY INDEPENDENT

JS HELD

Find your expert.®

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.