Marsh

County Reinsurance Limited Cyber Claims and Incident Response Training

November 12, 2025

Presenters

Marsh Cyber Team

Tom Fuhrman

Senior Consultant, Cybersecurity Consulting, US

Tom Fuhrman is a senior cybersecurity consultant in Marsh Advisory. A recognized business leader, consultant, and thought leader in cybersecurity, he has supported clients of all sizes in all major industry sectors. He has 20+ years of cybersecurity consulting and business leadership experience and has held senior leadership positions in other cybersecurity consultancies.

Jim Holtzclaw

Senior Vice President, Cybersecurity Consulting, US

Jim is a senior cybersecurity consultant with over 32 years of experience and leads a team of cybersecurity consultants within Marsh Advisory providing cybersecurity expertise and working to identify, develop, implement, conduct, and execute Marsh's cybersecurity consulting strategy, capabilities, and services in North America.

Olivia Colloca

Assistant Vice President, Cyber Claims Advocacy & Cyber Incident Management, US

Olivia is responsible for informing clients about cyber incident response best practices, walking clients through the cyber claims process in preparation of a cyber event and providing clients with access to Marsh digital offerings.

Mark Massey

Managing Director, Forensic Accounting & Claims Services, US

Mark specializes in forensic accounting, insurance claims, litigation support, and the provision of expert witness testimony. He has extensive experience with complex risks including cyber and property damage triggered business interruption insurance claims, corporate fraud, corruption exposures, and SEC investigations.

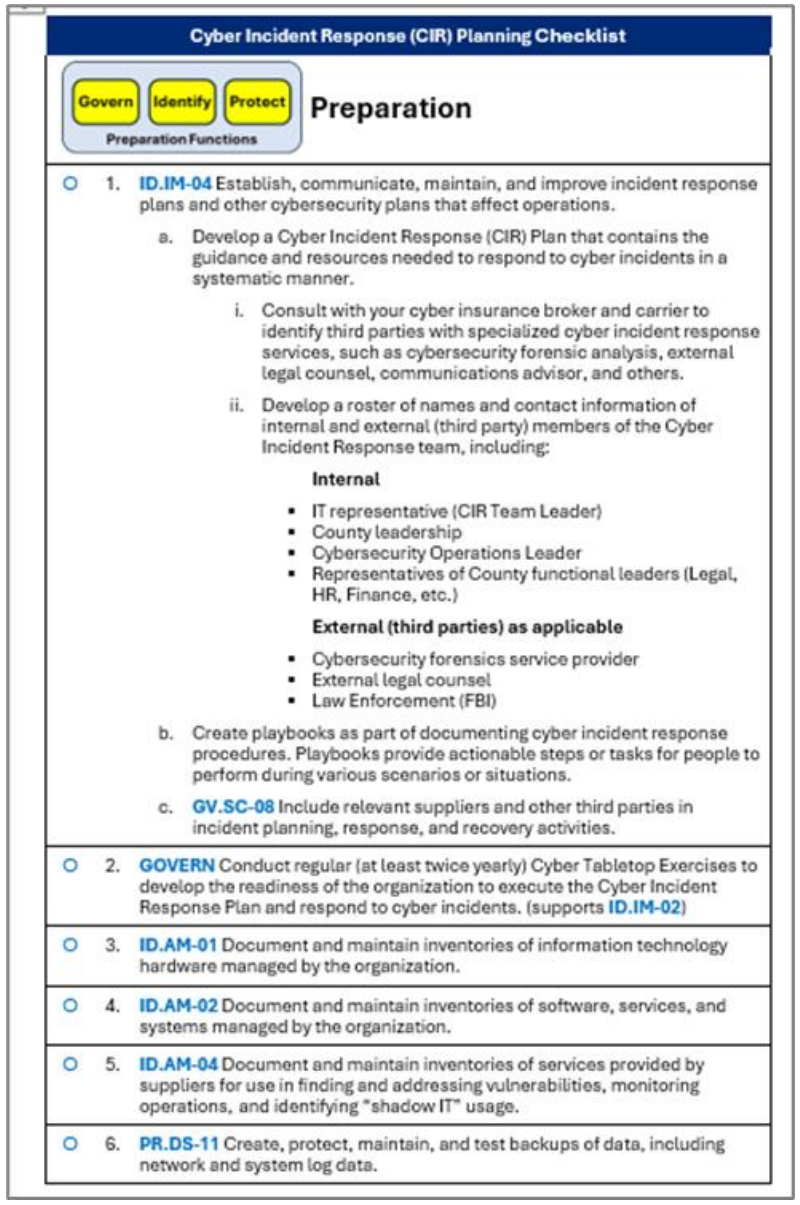
1. Incident Response Checklist and Preparedness
2. Polling Questions
3. Cyber Incident and Claims Protocol
4. The Cyber BI Claim Process
    - First Steps To Financial Recovery
    - Cyber Claim Template Walkthrough

Agenda

Incident Response Checklist and Preparedness

Cyber Incident Response (CIR) Planning checklist

Purpose: This checklist is designed to help organizations improve their *preparedness* to respond to cyber incidents. The steps of this checklist also create the foundation upon which the Cyber Incident Response (CIR) Plan is built. This checklist is *not a substitute* for a CIR Plan.



Cyber Incident Response (CIR) Planning Checklist

Govern | Identify | Protect — Preparation Functions

Preparation

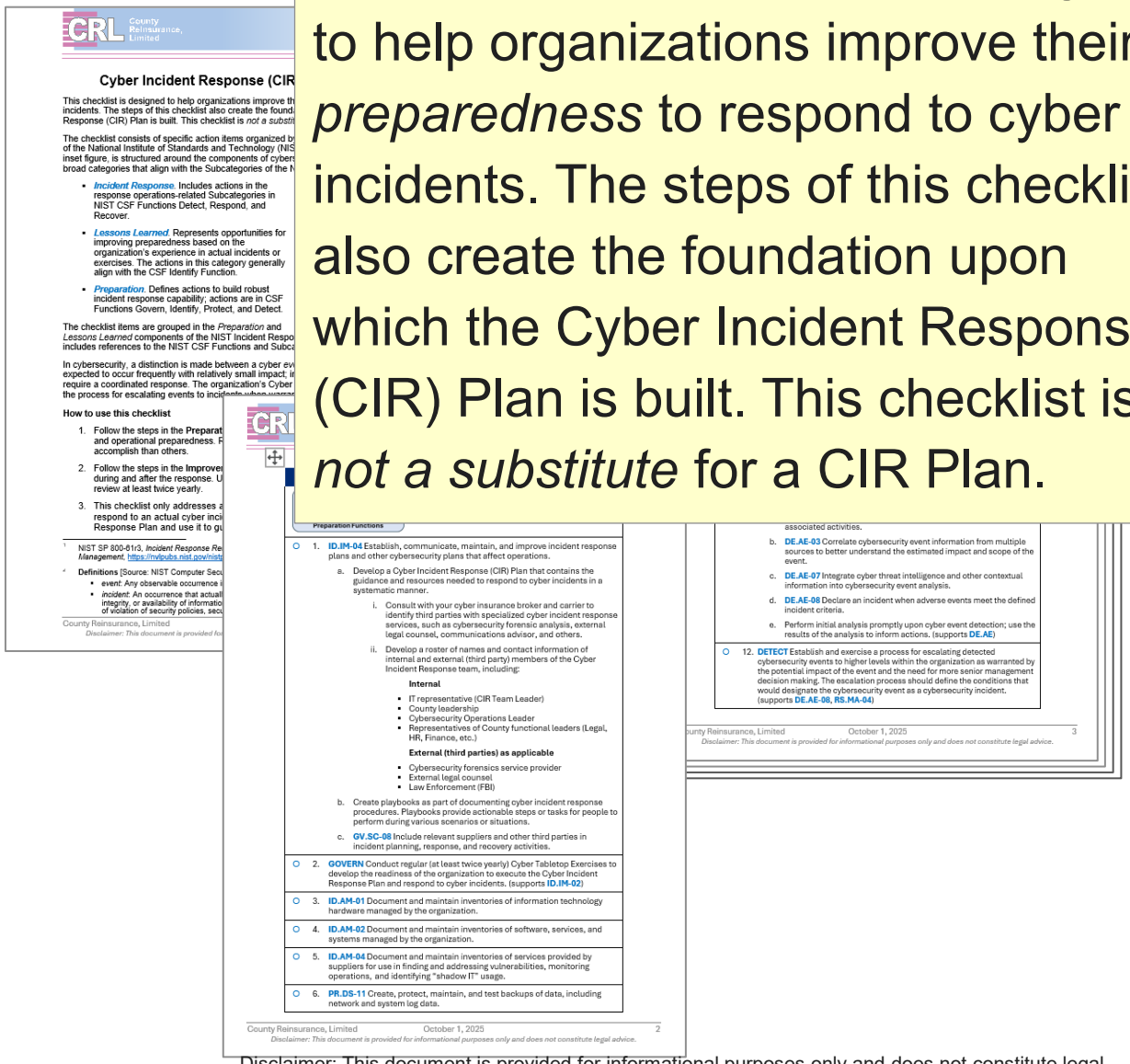
- 1. **ID.IM-04** Establish, communicate, maintain, and improve incident response plans and other cybersecurity plans that affect operations.
  - a. Develop a Cyber Incident Response (CIR) Plan that contains the guidance and resources needed to respond to cyber incidents in a systematic manner.
    - i. Consult with your cyber insurance broker and carrier to identify third parties with specialized cyber incident response services, such as cybersecurity forensic analysis, external legal counsel, communications advisor, and others.
    - ii. Develop a roster of names and contact information of internal and external (third party) members of the Cyber Incident Response team, including:

      Internal

      - IT representative (CIR Team Leader)
      - County leadership
      - Cybersecurity Operations Leader
      - Representatives of County functional leaders (Legal, HR, Finance, etc.)

      External (third parties) as applicable

      - Cybersecurity forensics service provider
      - External legal counsel
      - Law Enforcement (FBI)
  - b. Create playbooks as part of documenting cyber incident response procedures. Playbooks provide actionable steps or tasks for people to perform during various scenarios or situations.
  - c. **GV.SC-08** Include relevant suppliers and other third parties in incident planning, response, and recovery activities.
- 2. **GOVERN** Conduct regular (at least twice yearly) Cyber Tabletop Exercises to develop the readiness of the organization to execute the Cyber Incident Response Plan and respond to cyber incidents. (supports **ID.IM-02**)
- 3. **ID.AM-01** Document and maintain inventories of information technology hardware managed by the organization.
- 4. **ID.AM-02** Document and maintain inventories of software, services, and systems managed by the organization.
- 5. **ID.AM-04** Document and maintain inventories of services provided by suppliers for use in finding and addressing vulnerabilities, monitoring operations, and identifying "shadow IT" usage.
- 6. **PR.DS-11** Create, protect, maintain, and test backups of data, including network and system log data.

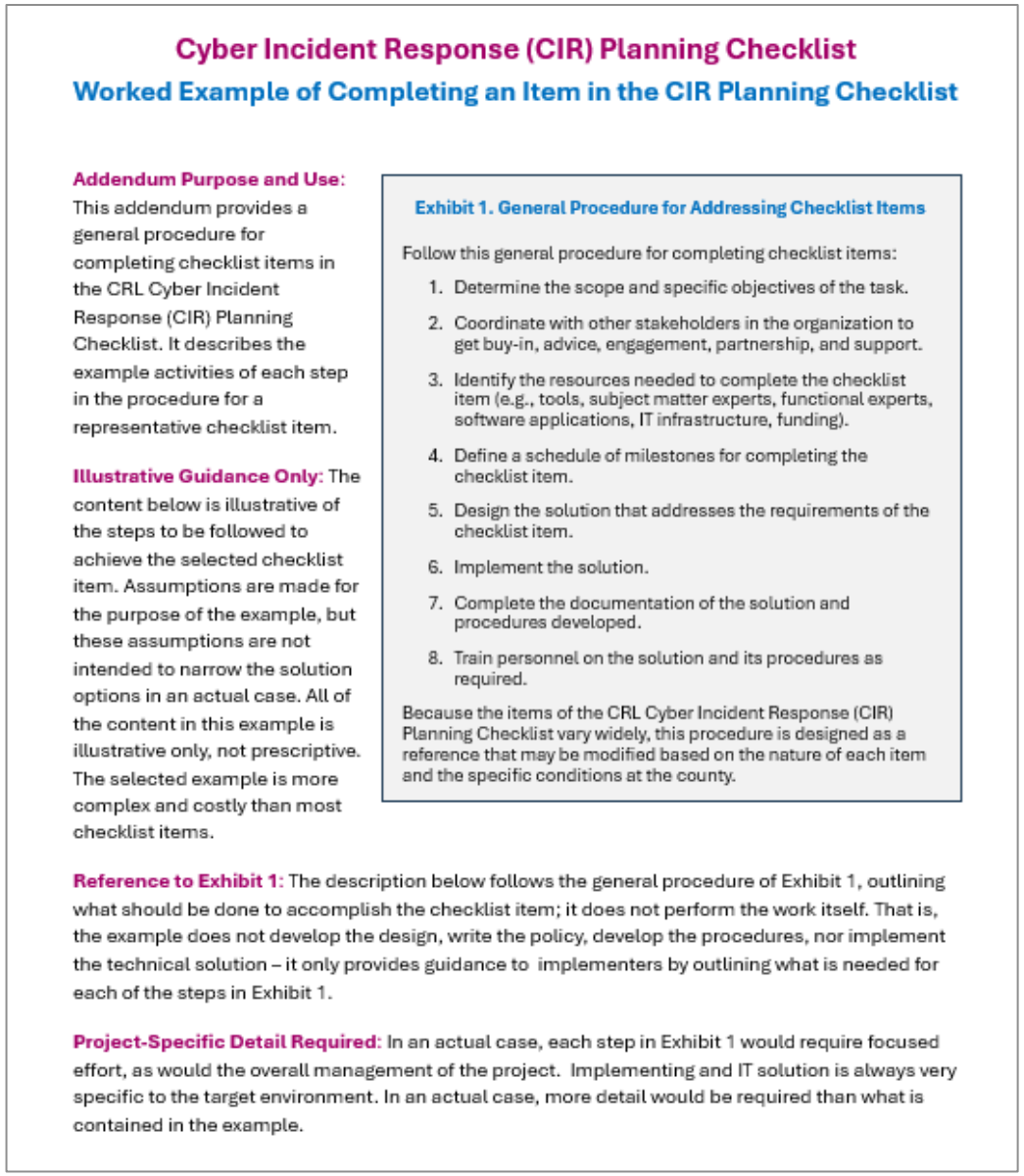


Disclaimer: This document is provided for informational purposes only and does not constitute legal advice.

“Worked example” of completing a Planning checklist step

Purpose: The worked example document is designated as an “Addendum to the Cyber Incident Response Planning Checklist”. It includes a preface containing a general procedure for completing checklist items found in the CRL Cyber Incident Response (CIR) Planning Checklist, and one detailed example.

Checklist Item 6 (**PR.DS-11** “Create, protect, maintain, and test backups of data, including network and system log data.”) was selected as the exemplar because of its importance and relative complexity. The example follows the steps of the general procedure.



Cyber Incident Response (CIR) Planning Checklist

Worked Example of Completing an Item in the CIR Planning Checklist

Addendum Purpose and Use: This addendum provides a general procedure for completing checklist items in the CRL Cyber Incident Response (CIR) Planning Checklist. It describes the example activities of each step in the procedure for a representative checklist item.

Illustrative Guidance Only: The content below is illustrative of the steps to be followed to achieve the selected checklist item. Assumptions are made for the purpose of the example, but these assumptions are not intended to narrow the solution options in an actual case. All of the content in this example is illustrative only, not prescriptive. The selected example is more complex and costly than most checklist items.

Exhibit 1. General Procedure for Addressing Checklist Items

Follow this general procedure for completing checklist items:

1. Determine the scope and specific objectives of the task.
2. Coordinate with other stakeholders in the organization to get buy-in, advice, engagement, partnership, and support.
3. Identify the resources needed to complete the checklist item (e.g., tools, subject matter experts, functional experts, software applications, IT infrastructure, funding).
4. Define a schedule of milestones for completing the checklist item.
5. Design the solution that addresses the requirements of the checklist item.
6. Implement the solution.
7. Complete the documentation of the solution and procedures developed.
8. Train personnel on the solution and its procedures as required.

Because the items of the CRL Cyber Incident Response (CIR) Planning Checklist vary widely, this procedure is designed as a reference that may be modified based on the nature of each item and the specific conditions at the county.

Reference to Exhibit 1: The description below follows the general procedure of Exhibit 1, outlining what should be done to accomplish the checklist item; it does not perform the work itself. That is, the example does not develop the design, write the policy, develop the procedures, nor implement the technical solution – it only provides guidance to implementers by outlining what is needed for each of the steps in Exhibit 1.

Project-Specific Detail Required: In an actual case, each step in Exhibit 1 would require focused effort, as would the overall management of the project. Implementing and IT solution is always very specific to the target environment. In an actual case, more detail would be required than what is contained in the example.

First 24 hours Cyber Incident Response Checklist

Purpose: This document is a checklist of actions to be performed – and actions to be avoided – from the immediate response through full recovery. Ideally, this checklist is used in conjunction with an organizational Cyber Incident Response (CIR) Plan. This checklist has 27 items.

CRL County Reinsurance, Limited

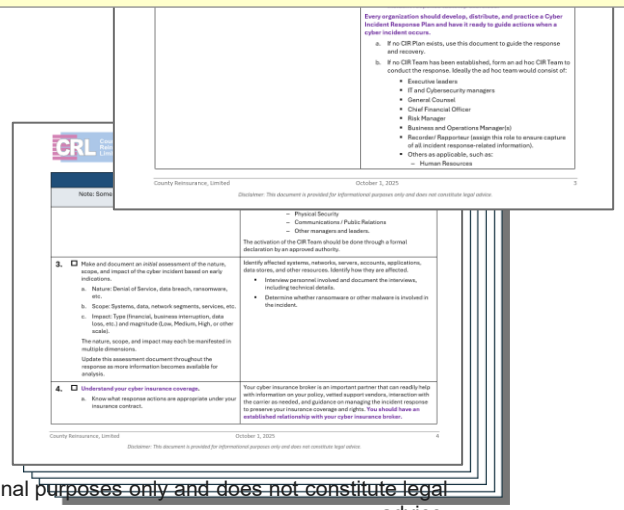
Cyber Incident Response Checklist

The Action Steps in this checklist are organized sequentially, but the Cyber Incident Response (CIR) Team should make adjustmen execution as necessary while recognizing that some steps depend on the completion of others. Additionally, some steps may be accomplished in parallel.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparednes **These actions are highlighted with purple bold font.**	
IMMEDIATE RESPONSE	*The Action Steps of this stage of the effort organize the response arou the categories of Containment, Eradication, and Recovery.*
1. ☐ Document the date and time that internal IT or IT Security personnel detected or were informed of the cyber incident / breach.	Recording the time of detection or notification will be important in analyzing the incident and determining its impact. This should be the beginning of an official record of all discoveries, decisions, and actions to support subsequent review of the response and an insurance claim if needed.
2. ☐ Notify the leader of the cyber incident and launch the organization's response. a. Activate the **Cyber Incident Response (CIR) Plan** following approval by the appropriate executive(s) or senior manager(s). b. Activate the **CIR Team**.	Strong informed leadership is crucial to effective response and recovery. a. **The role of Cyber Incident Response Leader should be pre-assigned, and the designated leader should receive instruction in the responsibilities of the role.** If no Cyber Incident Response Leader has been pre-assigned, a leader should be designated consistent with Items a, b, c, and d below: a. The leader should be an executive with decision-making authority such as the Chief Information Officer, Director of IT, Superintendent, or equivalent/designee.

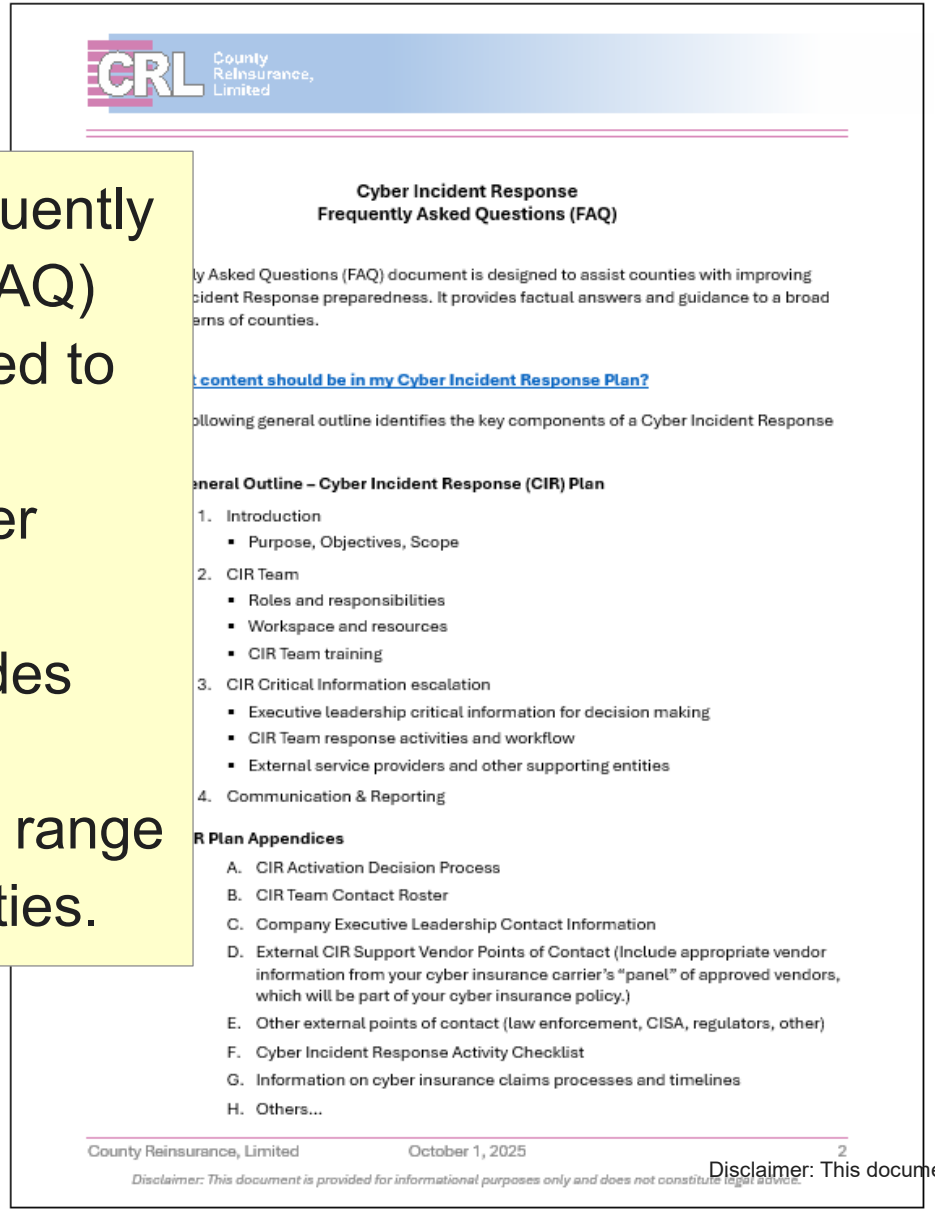
County Reinsurance, Limited October 1, 2025 2

Disclaimer: This document is provided for informational purposes only and does not constitute legal advi



Frequently Asked Questions (FAQ) document

Purpose: This Frequently Asked Questions (FAQ) document is designed to assist counties with improving their Cyber Incident Response capabilities. It provides factual answers and guidance to a broad range of concerns of counties.



County Reinsurance, Limited

Cyber Incident Response
Frequently Asked Questions (FAQ)

…y Asked Questions (FAQ) document is designed to assist counties with improving …cident Response preparedness. It provides factual answers and guidance to a broad …erns of counties.

…t content should be in my Cyber Incident Response Plan?

…llowing general outline identifies the key components of a Cyber Incident Response …

…neral Outline – Cyber Incident Response (CIR) Plan

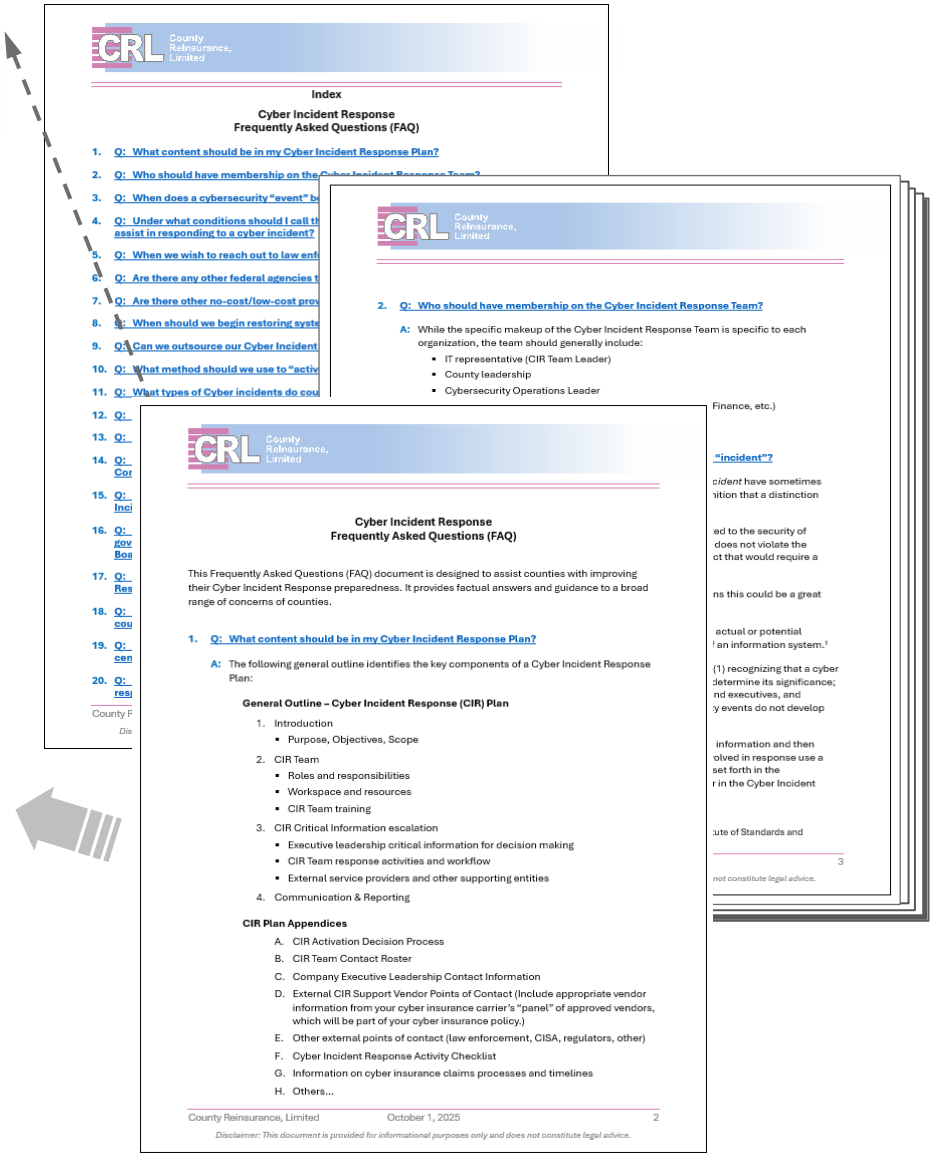
1. Introduction
   - Purpose, Objectives, Scope
2. CIR Team
   - Roles and responsibilities
   - Workspace and resources
   - CIR Team training
3. CIR Critical Information escalation
   - Executive leadership critical information for decision making
   - CIR Team response activities and workflow
   - External service providers and other supporting entities
4. Communication & Reporting

…R Plan Appendices

A. CIR Activation Decision Process
B. CIR Team Contact Roster
C. Company Executive Leadership Contact Information
D. External CIR Support Vendor Points of Contact (Include appropriate vendor information from your cyber insurance carrier's "panel" of approved vendors, which will be part of your cyber insurance policy.)
E. Other external points of contact (law enforcement, CISA, regulators, other)
F. Cyber Incident Response Activity Checklist
G. Information on cyber insurance claims processes and timelines
H. Others…

County Reinsurance, Limited October 1, 2025 2

Disclaimer: This document is provided for informational purposes only and does not constitute legal advice.



County Reinsurance, Limited

Index

Cyber Incident Response
Frequently Asked Questions (FAQ)

1. Q: What content should be in my Cyber Incident Response Plan?
2. Q: Who should have membership on the Cyber Incident Response Team?
3. Q: When does a cybersecurity "event" b…
4. Q: Under what conditions should I call t… assist in responding to a cyber incident?
5. Q: When we wish to reach out to law enf…
6. Q: Are there any other federal agencies t…
7. Q: Are there other no-cost/low-cost prov…
8. Q: When should we begin restoring syste…
9. Q: Can we outsource our Cyber Incident …
10. Q: What method should we use to "activ…
11. Q: What types of Cyber incidents do cou…
12. Q:
13. Q:
14. Q: Cor…
15. Q: Inci…
16. Q: gov… Bos…
17. Q: Res…
18. Q: cou…
19. Q: cen…
20. Q: resi…

County F…

Dis…

2. Q: Who should have membership on the Cyber Incident Response Team?

A: While the specific makeup of the Cyber Incident Response Team is specific to each organization, the team should generally include:

- IT representative (CIR Team Leader)
- County leadership
- Cybersecurity Operations Leader

Finance, etc.)

"incident"?

cident have sometimes …ition that a distinction …

…ed to the security of … does not violate the …ct that would require a …

…ns this could be a great …

…actual or potential …an information system.[1]

(1) recognizing that a cyber …determine its significance; …nd executives, and …y events do not develop …

…information and then …olved in response use a …set forth in the …r in the Cyber Incident …

…ute of Standards and …

3

…not constitute legal advice.

County Reinsurance, Limited

Cyber Incident Response
Frequently Asked Questions (FAQ)

This Frequently Asked Questions (FAQ) document is designed to assist counties with improving their Cyber Incident Response preparedness. It provides factual answers and guidance to a broad range of concerns of counties.

1. Q: What content should be in my Cyber Incident Response Plan?

A: The following general outline identifies the key components of a Cyber Incident Response Plan:

General Outline – Cyber Incident Response (CIR) Plan

1. Introduction
   - Purpose, Objectives, Scope
2. CIR Team
   - Roles and responsibilities
   - Workspace and resources
   - CIR Team training
3. CIR Critical Information escalation
   - Executive leadership critical information for decision making
   - CIR Team response activities and workflow
   - External service providers and other supporting entities
4. Communication & Reporting

CIR Plan Appendices

A. CIR Activation Decision Process
B. CIR Team Contact Roster
C. Company Executive Leadership Contact Information
D. External CIR Support Vendor Points of Contact (Include appropriate vendor information from your cyber insurance carrier's "panel" of approved vendors, which will be part of your cyber insurance policy.)
E. Other external points of contact (law enforcement, CISA, regulators, other)
F. Cyber Incident Response Activity Checklist
G. Information on cyber insurance claims processes and timelines
H. Others…

County Reinsurance, Limited October 1, 2025 2

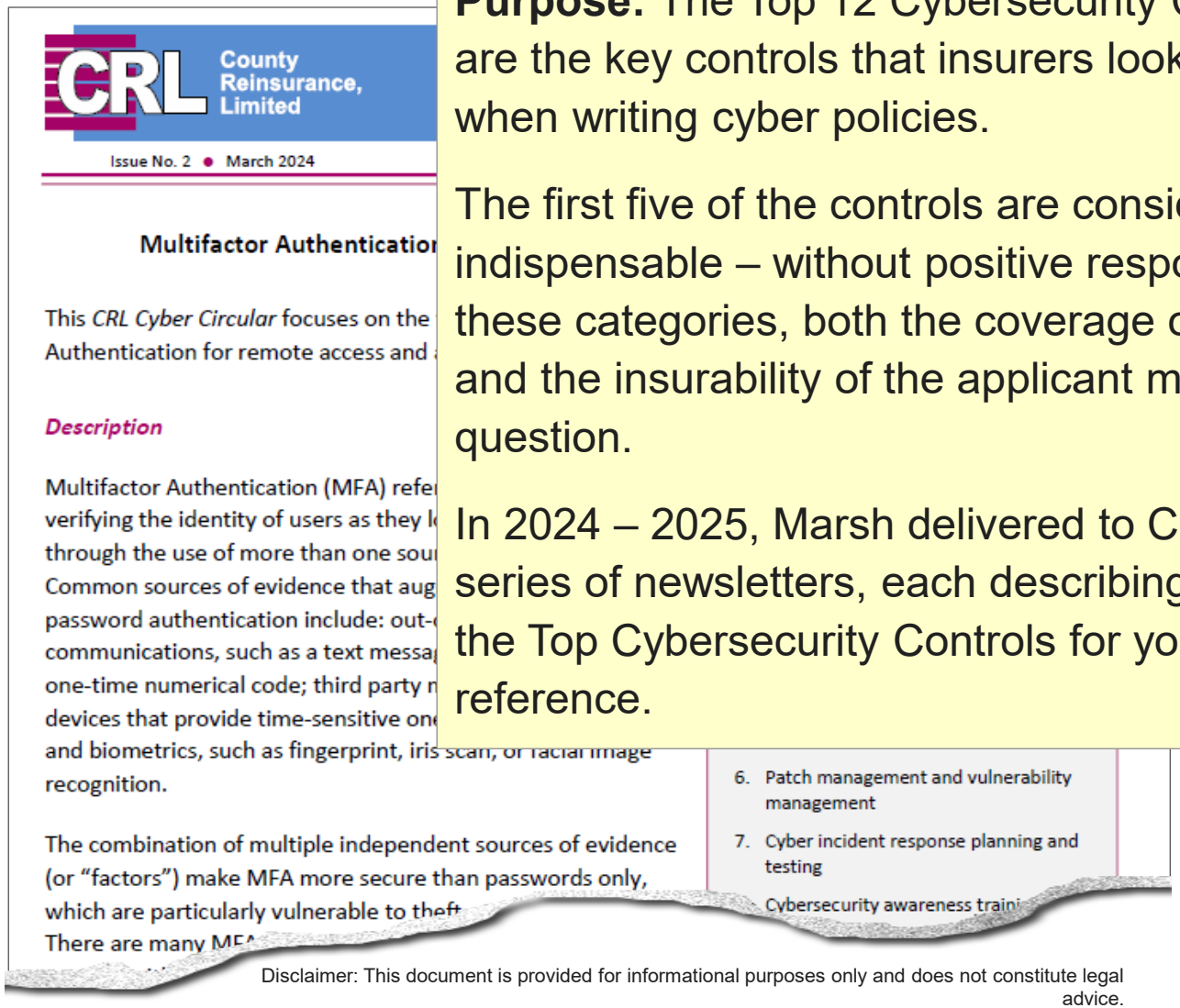
Disclaimer: This document is provided for informational purposes only and does not constitute legal advice.

Marsh Top 12 Cybersecurity Controls

Key controls that insurers look for when writing cyber policies

Top 12 Cybersecurity Controls

1. **Multifactor authentication for remote access and admin/privileged controls**
2. **Endpoint Detection and Response (EDR)**
3. **Secured, encrypted, and tested backups**
4. **Privileged Access Management (PAM)**
5. **Email filtering and web security**
6. Patch management and vulnerability management
7. Cyber incident response planning and testing
8. Cybersecurity awareness training and phishing testing
9. Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
10. Logging and monitoring/network protections
11. End-of-life systems replaced or protected
12. Vendor/digital supply chain risk management


CRL County Reinsurance, Limited

Issue No. 2 • March 2024

Multifactor Authentication

This *CRL Cyber Circular* focuses on the
Authentication for remote access and

Description

Multifactor Authentication (MFA) refe
verifying the identity of users as they l
through the use of more than one sou
Common sources of evidence that aug
password authentication include: out-
communications, such as a text messa
one-time numerical code; third party
devices that provide time-sensitive on
and biometrics, such as fingerprint, iris scan, or facial image
recognition.

The combination of multiple independent sources of evidence
(or "factors") make MFA more secure than passwords only,
which are particularly vulnerable to theft
There are many MF

6. Patch management and vulnerability management
7. Cyber incident response planning and testing
Cybersecurity awareness traini

Purpose: The Top 12 Cybersecurity Controls are the key controls that insurers look for when writing cyber policies.

The first five of the controls are considered indispensable – without positive responses in these categories, both the coverage offered and the insurability of the applicant may be in question.

In 2024 – 2025, Marsh delivered to CRL a series of newsletters, each describing one of the Top Cybersecurity Controls for your reference.

Defining a Cyber Incident and Event

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

Cybersecurity Event: Also called an "event" is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. **Adverse events** are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

Cybersecurity Incident: Also called an "incident" is activity that is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. These activities usually include successfully gaining unauthorized access to IT systems, network, and/or data resident in the breached systems. Note: A single or multiple adverse events as described above can be determined by the Chief Information Security Officer or senior Cybersecurity Analyst to be an incident

What is an incident?

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

In general, an incident is a violation of computer security policies, acceptable use policies, or standard computer security practices.

Some examples are:

1. A perpetrator obtains unauthorized access to sensitive data and threatens to release the details to the press if the organization does not pay a designated sum of money.

2. A hacker launches a ransomware attack by exploiting a vulnerability in a platform provided by a Third party.

3. Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.

4. A user provides illegal copies of software to others through peer-to-peer file sharing services.

Cyber Incident Severity Levels and Descriptions

Level	Severity Description	Reaction	Cyber Incident Examples
1	Widespread impact and/or large number of critical systems impacted; high risk of compromise and disruption to IT systems, applications, and infrastructure. Critical infrastructure, IT systems, and/or application(s) impacts; Significant widespread data breach; impacts to multiple business units that may lead to severe damage to systems. These are high-risk incidents that have the potential to cause severe damage to the business and operations environment. **All Sev-1 incidents are considered major incidents.**	**Activate CIR Team (Full Response)**	Distributed Denial of Service attack(s), enterprise-wide malware attack impacting systems and infrastructure and multiple business units (BUs). Significant critical application(s), operating system(s), or infrastructure vulnerability; data breach impacting employees and/or customers; zero-day vulnerability; enterprise wide malware outbreak and propagation.
2	Impact to a single business unit's applications or infrastructure; typically limited impact in nature and not widespread.	**Activate with Specific Activities and/or CIR Team functions**	Malware infection that is limited to a single business unit or functional group; lost IT asset containing critical application(s) or data; unauthorized creation of IDs on critical systems; user-caused contiguous failed/successful login attempts; failed attempts of tampering with critical systems, applications, audit log files, and databases; uncleaned malware in a single user machine; phishing or spear-phishing activity targeting a single user or small group of users.

Cont'd

Cyber Incident Severity Levels and Descriptions

Continued

Level	Severity Description	Reaction	Cyber Incident Examples
3	Impact a single end-user or non-critical business processes. No direct impact to core business operations; possible impact to supporting or auxiliary IT systems and/or applications that support daily operations; includes unauthorized activity or policy violation.	**Activate with Limited Actions or Increased Monitoring only**	Widespread scans and probes, discovery scanning; information gathering scripts; other reconnaissance probes; downloading of unauthorized software, scripts or files; use of unauthorized P2P applications; activities that is unusual in nature that may require continued monitoring for awareness.
4	No to Very Small impact to business operations. Sev-4 is usually an informational alert in nature as well as false positives. There is no impact to any business operations.	**No Action Required**	A report regarding unusual activity that has been detected; a series of false positives that requires change to audit logging for impacted devices/IT systems.

Notes:

1. Severity levels are used to link the incident significance and the business impact.
2. The description should ease identification of the impact and is used to simplify response decisions where possible.
3. For Levels 3 and 4 (Sev-3, Sev-4), if there is an “Activate CIR Plan response with Minimal or Limited Activities,” This activation requires the activation decision to define what minimal activities includes.

Polling Questions

Cyber Incident and Claims Protocol

Cyber Incident and Claims Protocol

What to do in the event of a cyber incident

Step 1

Discovery of an actual or suspected cyber-incident

- Upon discovery of an actual or reasonably suspected cyber-incident, start to gather known information such as:
  - Description of event,
  - When event was discovered,
  - How event was discovered, and
  - Any steps/actions taken to date

Step 2

Engage breach counsel & digital forensics firm

- Outreach to breach counsel will initiate a triage call to determine the scope of the incident.
- Outreach to digital forensics firm will begin forensic investigation following a cyber incident
- **Note: Breach counsel should engage digital forensics firm in order to preserve privilege**

Step 3

Engage additional vendors as needed

- Depending on the nature of the cyber incident, additional vendors may need to be involved. Be sure to have breach counsel engage any additional vendors to preserve attorney-client privilege.

When to Bring in Breach Counsel?

To protect your privilege, you should consider engagement of breach counsel so they can assist you in determining the extent of the incident / obligations you may have to investigate the investigation

- Data breach meaning:
  - Theft, loss, or unauthorized disclosure of personally identifiable information or third-party information that is in the care, custody or control of the your organization or a third party for whose theft, loss or unauthorized disclosure of personally identifiable information or third-party information where your organization is liable

- Security breach, meaning a failure of computer security to prevent:
  - Unauthorized access or use of computer systems, including unauthorized access or use resulting from the theft of a password from a computer system or your organization;
  - A denial of service attack affecting computer systems;
  - A denial of service attack affecting computer systems that are not owned, operated or controlled by your organization; or
  - Infection of computer systems by malicious code or transmission of malicious code from computer systems

Cyber Incident Response Considerations

How to enable a successful cyber incident response

Potential topics of discussion during the initial triage call:

- How and when your organization become aware of the event
- The individual that became aware of the event
- General types of equipment impacted such as email, financial reporting, network drives, internet sales, operations, HR systems, manufacturing, etc.
- Data potentially affected such as customer, vendor, and/or employee data
- Any immediate affect the event is having on the company's operations, such as downtime
- Any involvement of a loss of funds, payment fraud or ransom/extortion demand
- If a ransomware event, the extortion demand deadline if known
    - Have you received a demand yet? Did the TA identify themselves? Any indication of data exfiltration?
- The extent third parties'/customers' systems are involved or affected
- Response and remediation actions taken to date such as internal IT is working on the incident, systems shut down, IT contractors already hired, attorneys retained, etc.

Additional tips:

Keep your answers to the questions on the left fact based, you do not want to speculate on any of the unknown information relevant to the cyber incident

Allow breach counsel to engage additional vendors in order to preserve privilege

Do not submit event as a *Breach* since the term has legal ramifications. Instead of breach, use *cyber incident, cyber event, cyber loss, etc.*

Keep offline, hard copies of any critical document in case your corporate systems are compromised

Vendor Selection

Breach counsel and digital forensics firm should be identified prior to a cyber incident as these will be the first vendors engaged

A retainer may be put in place with breach counsel and/or digital forensics firm to guarantee capacity

It may be helpful to meet with breach counsel and digital forensics firms prior to selection to ensure expertise and experience in the industry

Claims Scenario: Single Entity

First-Party Incident – Ransomware Incident

1. Immediately stop using ordinary email systems if there is known infiltration into the system
   - Consider using an out-of-band communication system to continue speaking
2. Engage breach counsel as soon as practicable
   - Breach counsel will give you guidance in terms of engaging additional vendors to preserve attorney client privilege (i.e. digital forensics/restoration firms to get your systems back up and running and extortion service providers to interact with the threat actor), advising if notification to law enforcement is required and next steps of what should be done
3. Do not contact the threat actor directly
   - An extortion service provider may be utilized to:
     - Provide information about the threat actor
     - Negotiate directly with the threat actor
     - Obtain proof that decryption keys will work if a payment is made
     - Procure cryptocurrency
     - Perform an OFAC compliance check
     - Facilitate payment

Claims Scenario: Single Entity Continued

First-Party Incident – Ransomware Incident

4. Think about the following considerations when deciding whether to pay the ransom demand or not: (ultimately, this will be a business decision for your organization to make)
   - Feasibility and time needed to recover data and systems; and criticality of those systems
   - Impact of public disclosure of data
   - Ability to restore (backups) without paying the ransom
   - Ability to reduce the ransom amount
   - Factoring whether an encryption key will work if the ransom is paid
   - Cost of the ransom versus the estimated cost of restoration
5. Maintain proper records and track data recovery and restoration costs
   - Screenshot or copy of the initial extortion demand and communications with the threat actors
   - Communications with law enforcement
   - Proof of payment
   - OFAC due diligence documentation
   - Document costs of business impacts, i.e. loss or reduction in revenue, slow down or interference with operations, additional expenses incurred to remediate the event (i.e. hourly employee overtime)

Claims Scenario: Multiple Entities

Third-Party Incident – Usage of Common Vendor

- Report to Insurer and determine full extent of how many entities are impacted
- Contact breach counsel
  - Breach counsel will give you guidance in terms of engaging additional vendors to preserve attorney client privilege (i.e. digital forensics/restoration firms)
  - Coordinate with other entities to determine if the same breach counsel is being used. Using the same breach counsel may be helpful to in terms of efficiency, pricing and engagement of additional vendors (working with multiple entities may be able to bring your matter to the front of the queue)
- Figure out financial / data impact to your entity
  - Counsel will determine data impact, but you will need to be able to determine the type of information that has been impacted
- Restore systems if need be
- Track any type of financial loss
  - Be sure to track any costs that are incurred that are not normal business costs (i.e. hourly employees working overtime to manually input data) to be able to so show the impact to insurer if loss rolls up and insurance kicks in
- Monitor any impact to others as lawsuits may result

Incident Response Vendors

Roles and responsibilities of the parties involved

Breach Counsel

Law firm engaged to provide legal incident response assistance. Breach Counsel will assist in coordinating the entire cyber-incident by identifying and engaging additional third party vendors that may be necessary in incident response and restoration efforts.

Digital Forensics and Incident Response (DFIR)

Firm engaged to perform a forensics investigation following a cyber-incident. A forensics investigation can determine the existence, cause, source and scope of a cyber-incident, and if applicable, to mitigate, terminate, remove and/or otherwise remedy such cyber-incident. DFIR providers may offer extortion services.

Extortion Service Providers

Firm engaged to facilitate and negotiate extortion threats on behalf of an organization. The firm can provide an overall profile on the threat actors, contact and communicate with the threat actors, negotiate and facilitate payments, and provide OFAC due diligence documentation. Digital Forensics and Incident Response (DFIR) providers may offer this service.

Notification and Call Center Service Providers

Firms that provide data breach notification and related call center services that assist an organization in fulfilling regulatory or other notification obligations

Crisis Communications and Public Relations

Firms that specialize in crisis communication and public relations services to assist in minimizing and remedying harm to an organization as a result of a cyber-incident.

Credit Monitoring and Identity Protection

Firms that provide credit, fraud, password and/or identity protection, freezing, thawing, locking, theft, call center, restoration or monitoring services for individuals affected by a data breach.

Data Recovery and Restoration

Firm engaged to restore compromised data and systems to pre-incident business operations. Restoration and recovery services may include, but are not limited to, eradicating external threats from corporate systems, remediating additional vulnerabilities on the system, rebuilding systems and infrastructure, and restoring operations from decryption keys or backups. DFIR providers may offer restoration and recovery services

e-Discovery and Document Review

Firm engaged to analyze compromised data to determine scope of a cyber-incident and applicable notification obligations. Based upon provided search terms, document reviewers will find sensitive data that may trigger relevant state, federal, or international breach notification laws. Services may include identifying the current addresses of impacted individuals. Services may be performed domestically or offshore.

The Cyber BI Claim Process

First Steps To Financial Recovery

Cyber Claim Template Walkthrough

Business Interruption And The First Steps To Recovery

Time Element: Business Interruption and Extra Expense

The purpose of time element coverage is to put the policyholder back in the same financial position they would have been in had the loss not occurred.

BI – 201 Answering base line Forensic Questions

Digital Forensic Incident Response Investigation vs. Forensic Accounting

The Digital Forensic Incident Response ("DFIR") exercise is designed to answer specific questions:

- How did the Threat Actor (TA) gain access?
- Is the TA still on the network?
- Has the TA been removed?
- Did the TA create a back door to re-enter the environment?
- What data was exposed? Has data been exfiltrated?
- Has the system been re-secured?

- The Forensic Accounting exercise answers completely different questions:

- What are all the likely heads of financial damage?
- What financial data is necessary to document the loss, underpinned by appropriate/reliable documentation?
- Is there an income loss directly related to the insured cyber event?
- Are expenses incurred reasonable and necessary?
- Develops a measure of loss in accordance with key policy terms. Follow the first three rules of insurance:
  1. Read the Policy
  2. Read the Policy
  3. Read the Policy

A Cyber Incident Response process is a time sensitive crisis management exercise
A Cyber Insurance Claim is a business process exercise

Cyber BI – 301 Path of Least Resistance

Multipliers of Loss Complexity Factors

- Regulatory Fines and Penalties
- Significant Legal Fees and Investigation costs
- Significant notification and credit monitoring cost
- Large Income Loss/ Significant Extra Expenses
- Widespread customer liability exposure likely

Assess Complexity of Loss + Define Path of Least Resistance

BI – 301 Path of Least Resistance

Pool Aggregate Limit: $10,000,000

Per Event: $1,000,000

Take the time to assess complexity of loss and if policy limits are at risk. If it's likely that the event in question will exhaust the per event limit take the time to develop a **path of least resistance** to align key stakeholders and facilitate timely claim payout.

Force Multipliers Associated with Cyber Losses:

Assess Complexity of Loss + Define Path of Least Resistance

A combination of any of these 5 factors need to consider the competing demands

Use coverage aligned to key stakeholder needs (Legal vs. Finance)

Potential Issues That Inhibit/Extend Your Loss Settlement

- System Restoration Timelines
- 3rd Party Liability Damages
- Coverage/Measurement Challenges
- Extra Expense and Expense to Reduce the Loss
- Stakeholder Management

Driving Claim Preparation, Review and Settlement

1

Understand key stake holder needs

2

Each cyber claim element has its own complexity: Drive parallel paths.

- IT Restoration
- Vendor Expenses
- 3rd Party Liability Claims
- Income Loss

3

Claim visualizations and query driven.

Data analytics to add stakeholder value (Legal, IT, Finance, Board).

4

Active project management to meet timelines/ deadlines.

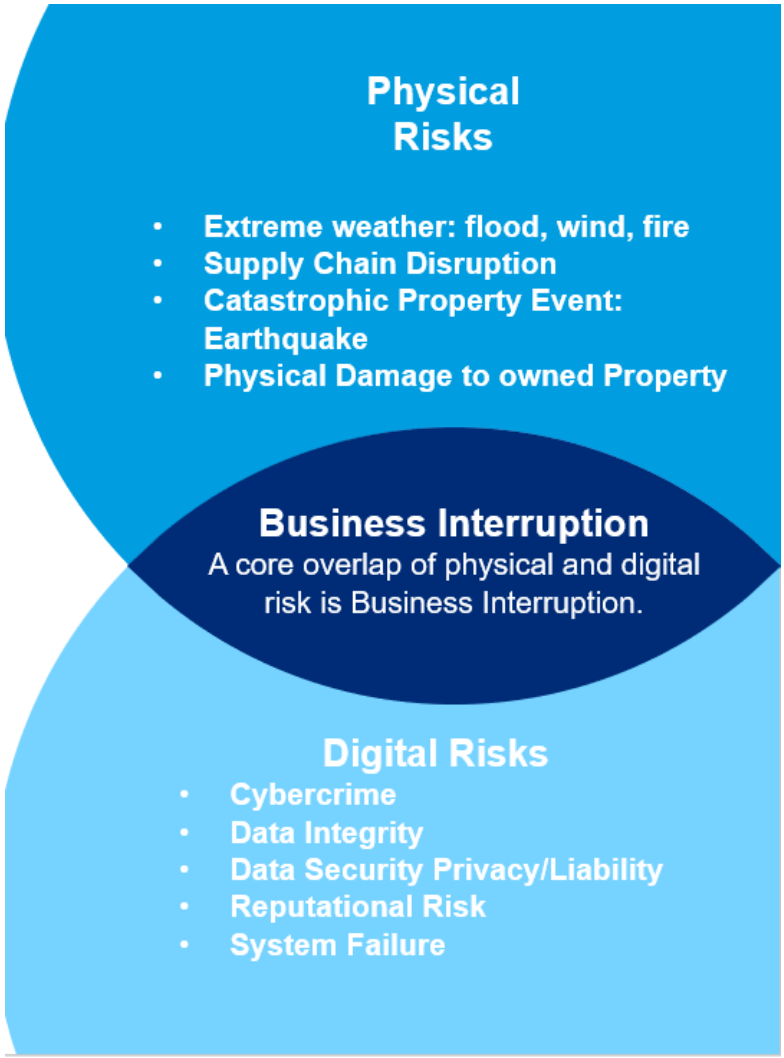
5

Reconciliation of Differences Inability to reconcile competing claim figures create high friction negotiation.

Cyber Losses are Not Property Losses

Same concepts but different Underlying drivers of Loss

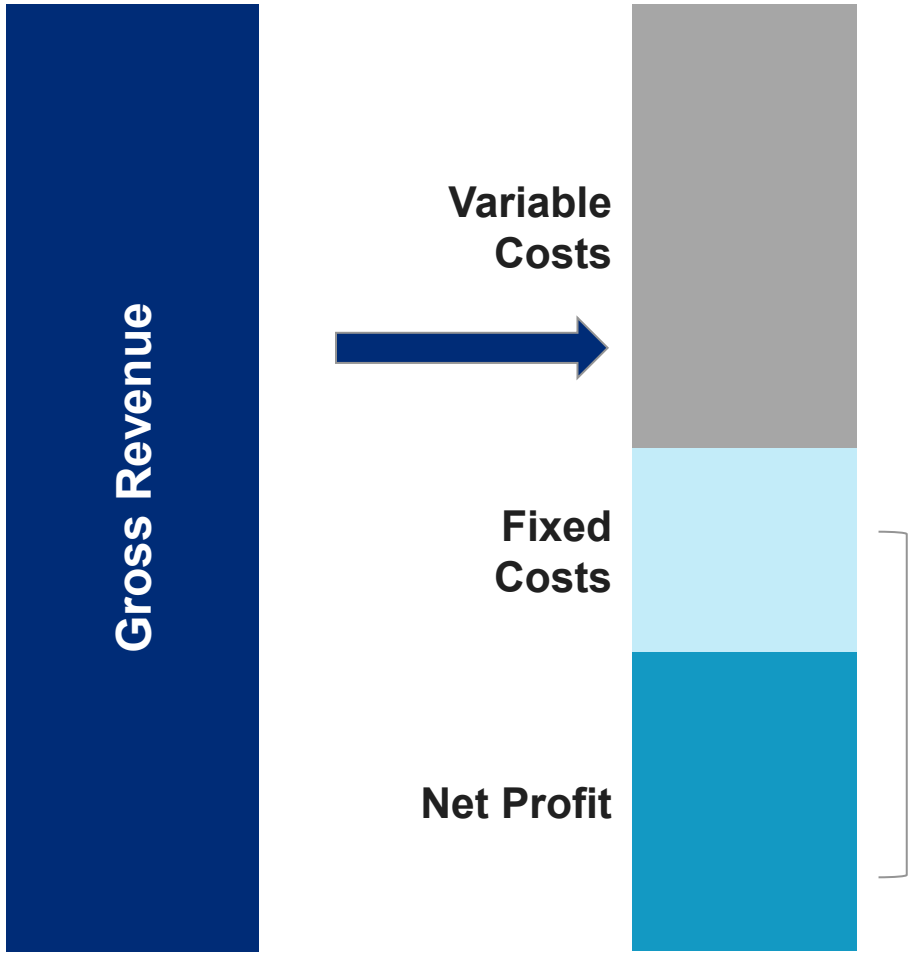
Key Concepts	Property Loss	Cyber Loss
Period of Restoration	• Restoration periods for major property losses measured in months and sometimes years	• Restoration period measured in hours, days, and weeks
Loss of Income	• Very often partial losses with slow ramp to full recovery. Rarely if ever 100% shutdown events.	• Often 100% shut down events for very short period with relatively quick system ramp back to normal
Mitigation	• Ability to mitigate from alternate channels/locations, existing inventory	• All channels impacted from on-line, to POS systems, wholesale distribution
Force Multipliers of Complexity	• Hypothetical recovery timelines, wide area damage issues, inventory valuation, Actual Cash Value, Replacement Cost, etc. Limits losses quite uncommon.	• Morphing risk, data privacy liability, regulatory risk, ransom payments. Limits losses extremely common.



Appendix of Materials

Business Interruption And The First Steps To Recovery

Gross Earnings and Gross Profits Demystified



Gross Earnings

measures the sales value of lost production less saved costs and non-continuing expenses.

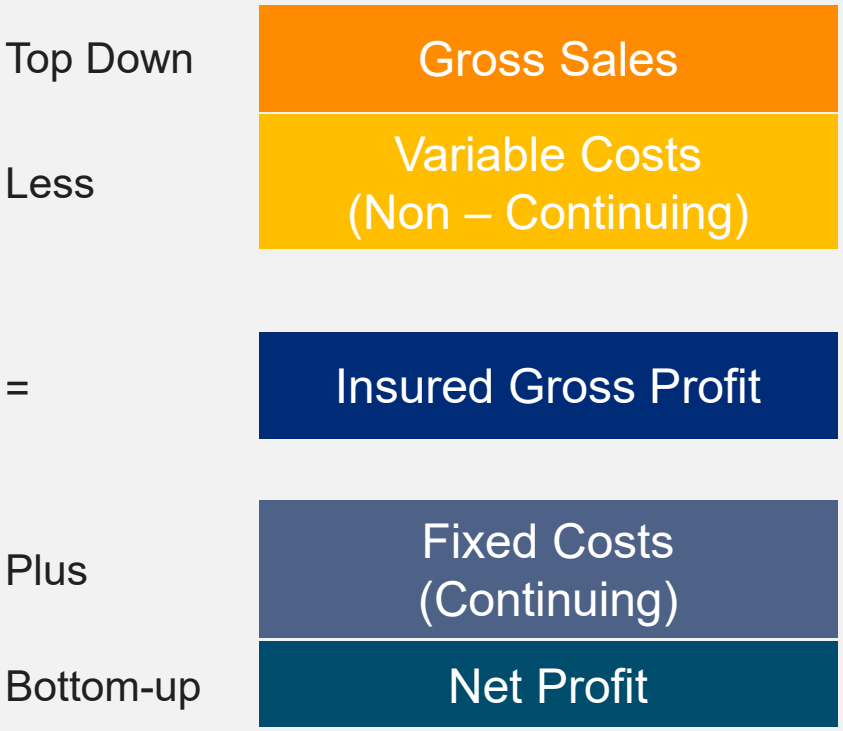
Business Interruption

measures the change in net profit and continuing expenses.

Gross Profits

measures the reduction in revenue (turnover) and subtracts variable costs (rate of gross profit).

The Business Interruption Income Statement



The analysis can be done in Either Direction:

1. Top Down
2. Bottom Up

Business Interruption And The First Steps To Recovery

Typical Cyber Claim Preparation Process

1 Review Policy

Outline Understanding of:

- Key Coverage Provisions
- Limits
- Retentions
- Increased costs cover
- Endorsements
- Basis of settlement
- Proof of Loss Deadlines

2 Initial Claim Overview

Discuss:

- Nature of Loss
- Confirm Triggers
- Confirm Response Vendors
- Extra Expense/Mitigation
- Potential issues

3 Cyber Claim Kick-Off Meeting

- Cyber Insurer Loss Adjuster
- Insurer's experts – IT/IR
- Risk manager/client contact(s)
- Insured Legal
- Insured IT
- Claim Preparer

4 Request for Information

Detailed monthly profit and loss statements

- SOW's, payroll data
- Cost Center recording response costs
- All SOW's, purchase orders, invoices, proof of payment for any system restoration or Extra Expense items

5 Formulate Estimate of Loss

Consider:

- Unusual Loss aspects
- Loss adjuster concerns/requests
- Precedents/prior claims
- Basis of interim claim estimates
- Internal discussion and agreements

Ongoing discussions with client, claim preparer, adjuster and other key

6 Analysis of Data

Data entry and analysis:

- Reconcile data to explanations
- Special circumstances
- Avoided costs
- Additional costs
- Formulate initial claim model

7 Present Initial Findings

- Findings based on data analysis and interviews
- Discuss reasonableness of results
- Agree on final approach
- Request additional info, if needed

8 Prepare Formal Claim

Arrange schedules

- Organize supporting documentation
- Link supporting documentation to schedules and findings
- Get final approval/sign off from client on final numbers

9 Review With Loss Adjuster

- Consider/respond to adjuster's comments
- Calculate effect of adjuster views
- Review issues, strengths, and weaknesses of loss
- Adjuster's methods and conclusions
- Discuss with client and agree on best course of action

10 Negotiate Final Outcome

11 Adjuster Report to Insurer

12 Insured Paid

The Art And Science Of Business Interruption Measurement

Extra Expense vs Expediting Expenses

SPENDING MONEY TO SAVE MONEY

Extra Expense

- Expenses to reduce loss associated with business interruption, subject to an economic test.
- “Pure” extra expense to continue operations as near normal as possible.
- Identified by specific invoices.
- Identified by analyses of income statement expense accounts – excess expenses over and above normal expenses.

Expediting Expenses

- Expenses which reduce the period of interruption, for example expediting restoration of computer systems, and asset replacement (laptops, servers, etc.).

Business Interruption And The First Steps To Recovery

First Steps to Recovery

- Review cyber policy coverage and adequacy of insurance.
- Identify your claims team:
  - Designate personnel who are knowledgeable with regard to the financial documents and the areas of the business affected by the loss.
  - Claims professionals with industry knowledge and relevant loss experience:
    - Cyber claim advocates (policy experts for the insured).
    - Forensic accountants.
    - Other consultants – Legal, IR Firms, Notification, Credit Monitoring, Public Relations, Data Recovery, System Recovery

Business Interruption And The First Steps To Recovery

Immediate Response List

- Contact your property broker/claims advocate, who will typically notify your insurers of the loss. This is done in parallel of initiating the Incident Response plan.
- Consider the availability and use of panel vendors and pre-approval requirements. Best practice dictates the client would have a pre-approved IR plan that aligns to policy requirements.
- Following the initiation of the IR exercise, set up initial meetings with your claims team (local management, broker/claims advocate, claim preparation professionals, other technical experts) and your insurer's claims team (adjusters and various experts). Begin gathering the documents necessary to substantiate your loss to insurers.
- Engage FACS to facilitate the exercise

Glossary of Key Terms

Glossary of Key Terms & Concepts

Privacy and Security Events and 3rd Party Liability

Privacy or Security Event

The actual or reasonably suspected theft, loss or unauthorized disclosure of Personally Identifiable Information in the care, custody or control of the Named Member, or a failure of the security of a Computer System leading to unauthorized access or use, a denial of service attack, or the transmission of malicious code.

Computer System

Computers and associated devices and equipment operated by the Named Member, or operated by a 3rd party service provider to provide IT services to the Named Member.

Personal Information

An individual's name in combination with one or more of the following: "nonpublic information" per GLBA, medical information, SSN, driver's license or state ID number, payment card info, financial account info and passwords, or other nonpublic information protected by state, federal or foreign law.

Claim

Any demand, Suit for damages, Regulatory Proceeding or PCI-DSS Assessment resulting from a Privacy or Security Event.

Privacy or Security Event Liability

Claims Expenses and Damages a Covered Person becomes legally obligated to pay resulting from a civil proceeding stemming from a Privacy or Security Event.

Sample Claim: A breach of your computer network leads to loss of sensitive customer information. Customers file suit against you for the failure to protect their private data.

Regulatory Proceeding

Responding to a request for information, civil investigative demand, Suit, civil investigation or proceeding commenced by any domestic or foreign governmental regulatory entity resulting from a Privacy or Security Event. Covered penalties include civil fines or monetary penalties as well as funds deposited into an equitable relief fund for consumer claims.

Sample Claim: A EU data protection authority investigates a potential GDPR violation.

PCI-DSS

Penalties levied as a result of noncompliance with Payment Card Industry Data Security Standards, when noncompliance results in a Privacy or Security Event.

Glossary of Key Terms & Concepts

1st Party Response Costs

Privacy Response Expenses

Reasonable and necessary costs incurred after a Privacy or Security Event for the services of a security expert to determine the scope and cause of an event, a breach counsel to determine the Named Member's legal obligations as a result of an event, providing notification to impacted individuals, providing identity theft protection services, and hiring a public relations consultant to mitigate reputational damage.

Electronic Equipment and Electronic Data Damage

Costs associated with damage to or loss of use of electronic equipment caused by a cyber security attack, as well as attempting to restore, recreate or recollected impacted Electronic Data.

Sample Claim: After a cyber event that impairs your IT (or OT) network, costs are incurred to hire an IT forensics firm to determine whether the information can be restored. The data is recreated and restored.

Cyber Extortion

A credible threat including a demand for extortion payment directed at a Covered Person to attack the confidentiality, integrity or availability of confidential information, or deploy malicious code, damage, or restrict access to a Computer System. Covered costs include expenses incurred as a result of the extortion as well as funds, including cryptocurrency, paid to the threat actor to terminate the extortion threat.

Sample Claim: Your employee unwittingly clicks a link in a phishing email resulting in ransomware locking out your ability to utilize business critical technology until a ransom demand is paid (or you're able to restore your network from back-ups).

Network Interruption Costs

Business Income Loss, Expenses to Reduce Loss, Extra Expenses and Proof of Loss Preparation Costs incurred as a result of a Security Event causing a Material Interruption lasting longer than the Waiting Period in the policy declarations.

Period of Indemnity

The period of time beginning at the end of the Waiting Hours and ending once the Named Member's Computer Systems are operating as they were before the Security Event

Business Income Loss

Net profits that would have been earned as well as necessary continuing charges and expenses during the Period of Indemnity after a Security Event.

Material Interruption

Actual and measurable interruption or suspension of business operations as a result of a cyber attack.

Expenses to Reduce Loss & Extra Expenses

Costs incurred beyond normal operating expenses in order to reduce Business Income Loss or reduce the Period of Indemnity, as well as costs that would not have occurred if not for a Material Interruption

Proof of Loss Preparation Costs

Costs for a 3rd party forensic accounting firm to establish and prove the amount of loss when submitting a claim for insurance reimbursement.

A business of Marsh McLennan