County Reinsurance, Limited

Cyber Incident Response Checklist

27 Action Steps from Discovery through Recovery

The actions taken following the discovery of a significant cyber incident or data breach are critical to getting the organization on the path to normal business operations. 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. If no CIR Plan exists, the steps of this checklist should guide incident response and recovery

This table identifies actions that SHOULD NOT be taken. Ensure that all persons with access to IT systems abide by the prohibitions shown below throughout the response and recovery.

All leaders in the organization must "own" cyber risk and collaborate to restore operations; the items identified here apply to all leaders and practitioners.

The "DO NOT DO" List
DO NOT ignore the incident; it will not get better with time.
DO NOT make any public statement(s) or share any information regarding the incident through the entire response and recovery effort; only external messaging authorized by the CIR Team leaders is permitted. ▪ Poorly crafted internal or external messages can complicate incident response and recovery.
DO NOT hand over the incident response to your Managed Service Provider (if any). The MSP's role in incident response should be defined in their service agreement. Ensure the MSP's capabilities and responsibilities are understood. The organization must actively control the overall effort.
DO NOT power down systems or servers; do not erase hard drives; do not take other action that might destroy valuable forensic evidence until a decision regarding cyber forensics is made and the CIR Team leaders approve. ▪ The affected systems should remain "on" so that the IT security and forensics specialists can gather the evidence that may be in volatile memory or on hard drives or other storage devices.
DO NOT probe computers and affected systems in an attempt to determine what has happened except in support of the cyber forensic team and with the approval of the CIR Team leaders.
DO NOT image or copy data nor connect storage devices to affected systems except in support of the cyber forensic team and with the approval of the CIR Team leaders.
DO NOT send any emails internally or externally until the email system is confirmed to be uncompromised and the CIR Team leaders authorize its use.
DO NOT run antivirus programs or utilities following the malicious activity unless the Cyber Incident Response Team leaders authorize their use.
DO NOT reconnect affected systems that may have gone offline unless the CIR Team leaders approve. ▪ Activity associated with affected systems could let the attacker know that they have been successful or had the desired impact. ▪ Preserve the IT systems and servers for possible evidence.

Cyber Incident Response Checklist

The Action Steps in this checklist are organized sequentially, but the Cyber Incident Response (CIR) Team should make adjustments in 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 preparedness. **These actions are highlighted with purple bold font.**	
IMMEDIATE RESPONSE	*The Action Steps of this stage of the effort organize the response around 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.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
	b. The designated leader should be available and prepared to dedicate full-time to the incident response. c. The designated leader should move quickly to assert authority and coordinate the response. d. More than one person may have leadership responsibility; ensure they coordinate their decisions. e. **Incident response leaders should participate in regular incident response tabletop exercises.** **Every organization should develop, distribute, and practice a Cyber Incident Response Plan and have it ready to guide actions when a cyber incident occurs.** a. If no CIR Plan exists, use this document to guide the response and recovery. b. If no CIR Team has been established, form an ad hoc CIR Team to conduct the response. Ideally the ad hoc team would consist of: ▪ Executive leaders ▪ IT and Cybersecurity managers ▪ General Counsel ▪ Chief Financial Officer ▪ Risk Manager ▪ Business and Operations Manager(s) ▪ Recorder/ Rapporteur (assign this role to ensure capture of all incident response-related information). ▪ Others as applicable, such as: – Human Resources

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
	– Physical Security – Communications / Public Relations – Other managers and leaders. The activation of the CIR Team should be done through a formal declaration by an approved authority.
3. ☐ Make and document an *initial* assessment of the nature, scope, and impact of the cyber incident based on early indications. a. Nature: Denial of Service, data breach, ransomware, etc. b. Scope: Systems, data, network segments, services, etc. c. Impact: Type (financial, business interruption, data loss, etc.) and magnitude (Low, Medium, High, or other scale). The nature, scope, and impact may each be manifested in multiple dimensions. Update this assessment document throughout the response as more information becomes available for analysis.	Identify affected systems, networks, servers, accounts, applications, data stores, and other resources. Identify how they are affected. ▪ Interview personnel involved and document the interviews, including technical details. ▪ Determine whether ransomware or other malware is involved in the incident.
4. ☐ **Understand your cyber insurance coverage.** a. Know what response actions are appropriate under your insurance contract.	Your cyber insurance broker is an important partner that can readily help with information on your policy, vetted support vendors, interaction with the carrier as needed, and guidance on managing the incident response to preserve your insurance coverage and rights. **You should have an established relationship with your cyber insurance broker.**

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
b. Establish and maintain a dialog with your cyber broker throughout the incident and afterwards if claims will be filed.	
5. ☐ To initially contain the threat, IT professional staff may disconnect affected IT systems from the Internet by unplugging them from wired networks and disconnecting them from wireless networks or devices. a. Record the date and time when these actions are taken. b. Do not remove power from these systems at this time.	Considerations for taking a system offline include: ▪ The operational status of the system (is it functioning?). Record this status. ▪ The criticality of the system to the organization's operations. ▪ Whether allowing the system or resource to remain connected to the network would increase risk or worsen the impact of the incident. ▪ The possibility that the system or its data have been compromised in some way.
6. ☐ Activate a "privileged" reporting and communications channel for internal communications related to the cyber incident response. a. Consider defining channels with tools such as: cellphone, text message, group chat apps, conference bridge. b. The channel should provide conferencing capability. c. Access to the channel should be controlled and limited to those authorized. d. Ensure that the selected channel protects the confidentiality of sensitive data, and that any archive records created by the selected system are accessible and deletable.	The channel should be independent of the enterprise IT network, which may be affected or compromised by the cyber incident. **Ideally, arrangements for this channel are made in advance. If so, this capability should be described in the Cyber Incident Response Plan.** If the organization normally uses Voice over Internet Protocol (VoIP) phones on the IT network that has been affected by the cyber incident, the VOIP system may may not be available. Examples of alternative channels include web conferencing capability such as Slack, GoToMeeting, or Zoom using a smartphone, tablet, or personal computer. Connections to these platforms should be independent of the corporate IT networks – e.g., via an external wireless connection.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
7. ☐ Identify and engage approved external service providers: a. Qualified Cyber Legal Counsel ("Breach Coach"). b. Independent cybersecurity forensic analysis specialists. **Set up longer-term arrangements with these vendors now so support will be available in future cyber incidents.** Notify your cyber insurance broker and carrier of the incident and to alert them of a potential claim. Confer with them to identify, contact, and coordinate with vetted partners for cyber incident response support.	**Arrangements (e.g., on-call contract or service agreement, retainer, pre-coordination, or other mechanism) with specialty service providers should be in place IN ADVANCE of any cyber incident that would require these services.** Such arrangements are normally identified in the CIR Plan. The following support vendors should be included: **Primary** 1. External cyber legal counsel ("Breach Coach"). 2. Cyber forensics support vendor. **Set up an arrangement now so support will be available in future cyber incidents.** **Optional** 1. Ransom extortion expert support provider (for ransomware incidents) 2. Public Relations / Media Relations support vendor 3. Identity Theft and credit monitoring support provider 4. IT and/or cybersecurity engineering support provider 5. Others as may be identified. In the absence of existing arrangements, move quickly because arranging this support might take days. Primary Items 1 and 2 in the list above should be the priority. **Document the names, phone numbers, and email addresses of primary and alternate Points of Contact (POCs) for each service provider. Include this information in the CIR Plan.**

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
	Ideally, these support vendors are vetted with your cyber insurance provider so you understand what costs may be covered by cyber insurance. The dialog with your cyber insurance broker should continue through the response and beyond.
8. ☐ Use a calendar to lay out a top-level schedule for the response and recovery, including: a. Approximate timelines and key activities of the response phases: Containment, Eradication, Recovery. b. Periodic information sharing meetings within the CIR Team and with executive leaders. c. Coordination meetings between IT, IT Security, and external technical service providers regarding the specific technical actions to be taken. d. Periodic reports to organizational leaders.	The CIR Team should escalate items that require senior-level decision-making, approval, or other action. The CIR Team should be aware of what information the executive team will need and how frequently they wish to be updated. This initial schedule may extend over only a few days, though all follow-up work may require weeks. The schedule should be updated until recovery is complete. Often cyber forensics providers can also assist with tasks in all phases of the response.
9. ☐ **Build on the existing communications plan (or develop a new ad hoc communications plan) to inform stakeholders, partners, clients, and employees about the cyber incident as the response unfolds. The plan should:** a. Leverage the organization's **Crisis Management Plan**, which will have much of the needed information as well as tools and existing processes for communications. **b. Define the precepts governing all internal and external communications related to the cyber**	**The communications plan should be approved by legal counsel and executive leadership.** The ad hoc plan should be documented, it should set the parameters for internal and external communications, and it should be designed for immediate application to the situation. Many counties have emergency response plans that may identify emergency response communications processes to reach all employees. This capability could also be used to support meetings for selected personnel or groups. Examples include the Motorola Rave

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
incident, its impact, and the organization's response activities. c. Define processes for review and approval of messages. d. Identify main points to be communicated in each response phase: Containment, Eradication, Recovery. e. Define message distribution channels.	(https://view.motorolasolutions.com/en-us-rave-alert-government) and AlertMedia (www.alertmedia.com)
10. ☐ Incorporate into the top-level schedule (Action Step 8 above) a staffing plan to support extended operations for the team if 24-hour operations is anticipated. a. Document a tentative schedule of daily shifts to ensure 24-hour coverage for all key response functions. b. Assign ownership of the Action Steps of this checklist to specific individuals, and ensure they are capable of driving them to completion while coordinating across the CIR Team.	Ensure the incident response leader is fully apprised of, and approves of, the top-level schedule. This schedule should be managed centrally as a "living document" for the duration of the response.
11. ☐ Build on the results of Action Step 3 to more rigorously compile information on the following to support further analysis, eradication, and recovery of systems and data: a. When were access credentials reviewed, strengthened, and updated? b. Are clean backups available and up to date? c. What is the security patch status of all systems, security appliances, and network components?	If the incident involves destruction of data or loss of data integrity (such as in a ransomware incident), understanding the availability and quality of secure backups *in detail* is a primary consideration. In many cases, data backups (including server images and configuration files) are found to be incomplete, of questionable integrity, or nonexistent. If reliable and useful backups are available, IT operations personnel must not attempt to restore the data until any active malware is neutralized and the state of the network is understood and determined to be safe.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
d. What network and system logs are available?	Recovery of data should be an established practice with documented procedures that are regularly tested. The location(s) of the secured data, the sequence in which data should be restored, and other relevant details should all be included in the procedures. Data should only be restored when the network and systems are known to be in a safe state with all malware and associated artifacts eliminated. Regular testing of restoration procedures and ensuring that incremental (daily or weekly) backups are actually being performed are critical to ensure that they will actually work when needed.
CONTAINMENT	*The goal of the Containment phase is to prevent further spread of the incident and limit its impact.*
12. ☐ Add Containment and Eradication messaging to the communications plan.	Information about Containment and Recovery is very sensitive. Public messaging should be minimized, and any proposed messages should be approved by organizational executive leaders.
13. ☐ Coordinate with the cybersecurity forensic analysis specialists to build on the results of Action Steps 3 and 11 and establish what has taken place during the incident: a. Determine if malware is present, and where. b. Determine whether a third party (e.g., vendor, customer, service provider, cloud provider) was involved in the cyber incident. c. Examine any messages that may have been received from the threat actor, which is common in ransomware attacks.	Report findings to the CIR Team for their awareness and to identify actions that may be required. Ensure that all discoveries, decisions, and other actions are documented to create an official record of the response and to support an insurance claim if needed later. Risk Management should spot check the record as it is developed. Final determination of whether PII was compromised should be made later in the response (at least After Action Step 18). Consult with legal counsel.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
d. Determine and document the sequence of observed events that occurred during the incident and the assets and resources that were involved in each of those events. e. Identify affected systems and data, their criticality, and the type of impact caused by the disruption or degradation of their operations. f. Make a preliminary determination of whether Personally Identifiable Information (PII) or other sensitive personal data was compromised. g. Attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident. Record the analysis and findings in the official record of the response.	
14. ☐ Consider involving law enforcement and/or regulators (if appropriate). a. This decision should be made with the advice of executive leaders and experienced external cyber legal counsel.	Law enforcement (e.g., local FBI field office) should be notified because they may have intelligence about the threat actor that could aid incident response. ▪ Any available cyber intelligence may help with prioritizing actions to be taken. ▪ In the case of a ransomware attack, cyber intelligence may help with decision making regarding ransom payment.
15. ☐ Engage with cyber forensic analysis specialists to identify and secure evidence of the cyber incident – computers, servers, data, etc.	Record all actions performed during the investigation and preserve the integrity and provenance of the records. Document all actions taken to mitigate, contain, eradicate, and recover from the cyber incident.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
a. Preserve and secure computer system and server logs to prevent tampering. b. Move full forensic disk images to sanitized write-protectable or write-once media for analysis rather than analyzing file system backups.	All logged activities should include the date, time, and names of the individuals involved.
16. ☐ Notify external parties of the cybersecurity incident based on your legal, contractual, and insurance notification obligations. This may include: a. External parties to whom you have a disclosure obligation. b. Vendors or business partners who may have access to your network, systems, or data. c. Law enforcement. See Action Step 14. d. Regulatory or other government agencies as required.	Notifications should involve executive leaders and experienced cyber legal counsel. Your cyber insurance broker and carrier may provide advice on support services that may be available to you. Notify key subcontractors and customers for which there may be cybersecurity contractual requirements. Such contracts should be identified, and the Contracts and Finance organization(s) should maintain a list of these contracts, their customers, and a primary and alternate POC for notification in case of a significant cyber incident. This is critical to minimize the impact and possible litigation that may occur related to contractual obligations.
17. ☐ Add a series of regular (e.g., daily, twice daily, etc.) internal information sharing meetings with the organization's executive leaders to the overall response calendar (Action Step 8 above). a. Coordination between the CIR Team and executive leaders will enable the CIR team to escalate issues to support timely decision making.	The CIR Team should be aware of what information the executive team wants to know about and how frequently they wish to be updated. **(This is normally part of a "Critical Information List" [CIL] that should be included in the CIR Plan).** Additionally, the CIR Team should be prepared to escalate items that require executive leadership coordination and approval.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
18. ☐ IT, IT Security, and the cyber forensics service provider should collaborate to limit damage, find root causes, and contain the incident and limit its impact. Containment should include: a. Selectively and methodically shutting down parts of the IT enterprise (cloud-based and on-premises servers) to allow for wiping and rebuilding enterprise networking devices and servers. Testing containment strategies in a lab or separate segment of the IT enterprise to ensure their effectiveness. b. Developing an understanding of the full extent of the data compromise, identifying the number of PII records, the specific financial data, number of Protected Health Data records, and other categories of data.	Once the incident is successfully contained, eradication, and other mitigation activities are implemented. Knowing the full extent of the data compromise is essential for effective restoration as well as for managing liabilities for data loss and the actions needed to address it (e.g., notifications, disclosure, impact remediation, insurance questions) Ensure that the activities of this Action Step are included in the official record.
19. ☐ Apply all necessary security patches and updates to establish a new baseline.	**Patching processes are not optimal in many enterprises; implement improvements as needed.** Test patches to ensure they do not disrupt or impair applications hosted on or dependent upon the IT system. Testing should be conducted on a stand-alone replicated IT environment that is representative of the currently deployed environment.
20. ☐ Based on the findings of the forensic analysis, identify improvements in cybersecurity controls that should be implemented.	Improvements may include, for example, enhanced access controls (two- or multi-factor access control), increased segmentation and logging, improved monitoring, automated audit logging to identify unauthorized behaviors, hardened configurations, and other controls.

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
ERADICATION	*The goal of the Eradication phase is to eliminate all malware, code fragments, or other traces of the incident.*
21. ☐ IT, IT infrastructure, IT Security, IT Operations, and the cyber forensic analysis specialists should coordinate to define the sequence of procedures and steps for eradication of malware or other artifacts left in systems and storage as a result of the cyber incident. a. Do not begin executing the sequence of steps until the CIR Team formally approves it. b. Upon completion of the eradication plan and before restoring the data, conduct a full Indications of Compromise (IoC) assessment and associated corrective actions to ensure that all artifacts and other traces of hacker activity have been eradicated.	**A basic plan for recovery of systems and data may already be available (for example, in the Disaster Recovery Plan).** If not, then develop an ad hoc plan with the coordination of the cyber forensic analysis specialists, IT, and the CIR Team. The ad hoc plan should include: ▪ Running antivirus and anti-malware scans on the affected systems. ▪ Uninstalling or deleting affected data or software. ▪ Applying all necessary security patches and updates. ▪ Rebooting or reinstalling the operating systems of servers, endpoints, and other network resources if needed.
22. ☐ Verify the integrity of backups and other restoration assets before using them for restoration.	If unaffected backups are available, start by conducting test restores in an isolated environment, avoiding any risk of re-infection. Data backups should be scanned thoroughly and should be determined to be "clean" prior to testing and actual restoration. Scanning and integrity checks should be a part of the critical data validation process. Forensics service providers should assist in the validation of the backup critical data prior to testing and restoration.
RECOVERY	*The goal of the Recovery phase is to restore data and system functionality and return to normal operations.*

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
23. ☐ Execute the recovery plan when approved by the IT and CIR Team leadership. a. Ensure Action Steps 21 and 22 are complete before initiating recovery procedures.	**The recovery plan should include:** ▪ **Procedures to make a firm determination that all malware and other residual artifacts of the compromise have been eliminated, and that data backups are known to be clean and uncompromised.** ▪ **Critical data should be restored first, followed by lower priority data if needed for business operations.** ▪ **Requirements to conduct test restores in an isolated environment, avoiding any risk of re-infection.** ▪ **Procedures for restoring systems to normal operation.** ▪ **Monitoring the restored systems for any signs of persistent threats.**
24. ☐ Add Recovery-specific messaging to the communications plan.	Inform users and stakeholders of the status and timeline of the recovery. Draft messaging should be approved by organizational leaders.
25. ☐ Change all security access and passwords as soon as possible to prevent further malicious activity or expansion of the cyber incident.	Once IT systems and servers are cleared for operations, passwords and access control measures should be reimplemented to minimize the possibility of reinfection and unauthorized access.
26. ☐ Maintain and improve the **CIR Plan** and associated procedures based on results and lessons learned from the incident response. a. Assign corrective actions for all gaps and weaknesses to appropriate personnel.	**Formally implement technical exercises and tests of recovery processes at a frequency acceptable to the organization (a minimum of quarterly is recommended).** Conduct CIR Team quarterly tabletop exercises based on realistic cyber scenarios. The Crisis Management Team (CMT) / Executive Leadership

ACTION STEPS	Additional Information
Note: Some actions identified in this checklist should be accomplished prior to any cyber incident as part of preparedness. **These actions are highlighted with purple bold font.**	
b. Schedule and plan for annual reviews (or more frequent reviews if required).	should conduct cyber tabletop exercises at least annually. Engage an external experienced cyber tabletop exercise provider for best results. Update the CIR Plan, IT Disaster Recovery plan, and associated policies and procedures.
27. ☐ In the weeks and months following the recovery, implement cybersecurity improvements identified in Action Step 20 and other improvements based on the learnings from this incident.	A policy and process of continuous improvement should be adopted to reduce the likelihood and impact of future cyber incidents.