County Reinsurance, Limited

Index

Cyber Incident Response
Frequently Asked Questions (FAQ)

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…

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
- Representatives of County functional leaders (Legal, HR, Finance, etc.)
- Others …

3. Q: When does a cybersecurity "event" become a cybersecurity "incident"?

A: Historically, the terms *cybersecurity event* and *cybersecurity incident* have sometimes been treated as synonyms. Today, however, there is wide recognition that a distinction should be made between the two terms:

- A cybersecurity *event* is an anomalous occurrence related to the security of information technology networks, systems, or data that does not violate the organization's cybersecurity policies nor cause an impact that would require a concerted response effort.

  Most enterprises experience many (for large organizations this could be a great many) cybersecurity events in a day.

- A cybersecurity *incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system.[1]

Escalation is the process by which an organization moves from (1) recognizing that a cyber event has occurred; to (2) conducting a preliminary analysis to determine its significance; to (3) designating it as an incident, informing senior managers and executives, and activating the Cyber Incident Response Plan. Most cybersecurity events do not develop into cybersecurity incidents.

These definitions may be augmented with organization-specific information and then formally adopted and promulgated to ensure that personnel involved in response use a common vocabulary. Pre-defined escalation criteria should be set forth in the organization's Cyber Incident Response Policy, if there is one, or in the Cyber Incident Response Plan if there is no documented governing policy.

[1] Abridged from *Glossary,* Computer Security Resource Center, National Institute of Standards and Technology (NIST). https://csrc.nist.gov/glossary/

4. Q: Under what conditions should I call the FBI or other law enforcement agencies to assist in responding to a cyber incident?

A: The decision factors over engaging the FBI or other law enforcement agencies should be identified in the Cyber Incident Response. Typically, these factors include:

- The complexity of the incident.
- The threat actor demands a ransom to recover data (e.g., in a ransomware attack).
- Tactics, techniques, and procedures used by the threat actor align with known parties in the threat actor community.
- Whether the cyber attack involved exploitation or corruption of the Internet routing infrastructure, including DNS and DDOS attacks.
- The advice of counsel, both the county attorney and the external cyber counsel (Breach Coach).
- Approval of the Cyber Incident Response Team leaders and the county authorities.

5. Q: When we wish to reach out to law enforcement, how should we do it?

A: The external cyber legal counsel ("Breach Coach"), in coordination with the county attorney, can advise on whether, when, and how to notify law enforcement. The Cyber Incident Response Plan should include the contract information for the nearest FBI Field Office.

Counties typically have existing relationships with the FBI for reasons such as: law enforcement coordination; community safety, sharing of intelligence and criminal information; technical assistance; coordination during emergencies; and joint efforts to address specific issues such as drug trafficking, human trafficking, or violent crime. The FBI is the lead federal agency for investigating cyberattacks and intrusions and has the capability to assist with incident response.

Established relationships between the county and the FBI should be expanded to include Cyber Incident Response.

6. Q: Are there any other federal agencies that can help us with cyber incident response?

Other federal and state-level agencies have capabilities and resources to assist in cyber incident response. Counties should reach out to these federal and state organizations (as applicable) as part of cybersecurity preparedness to understand what they can offer in cyber incident response, how to obtain their support, and to identify points of contact.

Federal Level

Cybersecurity and Infrastructure Security Agency (CISA). Lead agency for coordinating national efforts to protect critical infrastructure, including private sector entities. A potential resource for counties in incident response:

- Technical assistance and guidance during cyber incidents, including malware analysis, vulnerability mitigation, and recovery strategies.
- Deploys subject matter experts to assist in managing and mitigating cyber incidents.
- Facilitates information sharing and collaborates with private sector partners to enhance resilience.

Multi-State Information Sharing and Analysis Center (MS-ISAC). Managed by CISA, MS-ISAC is a resource for state, local, tribal, and territorial governments.

- Provides real-time threat intelligence, alerts, and vulnerability management tailored to local government needs.
- Offers cybersecurity training, best practices, and incident response assistance specifically for counties and municipalities.
- Acts as a trusted information-sharing platform among local governments.

State Level

Some larger states have dedicated cybersecurity offices or agencies that provide incident response support, threat intelligence, and best practices tailored for state and local government entities.

Several states have established State Cybersecurity Incident Response Teams (CSIRTs) or Security Operations Centers (SOCs) that serve as central points for incident response, threat analysis, and coordination for government agencies. These teams may be able to provide real-time threat monitoring, incident handling and mitigation support, and threat intelligence sharing.

In addition, some states operate online portals for sharing cybersecurity alerts, vulnerabilities, and best practices among government agencies. These platforms can facilitate communication and coordination during cyber incidents.

7. Q: Are there other no-cost/low-cost providers of cyber incident response support?

A: In addition to the federal and state government organizations and the Multi-State Information Sharing and Analysis Center (MS-ISAC), you may find useful cyber incident response resources from the following organizations:

Your cyber insurance broker. Some cyber insurance brokers offer useful cyber incident response resources, such as:

- Notifying insurers.
- Recommending external specialists.
- Preparing, submitting, and managing insurance claims.
- Providing forensic accounting services to document timelines, estimate recovery periods, assess financial impact, and present claim components.

Cyber insurance carriers. Some cyber insurance carriers offer low or no-cost services such as tabletop exercises, cyber risk assessments, incident response planning, continuous monitoring, and others.

SANS Institute. The SANS institute offers a range of no-cost cybersecurity training and education materials, including:

- White papers, "cheat sheets", and a subscription newsletter providing information on vulnerabilities and security awareness tips.
- Webinars on incident response, threat detection, and other topics that can help county officials understand incident response procedures.

8. Q: When should we begin restoring systems and data after a cyber incident?

A: Deciding when to begin restoring systems and data after a cyber incident depends on the nature of the incident. County-specific decision factors should be thought through in advance and the Response Team and IT personnel should all be familiar with them.

A primary consideration is to ensure that backup data is not compromised by being restored to live systems. All malware and associated artifacts should be completely eradicated from the environment before systems and data are restored.

Priorities for restoration should be identified in the Business Continuity Plan.

9. Q: Can we outsource our Cyber Incident Response process?

A: Some portions of the Cyber Incident Response processes can (and should) be outsourced to specialized service providers. These include:

- Cyber forensic analysis providers.
- External Legal Counsel ("Breach Coach").
- Cyber extortion expert.
- Law enforcement/cyber intelligence resources.
- Public Affairs support.

You should retain decision making authority for: accessing and examining user accounts; access privileges for response personnel; backups; deciding whether to pay a threat actor ransom demand (in the case of ransomware); public communications; and other topics. Ultimately, the organization is responsible for the CIR process and recovery following a cyber incident and this responsibility cannot be delegated to a third party.

10. Q: What method should we use to "activate" the Cyber Incident Response (CIR) Team?

A: The method for activating the Cyber Incident Response (CIR) Team should be spelled out in the Cyber Incident Response Plan. Methods generally include use of a contact roster with emergency contact cellphone numbers for the CIR Team members. Text messaging can also be used. Some counties may have an emergency alert platform that can generate secure alerts targeted to a specific group such as the CIR Team.

These or other "out-of-band" communication methods should be used to activate the CIR Team instead of the corporate email system because the email system may have been infiltrated or compromised by the cyber threat actor.

11. Q: What types of cyber incidents do counties experience?

A: Counties experience the same types of cyber incidents that other entities in both private and public sectors experience. Cyber incidents are manifested in the three foundational dimensions of cybersecurity: Confidentiality, Availability, and Integrity.

A data breach – the theft, loss, or unauthorized disclosure of personally identifiable information or third-party information of which you have custody – is a breach of confidentiality. A Distributed Denial of Service (DDOS) attack causes a loss of availability. A malware attack causes a loss of integrity at a minimum and possibly a loss of confidentiality and integrity as well. Ransomware attacks are widely deployed by threat actors in both targeted and untargeted attacks. As with most cyber incidents, a ransomware attack will impact more than one of the foundational dimensions.

Many cyber incidents begin with a phishing attempt to obtain user credentials for access to networks, systems, and data.

12. Q: How should we design and conduct Cyber Incident Response exercises?

A: Ideally, Cyber Incident Response Tabletop Exercises should be conducted quarterly, with different objectives, participants, and scenarios within a structured training plan. Exercises should be:

- Conducted by an experienced cyber incident exercise facilitator.
- Scenario-based, in which participants are presented with a realistic hypothetical cyber incident situation about their organization.

- Designed to give the CIR Team the opportunity to practice CIR response in a controlled environment to build experience that can be applied to real-world incidents that might occur.
- Include an after-action report that summarizes the scenario for reference and identifies key learnings (positive exercise results and any identified gaps or weaknesses requiring corrective action, along with internal Points of Contact (POCs) for action items related to the gaps and weaknesses) to improve cyber incident response in the future.

The CIR Team should convene and carry out the procedures in the CIR Plan, deliberating and making decisions that then influence the evolution of the scenario.

At a minimum, a cyber exercise should be conducted at least annually.

The core Cyber Incident Response Team should participate in all exercises, but other participants may be needed for specific objectives or scenarios, including selected senior county officials and functional leaders to allow them to develop "muscle memory" related to incident response crisis decision-making.

13. Q: What types of Cyber Incident Response exercises exist and when does each apply?

A: A Cyber Incident Response exercise can be of several types:

- Tabletop Exercises. Scenario-based simulations of responding to a cyber incident against the organization. TTXs can enable the Cyber Incident Response Team to:
  - Practice working together to execute the Cyber Incident Response Plan in a simulated real-world environment.
  - Build "muscle memory" regarding the structure, processes, and pacing of cyber incident response.
  - Identify strengths and weaknesses in the Cyber Incident Response Plan that require corrective action and improvement.
- Tests or exercises to validate cyber incident crisis communications for various stakeholders including the county board, county executive/senior leadership, county personnel, subcontractors and partners, and others including the community at large. This type of exercise allows and supports the development of messaging templates and examples that can be emulated for a real-world cyber incident.
- Board of Supervisors-level exercises should be conducted to educate board members and executive leadership and test any strategic-level decision-making processes and procedures that may require board involvement.

- Tactical-level exercises are the lowest level exercises and involve analysts, engineers, and technical staff involved in activities that would support specific analyses, technical processes, and procedures that support cyber incident response.

14. Q: How do the Cyber Incident Response Plan, Disaster Recovery Plan, and Business Continuity Plan relate to each other? Do I need all three?

A: The Cyber Incident Response Plan, Disaster Recovery Plan, and Business Continuity Plan are inter-related and functionally distinct. Planning in each of these functional areas is important, and generally they are created as separate plans. Some organizations, particularly smaller organizations, may choose to group them together with each plan being a separate section of a single document.

Whatever is the case with your organization, these plans, procedures and processes should be reviewed to ensure that they adequately address and document – with the necessary detail – the support of the organization. Further, these processes, procedures and details must also provide for an acceptable level of incident response, data restoration, IT systems rebuilding, and overall recovery within an acceptable time period that achieves overall IT enterprise resilience.

These documents should be protected in accordance with enterprise data protection policies.

All documentation of this nature should be reviewed and updated at least annually to ensure it remains current and addresses changes to the IT and cybersecurity environment.

15. Q: How should we inform county senior managers and executives of their roles in Cyber Incident Response?

A: Executives should have defined roles in Cyber Incident Response, usually articulated in the Cyber Incident Response Plan. These roles should be definitively communicated in training sessions and should be practiced in Cyber Incident Response exercises.

16. Q: Should the county's senior-most governance body – which may be called the Board of Commissioners, Board of Supervisors, County Commission, etc. – be involved in Cyber Incident Response?

A: Yes, the county commissioners (or equivalent) should be involved in Cyber Incident Response.

Specific Cyber Incident Response roles and expectations of the governance body may vary with their established roles and processes, as well as the strengths and cybersecurity expertise of the members. Typically, the governance body oversees the management of risk within the organization, which is normally a long-term strategic activity. However, members of this body are regularly called upon to make or approve operational decisions of the executive team. Such decisions may include those related to capital expenditures, investments, legal and compliance issues, branding and reputation-related issues, Human Resources initiatives, and others.

Specific roles of the governance body in Cyber Incident Response should be described in the Cyber Incident Response Plan.

17. Q: What capabilities should we have for communicating within the Cyber Incident Response Team?

A: In general, channels of communication between cybersecurity professionals and executives should be established and used on a routine basis for ensuring situation awareness.

Your Cyber Incident Response Plan should provide information on how the Cyber Incident Response Team should communicate internally when activated in response to a cyber incident. The Cyber Incident Response Team should include executives and managers along with IT and IT Security operations personnel and others.

A strategy for providing intra-team communications should be put in place, considering:

- The incident itself, or the organization's response to it, might make your usual business communications channels (such as email, MS Teams, teleconference platforms, or internal chat apps) unavailable, unreliable, or compromised.
- Cell phone service may be available but may not be sufficiently secure for response communications.
- Additionally, the communications solution should provide for communications with external service providers that are involved in the response as part of the extended Cyber Incident Response Team.
- Security requirements for voice and data communications may narrow the choices of communications methods.

18. Q: Since our county has a county attorney, would we still need to contract with external counsel for cyber incident response?

A: As the primary legal advisor and prosecutor for the county, the County Attorney has a vital role to play in representing the legal interests of the county during cyber incident response. The county attorney's understanding of local, state, and federal laws is not matched by any other participant in cyber incident response. However, effective CIR still requires that legal counsel have specialized cybersecurity experience and expertise, which county attorneys may not have.

The collaboration between an external cyber counsel and the county attorney is therefore critical to execution of the incident response. Together their role is to (1) influence the response strategy based on legal considerations; (2) advise on courses of action regarding specific cyber incident situations (e.g., privacy impacts of data breaches, response to ransom demands, impact of the cyber incident on the operations of other agencies of the county, and potential impacts on public safety); and (3) ensure that the senior executives of the country and the leaders of the CIR Team understand the law as it pertains to the cyber incident.

Breach counsel and a digital forensics partner should be identified prior to a cyber incident as these will be the first vendors engaged. Breach counsel can provide guidance on engaging additional vendors to preserve attorney client privilege (i.e. digital forensics/restoration firms 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

19. Q: Do the cyber forensics analysts have to come to the physical location of the data center to do their work?

A: Cyber forensics specialists typically do not go to the physical site of the company's data center or key IT resources for their data collection and analysis. Forensic investigations are usually conducted remotely using secure remote access tools and encrypted communications. However, there may be situations in which the forensics team would have to physically go to your site, and that possibility should be anticipated in your planning.

You should establish a relationship with a cyber forensics company that will enable them to respond rapidly if an incident were to occur. You should understand how they would approach a cyber incident at your organization. The county attorney's office should examine the proposed agreement.

20. Q: Our IT environment is entirely in the cloud. How does this affect cyber incident response?

A: At a high level, cyber incident response for a cloud-based infrastructure and for an on-premises operation are the same; at the technical level they are quite different. Cloud infrastructure operates on a "shared responsibility" model. The county must clearly understand which party is responsible for which cybersecurity duties. Counties should consult with their cloud provider to understand how the shared responsibility for cybersecurity in cloud computing is defined in the Service Level Agreement (SLA) and other contract documents governing the relationship.

The technical differences of cyber incident response in the cloud primarily affect the tools and techniques forensic analysts use in their work, and also how the processes are defined for restoration of data in the aftermath of the event. Without physical access to servers, the cyber forensics provider cannot directly capture forensic images of hard drives, cannot install diagnostic utilities, and may not have the logs they would normally expect in an on-premises operation. Although forensic analysis in a cloud environment is complicated by the distributed nature of data, dynamic resource allocation, and multi-tenancy, specialized cloud forensics tools are available and widely used to analyze digital assets, collect and preserve evidence, and report on data from cloud-based systems.

Counties should choose a cyber forensics service provider that has the specialized tools and expertise to work effectively in both cloud and on-premises environments. Additionally, the county Cyber Incident Response Plan should be built for the specific enterprise context with attention to the resources needed for cloud and non-cloud environments.