CYBERSECURITY RISK MANAGEMENT

How to Write an Effective Cyber Incident Response Plan

FORWARD

How to Use this Guide: An incident can be one of the greatest teachers. Like battle-hardened soldiers, incident responders are subjected to the rigors of real, tangible cyber threats. Those that endure receive invaluable experience that can help improve future incident response. At TCDI, we have helped hundreds of organizations prepare for and respond to incidents of all sizes. The biggest takeaway – an Incident Response Plan (IRP) is non-negotiable.

Mature IRPs are typically built through experience – either by hiring an incident response analyst or by teams who, over time and across multiple incident scenarios, meticulously finetune the processes for their company. The more mature and sophisticated the IRP becomes, the more specific to the organization the IRP becomes as it aligns to the organization's cybersecurity goals and strategy.

This detailed document provides a generalized IRP template to demonstrate where to begin building your IRP on a conceptual level. We also provide explanations as to why each section is important and how to further build out a tailored and mature IRP for your organization on top of the generalized IRP template.

We understand that drafting an IRP can be daunting, especially if you're unfamiliar with responding and recovering from (arguably inevitable) security incidents. The reality is that the likeliness of being attacked is more probable than possible. It has become essential in today's digital world to be prepared to protect your organization, the vendors in your supply chain, and the customers you support from cyberattacks.

-Alexandra Hinton, Eric Vanderberg, & Tom MacKenzie

TCDI is here to help at every step of the way. Our cybersecurity engineers have written hundreds of IRPs for businesses of all sizes and industries. If you get stuck on any steps in your IR plan, we offer tailored solutions to meet your needs. Services range from Chief Information Security Officer (CISO) On-Demand consulting to help answer questions on an as needed basis to Policy and Plan Development where our cybersecurity team will draft a customized IRP to your organization's security objectives.

DEFINE: WHAT CONSTITUTES AN INCIDENT FOR YOUR BUSINESS?

When you start IR planning, one of the first things to consider is what constitutes an incident for your business? You will want to have a definition for an incident in your plan. We define an incident as an event that is deemed to have caused harm to the company, or harm to its customers, partners, or stakeholders via company systems or employees.

Here are a few **examples of incidents** to consider for your organization:

1. **A Data Breach**:
   - Most businesses will consider a data breach an incident. This is typically the most significate incident a business can have, and it can occur in many different ways.
     - Files uploaded to an unknown destination
     - Confidential information found on public sources (i.e., the dark web)
     - Depending on the type of business you're in, files mistakenly sent to the wrong customer could constitute a data breach. There could be reporting responsibilities that come into play.

2. **Malicious Insider/s:**
   - Data is stolen to sell or be given away
   - Disgruntled employee destroys data
   - Employee downloads unapproved/illegal software containing malware or a backdoor

3. **Malware or Ransomware:**
   - Ransomware encrypts central data repository
   - Botnet causes company email and domain to be blacklisted due to spam
   - Malware makes hundreds of machines unusable
   - Denial of Service (DoS) attack renders the corporate site inaccessible

Do you know if your organization's data is on the dark web? TCDI's cybersecurity engineers can help you find out. Our team will scour the dark web markets and Darknet search engines to identify data, including but not limited to, employee names, personal and company email addresses, and company product information.

Employee data theft is a common concern for many organizations, especially when intellectual property is involved. Digital forensics can help organizations uncover what data was accessed and if it was removed or altered by being uploaded to a cloud-account, printed, downloaded to a thumb drive, or deleted.

4. **Social Engineering**
    - Social Engineering is a huge attack vector and where many incidents first originate. With a large number of remote employees, the timeline for identifying these types of attacks have increased drastically, providing they're discovered at all. The good news is that by providing consistent, on-going cybersecurity awareness training for your employees, you will significantly reduce your risk of exposure.
        - Employee clicks on phishing email and submits their company credentials or downloads a malware payload
        - Company instructed to change payment information
        - Fake CEO emails to instruct AP to make payments

5. **Lost or Stolen Devices**
    - This potential incident depends on the type of business and/or industry of your organization.
        - Employee loses a laptop while on vacation – if the laptop is encrypted, it may not rise to the level of triggering an IR plan response
        - Backup tapes are stolen from an employee's vehicle
            - This is not secure offsite storage
        - The phone of the CEO's assistant is stolen at a coffee shop
            - Depends on the type of information on the phone and encryption on the device

INFORMATION TECH REALM

Key System Failure

There is an overlap between disaster response & incident response and depends on your industry.

- Power Outage in the server room
- Non-redundant firewall failure

Data Loss or Corruption

- Hard drive failure on the main database server
- Administrator accidentally deletes the wrong virtual machine
- A restore overwrites production data
- Encryption key expires

Having a detailed business continuity and disaster recovery plan can be, in some instances, just as important as an incident response plan. Do you know what you would do if your systems went offline for a day? A week? Longer?

TCDI provides policy and plan development to help review your current plans and develop new ones to ensure your organization is ready for whatever comes its way.

Pre-Plan Considerations

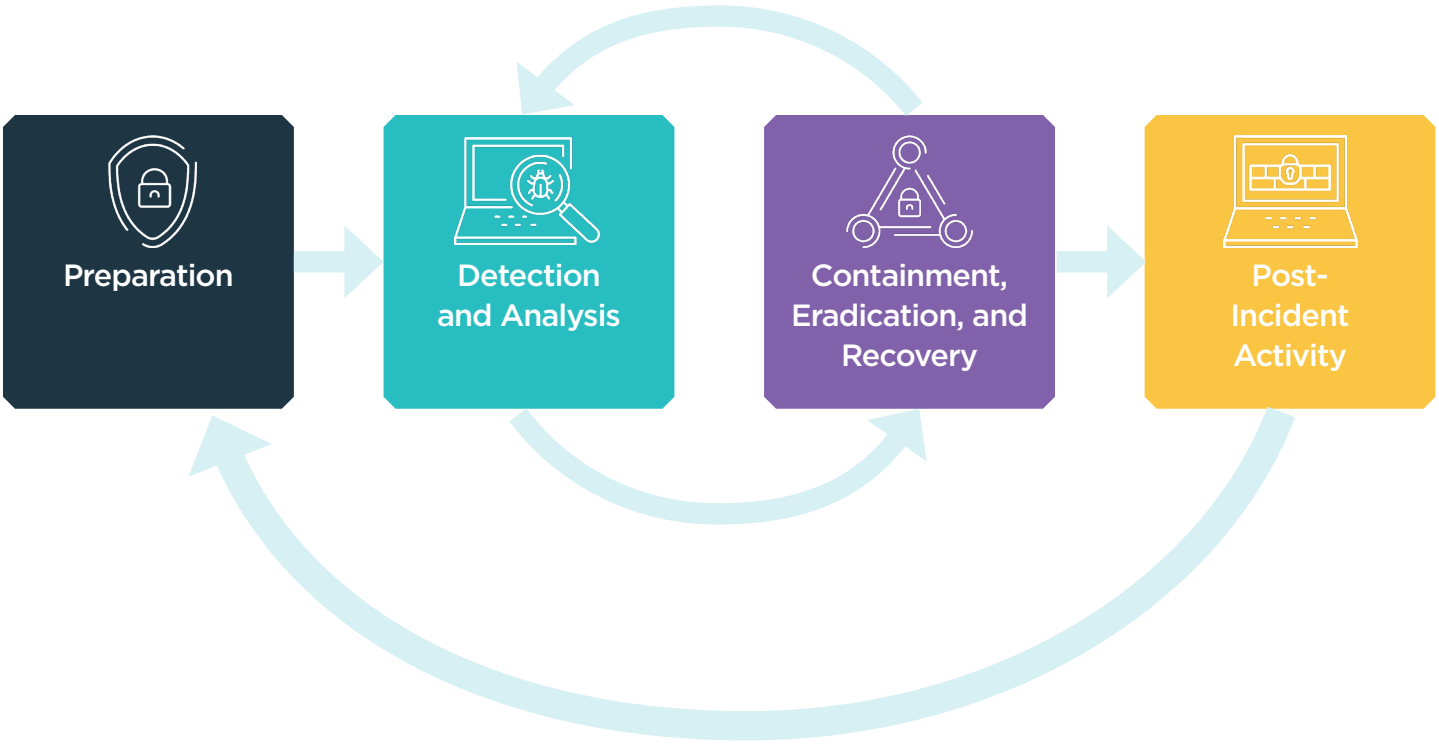
Prework before you launch into developing your IRP

- **Define your Capabilities**
  - What are the skills and knowledge of the IT & Information Security (IS) team? Do you even have an IT and IS team? Or do you outsource IT to a managed service provider (MSP)?
  - Do you need to hire a digital forensics incident response (DFIR) vendor to be on call if an incident does arise?
  - What is your organization's reporting responsibility?

- **Establish an Incident Response Policy**
  - What is the awareness within your organization of incident response?
  - Have you trained people on how to report on potential or suspected incidents?
  - Have you developed a hierarchy of incidents to help with response prioritization? There is a gradation you need to consider within your company.

- **Establish a Plan Model**
  - Should your IRP be a centralized, decentralized, or a hybrid model?
    - Are you going to control everything in a centralized fashion?
    - Are you a company that has so many different locations that you have to decentralize your IRP, with each of your locations having its own version?
    - Do you have a hybrid with a location-specific IRP, but it is covered under a corporate umbrella?
  - NIST puts out Computer Security Incident Handling Guide, which we highly recommend reading.
  - Response Steps: There are several IR models your company can choose from to create procedures for an IR lifecycle.
    - This is the 4-step model created by NIST. It is important to note that this is not a linear path. You may decide to use a 6-step model where Containment, Eradication, and Recovery are broken out separately for ease of organization.

INCIDENT RESPONSE LIFECYCLE



- Playbooks: Consider incorporating playbooks into your plan. Most models for dealing with an Incident leave out critical information. Organizations within different industries tend to have specific types of risk or vulnerabilities that lead to particular types of incidents. Your playbook should be developed and designed for your organization's particular set of risks. This will help cut down the time required for the different Incident Response phases. It will also establish a model that you will be able to follow very quickly and simply for each specific incident.
- Are you going to have third parties manage your incident response? Many companies find it difficult to navigate the technical and regulatory landscape on their own.

- **Outline Existing and Needed Tools**
  - What tools does your organization have that help you prevent and detect incidents, as well as help determine what happened after an event? Your organization might already have some of these tools in place. Maybe you've been meaning to implement more tools, and this exercise will surface which are priorities. Oftentimes this assessment will help your organization improve your cyber posture.
    - Firewalls
    - Intrusion Detection and Prevention Systems
    - Net Flow Analyzers
    - Vulnerability Scanners
    - Malware Detection or Prevention Systems
    - Availability Monitoring
    - Web Proxies
    - Centralized Monitoring
    - Penetration Testing conducted semi-annually by White Hat Hackers
    - Data Loss Prevention software
    - Encryption
    - User Awareness Training
    - ASV Scans
    - Anti-DDoS CDN measures

This analysis, combined with a third-party cybersecurity assessment, can help identify weaknesses in your cyber posture that will help your organization decide which tools and equipment take priority. TCDI's Cybersecurity Assessment takes a technical and compliance-based approach to provide you with a prioritized action plan to help you meet objectives while adhering to your organization's budget.

  - These preventative measures will be outlined in the Preparation section under "Baseline Protections."

PLAN ANATOMY

1. **Introduction**
    a. **Purpose**
    b. **Scope**
    c. **What is a security Incident?**
        i. We define an incident as: _____.
    d. **How to Recognize a Security Incident:**
        i. Identify what triggers your IRP?

2. **Roles and Responsibilities**
    a. **Contact Information:** Outline in good detail the titles, their responsibilities, and their contact information. We suggest naming the title, not the person. People often change, but titles don't.
        i. **Outside Resources:** Often many of these team members are outside of your organization. IT/IS, forensic, and legal roles are almost always outsourced. If there are not internal resources, knowledge, or skills inside the company, you need to consider outside resources.
        ii. **Roles to include on your Team:** Below are roles we consider a bare bones IR team. You can certainly include more roles as your company sees fit.

            1. **IR Team Leader**
                a. Coordinates/Guides
                b. Prioritizes Actions
                c. Key Decision Maker
                d. Usually Oversees Documentation & Reporting
                e. In many cases, they Update the Plan on an ongoing basis

            2. **IT/IS Lead**
                a. This person should have an in-depth knowledge of the systems and network infrastructure.

3. **Cybersecurity & Forensic Lead**
    a. Identification and Analysis
        i. They will be deeply involved in the stages or steps of identification and analysis of an incident. They will gather, review, and analyze logs and related information from various central and local safeguards, security measures, and controls.
    b. Containment -> Recovery
        i. They will also be deeply involved in the steps of containment, eradication and recovery
    c. After Action Solutions
        i. They will determine if policies, processes, technologies, security measures, or controls need to be updated to avoid a similar incident in the future.
    d. This is often outsourced to a third-party cybersecurity DFIR vendor

During the aftermath of a breach or other security incident, things can be chaotic. The last thing you want to be doing in the heat of an incident is searching for a Digital Forensics & Incident Response (DFIR) vendor on the fly.

With cybersecurity threats escalating in volume and intensity year over year, it's becoming common practice for businesses of all sizes to prepare for attacks by seeking out a security partner. Should a compromise occur, the DFIR firm springs to action to swiftly contain the incident and restore systems. Partnering with a DFIR firm minimizes the detriment and overall impact of attacks on organizations.

4. **Data Breach Attorney:** They can be either inside and outside counsel, but is usually outside counsel. If you don't have inside counsel, you should hire outside counsel. They know the complex and ever-changing regulations well, as well as the reporting requirements. Early involvement of an attorney is really important. If you have a data breach attorney involved, many of the conversations from the outset will be considered privileged, which can be helpful down the line if litigation comes into play.
    a. Data Breach Attorney - either Inside and Outside Counsel
    b. Legal Interpretations
    c. Notification Requirements
    d. Privilege

5. **Communications Lead:** Ensure that messaging is centrally coordinated through a communications team that is led by a communications lead. This is a key component of a plan, because ensuring the PR value of your response is well communicated is critical to your business' recovery.
    a. Coordinates Messaging – Internal & External
    b. Media Inquiries
    c. Press Releases
    d. Status Reporting
    e. Social Media / PR
    f. Customer Inquiries

6. **Finance:** With any significant incident response, you will have financial commitments. Finance will be able to help you understand what the cash flow implications are and help leaders understand what the company is and is not capable of doing. Often the financial lead is also the liaison with cyber, breach, and/or liability insurance that help cover some of the cost of an incident.
    a. Coordinates Financial Commitments
    b. Manages Cash Position
    c. Manages Bottom Line
    d. Coordinates Insurance

7. **President, CEO:** The President, CEO sets the tone for the incident. They may also be the one that allocates the funds associated with the incident. They can, and oftentimes are, the ones making public comments, especially if there Is not a PR representative at the helm. If the response raises to the level of regulators, they are the one that interfaces with regulators.
    a. Sets the Tone
    b. Allocates Funds
    c. Makes Public Comments
    d. Interfaces with Regulators

b. **Call Tree**

    i. A call tree will be used to assemble the IR team quickly, should an incident occur. It should include cell and home phone numbers.

c. **Responsibilities**

    i. Responsibilities include outlining preparation for security events, such as training and responsibilities during a security event.

3. Procedures

Depending on the IR model your organization chooses to follow, this section will vary slightly in how the steps are organized. However, the overall concept is the same.

a. **Preparation**

i. **Baseline Protections:** A few examples of protections your company might have in place are listed below.

1. Firewalls
2. Intrusion Detection and Prevention Systems
3. Net Flow Analyzers
4. Vulnerability Scanners
5. Malware Detection or Prevention Systems (same as anti-spam and antivirus software)
6. Availability Monitoring
7. Web Proxies
8. Centralized Monitoring
9. Penetration Testing conducted semi-annually by White Hat Hackers
10. Data Loss Prevention (DLP) software
11. Encryption
12. User Awareness Training
13. ASV Scans
14. Anti-DDoS CDN measures

ii. **Planning**

1. How often will it be reviewed? Will it be tested? Who is responsible?

2. Determine Resources / Data Criticality / Understand Infrastructure
   a. Analyze which systems components, services, and applications are most crucial to maintaining the operations of the business. Identify what critical data needs to be protected, where it is stored, and how valuable it is both to you and your attacker. These critical elements for your business will have priority if a security incident, as you have defined it, should occur.

b. Assess Risk
   i. Where are you most vulnerable. What are the risks that you have? How are you mitigating those risks? What sort of controls do you have in place? What sort of controls do you need to consider putting in place in the future to reduce your risk?

Our Certified Ethical Hackers (CEH) will launch a full-scale simulated attack to test how effective your cyber defenses, computers, network, and people are at deterring a hacker. At the conclusion of the test, we provide a report with a prioritized action plan. With the prioritized action plan, you can ensure you utilize your budget effectively to lower your overall risk and increase your security posture.

By taking corrective actions, you become more prepared for real-world threats when they come your way. This unparalleled insight into your organization's data security effectiveness is an essential component of operating a business in today's digital world.

ii. **Asset Audit**
   1. Which of your assets would cause the most damage if they were compromised? Which would cause a chain reaction that could affect multiple systems? Identify what critical data needs to be protected, where it is stored, and how valuable it is both to you and your attacker.

iii. **Categorize & Prioritize**
   1. **Categorize:** The way you respond to each type of threat will be different from one another. Each organization will have a unique set of threats to manage and a unique categorization of those threats. Below are a few examples of threats to consider.
   2. **Malware** (viruses, ransomware, key loggers)
   3. **DDoS attacks**
   4. **Hacking:** Hacktivism, Industrial espionage, Ransom & Extortion
   5. **Sensitive Data Shared:** Either intentionally by malicious users or accidentally by negligent employees
   6. **Prioritize:** Once you've identified and grouped threats for your organization, you will want to understand their urgency and impact. You'll use this to assess how important these threats are.
   7. **Chart of Urgency** (high medium low)/Impact (minor moderate severe)

iii. **Training**

1. How will training of the plan be conducted? Who will be involved?

2. Establish Policy
    a. What is the awareness within your organization of incident response?
    b. Have you trained people on how to report on potential or suspected incidents?
    c. Have you developed a prioritization within your company of incidents? Certain incidents rating higher than others. There is a gradation you need to consider within your company.

b. **Identification**

Detection of incidents will be generated from either automated systems or from manual human efforts. Once you feel like you have suffered an incident, this is where the rubber starts to meet the road.

In this phase, you're determining what happened. What type of incident did we suffer? Is it truly an incident or is it a false alarm?

Documentation is key, and by documenting potential incidents you can keep a historical record to help refine your IRP. Determining incident priority also occurs during this stage – does it require a full incident response or can it be handled internally?

Recap: What happened? What is it? Validate it. Document it. What is our priority? Is it reportable?

i. **Determine the Symptoms**

ii. **Identify the Nature of the Incident**

iii. **Identify and Preserve the Evidence**

1. You will need to preserve information so that further analysis can be done, which often includes hiring a forensic team to do forensic imaging.

With a DFIR partner in place, companies demonstrate to their cyber insurance brokers that they are taking proactive steps with their cybersecurity strategy. In turn, they greatly lower their risk profile and reduce premiums.

In the event an incident occurs, it is important to be ready to react swiftly. It is also important to forensically preserve data crucial to the investigation and reporting phase. A written report summarizing the facts around the incident is often required by cyber insurance, lawyers, regulatory enforcement agencies, and other stakeholders to understand the compromise, what data was affected, and recommendations for strategically moving forward.

iv. **Document**
    1. You should be documenting throughout an incident, as it will never be fresher in anyone's mind than as it happens.

v. **Report the Event/s**
    1. Is this incident reportable to regulators, the public, consumers that may have been involved, or clients based on contractual or moral obligations?

vi. **Messaging Templates**
    1. Depending on which types of incidents your company has identified are threats, outline an internal and external messaging template for each.

c. **Notifications**

i. Outline notification requirements and timelines.

d. **Containment**

i. During this phase, you're isolating what happened. Whether that's the isolation of network components, computer assets, malware, or ransomware, you are attempting to contain the threat from spreading within your network and causing further damage.

e. **Eradication**

i. The most important takeaway from this stage is to utilize the loop to ensure the threat has been fully contained. For example, it's quite possible that an attacker found multiple ways into your system. Isolation and containment are rarely simple or linear. Moreover, it's often extremely important to move quickly at this stage to minimize damage. Most companies utilize an experienced DFIR vendor for this process.

f. **Follow-up**

i. Additionally, in the end, you will have follow-up reporting to do. You will be communicating knowledge internally and, in some instances, externally. From this knowledge, you will want to implement preventative controls to rectify the weakness in your cybersecurity posture. Ultimately, you will be updating your IR plan.

1. Review why the incident occurred
2. Follow-up reporting
3. Communicate learnings
4. Implement Preventative Controls
5. Update Plan & Retrain Employees as Necessary

4. Key Dos and Don'ts

a. **Do:**

i. **Build your security program around a framework.** There are several frameworks to model your security program around by following their guidelines. Oftentimes industries will have a framework that is recommended. If you're outside of this norm, Center for Internet Security (CIS) controls puts out a top 20 controls list and consistently updates this as threats evolve. If you're adhering to the CIS top 20 controls, you're going to put yourself in a position of decent cybersecurity posture and security framework.

Understanding which regulations you should use to develop your security program can often be confusing, as many have overlapping qualities. Depending on your industry, non-compliance with specific regulations can even result in regulatory fees or loss of business. TCDI's cybersecurity assessment takes a holistic view of an organization's obligations and security controls to help determine whether you are adhering to relevant standards, as well as identify gaps that would otherwise leave your organization at unnecessary risk.

ii. **Implement Multi-Factor Authentication.** We recommend the implementation of MFA on every service available that has internet exposure. This includes clouds, external VPNs, Single-Sign on.

iii. **Increase visibility.** It is more than likely that each of the systems you have running has the option to turn on logs. When available, always opt-in for advanced logging. Utilize a centralized repository for these logs. In the event an incident occurs, you will be able to access these logs in a repository for examination into the cause of the incident for rapid containment. An example of a centralized repository is a SEIM. Oftentimes, if your organization is utilizing a SEIM, you can suppress an incident from occurring before it starts.

iv. **Understand your regulatory, legal, and contractual notification requirements.** You should have somebody on your team that knows this very well, and is tied into the privacy regulations, the data breach regulations and notifications requirements as they're different in almost every state. If you don't have someone internally that is an expert, you should have a hired 3rd party at your side.

By enabling a SIEM, you're able to create a baseline for your organization. What does that mean exactly? It means you know the little quirks that happen within your network that can help identify actual anomalies from false-positives quickly and efficiently. It not only helps you respond faster, but it saves effort, and if we're being honest, a lot of stress that often comes hand-in-hand with incident response. SIEM is just one portion of TCDI's CyberPulse 365 offering, which also includes vulnerability scanning, endpoint protection, and data loss prevention (DLP) technologies.

v. **Know when to engage law enforcement.** For some incidents, notifying law enforcement is required. For others it may not be. Your outside data breach attorney will certainly help you navigate this step.

vi. **Keep communications centralized.** This doesn't mean you're trying to hide information. It simply means that you're staying in front of information that is released to ensure it is accurate and timely on what is needed.

vii. **Test your plan regularly.** When an incident occurs, things will be chaotic. You want your team to have practiced with tabletop exercises annually or semi-annually.

viii. **Regularly assess the need and role of insurance.** Insurance does not replace controls. Do not fall victim to believing that because you have insurance in place, you don't need strong defenses and plans.

ix. **Make sure you print your Incident Response Plan!** Since portions of your network may not be accessible during an incident, a readily available hardcopy version will save time.

b. **Don't:**

i. **Wait to involve outside counsel.** They can guide you on the legal aspects of reporting as well as when to get law enforcement involved if necessary. Your communications with them will also be protected under attorney-client privilege.

ii. **Call it a breach unless you know it's a breach.** The term breach has legal and regulatory connotations. The nomenclature we recommend following at the outset is to refer to the suspicious activity as an event until you determine it is indeed an incident, then an incident until you determine it is in fact, a breach. event > incident > breach.

Did you know insurance often requires organizations to meet minimum cybersecurity standards to receive compensation for a data breach? This will vary based on your policy, but that could include items such as performing an annual penetration test, being compliant with a specific regulation, or have active monitoring on their network. Moreover, these proactive measures often must be performed by a neutral third-party to ensure the services are performed without bias and have thorough documentation. Do you know what your policy requires?

Ready to learn more?

Greg Michalek
(336) 232-5826
g_michalek@tcdi.com

TCDI
4508 Weybridge Lane
Greensboro, North Carolina 27407