# Cyber Incident Response Planning (CIRP) for Project Managers [1]

**Nazy Fouladirad**

Project managers play an important role within an organization and can be tasked with a wide range of assignments, from rolling out new technology investments to spearheading cloud adoption strategies.

At some point in their careers, some Project Managers may be called upon to assist with executing critical incident response planning and execution. With the increasing number of cybersecurity breaches in all industries, having a clear strategy in place is vital for ensuring the business has a clear path to follow when faced with a major cybersecurity crisis. And sticking to that path is essential.

While a PM should not be responsible for building an IR plan, they may be asked to help execute one. Below, we'll cover the essential elements necessary to an effective Cyber Incident Response Plan (CIRP) and the role that project managers may be asked to play along the way.

## Preparation Phase

One of the most important elements of CIRP is the planning and preparation phases. This is where project managers may work with their IT and security teams to ensure the execution of a thorough risk assessment. They may also need to gather the necessary information to build a plan around.

Part of this phase may involve documentation of all critical infrastructure assets and assembling a dedicated response team. Each team member should be given clear instructions on the role they'll play during an incident response. Define procedures and document the step-by-step processes for different types of breaches.

Other priorities in this phase include developing crisis communication protocols. This involves establishing clear guidelines for both internal and external stakeholders. Have

[1] How to cite this article: Fouladirad, N. (2025). Cyber Incident Response Planning (CIRP) for Project Managers, *PM World Journal*, Vol. XIV, Issue X, October.

pre-drafted public statements ready in advance to distribute immediately and mitigate any potential damage to public perception.

## Detection & Analysis

Having tools in place for quick threat detection and analysis as part of your CIRP can mean the difference between faster resolutions and several days or even weeks of system downtime. Your IT and security teams are likely incorporating network activity monitoring solutions that are designed to flag unusual activity as it occurs.

When an alarm does trigger, this should initiate certain tasks from security response teams who can quickly investigate the situation and see whether or not it’s an anomaly or something that needs to be acted on.

If a cyberbreach is detected, it’s essential to have a comprehensive detection and analysis checklist available for these teams to follow. A project manager may be asked to manage and help the team execute on this checklist. These lists will focus on taking methodical steps to identify the type of security threat, how widespread it is, and the potential it could have caused.

## Containment, Eradication & Recovery

When responding to a real threat, there are different stages that teams will need to navigate through. These are: containment, eradication, and recovery.

During containment, teams will be investigating the scope of a breach to discover not only where the attack originated from, but also how many other systems it may have impacted. Knowing this information makes containing the problem easier and allows for the deployment of various quarantine security elements.

After a threat is contained, security teams will need to have the systems in place to eliminate all traces of it, not only on their core systems, but also through any data backups that may be stored on or off premises.

At the same time or shortly after vulnerabilities are eliminated, recovery efforts should be underway to bring back up any systems that were taken offline.

## Key Considerations for Cyber Incident Response Planning

Outside of the planning stages themself, there are a few important considerations that an impactful CIRP will incorporate. This includes:

- **Third-Party Risk Management** - Incident response planning often involves more than just the business itself. Many times, a company's operations are deeply integrated with a wide range of outside vendors and partners. Third-party risk management practices as part of your CIRP help ensure that any incident originating with a third party is accounted for. If a third-party incident were to occur, you would need a clear understanding of what your partner is doing and whether any remediation tasks are your company's responsibility.

- **Compliance Frameworks** - For some organizations, especially those in highly specialized industries, adhering to strict compliance frameworks, such as the Cybersecurity Maturity Model Certification (CMMC), SOC, or ISO, can be a key requirement. Businesses should clearly understand the requirements of these regulatory guidelines, particularly when potentially partnering with outside consultants who can help keep their internal processes aligned with these strict standards.

- **Data Backup and Recovery Strategies** - One of the most essential elements of a CIRP is to have quality data backups of key databases and company systems at all times. These backups should be taken regularly, with more than one copy made and hosted both on-premise and off-site. This ensures that if one backup becomes compromised during a breach, another is available for use. Your CIRP will likely require calling on those backups for temporary or long-term use.

- Ongoing CIRP Maintenance: Your CIRP should be subjected to regular testing, exercises, simulations, and drills to validate its effectiveness. Plan regular updates to reflect technological changes or structure. This ensures you and your teams are always confident in their role and their options in the event of a cyber incident.

## Keep Your CIRP Effective Long-Term

Incident response planning isn't something that only security teams need to worry about. It impacts all teams and should be something that project management teams are aware of and prepared to respond to.

By following the key stages of incident response planning and integrating security measures into project lifecycles, the company can ensure that, in the event of a breach, it can still sustain operations while minimizing downtime.

## About the Author

### Nazy Fouladirad

California, USA

**Nazy Fouladirad** is President and COO of Tevora, a global leading cybersecurity consultancy. She has dedicated her career to creating a more secure business and online environment for organizations across the country and world. She is passionate about serving her community and acts as a board member for a local nonprofit organization.