**Prioritization of Efforts**

As the incident's dust settles, it is possible that a condition of perplexity and disbelief will emerge. The consequences of stressful workplace activities are well documented, and it is widely assumed that cyber-attacks, like all disputes,damage everyone engaged to recover from the incident you must keep everyone focused on the task at hand and ensure that the appropriate employees begin recovery activities in accordance with the incident response plan.

- **Addressing Psychological Impact:** Recognize potential psychological effects of the incident, such as perplexity and disbelief.

- **Employee Well-being:** Acknowledge the documented consequences of stressful workplace activities impact

- **Maintaining Focus:** Ensure all team members remain focused on recovery tasks despite the psychological impact

- **Guidance:** Provide clear direction and support to keep everyone aligned with the incident response plan.

- **Timely Action:** Ensure appropriate employees initiate recovery activities promptly according to the plan's guidelines..

**Damage Assessment**

Damage assessment is a critical step in understanding the impact of security incidents on confidentiality, integrity, and availability of information and assets. The severity of incidents can vary widely, from minor intrusions to significant data breaches or system-wide infections.

**Methods of Assessment:**

* - Utilization of system logs, intrusion detection logs, configuration records, incident response documentation, and comprehensive examination of systems and data storage.
* - Comparison of current state with established logs and documents to determine the type, scope, and extent of damage.
* - In some cases, involvement of computer forensics experts may be necessary, especially if incidents become part of criminal or civil proceedings.

**Recovery Process:**

1. - Identify and address vulnerabilities and weaknesses that allowed the incident to occur and spread.
2. - Evaluate and enhance preventive measures or implement new ones as necessary.
3. - Enhance monitoring capabilities for better detection and reporting of incidents.
4. - Utilize backups to restore lost or compromised data, adhering to established backup policies.
5. - Restore affected services and processes, ensuring they are evaluated, cleansed, and fully operational.
6. - Maintain continuous vigilance post-recovery to prevent future incidents, as attackers may attempt similar or different attacks

**Model for a Consolidated Contingency Plan​**

As the incident's dust settles, it is possible that a condition of perplexity and disbelief will emerge. The consequences of stressful workplace activities are well documented, and it is widely assumed that cyber-attacks, like all disputes, damage everyone engaged to recover from the incident you must keep everyone focused on the task at hand and ensure that the appropriate employees begin recovery activities in accordance with the incident response plan.

- **Maintain Focus:** Ensure all stakeholders remain focused on recovery tasks.

-  **Employee Engagement:** Involve appropriate employees according to the incident response plan.

**The planning document**

The incident reaction document is the first document prepared for the IR and DR document set. The IR and DR plan is developed by bringing together key stakeholders in an organization, such as the top computing executive, systems administrators, security administrators, and a few functional area managers. The first step is to determine who will be in charge of managing the document, which is usually the security administrator. A secretary is assigned to keep track of the planning session's actions and outcomes. The first step is to build separate incident response and disaster recovery teams. The two groups in this arrangement are made up of the same people as the planning committee, plus additional system administrators.

* - Structured guide
* - Outlines objectives and scope
* - Details resources and timeline
* - Roadmap for project planning and implementation
* - Ensures alignment and clarity among stakeholders