BCDR & Incident Response Computer Forensics and Crisis Management

Paul Gurke

BCDR & Incident Response Computer Forensics and Crisis Management

Incident Response

Incident response is broken up into 6 different phases; preparation, identification, containment, eradication, recovery and follow-up. This six-stage process is meant to be a framework that enables consistent results.

The preparation stage involves actions that foster expedition and quality for the consecutive phases. Anything that could be done ahead of an incident is worked in this phase. Some examples are creating document templates, process flow charts and training.

The identification phase can be broken down into 2 subfunctions; detection and analysis. The idea is that you will have some information at this point that needs to be analyzed in order to proceed any further. It may turn out to be a false positive or a major incident, this stage is where incident verification and scope of impact are identified.

Containment is where the first counter actions are performed. The primary goal is to minimize the damage. Depending on the type of the attack, some actions may be to block command and control servers in the firewall, stop services or just change passwords on affected accounts. It all depends on the type of incident underway.

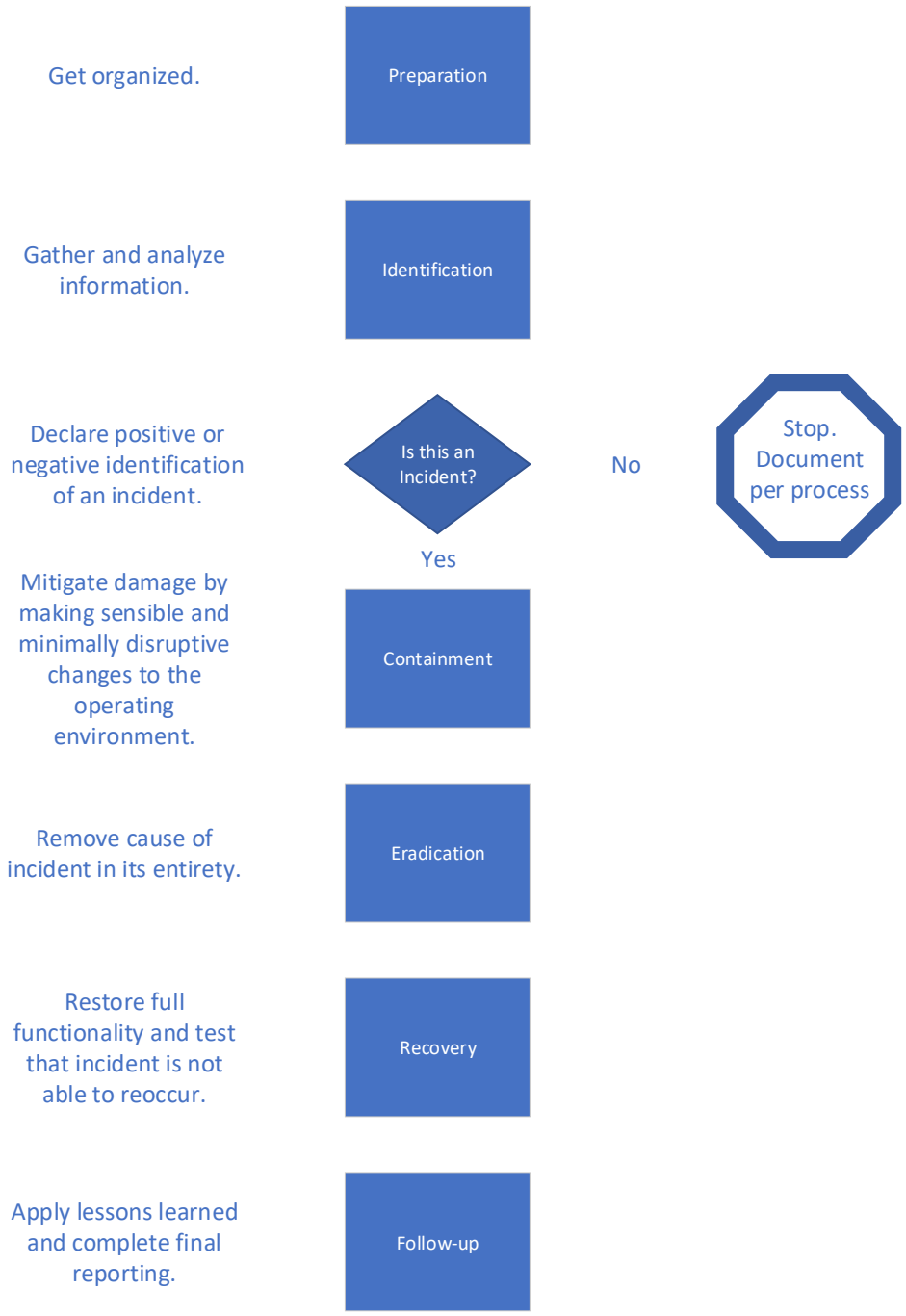
Eradication is where comprehensive action is taken to resolve the incident and remove all aspects of the incident's cause from the operating environment. This could be actions like patching, system hardening and of course rebuilding systems. Before any of this is done, the information on the incident is recorded as per the process defined from the first phase.

Recovery is a phase of creating normality. The functions of this phase can be further broken down into investigation, full restoration with verification, and testing that the environment is no longer vulnerable to the same incident. The previous steps may have

diminished the operating environment and the actions of this phase are intended to raise the functional level back to the previous baseline. In addition, a confidence level is created that the vulnerability has been removed.

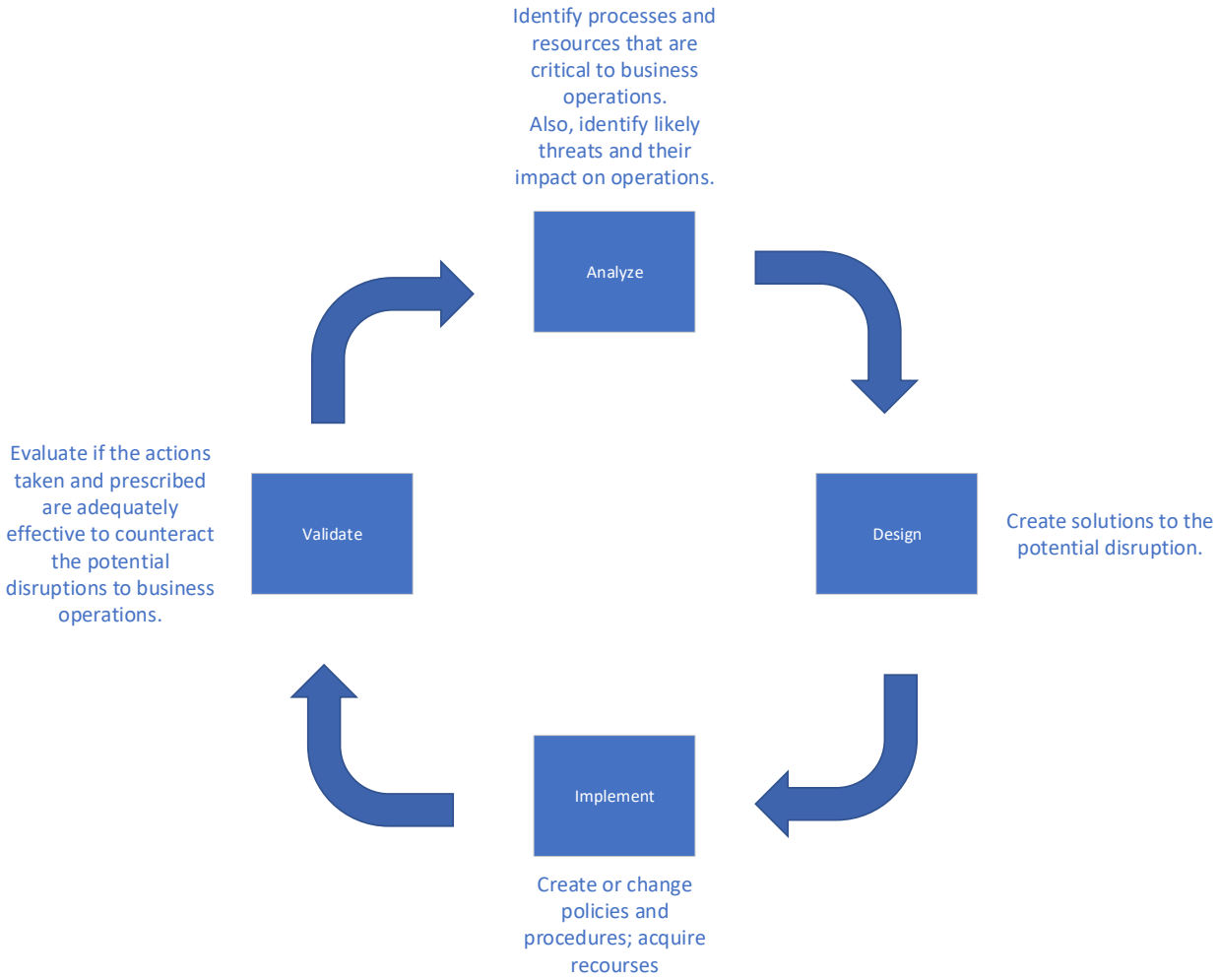
Finally, there is the follow-up phase. This is basically a wrap up phase. Verifications that the processes were followed and other meta and regulatory tasks are completed. This is also a great opportunity to evaluate the process as a whole and incorporate any lessons learned to refine the process to be more effective.

Incident Response



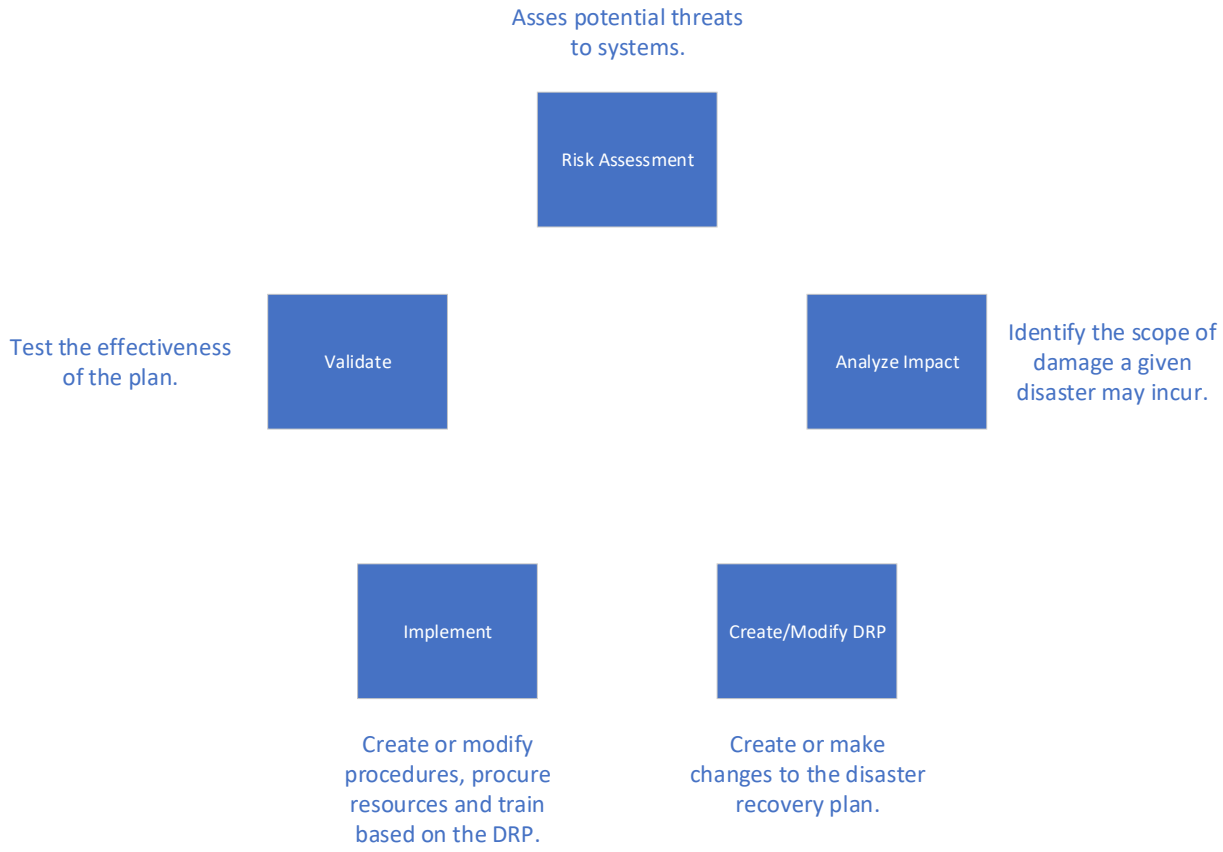
Business Continuity

Business continuity (BC) is the practice of identifying critical core business functions and having a plan to manage them during a major incident. This extends beyond disaster recovery (DR) and is generally concerning a higher-level view. Where DR may be focused on the servers that store business critical data, BC is only interested in the access of that same data. It may be acceptable in a BC plan to use paper copies of data that can be ran through a copier, where a DR plan is aimed at preventing that from happening.



Disaster Recovery

In contrast to business continuity, disaster recovery focuses on the technical aspects of recovering from various disasters. There is plenty of overlap between the two, and it could be argued that a disaster recovery plan is a subset of a business continuity plan.



Computer Forensics

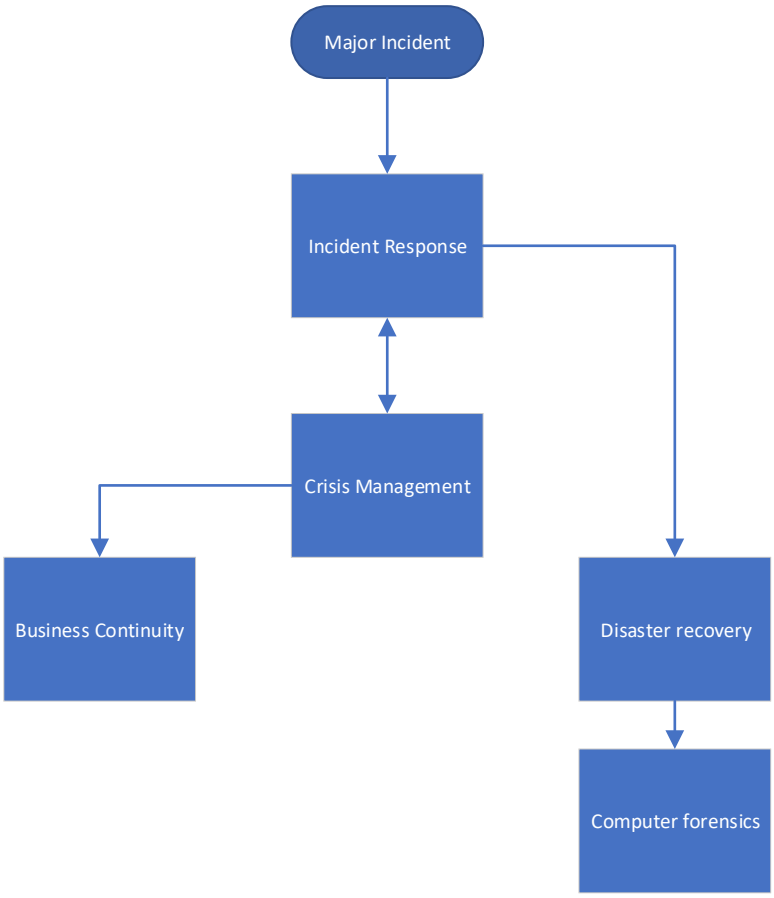
Computer forensics is the process of retrieving data with the intent to provide factual information without contaminating or casting doubt to its validity.

Crisis Management

Crisis management is topmost level of actions during a crisis. This is the key hub for information regarding the crisis that is shared with various entities both internal and external. It

is also where other management like tasks are performed from a centralized framework, like approving resources or removing roadblocks.

From the business's standpoint, the interrelation of incident response, crisis management, business continuity, disaster recovery and computer forensics during a major incident may be reflected like the chart below:



References

Mata, W. (2014, February 6). 15 Steps for Designing a Disaster Recovery Plan (DRP). Retrieved October 13, 2019, from Centre Technologies website: https://centretechnologies.com/15-steps-designing-successful-disaster-recovery-plan/

What is a Business Continuity Plan? PM in Under 5. (n.d.). Retrieved from https://www.youtube.com/watch?v=G9JANBmTdqA