BCDR & Incident Response Computer Forensics and Crisis Management

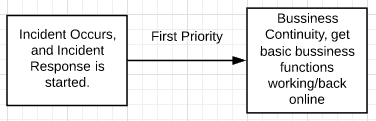
Andrew Maddox

University of Advancing Technology

The practice of incident response in the modern security system of most companies has been well defined and sectioned into different areas which each help play a role during the process of incident response. As is important to keep up, define and understand these trends as they are changing constantly. It is important to keep up with how each area interacts with the other and how the flow of a complete incident response will play out. In this paper I will be exploring how a possible incident will be dealt with by each part of the process and diagram how this flows together to complete the incident response event as a whole.

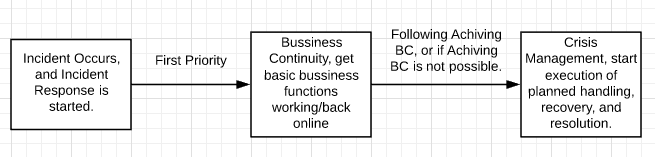
While the term incident response is very widespread and known by many, what many people don't think about is the term for normal business operation after an incident which in the end, is the real goal for many. Incident response as a whole is a tool to reach that goal if anything undesirable is to happen. Business continuity is the term that describes this regular function after an incident occurs, therefore it is the first aspect of incident response that we should be aware of as it is our primary objective. Business continuity can be kept in many ways, through keeping backup servers that are run at a separate location, even having temporary servers that only come online in case of a complete system failure as a temporary stopgap for consumers is a way to keep some functionality during an incident even if the entire main infrastructure is to be knocked offline. Keeping your business’s function down for as little time as possible, or no time at all, is the end goal of business continuity.

Here is the start of a chart showing this normal flow of an incident response:



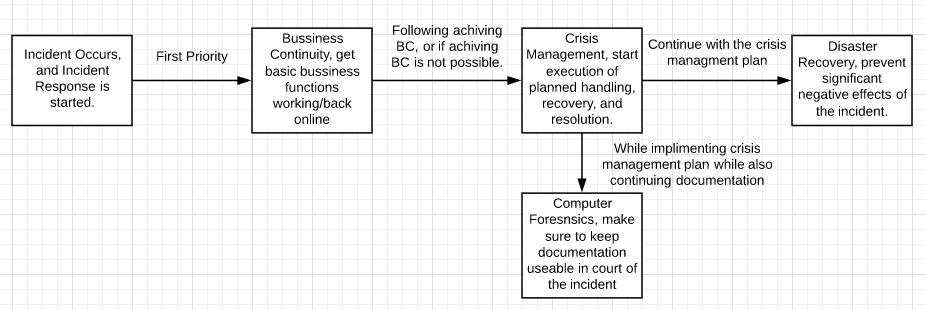
Soon after a company can achieve business continuity, or if they are unable to, they will enter the crisis management phase of the incident response. Crisis management is when a company starts the process of returning services and operations to their normal state and informing consumers of the problem, generally following a predefined and known plan. Planning for crisis management after an incident is equally important as understanding the process of incident response. Without a proper plan incident response effort are many times harder than they should otherwise be, which has a negative impact upon the rest of the process leading to further problems and downtime which is very bad for a company already in crisis.

Updated chart including crisis management:



The next steps are where the crisis management plan of action will be put into effect, where the handling, recovery, and resolution steps will take place. These actions take place in what are known as the disaster recovery and computer forensics stages. In the disaster recovery stage, the goal is to reduce or negate any significantly negative effects of the incident. This includes preventing damage to infrastructure and their consumers data, as well as preventing large damage to the image of the company. This is essential for a smooth return to normal operation after the incident has ended and is something which is usually a part of the crisis management plan which commonly has been pre-defined. The computer forensics stage is when workers will apply their investigative and analytical skills to gather evidence from computer technologies of the attack. The goal of this evidence gathering is to keep it for when or if a trial takes place against those who are responsible for the incident to use as evidence/proof.

Updated chart with computer forensics and disaster recovery:



While these steps are presented in the flowchart in a certain order, it is important to understand that not every action will have the exact same set of steps. Many individuals and entities make large sums of money selling incident response plans so they might all differ slightly. Not only that the order may be different, but in more developed incident response systems each process is often happening simultaneously to resolve the incident as quickly as possible. While the way and order these processes are implemented in vary, it is still important to understand that they are the essential components to a strong incident response.

References

Module 1 lectures.

Luttgens, J. T., Pepe, M., & Mandia, K. (2014). Incident response and computer forensics.

McGraw Hill.

6 Phases in the Incident Response Plan. (n.d.). Retrieved from

https://www.securitymetrics.com/blog/6-phases-incident-response-plan