BCDR, Incident Response, Computer Forensics and Crisis Management

Jose Ramirez

University of Advancing Technology

BCDR, Incident Response, Computer Forensics and Crisis Management

BCDR, incident response, computer forensics, and crisis management are an important part to every business. These departments all work together to reach the same goal/solution, to ensure a business can handle disasters. This means either prevent them altogether or manage to create a plan to comeback from one. In the following paragraphs, I will try to give a short summary of each department and how they work together to reach a common goal.

# BCDR

Business continuity and disaster recovery involves a BCDR team dedicated to creating plans and procedures that will be used during and after a disaster. Business continuity is the process of keeping your business “online” at all times, no matter what is going on, you want to be making money by staying up. At any point, if a business is “offline” it is losing money. Business continuity members are tasked with creating a procedure that will help mitigate loss. An example would be creating a backup server on an offsite location, this server can be used while the main servers come back online or are replaced. This would allow customers/users access to the services offered with little to no disruptions.

Disaster Recovery is self-explanatory, it is the process of recovering from a disaster. The DR team should have a thought-out plan on how the business will recover from various scenarios. Some common scenarios will include natural disasters, man made disasters and technical problems. Much like many of these teams, the DR team is also supposed to have a disaster recovery plan that will be executed after a disaster has occurred. Depending on the plan, the member will start making lists of items that need to be replace or fixed. DR members should also have a plan on what to do if there is nothing left, a total destruction scenario. As an example, DR members can have a plan in which the business is moved to a remote location, a cold or hot site would be some terms used to describe the new location. A cold site is usually just a building ready to be stocked with equipment and machinery. A hot site is a building ready to be used right away since it has everything the main site had. Backups are also an important part of disaster recovery, critical information needs to be backed up on a schedule and made available to all DR members, through a backup service or through physical tapes/drives.

# Incident Response & Computer Forensics

Incident response is the first to arrive at a scenario, this can either be an individual or an official team organized by the business. They are responsible for mitigating the problem or completely stopping it, the solution depends on the situation. If the situation involves computer systems, incident response will likely be tasked with stopping virus and worm infections and/or DDoS attacks. There are other threats that should not be ignored, but these are very common attacks used against businesses. In this scenario, incident response is responsible for isolating systems and stopping the attacks by any means. Shutting down systems can lead to more problems, but if it must be done, incident response will do it. Computer forensics are used to determine whether the problem has been solved and they are tasked with determining what happened during the attacks. What was used for the attack? How did they attack the system? Is there any evidence on who executed the attack? What vulnerability did they abuse? Is the threat still active? These are some questions that should be answered by the CF team after they’ve done their research. The reason incident response shouldn’t shut down systems is because it erases volatile memory. This means the CF team will have a harder time understanding what happened, since volatile memory holds important information that can be used by the CF team to determine the attack surface. Although both teams work together, computer forensics relies on incident response’s solution in hopes to be able to analyze the aftermath, assuming there is anything left.

# Crisis Management

The crisis management team oversees resource management and should properly communicate to management, shareholders, and clients/users about events that may impact the businesses continuity. This team is also responsible for contacting law enforcement/emergency services and third-party companies that are requested by the other teams or management. This is a heavily managed department since they oversee the deployment of all previously mentioned teams. They determine how much resources should be used to mitigate or fix a problem. A business wants to have a well trained and versed crisis management team, since they will be the ones reaching out to your clients/users and eventually the media. The way they phrase their responses should be taken into consideration. With that being said, the crisis management team should not misinform anyone about the events taking place. Clear communications are an important and desirable aspect of a good crisis response team. An important task they need to perform is keeping everyone updated on the event and what is being affected. This should be done immediately after gathering enough evidence and confirmation from the other teams.

# Diagram

Here is a diagram on what the whole process may end up looking like:



References

Rouse, M., Beaver, K., & Rosencrance, L. (2017). What is incident response? Definition from WhatIs.com. Retrieved from https://searchsecurity.techtarget.com/definition/incident-response

Rouse, M., & Crocetti, P. (2016). What is business continuity and disaster recovery (BCDR)? - Definition from WhatIs.com. Retrieved from https://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR

Software, G. (2017, September 15). What are Digital Forensics & Digital Forensics and Incident Response?. Retrieved from https://www.guidancesoftware.com/blog/digital-forensics/2017/09/15/what-are-digital-forensics-digital-forensics-and-incident-response