Alexander Cannell

10/06/2013

National Incident Management System

The National Incident Management System is a preparedness plan to be ready to handle any type of emergency, disaster, or incident. Federal Emergency Management Agency (FEMA) describes an National Incident Management System as a “systematic, proactive approach to guide departments and agencies all levels of government, non-governmental organizations, an the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of an incidents regardless of cause, size location or complexity, in order to reduce the loss of life and property and harm to the environment.” (FEMA, 05/08/13) The components of NIMS is Preparedness, Communications and Information Management, Resource Management, and Ongoing Information Management. Preparedness is getting response personnel ready and train for if an incident were to occur. Communications and Information Management is an important aspect of NIMS because without good Communications and Information Management there is a lot of confusion, just look at how the emergency response was on 9-11. Resource Management is a careful plan of where to allocate resources in an emergency.

- "National Incident Management System." *FEMA.gov*. FEMA, 8 May 2013. Web. 6 Oct. 2013. <www.fema.gov/national-incident-management-system>.

I did an internship here at Southern Utah University for Mark Walton in the network security department and I was able to help write and research an Incident Security Response for the Information Technology Department. An Information Security Response sometimes referred to as an “Incident”; “is any activity that harms or represents a serious threat to the whole or part of Southern Utah University computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PHI, or a crime or natural disaster that destroys access to or control of these resources. Routine detection and remediation of a ‘virus,’ ‘malware’ or similar issue that has little impact on the day-to-day business of the University is not considered an Incident under this policy.” (SANS, 2011) While doing the research, I learned that most Universities Incident Policies were along the same guide lines that SANS (System Administrator, Audit, Networking, and Security) put out.  Each policy consisted of Communicating the Incident, Containing the Damage and then Minimizing the risk, Identifying the type and severity of the compromise, Protecting Evidence, Notifying External Agencies, Recovering Systems, Assessing Incident Damage and Cost, and Reviewing the Response and Updating Policies. What I found interesting was none too little of these plans left out an obvious final part to the Incident Policy, which is what you did to fix the problem and what you learned from the incident. While the Incident Report is very important I think that rating the severity of the Incident is important. Say that you have many Incidents happening at once I would be very hard to tackle them all at the same time that is why we set a severity priority. So if you do have multiple situations that require your attention, you can set higher and lower priorities to these incidents.

- Wright, Craig. "The Incident Handlers Handbook." *www.sans.org*. SANS, 12 5 2011. Web. 25 Apr 2013. <http://www.sans.org/reading\_room/whitepapers/incident/incident-handlers-handbook\_33901>.