An incident is a series of events that have a negative impact on the organization.

* Goal is to minimize disruption to the business.

What is incident response?

* The ability to prepare for and respond to events that present a negative effect on our network.
* The goal is to limit (as much as possible) disruptions to the network and other business processes.
  + Forensic teams focus on collecting evidence.
* Planning must be done well in advance
  + Incident response team selected and trained: contract out if you cant afford your own team.
  + Formal policies and procedures written and posted: how to we determine what behavior is normal
    - Order of steps
    - What is team authorized to do
    - How to isolate the system
  + Necessary Tools provided
    - Forensic software
  + Support from senior management
    - Understanding of how critical incident response plans are

Incident Response Lifecycle

* Preparation. CISO+team
  + Defines the preparation work that has to be completed prior to having any capability to respond to incidents.
    - Coordinate planning and design
      * Identify incident management requirements
      * Obtain funding and sponsorship
      * Develop implementation plan
  + Coordinate implementation
    - Develop: Policies, processes, and plans
    - Establish incident handling criteria
    - Define criticality: how time sensitive service or process is. How much damage does the organization suffer if a system goes down.
      * Establish periods of criticality: determine how long systems can be down
    - Evaluate incident management capability. Do we have the resources necessary?
    - Define post mortem review
    - Define process change procedure
* Identify - is this really an attack or is it a false positive?
  + Identify unusual/suspicious activity that might compromise critical business functions or infrastructure. Sometimes there are false positives.
    - Proactive detection - conduct detective monitoring regularly
      * Honeypots - in DMZ, appeal to hackers
      * Scan for unauthorized servers or hosts
      * Analyze network traffic
      * Review audit logs and files
    - Reactive detection is essential as well to be able to quickly detect and attack
      * Inclusion detection
      * Review audit logs and files
* Contain - stop the spread of infection
  + Triage - what is causing the greatest damage. Where should we direct our efforts?
    - Process of sorting, categorizing, correlating, prioritizing and assigning incoming reports/events
    - Analyze what is known, then prioritize
    - Allows events to be managed based on order of criticality
  + Isolate infected system or network
    - Pull network cable - keep in mind we have to protect evidence.
    - Isolate segment
    - Ensure forensic measures are taken in case we have to gather evidence. This is why preparation is so important.
* Remediate and Eradicate
  + Remove malware - antivirus
  + Re-image and/or rebuild systems. No problem for client computers. However, its complex if we are looking at servers.
  + Restore from media (reinstall operating system) - rootkits imbed in Op Sys
  + Restore from backups
  + Delete/disable accounts, ports etc
  + System and network device hardening. Where was our system not hardened? What allowed this?
  + Increase log monitoring. Attackers often return to the same target.
  + Scan systems and networks - antivirus (nightly even!)
* Lessons Learned - document, document, document
  + Debrief incident response team
  + Document findings
  + Consider modifying security baselines - where did we fall short and what can we do differently?
  + Evaluate risk responses with goal of improvement
  + Re-train if necessary