Incident Management

- Privacy Incidents vs Information Security Incidents
- Know when to talk to legal, users, managers, directors
- Run a scenario from A to Z, how would you ...
- Good Practices for Running Incidents
    - How to delegate.
    - Who does what role.
    - How is communication managed + methods of communication.
    - When to stop an attack.
    - Understand risk of alerting attacker.
    - Ways an attacker may clean up / hide their attack.
    - When / how to inform upper management (manage expectations).
    - Metrics to assign Priorities (e.g. what needs to happen until you increase the prio for a case)
    - Use playbooks if available
- Important Things to Know and Understand
    - Type of alerts, how these are triggered.
    - Finding the root cause.
    - Understand stages of an attack (e.g. cyber-killchain)
    - Symptom vs Cause.
    - First principles vs in depth systems knowledge (why both are good).
    - Building timeline of events.
    - Understand why you should assume good intent, and how to work with people rather than against them.
    - Prevent future incidents with the same root cause
- Response models
    - SANS' PICERL (Preparation, Identification, Containement, Eradication, Recovery, Lessons learned)
    - Google's IMAG (Incident Management At Google)