

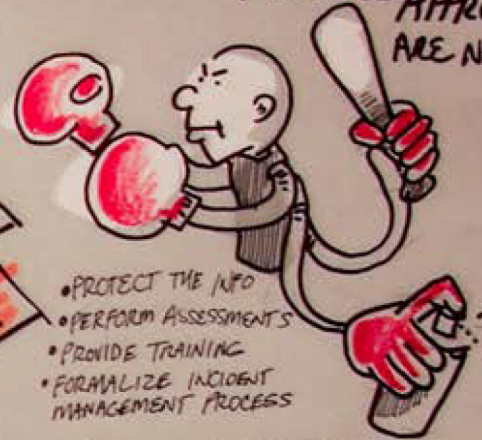
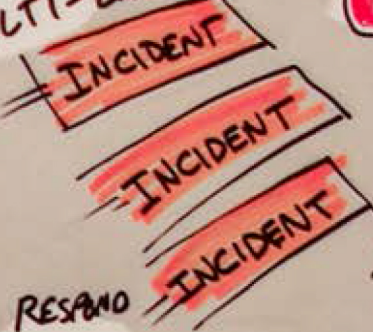
OVERVIEW OF SECURITY INCIDENT MANAGEMENT

MARK ZAJICEK

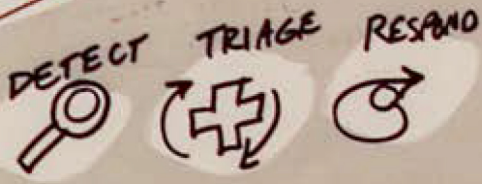
MULTIPLE APPROACHES ARE NEEDED

PROCESS-VS.-TECH THREATS CHANGE, AS DOES TECH, BUT GOOD PROCESSES ARE CONSISTENT

RESPONDING TO INCIDENTS INCIDENT ARE MULTI-LAYERED



- PROTECT THE INFO
- PERFORM ASSESSMENTS
- PROVIDE TRAINING
- FORMALIZE INCIDENT MANAGEMENT PROCESS



INCIDENT MANAGEMENT IS:

NOT JUST



BUT

KEY COMPONENT OF PLANNING

- IDENTIFY CRITICAL ASSETS
- IDENTIFY POINTS OF CONTACT

DOCUMENT YOUR PROCESS INCORPORATE BEST PRACTICES



EDUCATE EVERYONE TO HELP THEM PROTECT THEMSELVES



ELIMINATE BOTTLENECKS + SINGLE POINTS OF FAILURE → WEAKLINK ←

