

DUMPSTER FIRES: 6 THINGS ABOUT IR I LEARNED BY BEING A FIREFIGHTER





AGENDA

- Intro
- What is IR
- Firefighting 101
- IR vs. Firefighting
- Challenges
- Opportunities
- Summary
- Final Thoughts

INTRODUCTION





@INVESTIGATORCHI (Dr. Catherine J. Ullman)

- Sr. Information Security Forensic Analyst, University at Buffalo
- Staff: BsidеsROC, Wall of Sheep/Defcon, UB GenCyber Camp, CircleCityCon
- Volunteer: Skytalks, BsidеsLV
- Speaker: Wall of Sheep/Defcon, Circle City Con, Converge, BTV/Defcon, GRRCon, BlueTeamCon
- Certifications: GSEC, CEH, CFCE, MCSE
- M.F.S. (Master of Forensic Science), PhD, Philosophy



FIREFIGHTER, CITIZENS HOSE COMPANY, LFD

- State Fire Instructor – New York State Office of Fire Prevention and Control
- Corning Community College – 54 credits towards A.O.S. Fire Protection Technology
- Former New York State Certified Fire Investigator I
- Former New York State Certified Fire Investigator II
- National Certification Fire Instructor I
- Former Member of Juvenile Fire Intervention Response and Education Program of Western New York (J-F.I.R.E)



JIM LEPCARD DIGITAL IMAGING

WHAT IS INCIDENT RESPONSE?





INCIDENT RESPONSE

- All of the technical components required in order to analyze and contain an incident.*
- The process of addressing network events
 - can be both proactive and reactive
 - any event that affects the confidentiality, integrity and/or the availability of information

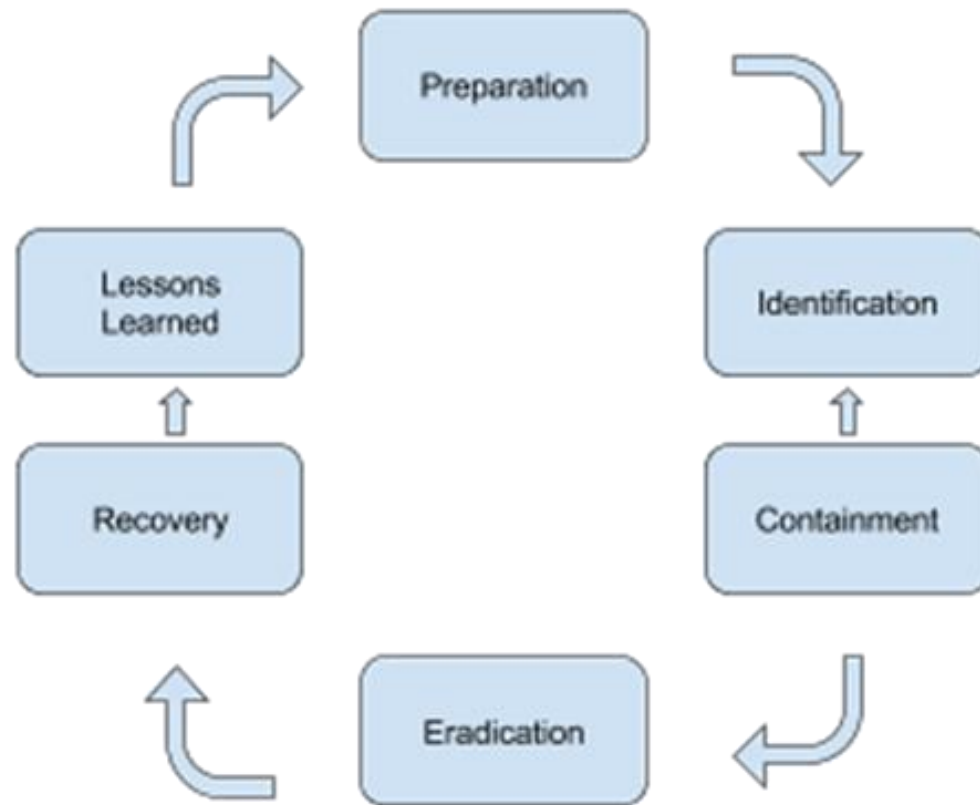
*differs slightly from incident handling



INCIDENT RESPONSE - GOALS

- Ensure awareness of significant security incidents
- Stop the attacker
- Minimize damage caused
- Prevent follow on attacks/future similar incidents

PHASES OF INCIDENT RESPONSE





TERMINOLOGY

- **Preparation:** documentation, tool building
- **Identification:** awareness of attacks
- **Containment:** patching, blocking C2, pull power
- **Eradication:** remediating/removing compromised hosts
- **Recovery:** restore business functions
- **Lessons Learned:** avoiding the same mistakes twice



INCIDENT HANDLING

- The logistics, communications, coordination, and planning functions needed in order to resolve an incident in a calm and efficient manner
- Ideally a separate role from those doing incident response

WHAT IS FIREFIGHTING?





FIREFIGHTING

- the act of attempting to prevent the spread of and extinguish significant unwanted fires in buildings, vehicles, woodlands, etc.



FIREFIGHTING/FIRST RESPONDER GOALS

- Protect the health and safety of themselves and the public
- Protect public and private property and the environment
- Minimize the disruption of community activities

PREPAREDNESS CYCLE





BREAKING IT DOWN

- **Mitigation** - Preventing future emergencies or minimizing their effects
 - Smoke detectors, sprinklers
- **Preparedness** - Preparing to handle an emergency
 - Building pre-plans, gear maintenance
- **Response** - Responding safely to an emergency
 - Save property/lives
- **Recovery** - Recovering from an emergency
 - Clean-up, restoration, repairs



Just doing my job...

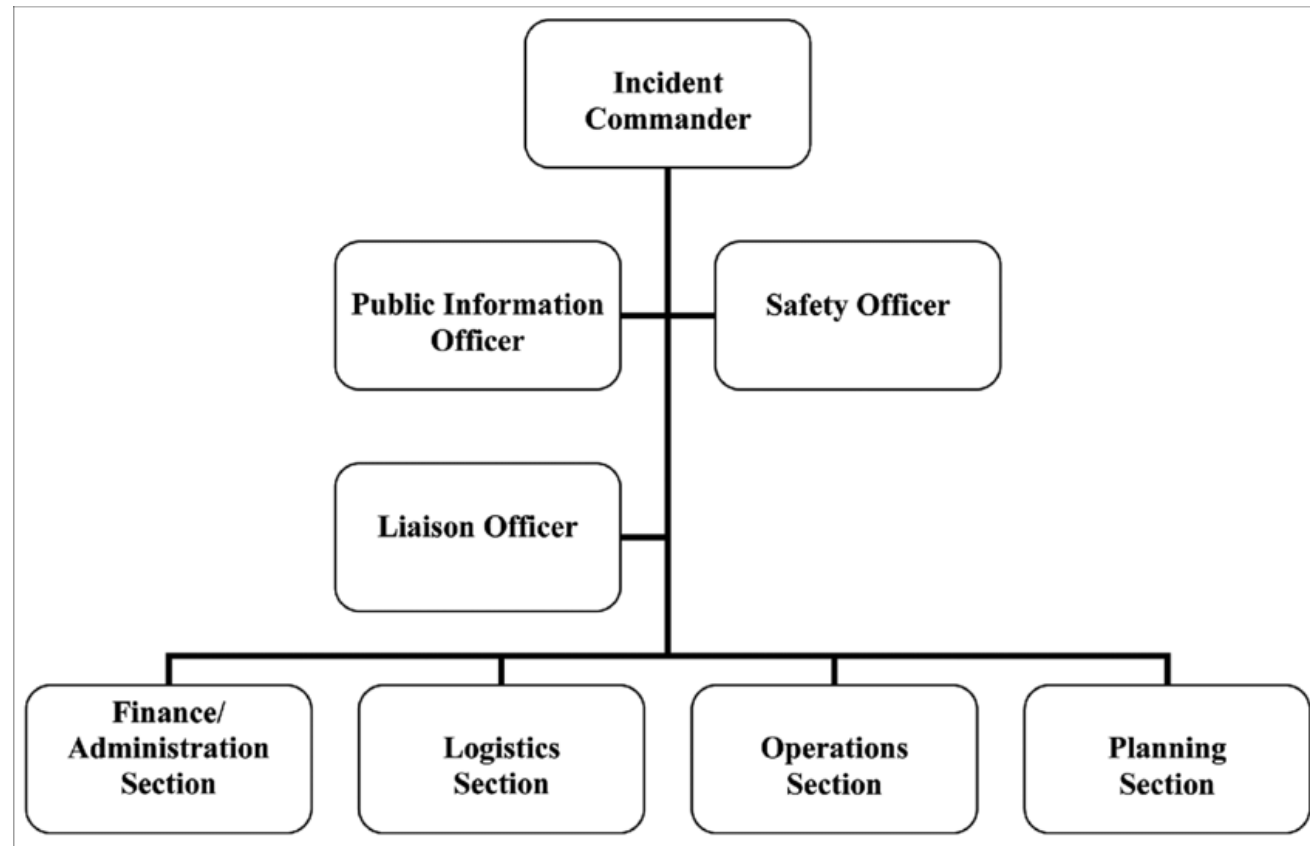


TERMINOLOGY

- **ICS (Incident Command System)**: is a standardized approach to the command, control, and coordination of emergency response providing a common hierarchy within which responders from multiple agencies can be effective.

“organized response to a problem”

INCIDENT COMMAND SYSTEM





BREAKING IT DOWN

- **Incident Command (IC):** Defines incident goals & operational objectives
- **Operations:** Strategy (approach)& tactics (actions)
- **Logistics:** Personnel, supplies, equipment
- **Planning:** Long-range planning/demobilization
- **Admin/Finance:** admin issues, \$, reg/compliance/licenses

IR VS. FIREFIGHTING





METHODOLOGY COMPARISON

Incident Response

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Firefighting

- Mitigation
- Preparation
- Response
- Recovery
- Lessons Learned



MISCONCEPTIONS

IR

- Every event is an incident
- Every incident is handled the same way
- Every incident is quickly solved
- Every person on an IR team needs to be a rock star
- Accurate attribution is always possible

Firefighting

- Firefighters are always paid
- Firefighters are always big, tough dudes
- Every fire is fought the same way
- Every fire is quickly extinguished
- Always a full-time job



DIFFERENCES

- IR rarely involves life safety except in health care
- IR teams are typically paid
- IR teams use computers/software
- Firefighters have to wear special gear
- Firefighters often show up in special vehicles
- Firefighters use water/foam/chemicals



SIMILARITIES

- Focus on immediate issue first, later find the cause
- Triage used to determine best course of action
- Cyclic in nature starting with documentation/preplans
- Require thinking outside the box
- Often involve bringing in outside entities
- Sometimes have inside teams

CHALLENGES

Tunnel vision: Focusing on one item to the exclusivity of seeing the bigger picture, which can lead to making incorrect, inappropriate, or even dangerous decisions.





Did I miss something?

EXAMPLES – TUNNEL VISION

- Firefighting
 - What are the cones protecting?



EXAMPLES – TUNNEL VISION

- Incident Response
 - ***Is the scene safe?***
 - Malware or just misconfiguration?
 - Blind hardware acquisition
 - Ransomware or just phishing email?





CHALLENGES

Reactionary behavior - Allowing outside forces to influence decision making rather than relying on pre-plans, often forgetting to evaluate the bigger picture.

REACTIONARY BEHAVIOR - EXAMPLE

- Firefighting – Worchester Cold Storage Fire
 - December 3, 1999
 - 1906 meat packing plant
 - Basically vacant
 - Maze of meat lockers
 - 6 firefighter fatalities



REACTIONARY BEHAVIOR - EXAMPLE

- Incident Response
 - Forensics without clear/explicit goals
 - Just pulling network connections
 - Turning off machines
 - Suspending all accounts





CHALLENGES

Freelancing – Individuals or groups going off on their own without following any kind of chain of command or checking in with a team leader, which can lead to dangerous and/or reckless situations as well as bad feelings due to a lack of or miscommunication.

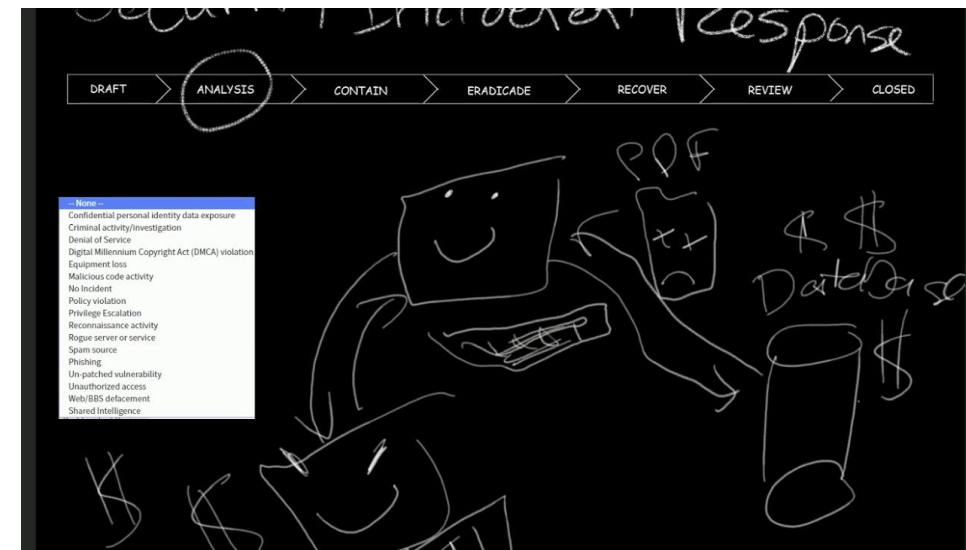
FREELANCING - EXAMPLES

- Firefighting
 - Crossing the streams
 - “Feeding” a fire via doors/windows



FREELANCING - EXAMPLES

- Incident Response
 - Collecting “all the things”
 - Not collecting the required items
 - Duplication of data collection
 - Data alteration/misrepresentation



OPPORTUNITIES

Patience – Taking a moment to determine whether there actually is an incident and/or what the best course of action is to take can have significant impact on whether or not a successful outcome is achieved.

Slow is fast



EXAMPLES - PATIENCE

Firefighting



EXAMPLES - PATIENCE

- Incident Response
 - OMGWTFBBQ!!!!!!! (Is it actually an incident?)
 - Time is important, but life safety important?
 - What is the REAL risk/implication?

The Chegg logo is displayed in a bold, orange, sans-serif font. The word "Chegg" is followed by a registered trademark symbol (®). The logo is centered horizontally in the lower half of the slide.



OPPORTUNITIES

Accountability – Knowing where team members are at all times to prevent physical hazards, duplication of effort, direct interference, and/or stepping on toes (literal or figurative) is critical to a successful incident.

EXAMPLES - ACCOUNTABILITY

- Firefighting:
 - Accountability tags



IR:
Swipe card access

Incident Access Log

Date: _____

Location: _____

Incident number: _____

Supervisor: _____

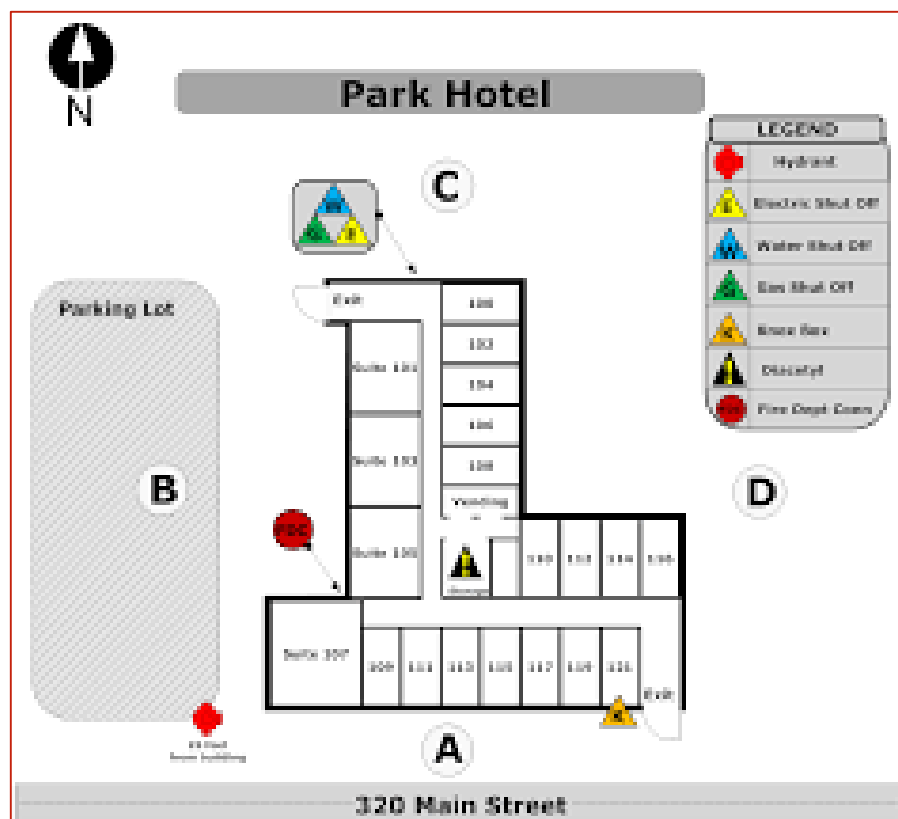
[illegible]

OPPORTUNITIES

Pre-planning - Knowing your environment either directly through your own documentation or the documentation provided to you, which should include data from tabletop and pre-mortem exercises, can sometimes provide “gotchas” that you might not otherwise realize or consider.


PRE-PLANNING EXAMPLES

- Firefighting



| ASHTABULA COUNTY FIRE DEPARTMENT PRE-PLAN | | | |
|---|--|--|----------------------|
| INFO | Name: Ashtabula Fire Department | | Occupancy: Fire Dept |
| | Address: 4326 Main Ave, Ashtabula | | Phone: 440-555-5555 |
| FIRE PROTECT. | <input checked="" type="checkbox"/> Special Hazards <input type="checkbox"/> Tier 2 Security Video User: Pwd: | | |
| | Detectors: <input checked="" type="checkbox"/> Smoke <input type="checkbox"/> Heat Sprinkler: <input type="checkbox"/> Full <input type="checkbox"/> Partial, <input type="checkbox"/> Standpipe | | |
| | <input checked="" type="checkbox"/> Knox Box Front Door left <input checked="" type="checkbox"/> Fire Pump Basement | | |
| | <input checked="" type="checkbox"/> Ann. Panel Front entryway <input type="checkbox"/> Alarm Panel | | |
| BLDG CONSTRUCT. | <input type="checkbox"/> FDC | | |
| | <input checked="" type="checkbox"/> Specialized Extinguishing: Hood suppressions system | | |
| | Width: 175 Length: 100 Stories: 2 Other: | | |
| | Type: II | | |
| BLDG ACCESS | Roof Structure: Steel Bar Joist | | |
| | <input checked="" type="checkbox"/> Roof Hazards 2 AC units | | |
| | <input checked="" type="checkbox"/> Parapet Wall Height: 1 ft | | |
| | Other: | | |
| BLDG ACCESS | Building Access: Rear Mandoor | | |
| | <input checked="" type="checkbox"/> Stairways: Rear and middle front | | |
| | <input type="checkbox"/> Elevators: | | |
| | <input checked="" type="checkbox"/> Roof Access: Top front stairway | | |
| BLDG ACCESS | <input checked="" type="checkbox"/> Basement <input type="checkbox"/> Full <input checked="" type="checkbox"/> Partial Access: Below the front stairway | | |

PRE-PLANNING EXAMPLES

- Incident Response
 - Tabletop exercises: Backdoors and Breaches!
 - Documentation
 - Incident response team/plan
- 



SUMMARY





THINK LIKE A FIREFIGHTER

- **Avoid tunnel vision** – do a “360” of the problem
- **Act, don’t react** – don’t be mislead by emotion
- **Don’t freelance** – follow the plan
- **Have patience** – take a “beat” before proceeding
- **Location, location, location** – documented accountability
- **Pre-plans rock** – less chaos = easier/safer response
- **Incident Command System** – organize your response

FINAL THOUGHTS



GREAT THINGS
NEVER
come from
COMFORT
ZONES



www.amerincupboard.net