Top Level Domain Incident Response “Recovery” Checklist

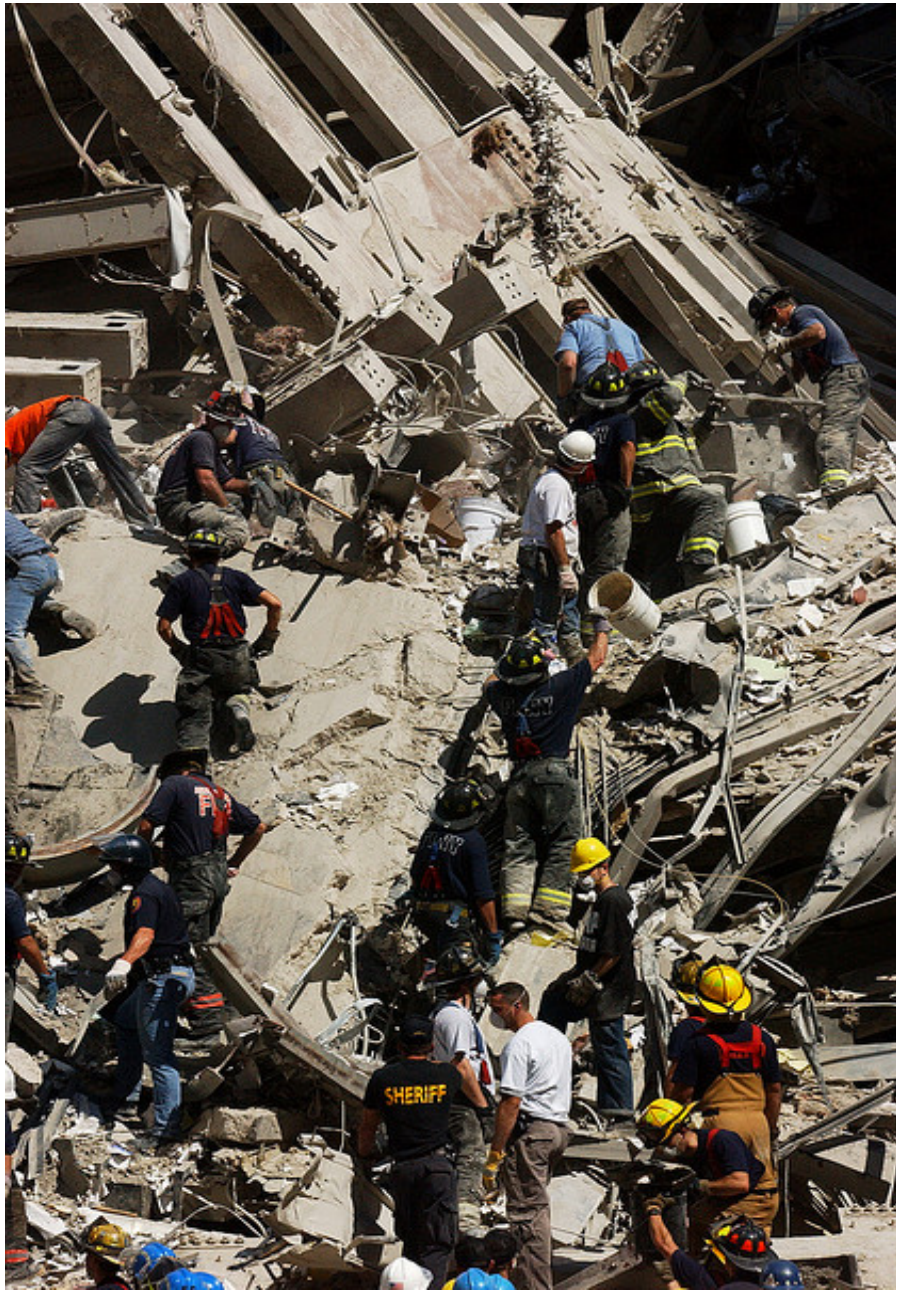
Dave Piscitello

VP Security and ICT Coordination

ICANN

Collaborative Effort

- ICANN security team
- MarkMonitor
- The affected registry operations staff
- NSRC
- Farsight



https://www.flickr.com/photos/slagheap/

Disclaimers

- High level:
  - not exhaustive
- Not legal advice
- Not a policy document

Guidelines

- List of actions a registry operator should consider if an authoritative name service is compromised

Time Horizons

What we cover

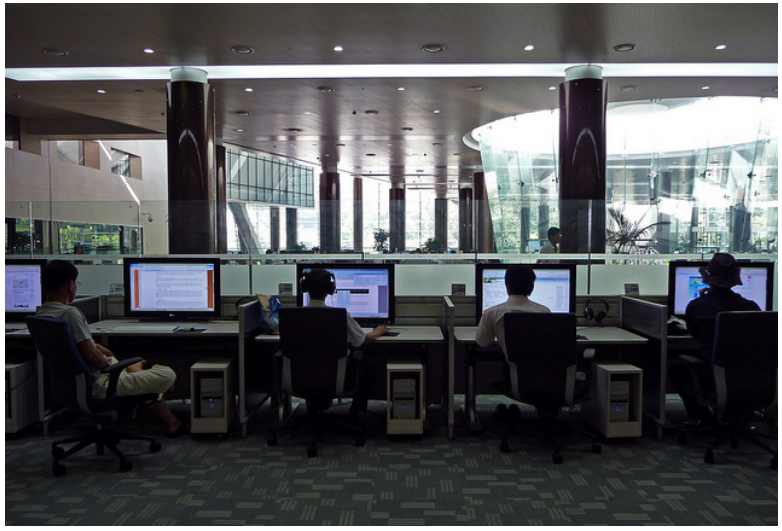
- Investigations Basics
  - Preserving the scene
  - Basic forensics
  - Reporting criminal acts

https://www.flickr.com/photos/projectexploration/

Restoring Service

- Building from scratch while “hardening” during this process
- Recovery or restoration of other affected services

https://www.flickr.com/photos/buildingblog/



https://www.flickr.com/photos/mosmanlibrary/

- Event monitoring considerations
- Intrusion detection and mitigation considerations

Improvement

Call for Backup

https://www.flickr.com/photos/donkeyhotey/

- ICANN ISSSR may be able to assist you directly
- Or we can invite trusted experts
- Assistance may already be in place
  - OpSec community already monitors most of DNS infrastructure