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

We Are Not Attorneys
but we know our tech...
Guidelines

• List of actions a registry operator should consider if an authoritative name service is compromised
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
- Event monitoring considerations
- Intrusion detection and mitigation considerations
Mistakes have the power to turn you into something better than before.
Call for Backup

- 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

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