A Prepper’s Guide to

The Incident Response Go-Bag

Reg Harnish, CISM, CISA, CISSP
GreyCastle Security
www.greycastlesecurity.com
@greycastlesec
Building an Incident Response Go-Bag

10-13 Things You Didn’t Think Of
Food
Water
Shelter
First Aid
Defense
Theft
Misuse
Malware
Intrusion
Disruption
Fig. 3.1(a): The Important Part
1. Investigation Tools

- USB Optical Drive
- LiveCD
- Network tap
- Latex gloves
- Anti-static bands
2. Forensic Tools

- Write blockers
- Evidence bags
- Faraday bags
- Forensic duplicators
  - Static
  - Volatile
  - Mobile
  - Macs
  - Solid state
3. Other Tools

- Power strips
- Cables
- Screwdrivers
- Duct tape
- Tin foil
- Flashlight
- Sharpies
4. Caution Tape

- Protect crime scene integrity using tape, signs or other communications
5. Log Book

- Record everything
- Digital camera
- Also bring Incident Reporting forms
6. Contact Lists

- IRT
- Management
- Cloud vendors
- ISPs
- Law Enforcement
- Also an organization chart to determine accountability
- Bring your business cards
7. Credit Card

- Hotel and travel expenses
- Gear and tools you forgot
8. Lawyer

- Litigation decision
- Cloud evidence
- Data Retention policy
- Data breach reporting requirements, including Safe Harbor
- Interpreting “appropriate” and “reasonable”
9. Backup

- Evidence should be collected by two people, if possible
- Extra CDs, flash drives
- Additional storage for imaging
- Variety of software that does the same thing
10. Communications

- Don’t use the client’s network for communications
- MiFi, JetPack or similar
11. Cyber Liability Insurance

- Understanding the terms and limits may influence the scope of response.
12. Common Sense

- Indicators of Compromise (IoCs)
- “Kill Chain”
- Imagination
- Xanax
13. Incident Response Plan

- Printed copies
- Process documentation
- Roles and responsibilities
Build Your Own Go Bag – Incident Response Resources
Incident Response Resources

- NIST Computer Security Incident Handling Guide
  http://csrc.nist.gov/publications/nistpubs/800-61-
  rev1/SP800-61rev1.pdf

  Response Teams (CSIRTs)

- ENISA Incident Handling Process
  http://www.enisa.europa.eu/activities/cert/support/incide
  nt-management/browsable/incident-handling-process
Incident Response Resources

- ForensicsWiki
  [http://forensicswiki.org/](http://forensicswiki.org/)

- SANS Incident Response Reading Room
  [http://www.sans.org/reading-room/whitepapers/incident](http://www.sans.org/reading-room/whitepapers/incident)

- Center for Internet Security
Data Breach Reporting Requirements

- Security Breach Notification Laws (by State)

- HIPAA HITECH Breach Notification Rule
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

- FTC Safeguards Rule
Final Thoughts
RON BURGUNDY ON ADVICE
Go Bag Tips

- Should be easy to carry
- The gear should be dedicated to Incident Response
- Should be reviewed regularly
- All gear should be tested before it goes into the field
“Everybody has a plan until they get punched in the face.”

- Mike Tyson
GOT QUESTIONS?
REG HARNISH
GREYCASTLE SECURITY
RHARNISH@GREYCASTLESECURITY.COM
@GREYCASTLESEC