You’ve Been Hacked - Now What?
10 Tips for Effective Response
Reg Harnish, CISM, CISA, CISSP
GreyCastle Security
Lahore, Pakistan – February 2011
Searching for “Brain” – the first computer virus
HOW DID WE GET HERE?
YOU’VE BEEN

NOW WHAT?

HACKED

GreyCastle security
1. Learn how to:

Perform Incident Triage

- Secure the crime scene
- Listen, assess and question conclusions
- Be flexible – prepare for surprises
- Manage expectations
2. Build your: Incident Response Team

- Find the best responders — they are unique
- Train responders regularly
- Give them explicit and flexible direction
3. Learn how to:

Perform Forensics

- Decide early if you’re going to litigate
- Allow your attorney to drive the investigation
- Establish secure storage location(s)
- Log everything
- Outsource forensics to the experts
4. Configure assets to:

Generate Intelligence

- Log events that may be needed for response
- Understand what “normal” is
5. Learn how to:

Perform Investigations

- Know what’s worth stealing
- Understand Indicators of Compromise (IoC)
- Preserve evidence correctly
- Prepare for the unexpected
6. Learn how to: Report Breaches

- Understand your reporting requirements
- Maintain notification templates
- Allow attorney to define “reasonable”
7. Make sure to:

**Test and Train Effectively**

- Test your Incident Response Plan
- Train teams on your Incident Response Plan
- Measure response capability
- Budget for testing and training
8. Get to:

Love Your Attorney

- Prepare to be sued by customers, partners, banks
- Allow legal team to drive data retention
- Sic attorney on cloud, hosting and other providers
- Include attorney in key decisions
9. Make sure to:

Manage IT Staff

- Keep IT staff from overstepping their capabilities
- Maintain contacts lists for law enforcement, digital forensics experts and attorneys
10. Consider:

**Cyber Liability Insurance**

- Minimize policy premiums by managing risk
- Understand the fine print
- Prepare for a battle
Standards

- NIST Computer Security Incident Handling Guide


- ENISA Incident Handling Process
Breach Reporting

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

- FTC Safeguards Rule
FINAL THOUGHTS
Know the difference between **EXPOSURE** AND **A BREACH**.
Know when to Cut Your Losses.
Learn how to SURVIVE.
GOT QUESTIONS?
REG HARNISH

CHIEF SECURITY STRATEGIST
GREYCASTLE SECURITY
@GREYCASTLESEC