ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Defending Freedom on the Electronic Frontier
454 SHOTWELL STREET, SAN FRANCISCO, CA, USA 415.436.9333 WWW.EFF.ORG

EFF Civil Liberties Director Jennifer Granick

What to do When You've Been Attacked

PRE-ATTACK PREPARATION: ESTABLISH A PROTOCOL

- Develop organizational policies that make clear who inside the company should be contacted, when law enforcement will be contacted, if and when monitoring will be done.
- Protocol should be policy and practice on information handling, information integrity, appropriate use of forensic tools, reporting to higher-ups, legal counsel, law enforcement.
- Need IT professionals trained in the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.
- Also, need to get mission critical servers back up and running.
- Last two goals can be contradictory. Someone will need to decide.

LEGAL ISSUES

- Liability for harm to customers
- Liability for harm to other systems attacked through yours
- Data breach notification requirements
- Preparing to find and prosecute the attacker
- Laws and regs differ for different industries and from state to state

DIGITAL FORENSICS

Forensic techniques are useful for investigating crimes and internal policy violations, reconstructing computer security incidents, troubleshooting operational problems, recovering from accidental system damage.

Collection: Never do forensics on the original media. Must determine what is relevant and mirror that data, in a manner that preserves the integrity of the data.

Examination: forensically analyse data while preserving its integrity.

Analysis: use legally justifiable techniques to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

Reporting: Description of the actions taken, how tools and procedures were selected, what other actions need to be performed, and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

ISSUES

- Cost, Response Time, Data Sensitivity
- Outside professionals or in-house? Level of training?
- Regular backups, maintainance and destruction
- Policies on when and how to audit
- Preserving integrity of audit records
- System for determining whether programs, data have been altered