International Municipal Lawyers Association
2014 Annual Conference
Baltimore, Maryland

September 10, 2014

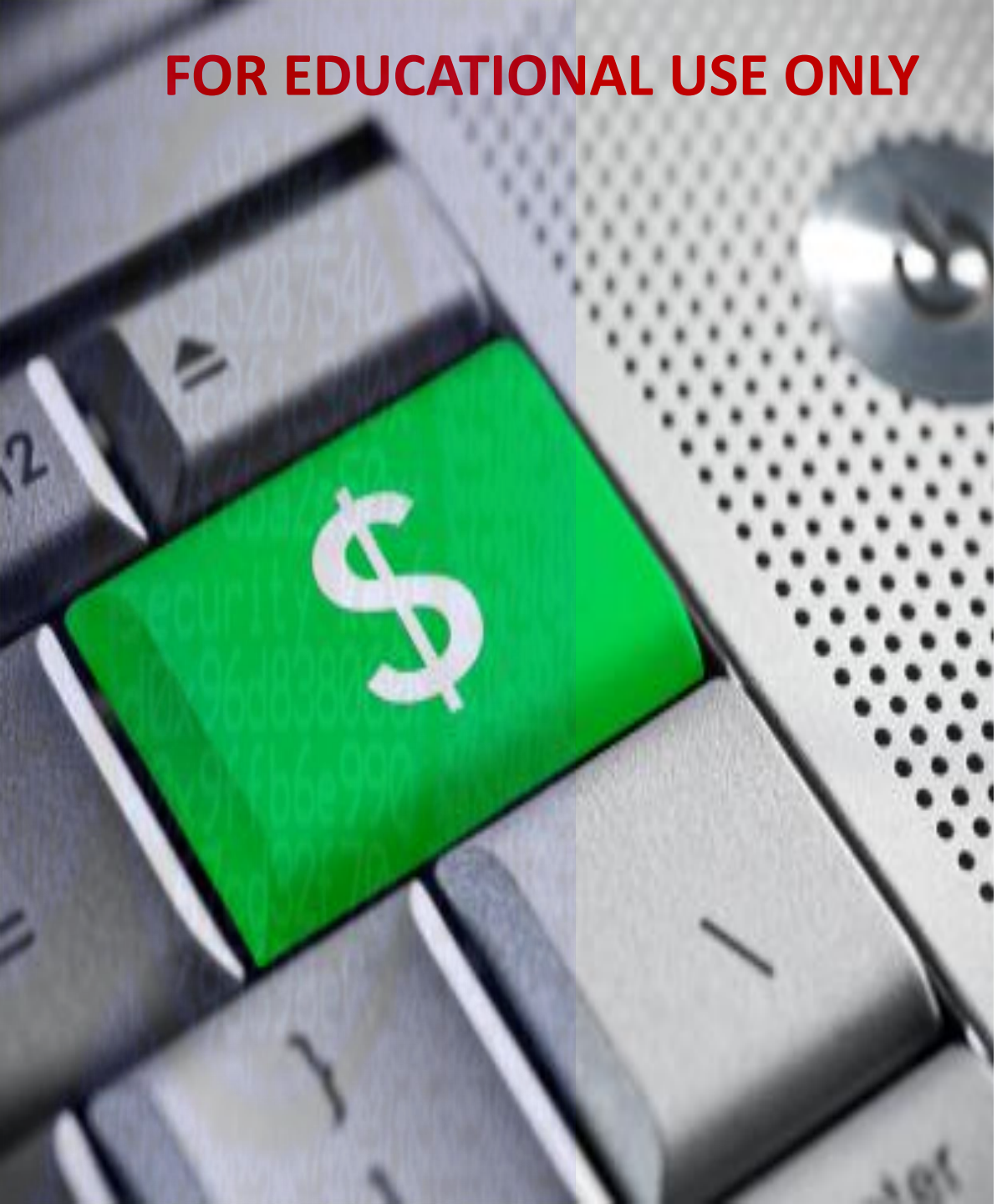
Work Session II: Technology

Cybercrimes – The Perfect Crime and Local Governments Not Immune

by

Matthew A.S. Esworthy
Shapiro Sher Guinot & Sandler
Baltimore, Maryland

©2014 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2014 Annual Conference, held September 10-14, 2014 in Baltimore, MD. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

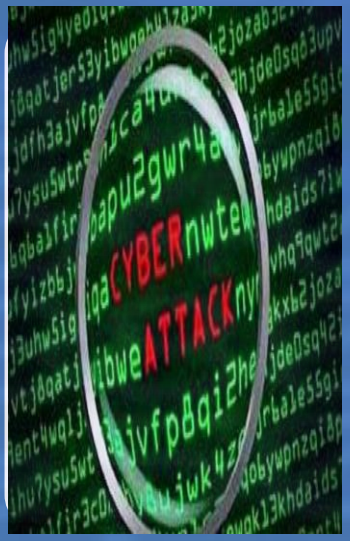


FOR EDUCATIONAL USE ONLY

SHAPIRO SHER GUINOT & SANDLER

CYBERCRIME : THE PERFECT CRIME

Matthew A. S. Esworthy, Esq.
Shapiro Sher Guinot & Sandler
36 South Charles Street
Suite 2000
Baltimore, MD 21201
410.385.4222 ph
410.539.7611 fax
mase@shapirosher.com

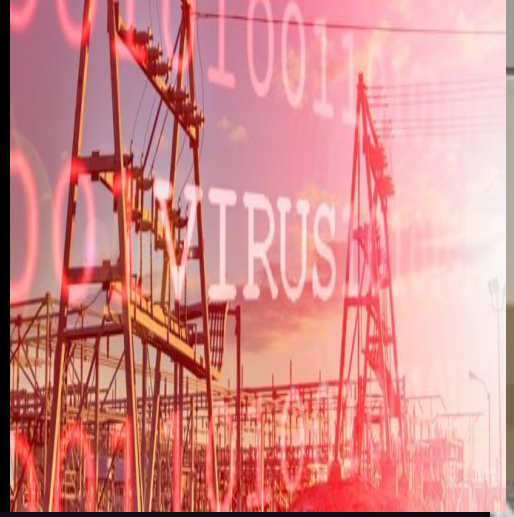


Cyberattacks



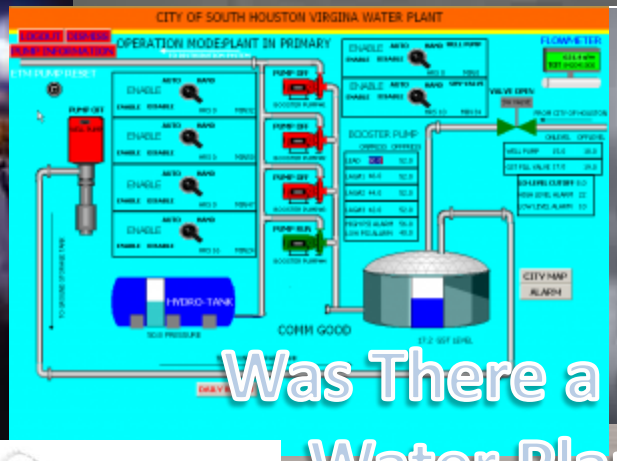
Data Breaches













Was There a Cyber Attack at Water Plant in Illinois?







Data Breach, Cybercrime Response

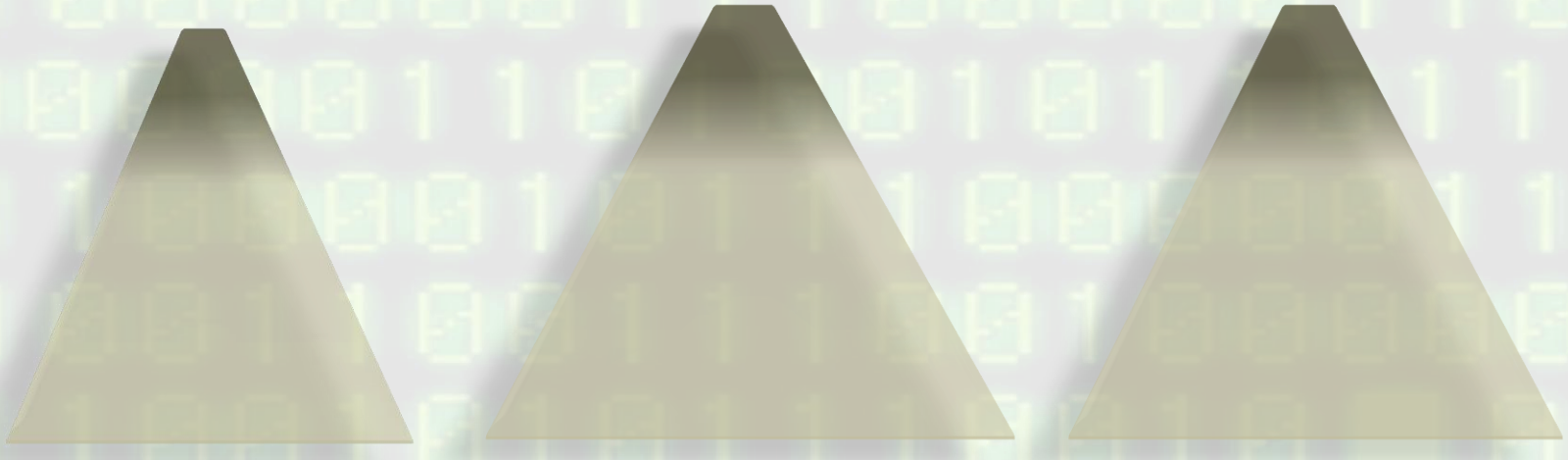
- State-sponsored and Industrial Espionage
- Theft of Intellectual Property
- Leaks of Confidential Information
- Lost Laptops, Servers, Backup Tapes
- Hacks, Unauthorized Access, Exceeding Authorized Access
- Cyber-extortion, Insider Trading
- Hacktivism (Anonymous)
- DOS

Unexpected Pathways

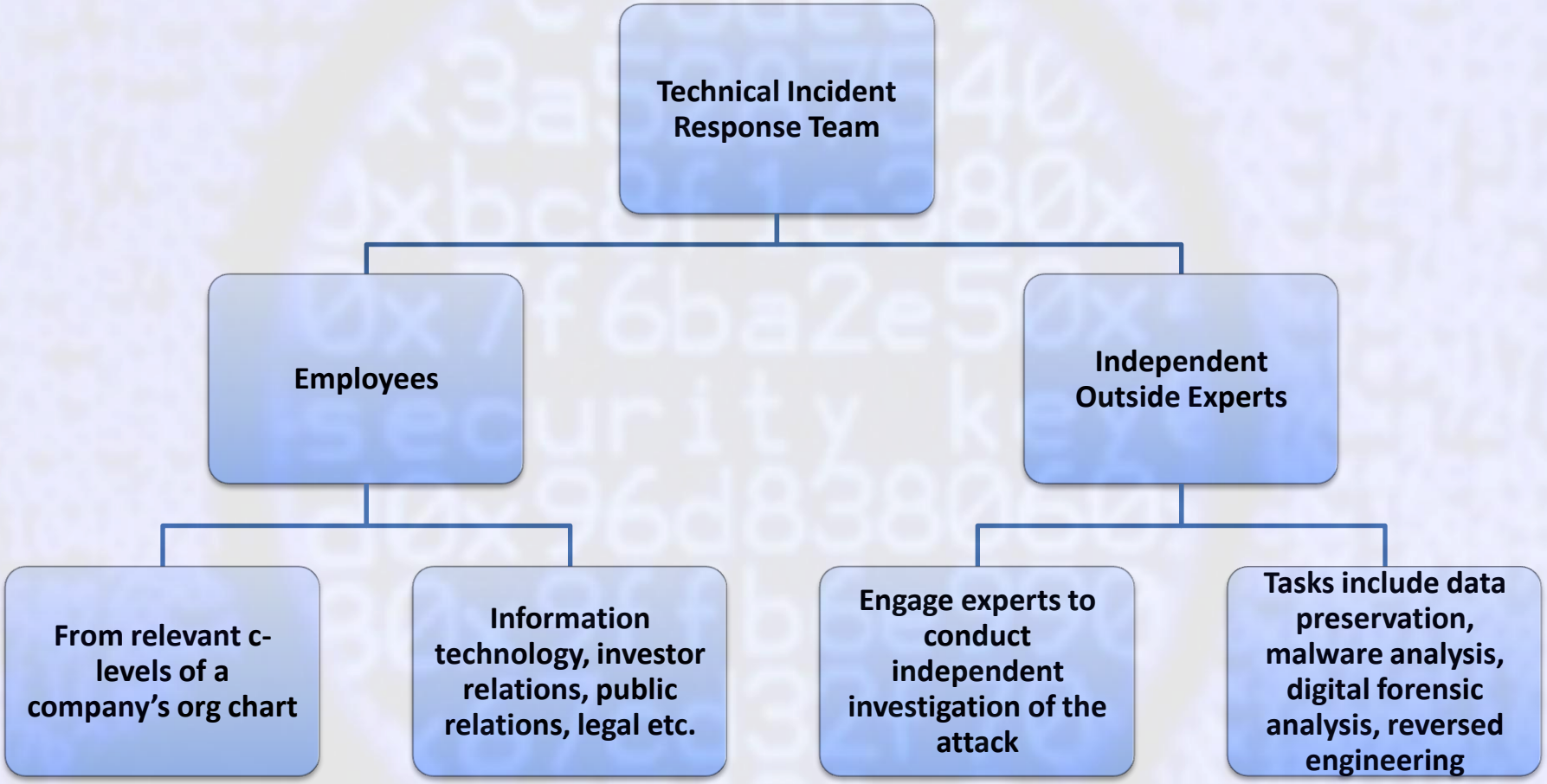
Law Firms

Public Relations Firms and Vendors

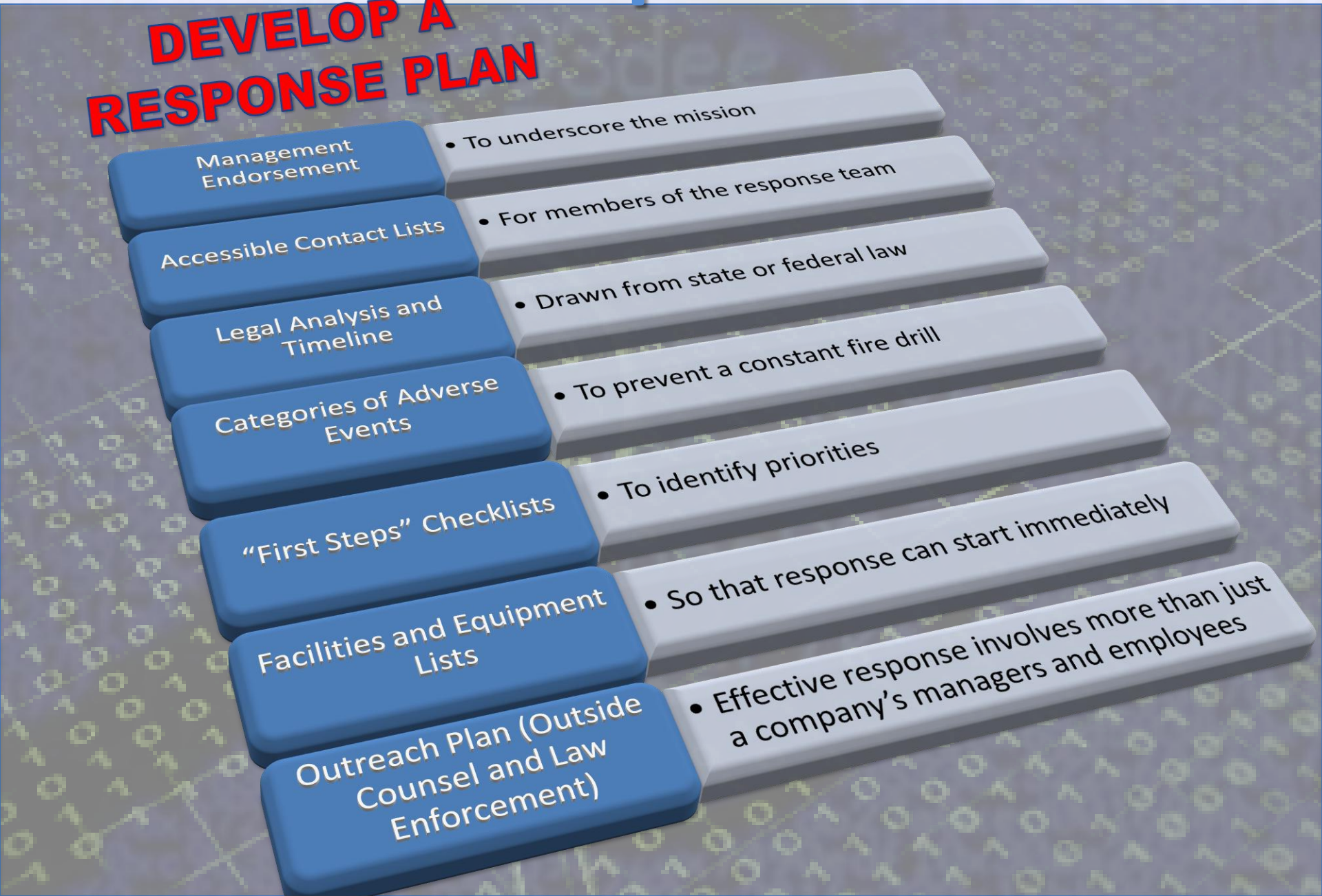
Other Related Parties



Response Team Formation



Prepare


DEVELOP A RESPONSE PLAN
Management Endorsement
• To underscore the mission
Accessible Contact Lists
• For members of the response team
Legal Analysis and Timeline
• Drawn from state or federal law
Categories of Adverse Events
• To prevent a constant fire drill
"First Steps" Checklists
• To identify priorities
Facilities and Equipment Lists
• So that response can start immediately
Outreach Plan (Outside Counsel and Law Enforcement)
• Effective response involves more than just a company's managers and employees

Preserve

- Assemble team, distribute list of responsibilities
- Unhook infected machines
- Call outside experts to forensically image
- Pull needed backups out of rotation and insert clean and patched machines
- Save off log files, keycard data and surveillance tapes
- Start real-time network packet capture
- Force administrator and user password change

Assess

Early Assessment:

- Type (if any) of lost or compromised data
- Time period of breach
- Initial volume estimate of data involved

Forensic Assessment:

- Analyze log files and hard drives
- Review memory/virtual memory
- Analyze and reverse engineer malware code
- Review live traffic captures
- Run behavioral profiling (Email Testing)

Law Enforcement Liaison









