

# South Carolina Computer Crime Center

Lt. Amanda Simmons  
South Carolina Law Enforcement Division  
803-896-7901

*South Carolina* COMPUTER CRIME CENTER  
A PARTNERSHIP WITH A FOCUS ON ENFORCEMENT AND PREVENTION

# INCIDENT RESPONSE DATA SECURITY BREACHES

- INCIDENT DISCOVERY AND REPORT
- INCIDENT CONFIRMATION
- USER INCIDENT HANDLING
- SYSTEM INCIDENT HANDLING
- INVESTIGATION
- LESSONS LEARNED AND RECOMMENDATIONS

# INCIDENT RESPONSE DATA SECURITY BREACHES

- INCIDENT DISCOVERY AND REPORT
  - Users who are reporting incident may notice:
    - Changes to Database
    - Changes to Websites

# INCIDENT RESPONSE DATA SECURITY BREACHES

- INCIDENT CONFIRMATION
  - Security Incident Response Team
    - Detailed notes
    - Who is involved in discovery process
    - What changes were made, if any
    - Existing Accounts
    - Potential for New Accounts
    - ID Pertinent Data

# INCIDENT RESPONSE DATA SECURITY BREACHES

- USER INCIDENT HANDLING
  - End Users cannot access the web page
  - Web page contents are changed
  - Web page behaves abnormally
  - Files from website contains a virus
  - Web page is unavailable

# INCIDENT RESPONSE DATA SECURITY BREACHES

- SYSTEM INCIDENT HANDLING
  - Server may be infected with virus
  - Files distributed from server contains virus
  - Server is down
  - Changes are detected by monitoring tool

# INCIDENT RESPONSE DATA SECURITY BREACHES

- INVESTIGATION
  - Internal Investigation
  - External Law Enforcement Investigation
    - Jurisdictional Issues
    - Actual Crime Committed
    - Financial Damages

# INCIDENT RESPONSE DATA SECURITY BREACHES

- INVESTIGATION-TYPES
  - UNAUTHORIZED ACCESS
  - DENIAL OF SERVICE ATTACKS
  - HOSTILE CODE
  - NETWORK PROBING

# INCIDENT RESPONSE DATA SECURITY BREACHES

- Log files from Firewalls and other network hardware/software
- Log files from compromised computer
- Full examination on compromised computers and/or other hardware

# INCIDENT RESPONSE DATA SECURITY BREACHES

- LESSONS LEARNED AND RECOMMENDATIONS
  - Team should evaluate the entire situation and provide recommendations for future prevention, etc.

# INCIDENT RESPONSE DATA SECURITY BREACHES

- Order Credit Reports
- Examine Credit Reports Carefully
- Consider a Security Freeze

# SC Code

- CHAPTER 16.
- COMPUTER CRIME ACT
- **SECTION 16-16-10.** Definitions.
- For purposes of this chapter:
- (a) “Computer” means a device that performs logical, arithmetic, and memory functions by manipulating impulses including, but not limited to, all input, output, processing, storage, computer software, and communication facilities that are connected or related to a computer in a computer system or computer network. For the purposes of this section, “computer” includes, but is not limited to, mainframes, servers, workstations, desktops, and notebooks; industrial controls such as programmable logic controllers and supervisory control and data acquisition systems; portable hand-held computing devices such as personal digital assistants and digital cellular telephones; data communications network devices such as routers and

# Minimize Your Risk

- Update virus protection regularly
- Don't download files from unknown source
- Use a hardware/software firewalls (*Cable and DSL lines*)
- Use a secure web browser (128 bit encryption)
- Laptop security
- Use monitoring devices

# QUESTIONS

??

Lt. Amanda Simmons  
South Carolina Law Enforcement Division  
803-896-7901