



# NSC Training Seminar

Jane Drews  
IT Security Officer  
The University of Iowa

# [ NSC: Defined ]

- Department **Network and Security Contact (NSC)** is a departmental employee who acts as a liaison and conduit for **timely and relevant information flow** between central networking and computer security personnel, and the departments on campus

# [ NSC Program Design ]

- Each department may have up to 2 contacts, a primary and a secondary
- An org/department may choose to “roll up” contacts to the next organizational level
  - College of Engineering
  - College of Business
  - UIHC/HealthCare Information Systems

# [ NSC Program Design ]

- Permanent university staff employed at least 50% time in the department (or unit)
- Regular employment validation to keep database up to date

# [ NSC Program Design ]

- Registration Information
  - Contact Name, Campus Address, Phone, Email address
  - Department Number(s)
  - Department Name
  - Buildings with staff or equipment
- <http://cio.uiowa.edu/itsecurity/incident/nsc-form.htm>

# [ NSC Program Design ]

- “NSC-building” e-mail *alerts* lists
  - Subscription only to NSC’s
  - Buildings your department housed in = lists you’re subscribed to
  - Confidential information
- “NSC-ALL” campus e-mail *notices* list
  - Open subscription
  - No confidential information sent

# [ How was I selected for this job? ]

- Program inception, 1998
  - DDDEO memo describing program, asked DEO to appoint 2 contacts per department
- Current Process
  - Contact remaining/current NSC for 2<sup>nd</sup> contact when one leaves, or
  - Contact DEO for name of new contact

# [ What is my role? ]

- **COMMUNICATION**

- Alerts from security office
- Outage notices from networking

- **INFORMATION SHARING**

- Security vulnerability scan results

- **LIAISON to SECURITY OFFICE**

- For security incident response, we contact you first

# [ What is (NOT) my role? ]

## ■ DISCIPLINARY ACTION

- Expected to review university or departmental policy with individuals when necessary
- Human Resources, et al determine if/when/what discipline is appropriate

## ■ FIXING PROBLEMS

- Expected to notify appropriate staffs of problems, not necessarily to fix them

# [ What do I need to know? ]

- How to contact *every* person in your department or unit, if necessary
- Where each person works (building)
- Who supports the equipment in your department
  - Web Servers, File Servers, etc
  - Workstations

# [ What do I need to know? ]

- University Computer Security Policy
  - Acceptable Use
  - Enterprise Password
  - Network Citizenship
  - Security Incident Escalation
  - Scanning
  - Your department's policies

# What do I need to know?

## USA Patriot Act: Terrorism - Exceptions to Federal Law

- Electronic Communications Privacy Act (ECPA)
  - If **law enforcement asks you to provide** the content of electronic communication, or information about users of, or traffic on, the University of Iowa network, **with or without written authorization**, contact the University IT Security Officer, CIO, or General Counsel
  - If your system(s) has been compromised by a computer trespasser and you wish to **have federal law enforcement investigate**, report the situation to the University IT Security Officer or CIO, who in consultation with General Counsel, will determine if a law enforcement investigation is appropriate
- Family Education Records Privacy Act (FERPA)
  - If you should access electronic information which you believe is an **emergency situation involving immediate danger of death or serious physical injury**, contact the Department of Public Safety (DPS - call 911) immediately, and then the University IT Security Officer or CIO

# Handling Computer Security Incidents: Basic Types

- Compromised machine
  - Confidential data? Passwords?
  - Repair or Rebuild?
- Misuse/AUP violations
  - E-mail harrassment, Threats, etc
  - Copyright infringement, Software piracy
  - Spam, Excessive bandwidth
  - Scanning/probing/attacking other systems
- Other: DoS, Theft, Data/Confidentiality, Account Compromise, Virus/Worm

# Handling Computer Security Incidents: Compromise

- Notice to you or “NSC-Building” from ITSO includes:
  - What & where is the problem
  - Actions taken, or need to be taken (i.e., port shut off)
  - Where to get more information
- Gather more information
  - Review ports list website for room/location
  - Determine if its “yours” – let ITSO know!
  - Request a security scan of computer (if not disabled)
- Resolve the issue, or forward to responsible party
- Reply/Notice to ITSO after resolution

# [ IT Security Website ]

- NSC-ALL Campus Notices
- Incident Help
- Resources
- Best Practices Guidance
- University IT Policy
- Services
- Education & Awareness

# [ Discussion ]

---

Questions?

Contact the IT Security Office

- 5-6332, or 4-0750
- [it-security@uiowa.edu](mailto:it-security@uiowa.edu)
- <http://cio.uiowa.edu/itsecurity>