NETWORK SECURITY CONTACTS (NSC)

2010

IT-Security Office
Outline

- Program History & Responsibilities

- Notice Types and how to handle
  - Compromise
  - Network Issues
  - Policy/legal
  - Other (education resources)
IT-Security Office

NSC ... what now?

define NSC
Program History

- Program inception, 1998
NSC – PROGRAM DESIGN
2 ‘default’ contacts - a primary and a secondary

Act as communication liaison (network outages, security)

An org/department may choose to “roll up” contacts to the next organizational level e.g. UIHC/HealthCare Information Systems or the College of Engineering
Program Design

- Permanent university staff employed at least 50% time in the department (or unit)

- Regular employment validation to keep database up to date – annual health checks
Program Design

- Registration Information
- Department Number(s)
- Department Name
- Buildings with staff or equipment

http://itsecurity.uiowa.edu/incident/nsc-form.shtml
Program Design

- Registered systems in USR
- Attempts will be made to contact owners directly.
null
System Edit: #-1

General Information - Once saved, Network Information and Contact Information sections will be made available.

- **Department:** Academic Advising Center
- **Room:**
- **Building:** 109 River Street
- **OS:** UNKNOWN
- **Critical System:**
- **Sensitive Data:**
- **Comments:**

**Purposes:**

- Web Server
- SMTP Server
- FTP Server
- Database Server
- Research
- File Server
- Networking Device

Back  Save
USR

Network Information

- Add MAC
- Add IP
- Associate IP
- Add FQDN

MAC: [input field]
IP: [input field]
MAC (optional): [input field]
IP: [input field]
FQDN: [input field]

Contact Information

- HawkJID: [input field]
- Access: [input field]
- Promote/Add User

Action | HawkID | Access | Email
--- | --- | --- | ---
Write | rvinson | Read | robert-vinson@uiowa.edu
Write | wstaal | Read | warren-staal@uiowa.edu

Add Group Access: [input field]
Action | Group | Access
--- | --- | ---
No items were found.
Various Email Lists

- **uiowa-security**
  - Training opportunities or Vendor notices
  - Current threats or incident information
  - Discussion

- **NSC-ALL**
  - General notices and Directives
  - Network issues or Training opportunities
Contact methods/resources

- **NSC-[building code]** – Buildings your department housed in = lists you’re subscribed to
  - Incident reports if system is not registered through USR

- **IT-ADMINS**
  - Occasionally send notices, though list audience is more general.
  - Collaboration, discussion on technical issues.
NSC – RESPONSIBILITIES
Essential things 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
Essential things to know

University IT Policies

http://cio.uiowa.edu/policy

- Acceptable Use
- Network Citizenship
- Your department’s policies
Essential things to know

Regulatory Compliance Issues, be familiar with as and where needed:

FERPA

HIPAA

GLBA

PCI-DSS

FISMA

And all of the appropriate security controls that apply to the type of data your department handles.

IT-Security Office
Handling Computer Security Incidents: Basic types

Situations you will receive notices

- Policy Violation
- Compromises - any confidential data on machine?
- Repair or Reformat?

Misuse/AUP violations

- E-mail harassment, Threats, etc
- Copyright infringement, Software piracy
Handling Computer Security Incidents: Process

If ITSO/Networking discovers a problem:

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)
You are receiving this message because the machine connected to the network port described below is compromised, and has been disabled by the University IT Security Office.

What should I do next?
Before anything is done to the machine, determine if it contains sensitive information such as social security numbers or individuals' health, education, or financial records. If it does, DO NOT perform any action on the machine before contacting the Security Office (call 335-6332 or email security@uiowa.edu). Searching for files, rebooting, making backups, logging on, as well as repair activities, are prohibited until an analysis of the compromise has taken place.

If there is no sensitive information on the machine, work together with the user of the system to perform a format/re-image to resolve the problem. This is usually the necessary task as it is virtually impossible to guarantee a tool or piece of software has "cleaned" or removed the threat.

If you need assistance with the repair of this machine please contact the Help Desk at 384-HELP (4357) or your local support personnel.
Compromise and Host Details

Compromise description: Rogue AV/Malware infected
Action required: Reimage the affected host

X-IP: 128.255.X.X
X-MAC: ba:ba:8b:5e:d6:ba
X-Port: lib:8@8:88
X-Jack: 88888-2
X-Room: 888
X-Building: lib
X-Location: ITS Campus Technology Services
X-NBT:
X-HawkID:
X-Category: compromise
X-Network: disabled

Frequently Asked Questions:
http://itsecurity.uiowa.edu/incidents/ports-faq.shtml

Additional Room and Jack information:
http://itsecurity.uiowa.edu/incidents/ports.shtml

To have your port enabled:
http://itsecurity.uiowa.edu/incidents/EnablePort-form.shtml
Handling Computer Security Incidents: Process

NSC Resolution:

- Contacting ITSO
- Requesting a security scan of computer (if not disabled)
- Resolve the issue, or forward to responsible party
Handling Computer Security Incidents: Process

If ‘YOU’ - the NSC discovers a problem:

- Follow the escalation procedures, foremost contact the ITSO as soon as possible

- Any need for/request from external Law Enforcement: You MUST consult the Office of the General Council or the ITSO before providing information
DISCIPLINARY ACTION

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

FIXING PROBLEMS

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

- Various E-Mail List Notices
  - http://itsecurity.uiowa.edu/incidents/
  - http://cio.uiowa.edu/policy/
  - http://itsecurity.uiowa.edu/usr/

- Miscellaneous resources and best practices
  - http://itsecurity.uiowa.edu/resources/

IT-Security Office
Questions?

Contact the IT Security Office on 5-6332
it-security@uiowa.edu
http://itsecurity.uiowa.edu