1. The Nature of Our Business
2. The Current Threat
3. What We Can All Do to Help
Information Security deals with the protection of three characteristics of information.

- Confidentiality - Keeping info private
- Integrity - Keeping info accurate
- Availability - Keeping info accessible (even in disasters)
“Sensitive Information” includes all data, in its original and duplicate form, which contains:

- “Personal Information,” as defined by the North Carolina Identity Theft Protection Act of 2005,
- “Protected Health Information” as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
- Student “education records,” as defined by the Family Educational Rights and Privacy Act (FERPA),
- “Customer record information,” as defined by the Gramm Leach Bliley Act (GLBA),
- “Card holder data,” as defined by the Payment Card Industry (PCI) Data Security Standard,
- Confidential “personnel information,” as defined by the State Personnel Act, and
- Information that is deemed to be confidential in accordance with the North Carolina Public Records Act.
Sensitive Information also includes any information that is protected by University policy from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of Sensitive Information may include, but are not limited to, research data, public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.

http://help.unc.edu/help/what-is-sensitive-data/ What is Sensitive Information?

http://help.unc.edu/help/legal-references-for-sensitive-data/ Legal References for Sensitive Information
We face a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities and a lack of comprehensive awareness of the threat.

Sensitive information is stolen daily. Many incidents, if not most, do not get reported.

In opposition to us are nation states, terrorist networks, organized criminal groups, hacktivists, and individuals of varying levels of access and technical sophistication.
Why Would Anyone Hack My Computer?

Are EDUs Different?

- Historically the mission supported, even required, openness.

- State EDUs have greater requirements for openness.

- Tend to have significantly more bandwidth than commercial entities.
Network Attack Events

- **2010**
  - We saw **1,000,000** connections denied by our network firewalls per week (1% of campus firewalled).
  - More than **200,000** blocked connections per week by our Intrusion Prevention Systems (IPS).

- **2012**
  - We saw **35,000,000** connections denied by our network firewalls per week (3% of campus firewalled).
  - Intrusion Prevention Systems blocked **3,000,000** million security events per week.

- **2013**
  - We saw **100,000,000** connections denied by our network firewalls per week (5% of campus firewalled).
  - Intrusion Prevention Systems blocked **7,000,000** connections last week.
Network Attack Events

Normalized Weekly Firewall Denials

IPS Blocked Connections
August 2014 Stats

- Firewalls Blocked **132 Million** unwanted connections last week.
- Tipping Points (intrusion prevention system) blocked **9 Million** security events last week.
- Only about 25% of campus is behind a firewall.
How Does it Happen?

- Loss or theft of an unencrypted device.
- Clicking a phishing link or just visiting a compromised site = drive-by download.
- Interception of credentials.
- Missing patches -- vendor acknowledges a vulnerability and creates a solution but not yet installed -- intruder needs access which MAY be defeated with a firewall.
- Zero day vulnerability -- vulnerability exists but vendor has not yet created a solution.
Intruders may search UNC-CH websites for roles/users who likely have access to sensitive data.

Try to discover computers associated with those users.

Phish, drive-by-download, intercept credentials, or leverage vulnerabilities against those users or computers.

Once compromised, lurk and understand the system they own without tripping over a wire that would alert us.
What We Can All Do to Help

- Above all: do not store sensitive information if you don’t need it.
- Mask, delete, or otherwise de-identify the sensitive information.
- Archive the data offline.
Top 10 Tips for Securing Sensitive Information

1. Patch Your Device
2. Don’t Get Phished
3. Use Strong Passwords
4. Use Anti-Virus and a Firewall
5. Use Secure Networks
6. Lock Your Computer
7. Observe Acceptable Use Policy
8. Protect Sensitive Information
9. Use Safe Web Browsing Strategies
10. Protect Your Data
Keep your operating system and application software patched and up to date.

- Hackers can exploit known vulnerabilities in outdated software to gain access to your computer.
- Your best defense is a patched and up-to-date computer.
Never respond to email, text messages or phone calls requesting passwords, account names or any sensitive or confidential information.

- Reputable organizations will never ask you for confidential information such as login credentials.
- E-Mail is easily forged and web sites can be obscured with Tiny URLs. (Where is http://bit.ly/1agWmbn?)
- If in doubt, reach out!
Use strong and unique passwords that are at least eight (8) characters in length with a mix of alphanumeric characters and symbols.

- Do not use dictionary words.
- Use a phrase (e.g. “We’re off to see the Wizard, the wonderful Wizard of OZ!” = Wo2stWtwWoO!).
- Do not share your password.
- Do not write your password down.
- Do not use it in automated scripts.
- Do not ask the system to “save” your password.
Install Anti-Virus and Firewall software on your computer.

- Update your Anti-Virus definitions frequently to detect new virus signatures.
- Use host-based Firewalls.
- Anti-Virus software can be downloaded from https://shareware.unc.edu or installed by AD policy.
Use secure network connections.

- When on campus use UNC-Secure wireless or a hardwired port.
- Secure your home router.
- Use the campus Virtual Private Network (VPN) when using any public, unsecured network access point. For information about the VPN visit http://help.unc.edu.
Don’t leave your computer logged in and unattended.

- You are responsible for any activity that occurs on your computer.
- Logoff or lock your computer when you are not present.
Do not use unlicensed or illegal copies of software or other electronic media.

- Use of unlicensed or illegal material is a violation of the UNC - Chapel Hill Acceptable Use Policy.
- Beware of using peer-to-peer file sharing software as it can easily lead to copyright violations and/or getting malware installed on your system or device.
If you must have sensitive University information on a portable device, the device **must** be encrypted.

- ITS offers PGP encryption for laptop computers.
- Don’t send sensitive information unencrypted to locations outside the UNC - CH network.
- You can use Microsoft Office or WinZip to encrypt the data and set a password.
- Sensitive University information cannot be stored on mobile devices without the approval of the department head (or their delegate) and the device must be encrypted.
Safe Web Browsing

Keep your web browser up-to-date with the latest patches.

- Use tools like $\text{https://browsercheck.qualys.com}$ to help keep your browser and add-ons up-to-date.
- Consider using an add-on such as $\text{NoScript}$ for Firefox for added protection.
- Set the browser security settings to medium or high and whitelist desirable sites that get blocked.
- Bookmark sites you frequently visit to guard against redirection to a malevolent site.
If you follow these tips and still get malware there is a possibility that your data may be lost.

- The most effective remedy for this is a good backup.
- Commercial services are available or backups can be stored on a flash drive or USB hard drive, or written to DVD(s).
- Backups should be stored in a secure remote location.
If you have a question or suspect a problem:

- 919-843-2594 (ORIS Help Line - applications).
- 919-962-ORIS: desktop support.
- Call the campus IT Response Center (ITRC) at 919-962-HELP. They are available 24/7, 365 days a year.

If you believe that sensitive University information is at risk you must:

- Notify the ITRC and either your supervisor or your Information Security Liaison (the Liaison for ORIS is Scott Wilber: (919) 962-2447, wilber@unc.edu).
- Stop, Drop, and Roll.

If University equipment is stolen:

- Notify your supervisor and campus police (919-962-8100).
Summary

- Know what sensitive information is and where it resides ... and why.
- Delete, archive, or safely store sensitive information.
- Patch and configure correctly (vulnerability scan to verify).
- Diversify and safely store credentials.
- Encrypt or de-identify sensitive information and only use when needed.
- Adopt less risky behaviors - be careful with browsing on sensitive systems, diversify passwords, etc.
- Encrypt mobile devices that store sensitive information.
- When in doubt about safety of sensitive information, ask.
QUESTIONS?

SUGGESTIONS?

TCLINE [AT] UNC.EDU