Securing Sensitive University Data

Kevin Fitzgerald
Office of the Provost

Securing Sensitive University Data

• Why: Multiple data breaches at OUHSC have risked the loss of patient information and caused an investigation by the Office of Civil Rights.
• What: Access to university business will be restricted.
• Who: Everyone accessing business on the wireless network.
• When: By October 2016.
• How: Only ‘Registered’ devices will be able to access the new HSCACCESS wireless network.
Breaches

- Over 158 million people have been affected by over 200,000 breaches as of April 2016.
- Nearly 100,000 people were affected in 32 breaches in the last month.

Hackers and thieves have made it impossible to continue using networks and the internet in the open way we have been using them for the last 20+ years.
Network Restrictions

• The new HSCACCESS wireless network will replace OUBASE.
  – New network will be in place no later than October 1st, but will be activated as soon as it is ready.
• Only registered devices will be allowed to connect to HSCACCESS.
• Wired ports in high risk areas and other identified areas will be disabled.

Devices

• You must complete an online form to get your device registered and enrolled.
• Devices must be confirmed as compliant with security requirements by a Tier 1 to be enrolled.
Registration

• Go to: www.ouhsc.edu/RegisterDevice
• Follow the directions, and press “Order Now”.
• A message will be sent to your Tier 1 who will contact you about enrolling your device so it will connect to HSCACCESS.

Laptops

• Your Tier 1 will ensure that this software is configured on the device before registering it.
  – Software agent showing the device in the “Managed State”
  – Drive Encryption or Management of Native Encryption installed and showing “Enabled” or “Active”
  – Anti Virus configured to update virus definition files on at least a daily basis and to perform scans on at least a weekly basis
  – Pulse Secure client installed and configured.
  – Require encrypted removable storage
  – It’s ok if you don’t understand this. The Tier 1 does.
Phones / Tablets

- When you connect your mobile device to the email server, the Secure Mobile Program policy is pushed to your phone:
  - 4 digit password required
  - Data is encrypted
  - Device locks after 15 minutes of inactivity
  - Local data on device deleted after 10 failed authentication attempts
- **Phones and Tablets must be in the Secure Mobile Program and registered to access the HSCACCESS network.**

Removable Storage

- USB Memory, portable hard drives, and all other forms of portable storage used for university business must be encrypted.
- Part of the software being installed on devices to make them compliant with the HSCACCESS network will require that any attached storage be encrypted.
Support - Employees

- Tier Ones are being supported by IT
- Multiple meetings to inform and train Tier 1s on the new requirements have been conducted and more are being scheduled.

Support - Students

- The IT Service Desk will provide support to students to get computers setup so they can access the new wireless network.
  - Some areas offer technical support to students through other means.
Privacy

• None of the software being installed as a part of this project affects the privacy of data on your personal device.

• IT cannot see data on your personal device.

Performance

• Encryption has little effect on modern computers.
  – Many modern computers have processing chips specifically for encryption so that it doesn’t affect performance.
  – Windows 7 Ultimate, Enterprise and up comes with a native encryption called ‘Bitlocker’ designed into the operating system.
  – Macs have a similar function called Filevault.
    • You can use the native encryption on your computer.
  – Old and/or cheap computers will have problems.
Other Details to Remember

- If a device is not connected to the OUHSC network for 30 days, it must be “re-connected” by a Tier 1.
  – Connecting via Virtual Private Network (VPN) from off campus is the same as connecting on campus.
- The HSCACCESS network won’t provide a warning or other information if your device is not registered. It just won’t work.

Questions?