Overview

- Information = Asset
- Threat Landscape
- Security Basics
- Policy Updates
Information = Asset

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budgets</td>
<td>Invoices, receipts, payments, planning, forecasting</td>
</tr>
<tr>
<td>HR Data</td>
<td>Compensation, pension, benefits, performance</td>
</tr>
<tr>
<td>Contracts</td>
<td>Terms &amp; conditions, nondisclosure, service agreements</td>
</tr>
<tr>
<td>Research</td>
<td>IP, patents, consent agreements, patient records</td>
</tr>
<tr>
<td>Personal</td>
<td>SSNs, credit cards, DoB, medical/health records, certificates</td>
</tr>
<tr>
<td>Professional</td>
<td>Accomplishments, CV, degrees, awards, reputation</td>
</tr>
</tbody>
</table>

“If it’s worth collecting, it’s worth protecting”
Higher Education Incident Experience (examples)

<table>
<thead>
<tr>
<th>Date</th>
<th>Institution</th>
<th>Source</th>
<th>Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov '16</td>
<td>Michigan State University</td>
<td>Unknown</td>
<td>400K</td>
</tr>
<tr>
<td>Jul '15</td>
<td>Harvard University (8 colleges)</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>May '15</td>
<td>Pennsylvania State (Engineering)</td>
<td>China</td>
<td>18K</td>
</tr>
<tr>
<td>Jul '14</td>
<td>University of Illinois Chicago</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>Mar '14</td>
<td>University of Wisconsin Parkside</td>
<td>Unknown</td>
<td>15K</td>
</tr>
<tr>
<td>Mar '14</td>
<td>North Dakota University</td>
<td>Unknown</td>
<td>290K</td>
</tr>
<tr>
<td>Feb '14</td>
<td>Indiana University</td>
<td>Unknown</td>
<td>146K</td>
</tr>
<tr>
<td>Feb '14</td>
<td>University of Maryland</td>
<td>Unknown</td>
<td>309K</td>
</tr>
</tbody>
</table>

https://www.privacyrights.org/data-breach
## Threat Landscape - Northwestern

<table>
<thead>
<tr>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptops unencrypted and stolen</td>
</tr>
<tr>
<td>Personal devices with University data, unencrypted and stolen</td>
</tr>
<tr>
<td>Phishing and insiders giving up credentials and personal information</td>
</tr>
<tr>
<td>Servers, storage devices exposed directly to the Internet with research data</td>
</tr>
<tr>
<td>Sensitive data sent through email without being secured (encrypted) and/or sent to commercial (e.g., gmail) and other external email systems</td>
</tr>
<tr>
<td>Misconfigured, unmanaged and unpatched devices</td>
</tr>
<tr>
<td>Constant external attempts to gain access to internal information (e.g., intellectual property)</td>
</tr>
</tbody>
</table>
External Threat Landscape

- Highly automated
- Indiscriminate and targeted attacks
- 24 X 7 – never takes a vacation, never takes a holiday
- Medical records now more “valuable” than financial (e.g., credit cards)
- Hacktivist – Criminal – Insider – Espionage – Terrorism - Warfare

https://cybermap.kaspersky.com/
Security Basics -1

• Is your data **sensitive** or **important** to your institution?
• Do you **know where** your data is?
  ❖ Do you know **who** has access and does this align with the project/grant data-handing requirements?
  ❖ Is data **encrypted**?
• Are you **aware** of University and departmental policies and follow them?
• Do you **restrict** physical **access** to your area?
Security Basics - 2

• Is there professional **training and technical support** in your environment?
• Are devices and systems patched to current levels, managed and under formal change control?
• Do you have defined data retention periods, secure data archival, backup and disposal?
• Is security software installed and kept current?
• NEVER disable security software or security settings!
• Phishing is sophisticated and becoming difficult to detect (i.e., do not click on email links).
Policy Updates – Feinberg School of Medicine

• Information Security & Access policy (rewritten)
• Device Security Policy (new, no non-public data on personal devices)
• Email: Auto-forwarding, commercial email not permitted
• Email Encryption
• Data Security Plans

http://www.feinberg.northwestern.edu/it/policies/information-security/index.html
Information Security & Access Policy (rewritten, 4/15/16)
* New item, re-enforced emphasis, better clarity

- * HIPAA/HITECH is the minimum standard for data handling
- * De-identification must comply with the HIPAA Privacy rule
- * Encryption is required (portable media, laptops, desktops, everything)
- Equipment, media, paper losses must be reported immediately
- * Access to data must be maintained consistent with job role & approved IRB protocol
- Complex passwords are required
- Device security features are never to be disabled
- Research data on approved storage only (no Box.com, no Cloud)
- * Use of commercial email systems are not permitted
- Data security plans are required
- Commercial vendors used in research require Dean’s office approval
- * No non-public NU data on personal devices
Policy Updates – Feinberg School of Medicine

Device Security Policy (new, 4/15/16)

- All devices: FSM IT managed & personal devices
- No non-public NU data on personal devices
- All devices must be encrypted and connection through only VPN
- Smartphones
  - Requires six-digit pin; and encryption enabled for Android devices
  - Limit of 30 days NU email
- Email synchronization to personal devices will be disabled on the NU email system for FSM
- Email synchronization via IMAP has been disabled
- Administrative rights will be phased-out
- Device management technology coming Fall 2016
Policy Updates – Feinberg School of Medicine

Email Auto-forwarding (revised 12/1/15)

• Email message and attachments can be forwarded and/or auto-forwarded only within approved Northwestern-affiliated email systems. Current list published in policy.
  - northwestern.edu
  - lfh.org
  - nmff.org
  - cadencehealth.org
  - livingwellcrc.org
  - nmh.org
  - cdh.org
  - luriechildrens.org
  - northwesternmedicine.org
  - childrensmemorial.org
  - nm.org
  - ric.org

• **Forwarding or auto-forwarding email messages and attachments to public email systems such as gmail.com, yahoo.com, or hotmail.com is not allowed.** * The use of public email systems are not approved for any research purpose at Northwestern University, Feinberg School of Medicine.

• Email systems fsm.northwestern.edu, u.northwestern.edu and md.northwestern.edu are Google public email systems and are not part of approved Northwestern-affiliated email systems for the exchange of research data and other sensitive information.
Policy Updates – Feinberg School of Medicine

Email Encryption (revised 12/1/15)

• Email message and attachments are required to be sent encrypted when containing PHI or PII.

• **Automatic Encryption** - Messages containing sensitive data sent from your @northwestern.edu e-mail address to or from recipients within Northwestern-affiliated domains are automatically encrypted and do not require additional effort. Northwestern-affiliated domains enabling automatic encryption:
  
  - northwestern.edu
  - lfh.org
  - nmff.org
  - cadencehealth.org
  - livingwellcrc.org
  - nmh.org
  - cdh.org
  - luriechildrens.org
  - northwesternmedicine.org
  - childrensmemorial.org
  - nm.org
  - ric.org

• **Manual Encryption** - Messages containing PHI or PII data sent from your @northwestern.edu e-mail address to non-Northwestern-affiliated environments will require manual encryption. Manually encrypted messages will be automatically quarantined.

• **Forced Encryption** - Email messages will be automatically encrypted and quarantined if manual encryption is not used and PHI or PII is suspected.
Policy Updates – Feinberg School of Medicine

Data Security Plans (effective 5/5/15)

• All NU IRB protocols for clinical research studies with principal investigator appointments at FSM require a documented data security plan.
  - Plans are required for all new clinical research studies
  - Plans are required for existing studies at continuing review/renewal
• Plan will be submitted through the RSS of the IRB/RSS system.
• 13 questions (e.g., data access, data flow, data storage)
• All plans submitted subject to review (1582 as of 6/6/16) and audit (388 as of 6/6/16).
• Increases awareness of security requirements.
Updates – Information & Systems Security/Compliance

• **Service Provider Security Assessment (SPSA) – January 2016**
  • Vendor prequalification
  • Select or Extended Survey
  • [http://www.it.northwestern.edu/about/departments/itms/cpo/assessment.html](http://www.it.northwestern.edu/about/departments/itms/cpo/assessment.html)

• **Expansion of Multifactor Authentication (DUO) – July 11, 2016**
  • Already used for FASIS Self-Service
  • NUFinancials, InfoED, CATracks, & Cognos Business Intel
  • [http://www.it.northwestern.edu/security/multi-factor-authentication/index.html](http://www.it.northwestern.edu/security/multi-factor-authentication/index.html)

• **Email Encryption (IronPort) – July 12, 2016**
  • Newly available to all Northwestern Collaboration email users
  • [http://www.it.northwestern.edu/transitions/2016/email-encryption.html](http://www.it.northwestern.edu/transitions/2016/email-encryption.html)
Security Contacts

NUIT - Information & Systems Security/Compliance
To report or make inquiries, contact the NUIT Help Desk at 847-491-4357 or 1-HELP (from on campus)
Email: security@northwestern.edu

FSM IT
To report or make inquiries, contact the NUIT Help Desk at 847-491-4357 or 1-HELP (from on campus)
Email (end user support): fsmhelp@northwestern.edu
Email (IT Security Policy): FSMIT-policy@northwestern.edu

Carl Cammarata, Senior Director
Chief Information Security Officer
Email: carl.cammarata@northwestern.edu
Office: 312-503-2822