Information & Systems Security/Compliance
Feinberg School of Medicine
Research Computing Services
Overview

• Information = Asset
• Threat Landscape
• Simple Steps to Security
• Process Improvements
• Research Computing Services
## Information = Asset

<table>
<thead>
<tr>
<th>Category</th>
<th>Data Types</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>
</tbody>
</table>

“If it’s worth collecting, it’s worth protecting”
## Threat Landscape

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Event Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/2017</td>
<td>University of California – Santa Cruz</td>
<td>Laptop stolen from researcher’s home</td>
<td>Narrative evaluations dating from 2000 to 2004 contained personally identifiable information including names, Social Security Numbers, student record information including: grades, narrative evaluations and email addresses</td>
</tr>
<tr>
<td>11/2016</td>
<td>Michigan State University</td>
<td>Database Hack</td>
<td>Names, Social Security numbers, MSU identification numbers, and in some cases, date of birth of some current and former students and employees</td>
</tr>
<tr>
<td>06/2016</td>
<td>University of Connecticut</td>
<td>Malware</td>
<td>Names, contact information, Social Security numbers, employment information, student academic information, research data and School of Engineering graduate level admissions data, credit card information, usernames and passwords</td>
</tr>
<tr>
<td>05/2016</td>
<td>City College of San Francisco</td>
<td>Phishing</td>
<td>Student names, addresses, Social Security numbers and financial aid data</td>
</tr>
</tbody>
</table>

[https://www.privacyrights.org/data-breach](https://www.privacyrights.org/data-breach)
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/
Simple Steps to Security

Configuration Management
• Replace default passwords with longer/stronger

Change Management
• Control changes to your environment

Patch Management
• Keep systems & applications current

Endpoint/User Management
• Encryption, Anti-malware, Anti-virus
• Phishing: Be aware, don’t click on links

“It just has to be ‘good enough’…”
Process Improvements

**Feinberg School of Medicine**

- Encryption: Computers, Mobile Devices and Email
- Email: Auto-forwarding, commercial email not permitted
- Personal devices: No non-public NU data, Device Security Policy
- Information Security Data Security Plans
- Research Use of EDW Data
- Hardware, Software, Data Storage Standards
- Information Security & Access Policy

http://www.feinberg.northwestern.edu/it/standards-policies/
Information & Systems Security/Compliance
Thomas P. Murphy, Chief Information Security Officer
Email: thomas.murphy@northwestern.edu
Office: (847) 467-6422

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

Research Computing Services
Joe Paris, Associate Director
Email: j-paris@northwestern.edu
Office: (847) 491-5365