Cybersecurity

Nowell A. Arnold
Deputy Chief Information Security Officer

Northwestern
Recent Trends and Events

<table>
<thead>
<tr>
<th>The World:</th>
<th>Higher Education:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verizon</strong></td>
<td><strong>WASHINGTON STATE UNIVERSITY</strong></td>
</tr>
<tr>
<td>14 million subscriber’s data</td>
<td>A hard drive containing the personal</td>
</tr>
<tr>
<td>breached</td>
<td>information of approximately <strong>one</strong></td>
</tr>
<tr>
<td><strong>Equifax</strong></td>
<td><strong>Stancof University</strong></td>
</tr>
<tr>
<td>145.5 million consumer’s data</td>
<td>Names, birthdates, Social Security</td>
</tr>
<tr>
<td>breached</td>
<td>numbers and salary information for</td>
</tr>
<tr>
<td></td>
<td>nearly 10,000 non-teaching university</td>
</tr>
<tr>
<td><strong>Whole Foods Market</strong></td>
<td>employees.</td>
</tr>
<tr>
<td>Malware on payment systems</td>
<td><strong>NYU</strong></td>
</tr>
<tr>
<td>(not disclosing number of records)</td>
<td></td>
</tr>
<tr>
<td><strong>Uber</strong></td>
<td><strong>Cornell University</strong></td>
</tr>
<tr>
<td>57 million user’s data</td>
<td><strong>University of Oxford</strong></td>
</tr>
<tr>
<td>breached</td>
<td><strong>University of Cambridge</strong></td>
</tr>
<tr>
<td>(paid hackers $100,000 to keep</td>
<td><strong>UCLA</strong></td>
</tr>
<tr>
<td>quiet)</td>
<td><strong>University of Washington</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recent Trends and Events

Northwestern:

**Impersonation**: Increased targeted email and phishing messages purporting to be from senior leaders. These messages include malicious links, ask for wire transfers, or contain language that threatens personal and institutional reputation.

**Phishing**: Despite blocking over eighty million spam and phishing messages each month, our community continues to fall prey using Northwestern and personal email accounts.

**Compromised accounts**: At least once per week, account-holders are duped into providing their passwords either through phishing messages or clickbait on web sites.

**Vulnerabilities**: Meltdown and Spectre global threat based on flaws in nearly all modern computer processors.

**Malware downloads**: Notification from U.S. Department of Justice that five devices within our networks were infected with Fruitfly malware which turns on the camera on a Mac. Northwestern Information Technology and school support areas eradicated.
The Northwestern Environment

- **Measures of scale:**
  - 65,000 NetIDs
  - 80,000 wired network ports (58,000 unique)
  - 6,000 wireless access points
  - Wireless access totals (Fall 2016): 135,000 unique devices accessed by NetID, 50,000 unique devices accessed by guests
  - Over 20,000 unique, unmanaged mobile devices connect each month
  - Accessed from more than 190 countries

- **Systems, servers, and storage:**
  - More than 6,000 servers
  - 3.0 petabytes of storage (equivalent to 25,000 DVRs)

- **Measures of volume:**
  - Six gigabits per second of inbound traffic
  - 150M email messages a month

- **Growth of external partnerships:**
  - 100+ cloud apps
  - 60+ service provider assessments per year

- **Attack Volume:**
  - 80 million spam/phishing emails blocked each month
  - 16 million Internet attacks blocked each month originating from:
    | Source Country          | Count |
    |-------------------------|-------|
    | United States           | 7.9M  |
    | China                   | 3.6M  |
    | Russian Federation      | 1.1M  |
    | Croatia                 | 877.6k|
    | Ukraine                 | 457.6k|
    | Korea Republic Of      | 374.7k|
    | United Kingdom          | 370.4k|
    | Netherlands             | 382.0k|
  - 20 compromised accounts/month
  - 10 compromised computers per month
  - 2-3 impactful events/year (loss or compromise of device, system, or account)
Northwestern’s Top Enterprise Information Security Risks

Major potential impacts of reputational damage and loss of confidence

Northwestern’s top enterprise information security risks have been identified in alignment with the Enterprise Risk Management (ERM) framework:

- Exposure or compromise of Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) data
- Exposure or compromise of data resulting from gaps in coordination of risk between the Feinberg School of Medicine and Northwestern Memorial Hospital Corporation (NMHC)
- Compromise of key research or institutional data
- Third-party vendor security
- Systems availability or disruption
- Breakdown in breach response
- Ransomware
Information Security Office

Enhance role definitions to increase capacity and maturity required to protect the University's information assets and to provide essential resources to help members of the Northwestern Community fully participate in this effort.

Chief Information Security Officer
- Ongoing development and delivery of a comprehensive, University-wide information security strategy and program
- Provides vision and leadership for the University's information security program
- Aligns program to incorporate best practices in information security.

Security Governance, Risk and Compliance
- Policy creation and maintenance
- Security and Compliance reviews
- Service Provider Security Assessments
- Audit response and Attestations
- Security Reporting
- Awareness and Training

Security Architecture and Engineering
- Incident response escalations
- Security controls and systems design, installation and documentation
- Security project management
- Project participation

Security Operations
- Incident response
- Security tool monitoring
- Threat detection and response
- Security email and ticket queue handling
- Digital Millennium Copyright Act (DMCA) abuse response
- Phishing response
- Compromised account response

External Service Providers
- In-depth Security and Risk Assessment and Consulting
  - Aon
  - Deloitte
  - KPMG
  - Nexum
  - PwC
  - Ron Gault Consulting
  - SecureWorks
  - BTAA OmniSOC
  - REN-ISAC
Information Security Support & Resources

• FSM
  847-491-4357 or 1-HELP (from on campus)

FSMIT-policy@northwestern.edu
http://www.feinberg.northwestern.edu/it/standards-policies/information-security/index.html

Carl Cammarata, Senior Director, Chief Information Security Officer, 312-503-2822
David Gundrum, Senior Information Security Analyst, 312-503-3869
Marvina Roebuck, Senior Information Security Analyst, 312-503-5735
Leon Tran, Information Security Analyst, 312-503-6140

• Northwestern Information Security Office (ISO)
  847-491-4357 or 1-HELP (from on campus)

security@northwestern.edu

Nowell A. Arnold, Deputy Chief Information Security Officer, 847-467-6422
Questions and Answers