Keys

- Business drivers
- Threat landscape
- Assets targeted
- UO strategy
- Defense (top 5)
Key drivers

1. **COMPLIANCE** increases business opportunities
   - DFAR, FAR (research)
   - HIPAA, FERPA
   - GDPR (EU persons)
   - Data Use Agreements
   - GLBA (financial aid)

2. **DATA BREACHES** cause financial & reputational losses

3. **DENIAL OF SERVICE** attacks disrupt operations

4. **SOCIAL RESPONSIBILITY** extends to data protection
Meet the adversary...

- Script Kiddies
- Hacktivists
- Hacktivist?
- Insiders
- Organized Crimes
- Nation States
89% of breaches had financial or espionage motive

Threat landscape, 2017

Source: Verizon Data Breach Investigation Report, 2017
Common attack methods

- Email
- Phone -vishing
- Text - smishing

- Password theft
- Backdoors
- Website exploits

- Ransomware
- Keystroke loggers
- Spyware
Assets targeted

**Sensitive Personal Data**
- SSNS, credit cards, banking information
- Medical records
- Donor records

**Intellectual Property**
- Export controlled info
- Trade secrets, proprietary information, prepatent info
- eBooks, online journals, paid subscriptions

**Real Money**
- Process attacks
Attacks on higherEd

University of Maryland computer security breach exposes 300,000 records

Washington State University 1,000,000 records, 2017

OSU, 2012: 21,000 records

Michigan State University confirms data breach of server containing 400,000 student, staff records

UCLA, 2017: 30,000 records

2016-2017: Multiple Accounts Payable fraud attacks
Attacks @ UO

State-Sponsored Data Heist, Mabna Institute

3/23/2018

• DOJ indictments – Mabna+9
• 3,800 professors across 144 US universities
• 30 TB of data @ $3.4B

10/2017

• 60 UO faculty and staff usernames and passwords stolen
• Target – library vendors' Intellectual Property
Dear Dr. [X],

I recently read your article: [Title]. It was very useful in my field of research. I wonder, if possible, to send me these articles to use in my current research:


Thanks for you Cooperation in Advance.
Assoc. Prof. [Name]
Dear Dr. [X],

I recently read your article: [Title]. It was very useful in my field of research. I wonder, if possible, to send me these articles to use in my current research:


Thanks for you cooperation in Advance.
Assoc. Prof. [Name]
Hello,

Please find attached the Look Ahead files for Friday March 2nd, 2018

Open

Kindly let me have your opinion

Michael Schill
541-346-3936
President
Hello,

Please find attached the Look Ahead files for Friday March 2nd, 2018


Kindly let me have your opinion

Michael Schill
541-346-3936
President
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Contact Us
Check Payment Decrypt
Other interesting attacks

- **Bitcoin** @ $9,200
- **Ethereum** @ $800
- **Monero** @ $206

Crypto Mining Rigs
## Vulnerability snapshot

<table>
<thead>
<tr>
<th><strong>ADDRESSES OWNED</strong></th>
<th><strong>ADDRESSES SCANNED</strong></th>
<th><strong>LATEST SCANS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>133,120 ↔</td>
<td>133,120 ↔</td>
<td>Addresses: December 4, 2017 — May 7, 2018</td>
</tr>
<tr>
<td>no change</td>
<td>no change</td>
<td>Vulnerabilities: April 30, 2018 — May 7, 2018</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>HOSTS</strong></th>
<th><strong>VULNERABLE HOSTS</strong></th>
<th><strong>VULNERABILITIES</strong></th>
<th><strong>SERVICES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>2,768 ↓</td>
<td>1,035 ↓</td>
<td>4,429 ↓</td>
<td>10,767 ↓</td>
</tr>
<tr>
<td>168 decrease</td>
<td>44 decrease</td>
<td>286 decrease</td>
<td>401 decrease</td>
</tr>
<tr>
<td></td>
<td>37% of hosts vulnerable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### VULNERABILITIES

<table>
<thead>
<tr>
<th><strong>CRITICAL</strong></th>
<th><strong>HIGH</strong></th>
<th><strong>MEDIUM</strong></th>
<th><strong>LOW</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>114 ↓</td>
<td>193 ↓</td>
<td>3,203 ↓</td>
<td>919 ↓</td>
</tr>
<tr>
<td>25 resolved</td>
<td>43 resolved</td>
<td>669 resolved</td>
<td>157 resolved</td>
</tr>
<tr>
<td>19 new</td>
<td>17 new</td>
<td>447 new</td>
<td>125 new</td>
</tr>
</tbody>
</table>

- Critical vulnerabilities have decreased by 114.
- High vulnerabilities have decreased by 193.
- Medium vulnerabilities have decreased by 3,203.
- Low vulnerabilities have decreased by 919.
- Total resolved vulnerabilities decreased by 1,141.
Strategy in development...

Vision

A knowledgeable and capable UO community working together to safeguard our digital assets and capabilities, while empowering excellence in teaching, research and services in a resilient cyber environment

Mission

To empower the UO community to leverage digital assets and capabilities, while defending our cyber environment from nefarious actors through proactive measures
Targeted near-term deliverables

Secure Computing for Oregon Research Environment

- Secure storage
- Secure compute
- Secure transfer
- Secure collaboration
- NIST 800-171
- DFAR, FAR
- System Security Plan
- DMP language
Top 5 defenses

- 2FA
- Phishaware
- Passphrase
- Updates
- Backup

Awareness & Vigilance
Key takeaways

- Key business drivers for security include compliance, breach, disruption and social responsibility risks
- Personal info and intellectual property are targeted
- Cybersecurity strategy requires increased knowledge and capability and a community working together
- Threats are great but basic controls can help - awareness, 2FA, ?hishaware, passphrases, software updates, and data backup