UO Cybersecurity Briefing

Leo F. Howell
Chief Information Security Officer
lfhowell@uoregon.edu

UNIVERSITY OF OREGON

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

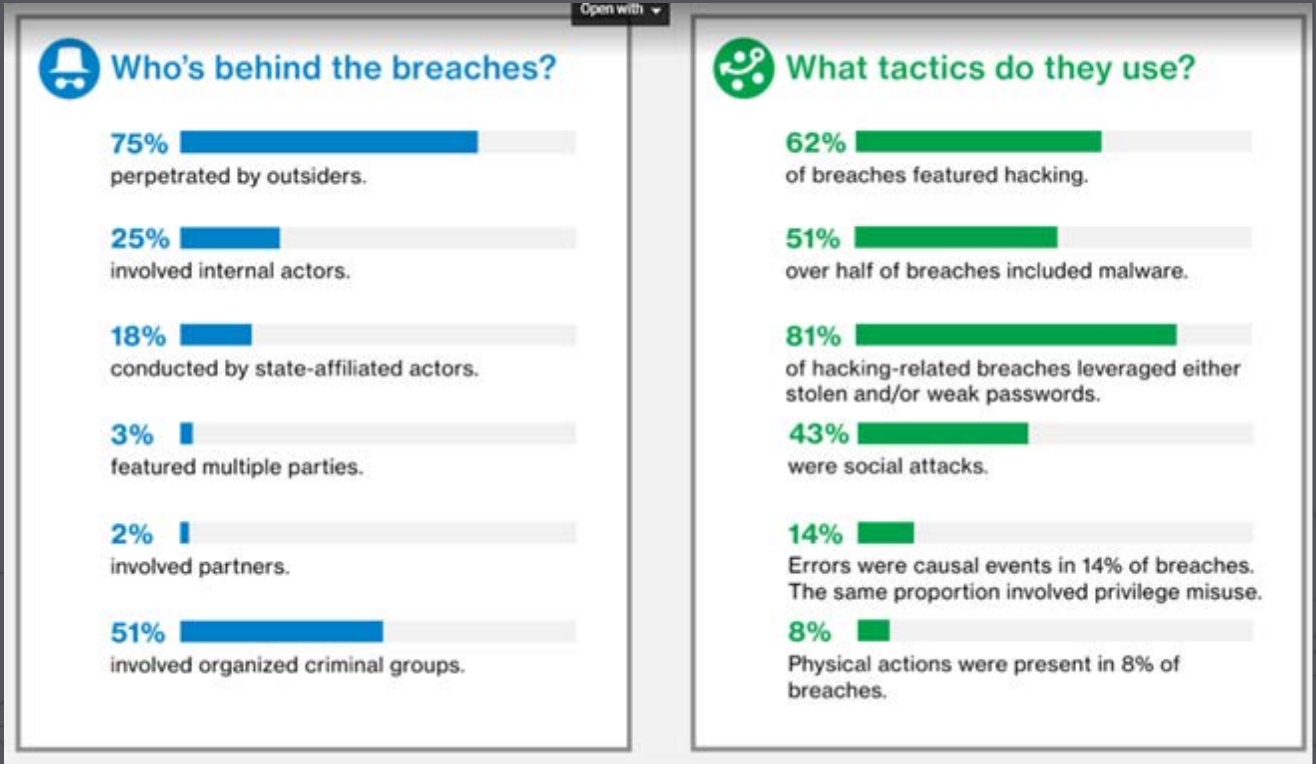
Nation States

Threat landscape, 2016

89% of breaches had **financial** or **espionage** motive

Source: Verizon Data Breach Investigation Report, 2016

Threat landscape, 2017



Source: Verizon Data Breach Investigation Report, 2017

Common attack methods

- Email
- Phone -vishing
- Text - smishing

Phishing

- Password theft
- Backdoors
- Website exploits

Hacking

- Ransomware
- Keystroke loggers
- Spyware

Malware

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

2014

UCLA, 2017: 30,000 records

Washington State University 1,000,000 records, 2017

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

POSTED: 4:55 PM, Nov 18, 2016
UPDATED: 3:24 PM, Nov 22, 2016

2016

OSU, 2012: 21,000 records

2016-2017: Multiple Accounts Payable fraud attacks

Attacks @ UO

State-Sponsored Data Heist, Mabna Institute

3/23/2018	10/2017
• DOJ indictments – Mabna+9 • 3,800 professors across 144 US universities • 30 TB of data @ $3.4B	• 60 UO faculty and staff usernames and passwords stolen • Target –library vendors' Intellectual Property

Can you spot the phish?

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:

http://shibboleth.uoregon.edud.in/idp/Authn/login.php?url=http://www.sciencedirect.com/science/article/pii/S03085961100HT00238

Thanks for you Cooperation in Advance.
Assoc. Prof. [Name]

Flattery, grammar, fake domain, urgency

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:*

*http://shibboleth.uoregon.**edud.in**/idp/Authn/login.php?url=http://www.sciencedirect.com/science/article/pii/S03085961100HT00238*

*Thanks **for you C**ooperation in **A**dvance.*
Assoc. Prof. [Name]

Phishing for Whales!

From: Michael Schill [mailto:markross@emailolympic.org]

Sent: Friday, March 02, 2018 2:02 PM

Subject: Michael Schill as Shared a file with you using One Drive

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

Sender impersonation, bad link, tone

From: Michael Schill [mailto:markross@emailolympic.org]

Sent: Friday, March 02, 2018 2:02 PM

Subject: Michael Schill as Shared a file with you using One Drive

Hello,

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

Open = http://ko-ontap.com/cat/index.html

Kindly let me have your opinion

Michael Schill
541-346-3936
President

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

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

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

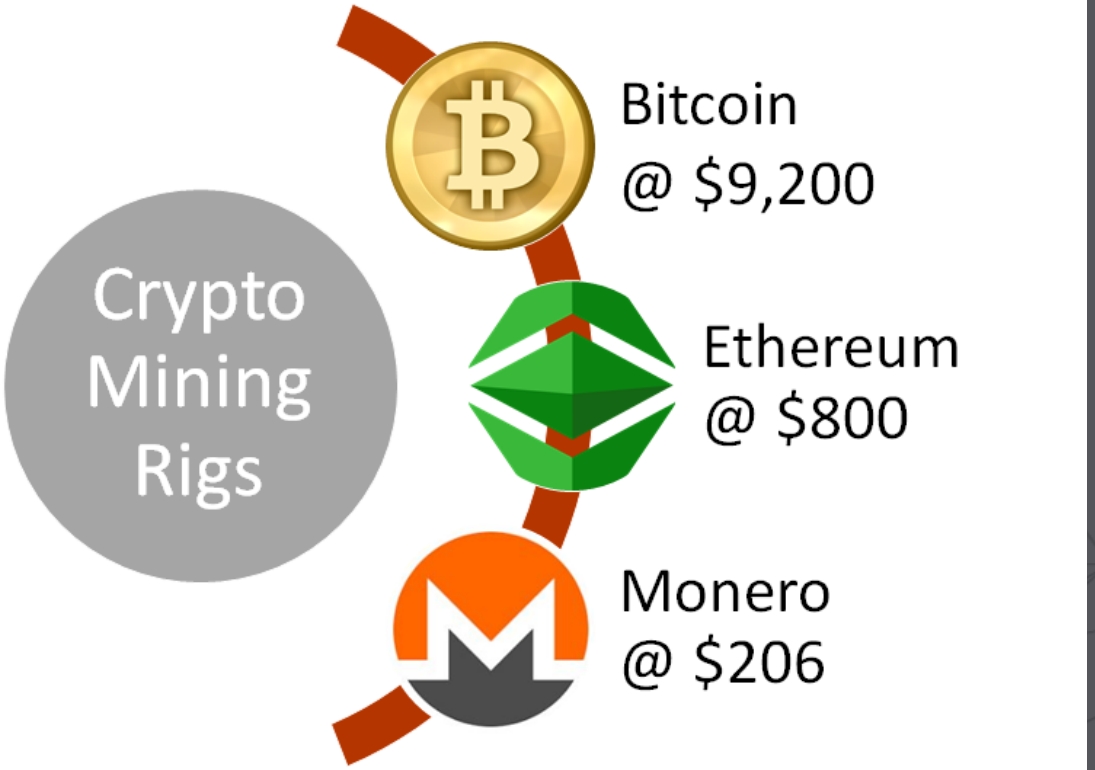
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Other interesting attacks



Vulnerability snapshot...

ADDRESSES OWNED

133,120 ↔

no change

ADDRESSES SCANNED

133,120 ↔

no change

100% of addresses scanned

LATEST SCANS

Addresses: December 4, 2017 — May 7, 2018

Vulnerabilities: April 30, 2018 — May 7, 2018

HOSTS

2,768 ⬇

168 decrease

VULNERABLE HOSTS

1,035 ⬇

44 decrease

37% of hosts vulnerable

VULNERABILITIES

4,429 ⬇

286 decrease

SERVICES

10,767 ⬇

401 decrease

VULNERABILITIES

CRITICAL

114 ⬇

25 resolved

19 new

HIGH

193 ⬇

43 resolved

17 new

MEDIUM

3,203 ⬇

669 resolved

447 new

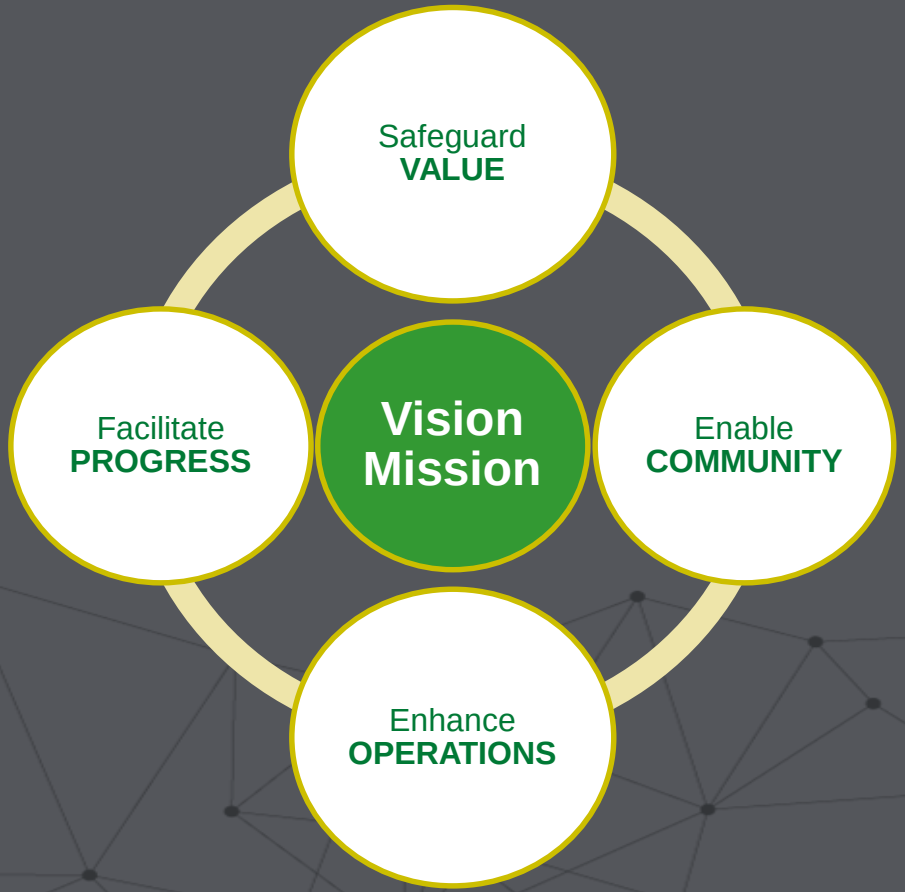
LOW

919 ⬇

157 resolved

125 new

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

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