# Cybersecurity Briefing for Researchers

***…protecting your IP and your life's work…***

Information Security Office
infosec@uoregon.edu
541-346-5837

UNIVERSITY OF OREGON

# Objectives

- Assets
- Requirements
- Threats
- Vulnerabilities
- Traveling
- Defense

# PART I
# ASSETS

# What are we protecting?

- **Data**
  - ***Confidentiality*** of sensitive information from unauthorized access
  - ***Integrity*** from unauthorized modification to ensure completeness, accuracy and consistency
  - ***Availability*** to ensure access when needed
- **IP** value derived from creative work, copyrights, patents,…
- **Reputation** re integrity in research and from false accusation (e.g., espionage)
- **University's** reputation, IP, operations

# Location of assets

- Computers
- Phones
- USB Drives
- Cloud
- Hardcopy
- Labs


OneDrive

Dropbox

# PART II
# REQUIREMENTS

# Requirements

**Compliance drivers**

- Data Use Agreements
- IRB protocol commitments
- Federal/International Laws: EAR/ITAR, FAR, HIPAA, FERPA, GDPR, …
- State Laws: Oregon Consumer Identity Theft Protection Act

**Common required controls**

| | | |
|---|---|---|
| Access Controls | Encryption | Data Backup |
| Awareness training | Security Monitoring | Physical Security |
| Ongoing Assessment | Transmission security | IR + Notifications |

# PART III
# THREATS

# Global Threats & Tactics

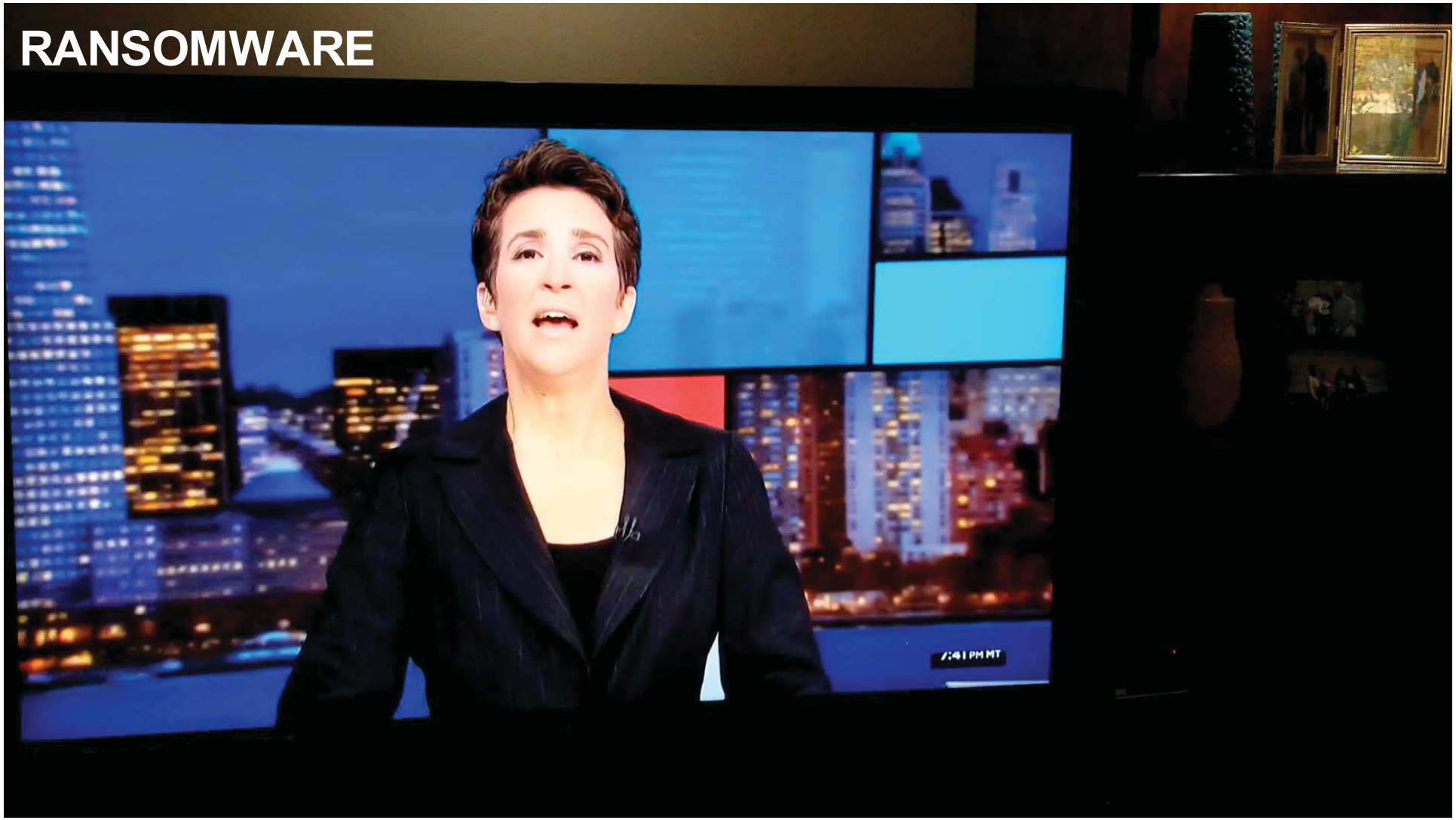

- China's **talent recruitment** or "**brain gain**" programs
- **Coercion** of foreign students, professors, guests
- Foreign **funding**, donations, joint-ventures
- Foreign **visitors** to campus

**What's good for China may be a threat to your research!**

# Federal response, a *threat*?

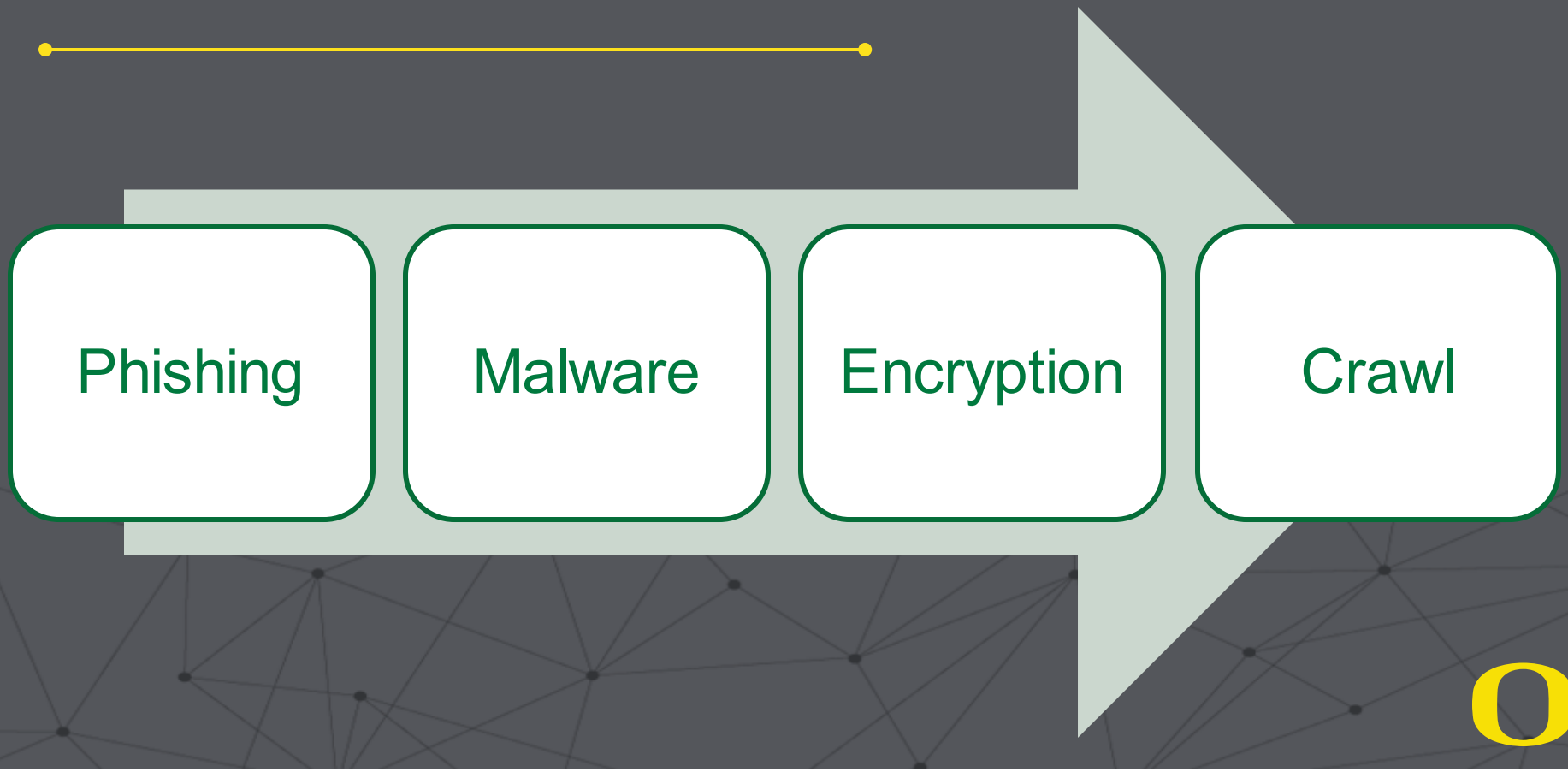
- Impact on **academic freedom** and international collaboration.
- **2018: NIH** warnings resulted in investigations at 55 universities that lead to faculty terminations for not disclosing international collaborations.
- **2018: DOD** decided against waiver for funding Flagship language programs at universities with Confucius institutes.
  **2018: DOD** requires stringent NIST 800-171 compliance for CUI data protection.
- **DUAs**: Funders have been and is expected to ratchet up security requirements to protect IP

# RANSOMWARE




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
Ransomware

# How is it done?



# Ransomware response

- Data
- System
- Full AppStack

Restore

- No guarantees
- Copycats
- ReHack

Pay

# PART IV
# VULNERABILITIES

# Weaknesses seen by ISO

- Susceptibility to ***phishing*** due to lack of awareness
- Insufficient data/system ***backups***
- Physical and logical ***access*** control – labs, offices, computers, hard files
- Unmanaged or unpatched systems
- Unsanctioned cloud storage
- International travel to high risk countries with regular work computers or phones with data

# PART V
# TRAVELING

# Before Leaving …

- ✓ Backup the computer user's profile and data.
- ✓ Remove applications that won't be used.
- ✓ Make sure devices and applications are up to date on patches.
- ✓ Verify Antivirus and Anti-Malware software is up to date and with the latest signatures.
- ✓ Install and review Qualys BrowserCheck.
- ✓ Verify that the user is running with the lowest possible privilege level.
- ✓ Provide charging devices for the trip (USB chargers offered at airports, restaurants, conferences, etc. may introduce malware).
- ✓ Make sure PINs are set on devices (Fingerprint + PIN is highly recommended).
- ✓ Make sure the device is using full disk encryption and requires a password on reboot.
- ✓ Setup user for UO VPN (note: depending on the country traveling to, local laws may apply regarding encryption).
- ✓ Forward your voicemail to email.
- ✓ Bring as little data as possible – just what is needed to get the job done.
- ✓ Do not store passwords or other credentials on the device, outside of a trusted and encrypted password management application.

# While There …

- ✓Pay attention to the environment
  - ✓ Be cognizant of individuals looking over your shoulders.
  - ✓ Do not accept any USB devices and definitely do not plug them into your devices.
  - ✓ Do not leave devices unsecured or out of your sight.
  - ✓ Keep track of the services that were accessed for reference after returning.
  - ✓ Do not accept any patches or updates for applications and systems.

# On Returning …

- ✓ Have the devices assessed by IT staff for possible malware and infections.
- ✓ Backup incoming profile and documents into a secure system.
- ✓ Wipe devices used while traveling.
- ✓ Reload profile that was backed up before the trip.
- ✓ Copy files from the incoming profile (e.g., Annotated documents) onto the device.
- ✓ From a trusted computer:
  - ✓ Change all PINs.
  - ✓ Reset Duck Id credentials.
  - ✓ Reset credentials for those services that were accessed while traveling.
- ✓ Review once again with Qualys BrowserCheck.
- ✓ Report any suspicious activities to the Information Security Office.

# PART VI
# DEFENSE

# On you…

1. Complete the ***Cybersecurity awareness training*** in MyTrack
2. ***Backup*** your data to O365, Crash Plan, IS Files, … (see IT)
3. ***Patch management*** - work with IT staff to manage your computers in JAMF or SCCM
4. Use ***UO VPN*** when off campus and work with IT staff to ***encrypt hard drives*** before travelling
5. Encrypt external media – USB, external hard drives, etc.
6. Use ***strong passwords*** and ***two-factor*** authentication
7. Avoid sending sensitive data in email or other insecure means
8. Require background screening and ensure sufficiency of NDAs

# On us…

1. ***Device loaner program*** for travel to high risk countries – China, Russia, Iraq, Iran, Afghanistan, Ukraine, Venezuela, …
2. ***Email Security.*** IS has implement controls to prevent users from browsing to known phishing sites and to reduce possible malware deliveries to inboxes
3. ***Secure network/services.*** ISO recommended secure services including the Allen Hall data center, UO OneDrive, IS Files, UO Cloud, Crash Plan
4. **2-factor** authentication is currently being rolled out campus wide
5. The Allen Hall datacenter is protected by firewalls and other controls
6. Contact ISO for help in securing your research projects
7. ISO continuously monitor network for suspicious activities

# PART VII
# TAKEAWAYS

# General phishing tips

- Mouse-over before you click
- Fake D0mains ***uoregon.edud***
- Flattery
- Urgency
- Unknown sender
- Unexpected tone
- Unusual request
- Letter Sub5titution5
- Bad Grammra

- Follow your gut!
- Ask a colleague if you are unsure
- Don’t trust links and phone numbers in email
- Ask Security by forwarding to phishing@uoregon.edu
- Look in the http://PhishTank.Uoregon.edu

# Remember …

- Your efforts will protect your data, IP, plus yours and UO's reputation
- Requirements for security include state, federal, international laws plus specific DUAs
- Partnership with ISO is critical to our defense - awareness training, patching, access control, backup, two-factor authentication, encryption, vigilance with international travel and welcoming visitors to campus

# Cybersecurity Briefing for Researchers

***…protecting your IP and your life's work…***

Information Security Office
infosec@uoregon.edu
541-346-5837

UNIVERSITY OF OREGON