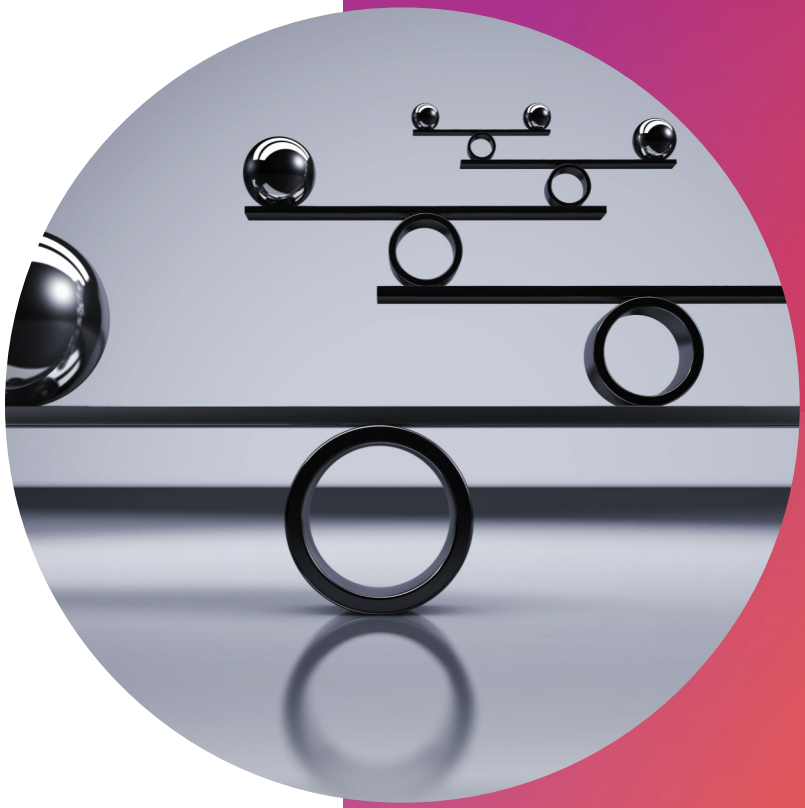
IT'S ABOUT THE MISSION

INFORMATION ASSURANCE AT UC SAN DIEGO



Michael Corn, CISO
Campus Lisa, August 13th, 2020

WHAT WE'RE NOT GOING TO TALK ABOUT

- What we've accomplished
- What I'm doing
- Whining about problems

WHAT WE WILL DISCUSS

1

What I've learned about UC San Diego

2

What are the challenges we're facing today

3

What these will look like in 5 years

The Same	Scale / Heterogeneity / Distributed IT / Budget
The Distinct	Health System – research DoD footprint ~~SDSC~~ / Qualcom Institute / SIO
The Idiosyncratic	System Influence / Pressure Scope and pace of ESR

UC SAN DIEGO

TODAY'S CHALLENGES

- Research Cyberinfrastructure
- Research Cyberinfrastructure
- Research Cyberinfrastructure
- Research Cyberinfrastructure
- Research Cyberinfrastructure
- Research Cyberinfrastructure
- Research Cyberinfrastructure
- Research Cyberinfrastructure

Cyberinfrastructure consists of computing systems, data storage systems, advanced instruments and data repositories, visualization environments, and people, all linked by high speed networks to make possible scholarly innovation and discoveries not otherwise possible. Cyberinfrastructure is a term first used by the National Science Foundation (NSF), and it typically is used to refer to information technology systems that provide particularly powerful and advanced capabilities.

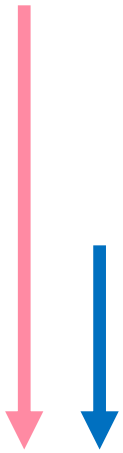
WHY NOW?

[Operator]: 'How can I accept $780,000? Is like, I worked for nothing. You can collect money in a couple of hours. You need to take is seriously. If we'll release our blog, student records/ data, I am 100% sure you will lose more than our price what we asked. We can agree to an price, but not like this, because I'll take this like an insult!'

How hackers extorted $1.14m from University of California, San Francisco

DATA/ACTIVITIES THAT'S ATTRACTIVE TO HACKERS

- National Security
- Political or Social Unrest
- Vaccine Research
- Other medical intellectual property
- Credentials to access 3rd party sites (banking, shopping)
- Any data that can be held for ransom
- Hacktivists looking to advance an agenda



Research Cyberinfrastructure

Work-a-Day

ABOUT OFFICE ENVIRONMENTS AKA WORK-A-DAY

- Patch your severs
- Auto-patch your laptops
- Deploy the campus anti-malware solution
- Deploy Qualys Cloud Agent
- Put your unit behind the campus firewalls (fully closed!)
- Back up everything (offline / read only)
- Join all hosts to AD

If you're not doing these things you are not doing your job.

If someone won't let you do your job, come and see me.

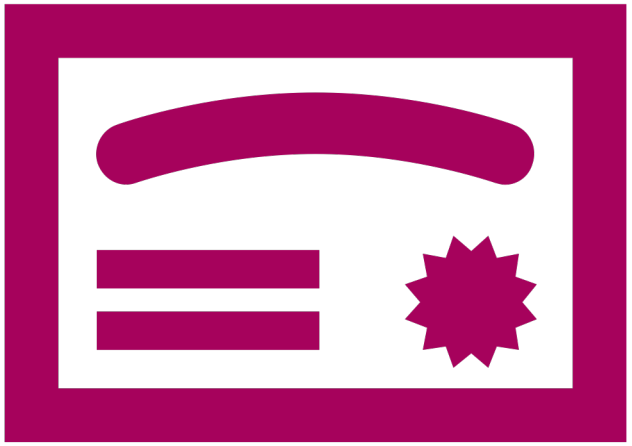
Go home and not worry about security at night.

WHY IS RESEARCH CYBERSECURITY HARD?

ENTERPRISE VS. RESEARCH

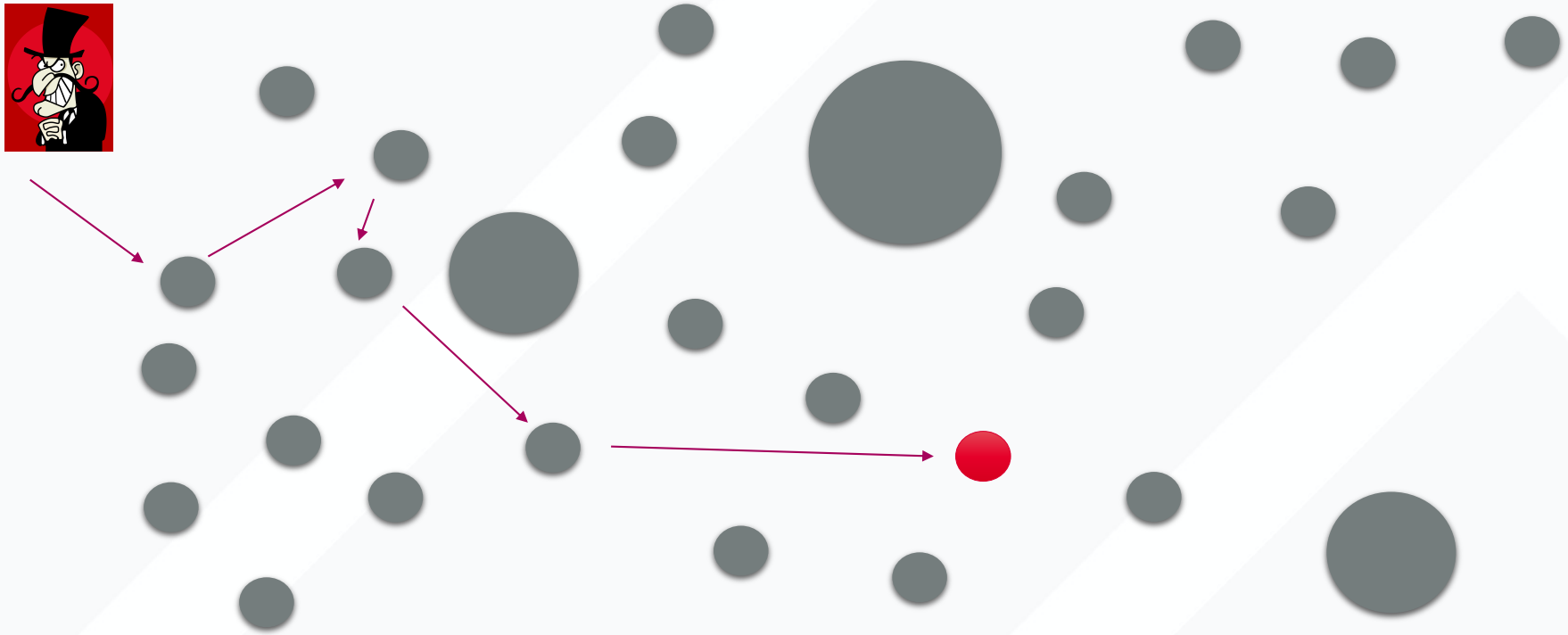
- More control
- Mostly COTS
- Offices, Data Centers, SaaS
- Mostly staff
- Office culture
- Predictable

- Less control
- Custom hardware/software lots of macgyvering
- Planes, Trains, and Automobiles
- Faculty
- Lab culture
- Unpredictable (but urgent)

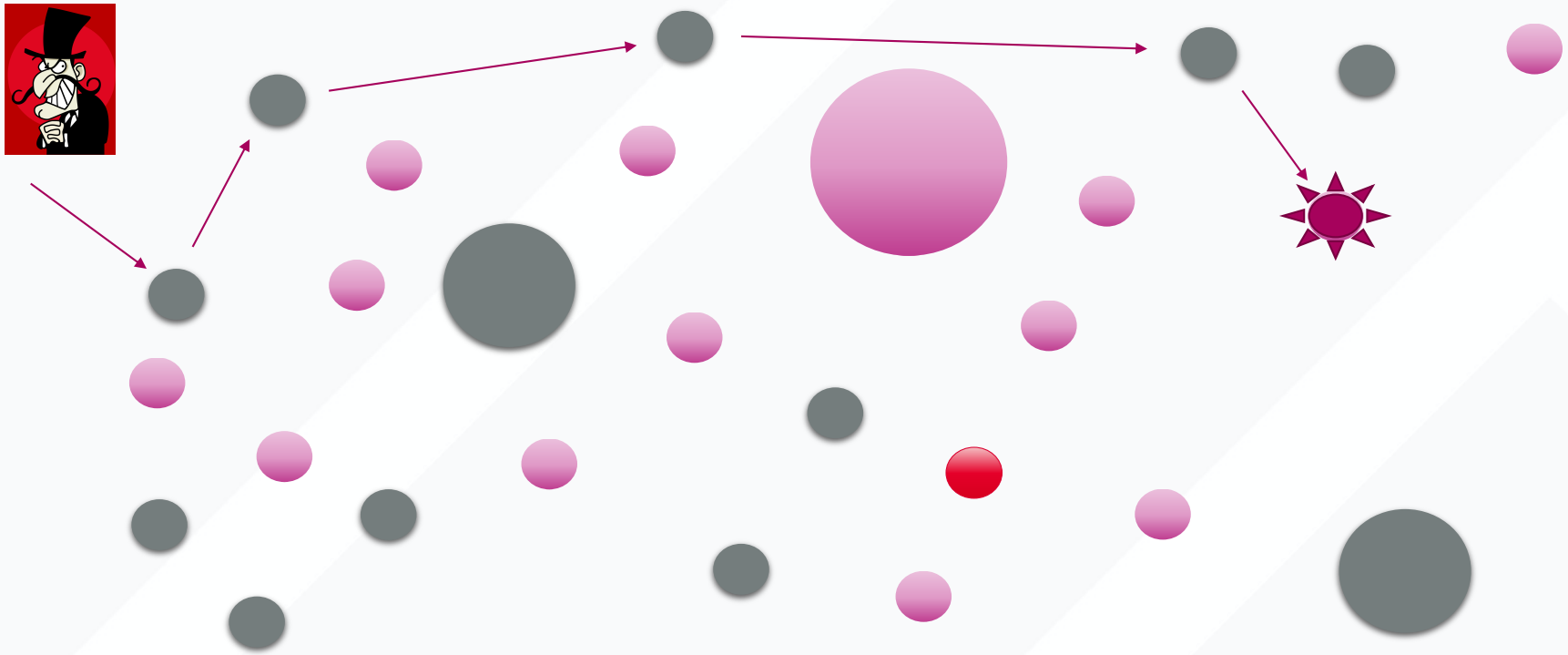


CYBERSECURITY CERTIFICATION FOR RESEARCH

EXAMPLE: RESEARCH LABS (UCSD HAS 1500)



HERD IMMUNITY TO PROTECT CYBERINFRASTRUCTURE



HERD IMMUNITY?

Classically (epidemiology)

- $V_c = R_0 - 1/R_0$

E.g., $R_0 = 4$ implies 1 case would lead to 4 cases and then to 16 cases. For the flu $R_0 = 1.3$. Thus $V_c = 53\%$ for the flu.

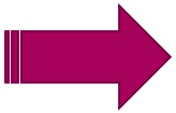
Term	Symbolic Expression	Definition
Basic reproduction number	R_0	Number of secondary cases generated by a typical infectious individual when the rest of the population is susceptible (ie, at the start of a novel outbreak)
Critical vaccination level	V_c	Proportion of the population that must be vaccinated to achieve herd immunity threshold, assuming that vaccination takes place at random
Vaccine effectiveness against transmission	E	Reduction in transmission of infection to and from vaccinated compared with control individuals in the same population (analogous to conventional vaccine efficacy but measuring protection against transmission rather than protection against disease).

https://academic.oup.com/cid/article/52/7/911/299077

CYBERSECURITY BASELINE

Required Practices

1. Use campus Active Directory accounts for all campus users when possible.
2. Use campus SSO if possible
3. Run the free campus provided anti-malware software and vulnerability identification software
4. Perform regular secure backups of data*
5. Use campus or Health provided email
6. Register lab contact information as part of self-certification process.



Implements these Technical Controls

- Restrict access to authorized users
- Use modern password practices
- Use MFA
- Identify and remediate system vulnerabilities
- Monitor activity for malicious behavior
- Scan files and downloads for malware
- Protect Intellectual Property from accidental or malicious loss
- Network segmentation to eliminate unneeded network traffic
- Protect email and users from email borne malware
- Report malicious activity and participate in incident response

CERTIFICATION PROCESS

- Biennial self-certification
  - random selection will be reviewed
  - high risk labs will be reviewed
  - reviews performed by unit IT + OIA + faculty

1. Spreadsheet provided to collect lab information
2. Data entered into online form (by anyone)
3. PI/Faculty/Researcher receives notice
4. PI reviews data and certifies its accuracy
5. Review team reviews certification
6. Certification complete

DATA REQUESTED

- Contact info: PI / Technical contacts / MSO
  - Number of grad students / visiting scholars
- Lab info
  - Network location
  - Critical hosts
  - Number machines running anti-malware & vulnerability detection software
  - Local accounts vs campus accounts and practices
- Backup strategy

CERTIFICATION TOOLS

https://assure.ucsd.edu

Describes:

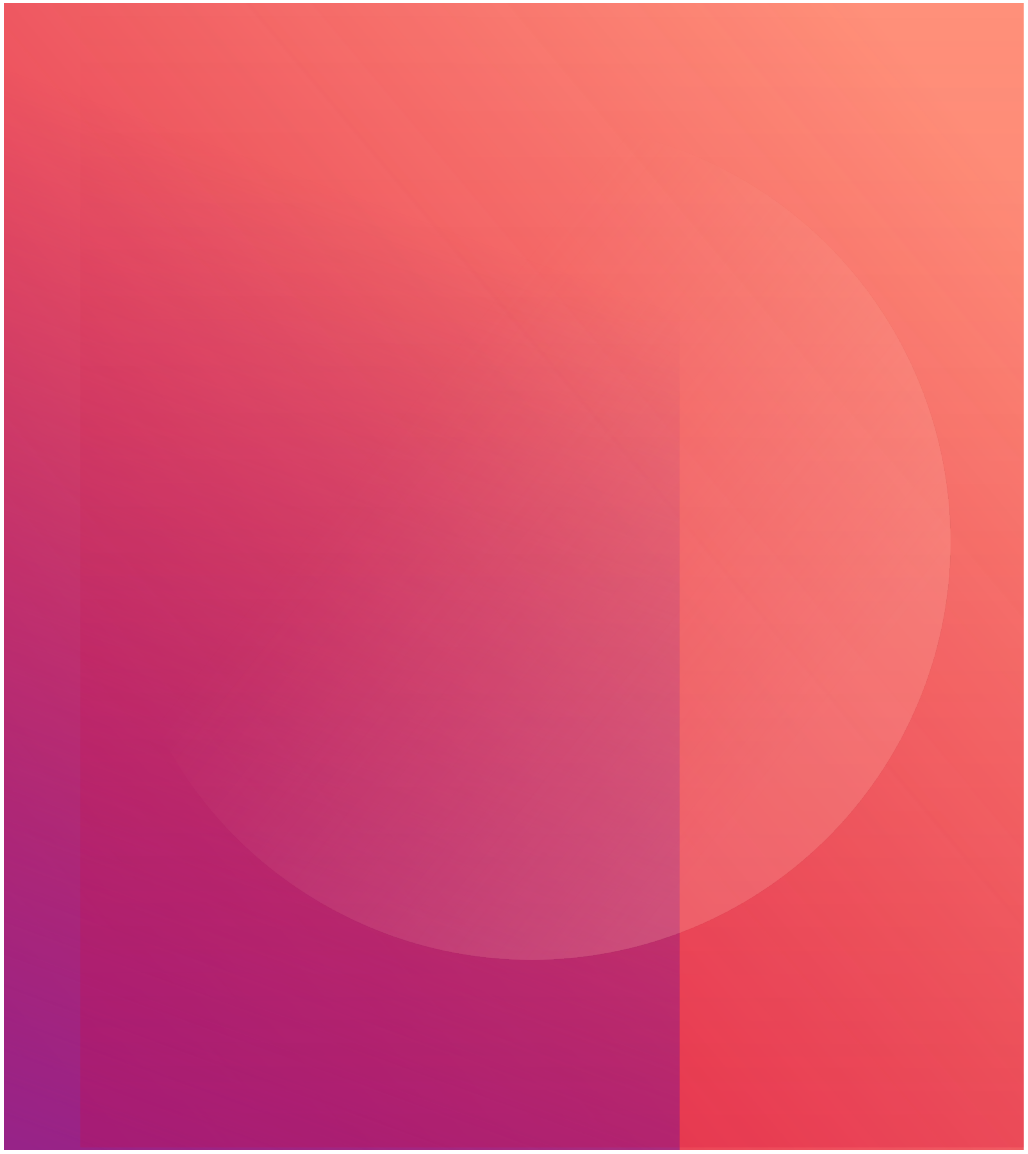
- Program overview
- Certification process
- Research cybersecurity baseline
- Support
- Link to secure portal

Secure Portal

- Tool downloads
- Quick start guides
    - Antimalware, vulnerability scanning
    - Joining AD
    - Configuring local accounts
    - Backup guidance
    - SSO integration guidance
    - DUO integration

SUPPORT FOR RESEARCHERS

- ccr-support@ucsd.edu
- Opens servicenow ticket (for tracking)
- Routes to Research IT who may reroute as appropriate
- Support team includes
  - Research IT staff
  - OIA staff
  - SDSC
  - Additional students being hired
  - Library data curation services
  - Unit IT



TOMORROW'S CHALLENGES

- The long tail of COVID
  - Personal devices, public networks
- Foreign Nationals, supply chain, applications
  - Huawei, WeChat
  - Personnel reviews, overseas work

THE OBVIOUS

THE NOT SO OBVIOUS

- What can we stop doing?
  - VPN?
  - Network monitoring? Instrumentation?
  - Endpoint management in the time of VDI
  - Firewalls in an era of SDNs?
  - System administration as code maintenance?
- Gmail / O365
- Gdrive/ Docs / OneDrive
- UCPath / OFC / Kuali Research
- Canvas
- Docusign
- AWS / GCloud / Azure
- Endpoints: AWS Desktops / Azure VD
- Soft Phones

THE DIFFICULT QUESTIONS

- What does the politicization of **everything** mean for information security?
- What does the triumph of SaaS / Cloud computing mean for security operations?
- Cyberattacks grow in frequency and sophistication exponentially – budget and resources are flat (esp. now).
- What is our end-game? Is security strategic or merely a tactical art form?

GOOD READS

- http://www.acls.org/uploadedFiles/Publications/Programs/Our_Cultural_Commonwealth.pdf
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7151357/
- My current hobby: https://medium.com/ciso-tuesdays
- Good (free) conference: https://www.trustedci.org/2020-nsf-summit