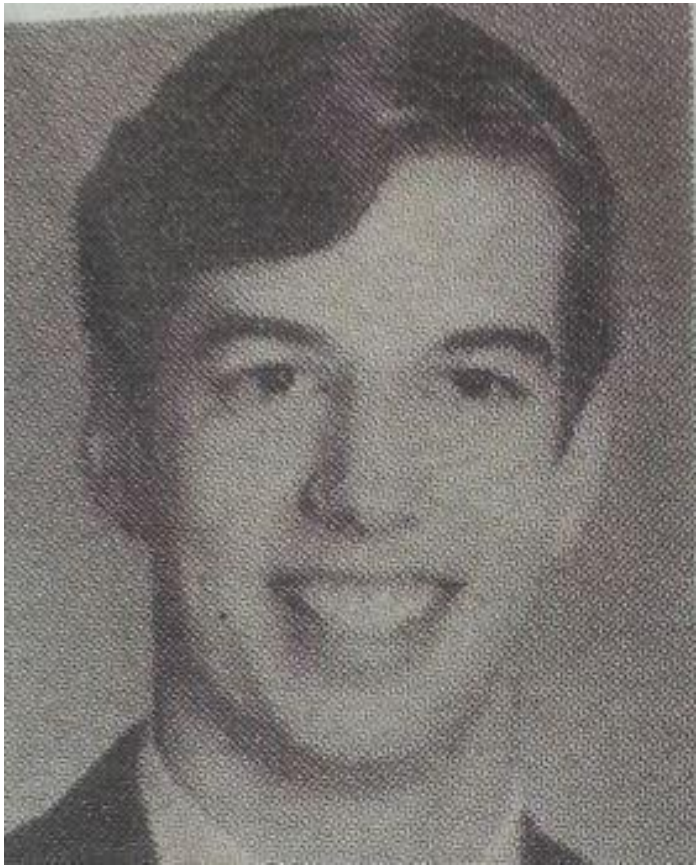

OmniSOC

OmniSOC

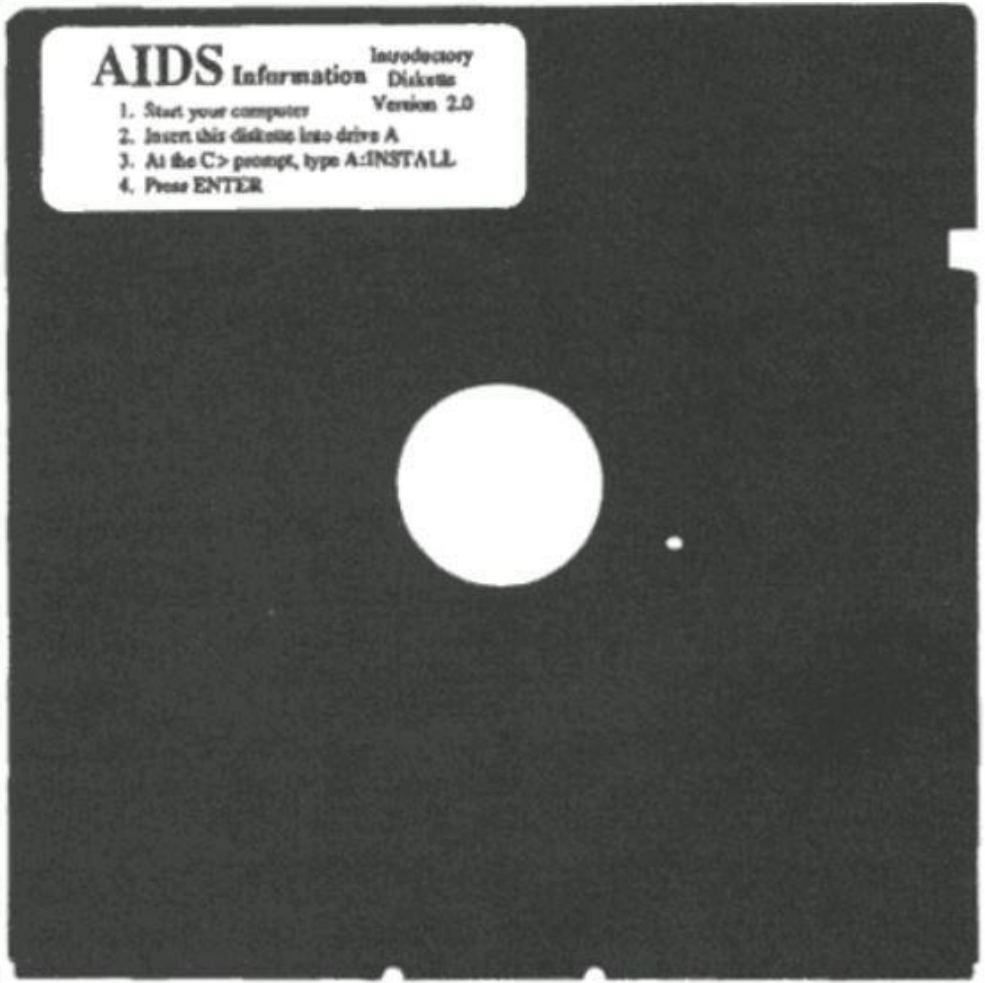
Cybersecurity
...but why?

Dr. Joseph L. Popp Jr.

1. Biologist
2. Got his Ph.D from Harvard
3. Wrote a book! It's… different.
4. Founded a butterfly conservatory
5. Was once extradited to the UK, but declared unfit to stand trial.



https://www.findagrave.com/memorial/78146552/joseph-l-popp


AIDS Information
Introductory
Diskette
Version 2.0
1. Start your computer
2. Insert this diskette into drive A
3. At the C> prompt, type A:INSTALL
4. Press ENTER

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the lifetime of your hard disk is US$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of $189 or $378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

The Business Model:

1. Distribute floppies by snail mail
2. Make computers unusable and demand ransom
3. Users send money by snail mail
4. ???
5. Probably don’t ever profit

What are we defending against?

It’s 2022 and we have data now!

Verizon Data Breach Investigation Report (DBIR)

www.verizon.com/business/resources/reports/dbir/

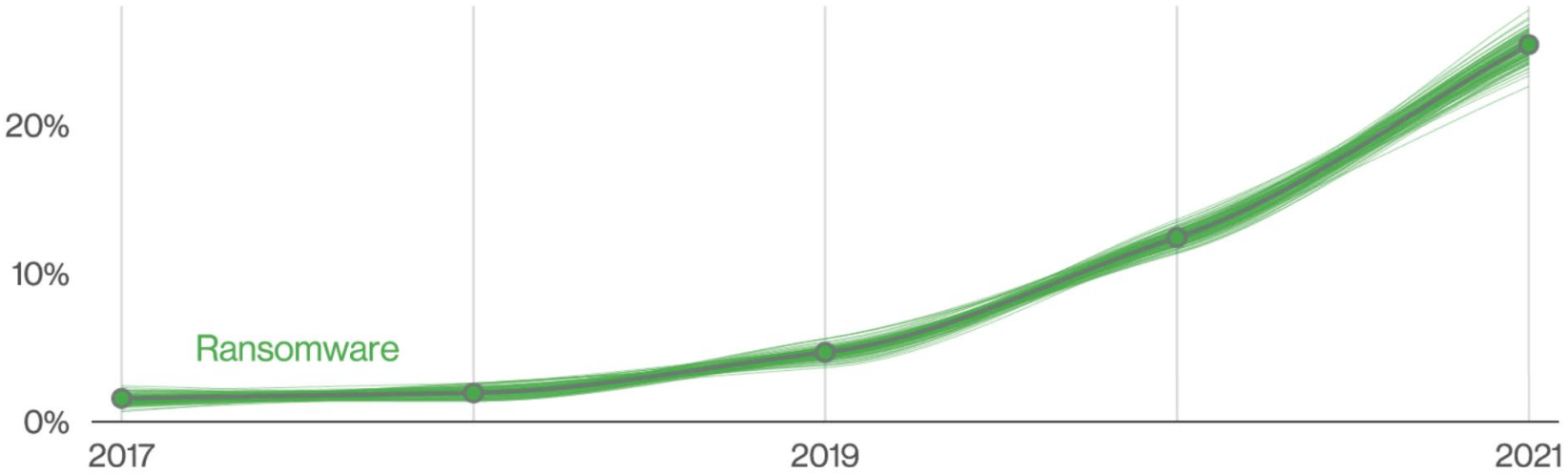


Figure 6. Ransomware over time in breaches

Why are they bothering?

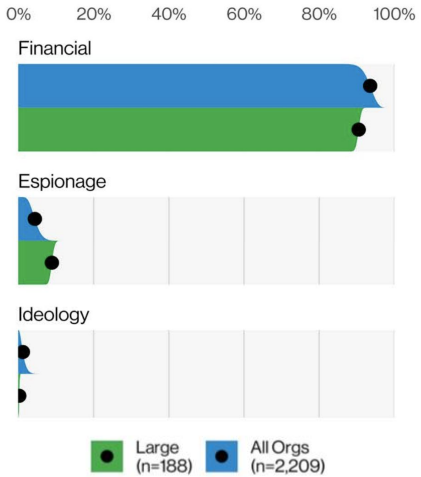


Figure 15. Motives in External actors by org size

1. Mostly money
2. Some espionage
3. There's overlap
4. The size of the org matters
5. ...and there's a **very** long tail of motives below this

How do they get in?

1. Stolen creds
2. Phishing (lets them steal creds)
3. Unpatched vulnerabilities

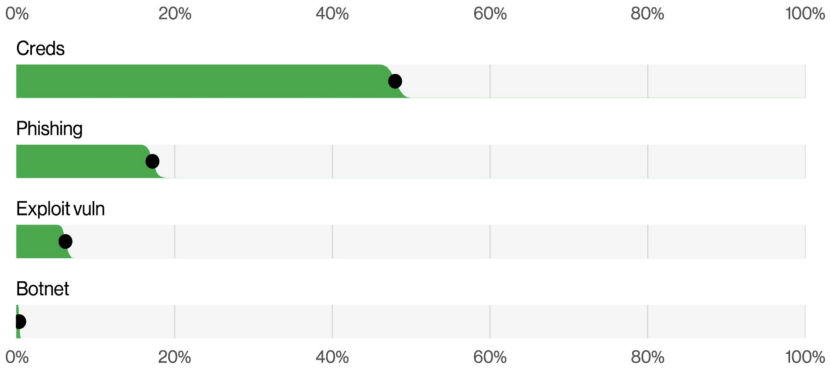


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

What are we defending against?

It’s 2022 and we have data now!

Verizon Data Breach Investigation Report (DBIR)

www.verizon.com/business/resources/reports/dbir/

Why us?

It doesn’t matter who we are.

It doesn’t matter whether we have something the attacker cares about.

All that matters to attackers is that we have something that **someone** cares about.

Someone includes us too.

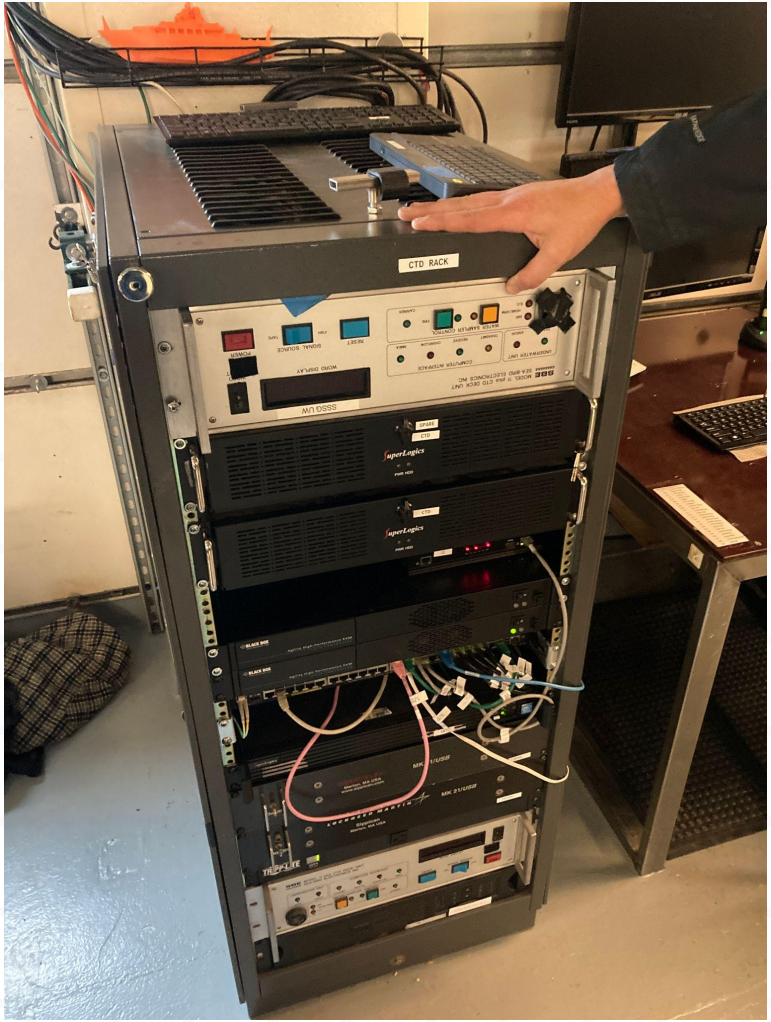
https://almascience.nrao.edu/news/alma-services-affected-by-cyberattack

All that matters to attackers is that we have something that **someone** cares about.

Someone includes us too.

Discussion

...and maybe some bonus slides


CTD RACK
SuperLogics
SuperLogics
TRIPP-LITE

Five easy to-dos:

Basics can go a long way.

1. Don’t reuse passwords
2. Apply software updates
3. Be careful with admin creds
4. Turn on multifactor authentication
5. Limit privileges

Decisions

cacr.iu.edu/principles

trustedci.org/framework

verizon.com/business/resources/reports/dbir

cisecurity.org/controls

cisecurity.org/cis-benchmarks/

Contact us!

Ryan Kiser - rlkiser@iu.edu

ARF Security Team - arfsec@iu.edu