



PennState



**CHALLENGES OF CYBERSECURITY**  
IN FACILITIES OPERATIONS

Tom Rodgers  
Director of Operational Technology  
Penn State University

1

---

---

---

---

---

---

---

---



AGENDA

A preview of what we will be covering today.

- 1  **About Me**  
Information about the instructor and a little background on how we got here.
- 2  **Operational Technology**  
A description of OT and why it's important in today's facilities.

2

---

---

---

---

---

---

---

---

- 3  **Cyber Evolution & AIC**  
How the digital environment is changing in SCADA systems and IOT and how we need to look at security differently.
- 4  **Attacks are being launched!**  
Real world examples of attacks on infrastructure.
- 5  **Network Security**  
How ownership and protection at the border is critical to limit risk to the institution.

3

---

---

---

---

---

---

---

---

**6 Inventory Management**  
Having an inventory and knowledge of what's in your environment is critical to protection.

**Identity & Access Management**  
IAM is one of the most important components to managing risk to ICS systems.

**7**

**8 Visibility**  
Capturing logs from systems and allowing agents on systems that could provide information to analysts for intrusion detection.

4

---

---

---

---

---

---

---

---

**9 Vulnerability Management**  
Keeping up with maintenance and patching system help decrease risk.

**Targeted Attacks**  
What do you do if you think your environment is compromised.

**10**

**11 Phishing**  
What I can do today to help protect my environment and practice good computing hygiene.

5

---

---

---

---

---

---

---

---

**OPERATIONAL TECHNOLOGY Director**

**About The Instructor**

I'm currently the Director of Operational Technology at Penn State University. Prior to joining the Office of the Physical Plant, I worked in the department of Cybersecurity and managed several different teams; Security Operations, Risk Management, and Identity Business Services. He's been in several academic and research technology roles during his nineteen-year tenure in Higher Education.

*Thomas Rodgers*  
**THOMAS RODGERS**  
PennState

6

---

---

---

---

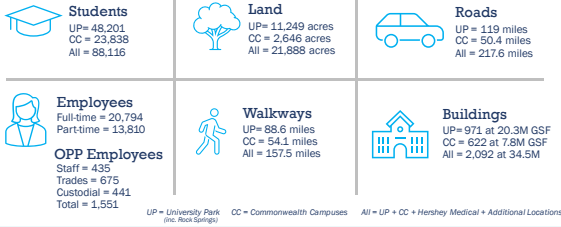
---

---

---

---

### Penn State at a Glance



7

---

---

---

---

---

---

---

---

---

---

### OPP Divisions of Labor

Operations	Design and Construction	Environmental Health and Safety	Planning, Design and Properties
Commonwealth Services	Business and Finance	College of Medicine Facilities	Administration



8

---

---

---

---

---

---

---

---

---

---


PennState

## OPERATIONAL TECHNOLOGY

Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. The term has become established to demonstrate the technological and functional differences between traditional information technology (IT) systems and industrial control systems environment, the so-called "IT in the non-carpeted areas".



9

---

---

---

---

---

---

---

---

---

---

**Security by obscurity**  
ICS devices are often more physical and more difficult to attack than traditional IT devices.

**Shift to the Internet**  
When ICS devices shifted to TCP/IP protocols, they became vulnerable to network security attacks because of system availability.

**Windows XP end of life**  
Several ICS vendors warned that recent versions of Windows may not be applying security patches effectively because they need their systems to operate with Windows XP.

**Specific threats on the rise**  
In 2015, there were an attack on Natural Water Company's ICS, which resulted in hackers changing the levels of chemicals used to treat tap water. In 2021, we had a similar attack in Oklaahoma (Link attached).

**CyberSecurity planning & policy**  
Following the CIA, Confidentiality, Integrity and Availability model of security principles, the most important for ICS systems is integrity and availability of systems and underlying the most. A custom plan and policies must focus on those key elements to be successful.

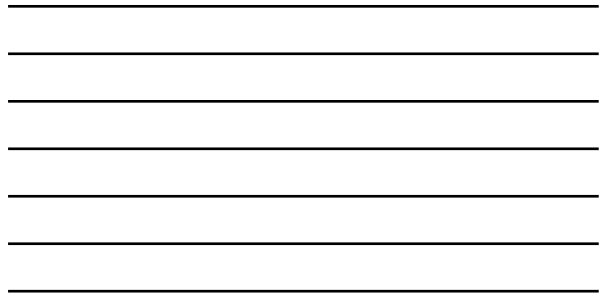
As ICS evolves security risk increases!

10

### Industrial Control Systems

An ICS is any device, instrumentation, and associated software and networks used to operate or automate industrial processes. Industrial control systems are critical infrastructure such as energy, communications, and transportation. Many of these systems connect to sensors and other devices over the internet – the industrial Internet of things (IIoT), which increases the ICS attack surface.

© 2022  
1007 8th St.  
10000, Toronto, ON



### AVAILABILITY INTEGRITY CONFIDENTIALITY

In the CIA Triad of security models, we need to make adjustments for ICS, SCADA and OT systems. Availability becomes the most important component of the model.

11



Hacker Changed Chemical Level in Florida City's Water System - WSJ

#### Hacker Changed Chemical Level in Florida City's Water System

Florida authorities say they are investigating how the breach at a water treatment plant occurred and whether it was intentional.

**By Arianna Cupo and Mike Wozniak** Feb. 8, 2023 7:50 am ET

A water treatment plant in Oklaahoma, Fla., was hacked, and the breach briefly increased the amount of lead used to treat water to a dangerous level, authorities said Monday.

A plant operator noticed the alteration Friday and immediately reversed it, sending a warning alert to the city's water supply. But the breach highlights the exposure of utilities to cyberattacks.

**Vulnerabilities Allowed Researchers to Remotely Lock and Unlock Doors**

Security researchers found several vulnerabilities that allowed them to take remote control of Internet-connected devices that communicate with...

Ukraine Power Grid Cyberattacks - black hat

Introduction

This post is about the 2015, 2016 and 2022 cyberattacks on the energy supply infrastructure in Ukraine. In 2015, the attack of the (Stuxnet) equipment (Stuxnet) hacking team left hundreds of thousands of consumers without power for hours and caused serious damage to the security of critical infrastructure worldwide. In 2016 and 2022, two incidents happened again when Stuxnet was used to disrupt the power supply in Ukraine.

This article briefly explains the three hacking attempts, the attacker's motivation, and how the intrusions contributed to the cybersecurity of similar environments.

**Target Hackers Broke In Via HVAC Company**

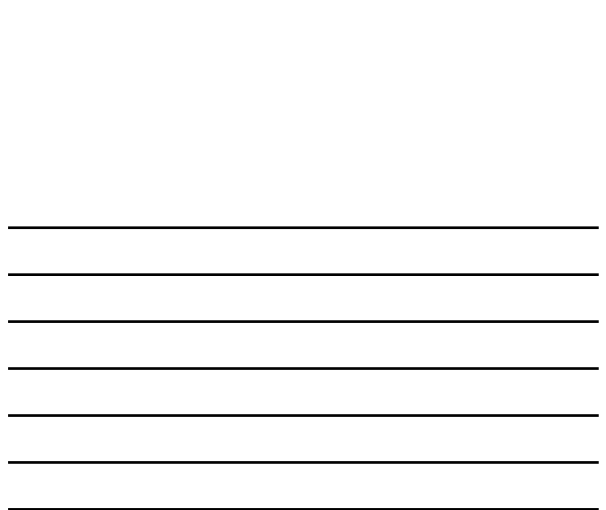
February 5, 2014 288 Comments

Last week, Target told reporters at The Hill that it had found out that the initial intrusion into its systems was traced back to several commercial HVAC units from a third-party vendor. Several days later, the vendor discovered that the vendor in question was a refrigeration, heating and air conditioning contractor that had worked as a contractor of Target in other cities.

Stuxnet broke in via investigators, again the evidence that broke into the vendor's network on Nov. 12, 2010 using research conducted under the name of the National Security Agency's (NSA) Operation Aurora.

Patrick Brackenridge, Boss, Florida confirmed that the U.S. Secret Service visited the company's office in connection with the Target investigation. He said he was interviewed about the incident. He said the research project started in 2010. He said he was interviewed about the incident. He said he was interviewed about the incident. He said he was interviewed about the incident.

12



**PennState**

## The EVOLUTION WILL CONTINUE

As you can see, we came from systems that only had internal threats as a risk factor, to systems that have external & internal threats. As actors become more sophisticated, we need to have incident response and risk mitigation plans in place.

Many security experts see a new wave of destructive attacks targeting ICS and want critical infrastructure owners to urgently update the security of their operational technology networks.

13

---

---

---

---

---

---

---

---

---

---

**PennState**

## NETWORK SECURITY

Property and facilities is very similar on how we should manage our digital environment. Many of the same principals apply in Cybersecurity!

14

---

---

---

---

---

---

---

---

---

---



15

---

---

---

---

---

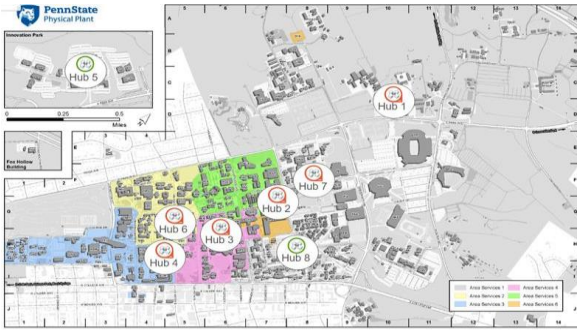
---

---

---

---

---



16

---

---

---

---

---

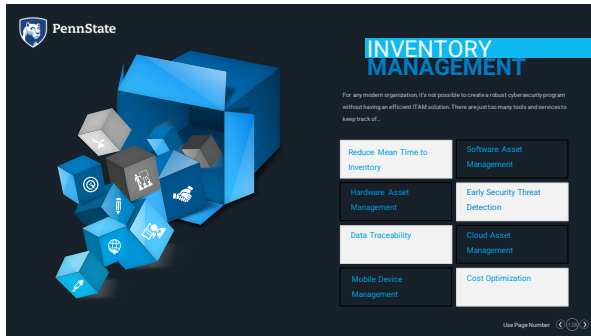
---

---

---

---

---



17

---

---

---

---

---

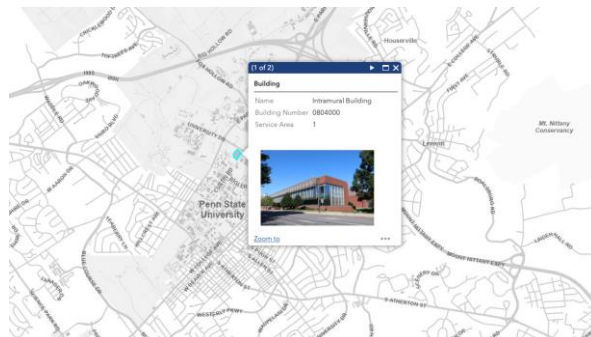
---

---

---

---

---



18

---

---

---

---

---

---

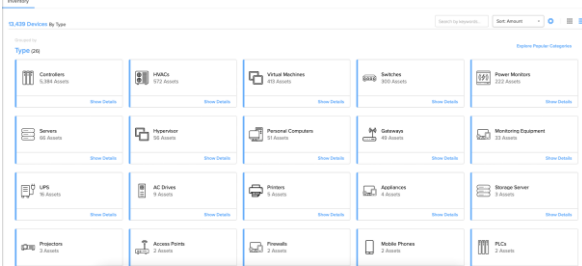
---

---

---

---

### Look At The INVENTORY



19

---

---

---

---

---

---

---

---

---

---

**PennState**  
**IDENTITY ACCESS MANAGEMENT**  
 Identity and access management is a specialty discipline within cybersecurity designed to ensure only the right people can access the appropriate data and resources – at the right times and for the right reasons.

- Provisioning
- Multifactor Authentication (2FA)
- Deprovisioning

20

---

---

---

---

---

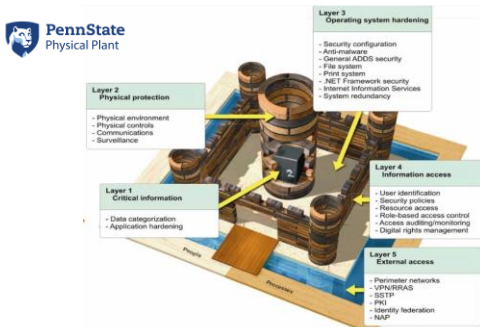
---

---

---

---

---



21

---

---

---

---

---

---

---

---

---

---



22

---

---

---

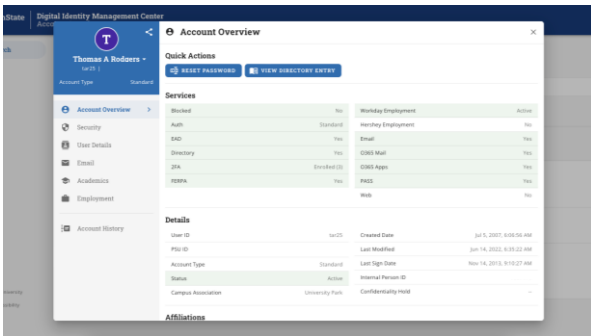
---

---

---

---

---



23

---

---

---

---

---

---

---

---



24

---

---

---

---

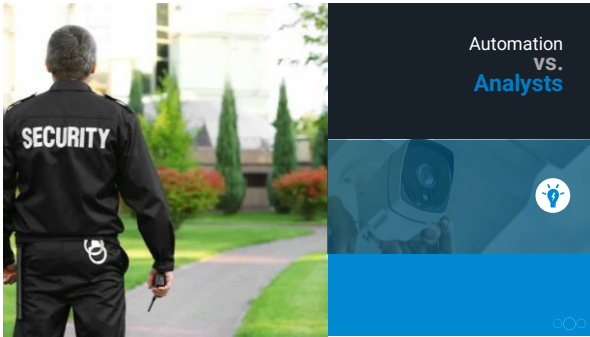
---

---

---

---





25

---

---

---

---

---

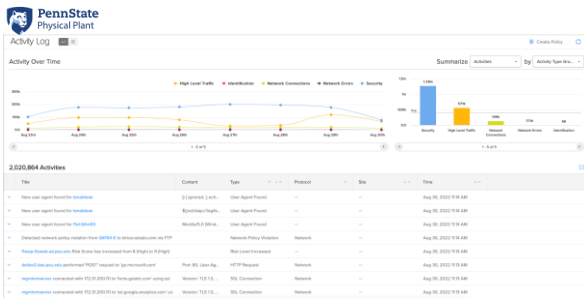
---

---

---

---

---



26

---

---

---

---

---

---

---

---

---

---



27

---

---

---

---

---

---

---

---

---

---



28

---

---

---

---

---

---

---

---

**Unit Security Dashboard**

**All Known Critical and High Vulnerabilities**  
 Click on your "Overdue" vulnerabilities first, then your "Overdue within 7 Days" view. This view is simply a consolidated view of all vulnerabilities regardless of whether they are overdue or not. Your scorecard are not impacted by these vulnerabilities unless the Top Overdue is 0.  
 Note that the vulnerability data below only updates once per day. Due to the timing of agent scans it may take up to 48 hours for a remediated vulnerability to be reflected on the dashboard. Scheduling a second agent scan will refresh the data with any updates.  
 Handy links: Request immediate removal of vulnerabilities on decommissioned host | Report a false positive | Request an exception | Vulnerability Management Servicebox knowledge base | Additional information on uvm

Rank	Risk ID	Type	Count	Risk %
1	Oracle Java 10 Multiple Vulnerabilities (July 2022 CVE)	Vulnerability	65	4.4%
2	CentOS 7 - kernel (CVE-2022-3526)	Vulnerability	55	4.2%
3	Ubuntu Focal 20.04 LTS - 1.8 Privilege Escalation (9954-9953-9954)	Vulnerability	54	4.0%
4	Redhat/Oracle Linux RHEL7 - Security Update (August 2022)	Vulnerability	50	4.0%
5	VMware ESX/ESXi 7.0 U3 - 1.8 Privilege Escalation (9954-9953-9954)	Vulnerability	47	3.5%
6	Debian 10-110-1 - Linux - security update	Vulnerability	38	3.1%
7	Debian 10-110-1 - openssl - security update	Vulnerability	36	3.0%

Counts chart showing Vulnerabilities Critical or High, Critical, and High over time from Mon Jul 24 to Mon Jul 31 2022.

29

---

---

---

---

---

---

---

---

**PennState**

**WE WERE TARGETED!**

Incident response (IR) is a set of information security policies and procedures that you can use to identify, contain, and eliminate cyberattacks. The goal of incident response is to enable an organization to quickly detect and halt attacks, minimize damage and prevent future attacks of the same type.

- Forensic Data
- Automation
- Disaster Recovery

30

---

---

---

---

---

---

---

---



31

---

---

---


---

---

---


---

---

 HOME EDUCATION & TRAINING POLICIES & STANDARDS PRIVACY SERVICES ABOUT OIS

**POLICIES & STANDARDS**  
Office of Information Security [REPORT AN INCIDENT](#)

**University Policies**

 **AD95: Information Assurance and IT Security**  
To establish an institution-wide security program designed to ensure the confidentiality, integrity, and availability of The Pennsylvania State University's ("Penn State" or "the University") information assets from unauthorized access, loss, alteration, or damage while supporting the open, information-sharing needs of our academic culture.

**AD96: Acceptable Use of University Information Resources**  
To establish and define the "acceptable use" of The Pennsylvania State University ("Penn State" or "University") electronic resources, including, but not limited to, computer facilities and services, computing resources, electronic mail services, and electronic information and data, and video and voice services, to support the educational, research and service missions of the University.

32

---

---

---

---

---

---

---

---



**WHAT IS THE MOST IMPORTANT THING I CAN DO RIGHT NOW?**



33

---

---

---

---

---

---

---

---



## WHAT IS PHISHING?

### THEFT BY FAMILIARITY

Phishing is an attempt to steal your personal information  
By posing as **someone you know or trust**

### TOP CYBERATTACK VECTOR

Of all attack vectors, **phishing** remains the most commonly exploited, and accounts for **90%** of all **successful** cyberattacks worldwide. Over the last year, there has been a 400% increase in phishing attacks!

34

---

---

---

---

---

---

---

---

---

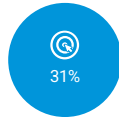
---



### HOW MANY HAVE BEEN REELED IN? PHISHING IS EFFECTIVE



Average cost of a data breach in 2021 to an institution at our scale.



DUO saw that an average of 31% of people click the phishing links. They also saw that 17% of users enter their credentials into the phishing site



Number of phishing attempts reported by Sonicwall from Jan - Sept 2021

35

---

---

---

---

---

---

---

---

---

---



### Penn State: **Big Pond** Bigger Phishes

Penn State remains one of the most highly targeted universities in the Big Ten

**850,000**  
Average daily malicious emails blocked by Microsoft O365

36

---

---

---

---

---

---

---

---

---

---



“ HOW DO I KNOW IT’S A PHISH? ”

Style

Does the writing style match the sender?

Action

Is the sender asking you to visit a site you don't recognize?

Grammar

Are there spelling or grammar errors, or missing words?

Email

Do you recognize the sender, and does the email address match?

Links

Sometimes, you can hover over links within emails to see where they're really going. Microsoft Office 365 helps protect us with Safe Links.

DON'T CLICK IF YOU AREN'T SURE!



37

---

---

---

---

---

---

---

---

---

---



Penn State Students Self-Phishing Campaign 2018



93,593 emails sent



34,001 (36.32%) users clicked



38

---

---

---

---

---

---

---

---

---

---



OK, I FELL FOR IT “ NOW WHAT? ”

Passwords



Change ALL your passwords, and don't use the same one for accounts.

PSU IT



There's no shame in contacting us! Call immediately to limit our risk.

Use Caution



In the future, if an email seems suspicious call the sender or email them directly.

Delete



Don't "test" the email. If you click, it may already be too late. Just delete!

39

---

---

---

---

---

---

---

---

---

---



TARODGERS@PSU.EDU

---

---

---

---

---

---

---

---