

CHALLENGES OF OPERATIONAL TECHNOLOGY
IN FACILITIES OPERATIONS

Tom Rodgers
AVP for Administration
Penn State University

1

AGENDA
A few topics of what we will be covering today.

- 1 About Me**
Information about the instructor and a little background on how we got here.
- 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.
- Attacks are being launched!**
Real world examples of attacks on infrastructure.
- 4**
- 5 Network Security**
How ownership and protection at the border is critical to limit risk to the institution.

3

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

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

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.

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

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

5

OPERATIONAL TECHNOLOGY
AVP for Administration

About The Instructor

I'm currently the Assistant Vice President for Administration, at Penn State University in the Office of the Physical Plant. Prior to joining OPP I worked in the department of Cybersecurity and managed several different teams: Operational Technology, Security Operations, Risk Management, and Identity Business Services. I've been in several academic and research technology roles during his twenty tenure in Higher Education.

Thomas Rodgers
THOMAS RODGERS
PennState

6

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".

7

Security by obscurity
ICS deployment is a combination of hardware and software that is difficult to attack by external entities.

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

Windows XP end of life
A hard endpoint for the current versions of Windows may not be applying security patches effectively because they need their system to operate with normal operations.

Specific threats on the rise
In 2015 there was an attack on Kenner Water Company's ICS, which resulted in a breach changing the levels of chemicals used in the tap water. In 2017, we had a similar attack in Odessa Florida. (see 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. Confidentiality is the most. A custom plan and policy must focus on those key elements to be successful.

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.

Source: NIST 800-82, SP800-810r1

As ICS evolves security risk increases!

8

APPA Leadership in Educational Facilities

**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.

9

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

Hacker Changed Chemical Level in Florida City's Water System

Public water in Orange, Polk and Volusia County sheriff's investigations have been launched



A digital breacher used a exploit to get into the control system of a water treatment plant and increase the amount of fluoride in the water supply.

By Jonny Lee

Updated Feb. 6, 2023 7:50 p.m. ET

A water treatment plant in Ocala, Fla., was hacked, and the intruder briefly increased the amount of fluoride in the water supply to a dangerous level, authorities said Monday.

A plant operator noticed the alteration Friday and immediately reversed it, avoiding adverse effects on 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 remotely lock and unlock doors on a building's access control system.

Ukraine Power Grid Cyberattacks



Introduction

This post is about the 2015, 2016 and 2017 cyberattacks on the energy supply infrastructure in Ukraine. In 2015, the attack of the Ukrainian power grid led to a loss of hundreds of thousands of consumers without power for hours and raised alarms over the security of critical infrastructure worldwide.

This article mostly explains the three hacking attempts, the attacker 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 had reports at The Hill Street plant and noticed that the initial breach into the system was from backdoor to network controllers that were obtained from a third party vendor. Since a one-off vulnerability in the vendor's software was a pre-requisite for getting a successful authentication that has existed at a number of locations at Target and other top retailers.

Quinn also said he investigated with the vendor that had the vendor's report on Nov. 15, 2011 using network controllers from their HVAC system. The vendor, Perm-based provider of refrigerant and HVAC systems.



Perm president Ross Panko confirmed that in U.S. Security Council used the company's software to connect with the network controllers that were obtained from a third party vendor.

Target investigators did not find any other vulnerabilities in the vendor's software. The vendor said they did not know any other vulnerabilities in the software. The vendor said they did not know any other vulnerabilities in the software.

Target spokeswoman Wendy Snyder said the company had no additional information to share, citing a "non-disclosure agreement."

10

Horizontal lines for note-taking.

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 IT and want critical infrastructure owners to urgently update the security of their operational technology networks.



11

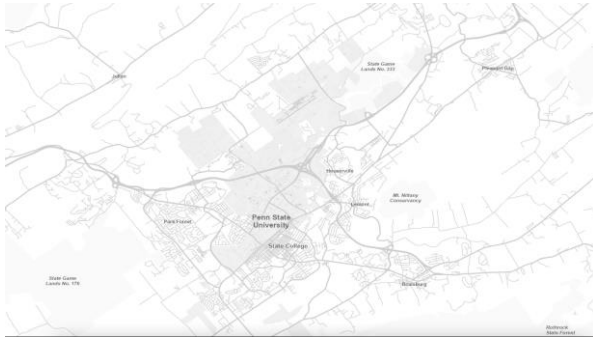
Horizontal lines for note-taking.

NETWORK SECURITY

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

12

Horizontal lines for note-taking.



13



14

INVENTORY MANAGEMENT

For any modern organization, it's not possible to create a robust cybersecurity program without having an efficient IAM solution. These are just too many tools and services to keep track of.

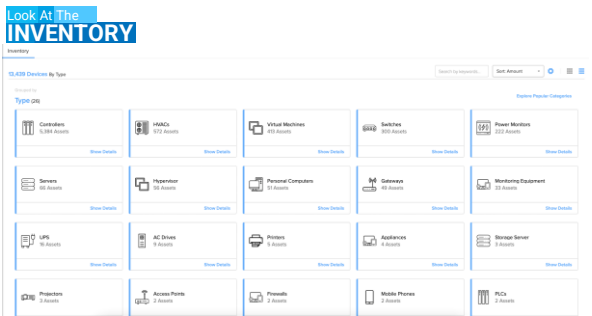
Reduce Mean Time to Inventory	Software Asset Management
Hardware Asset Management	Early Security Threat Detection
Data Traceability	Cloud Asset Management
Mobile Device Management	Cost Optimization

Use Page Number

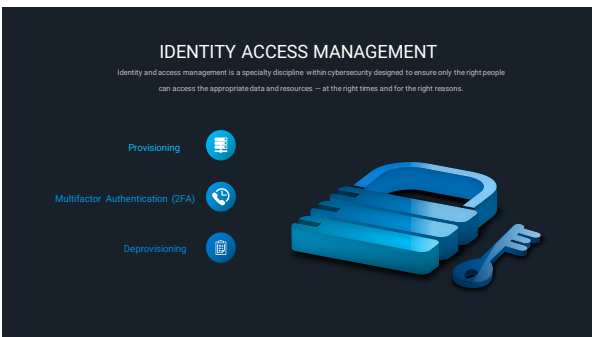
15



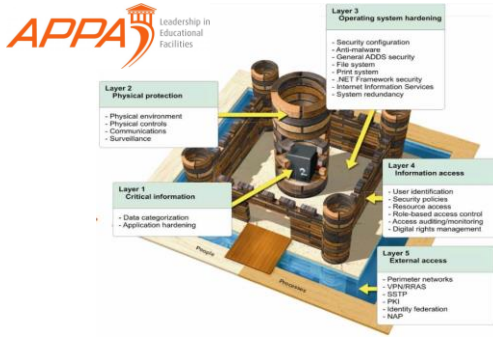
16



17



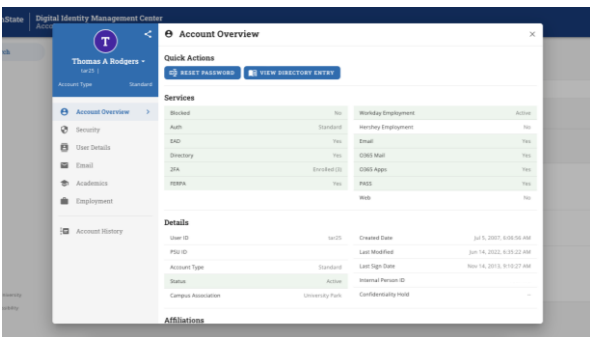
18



19



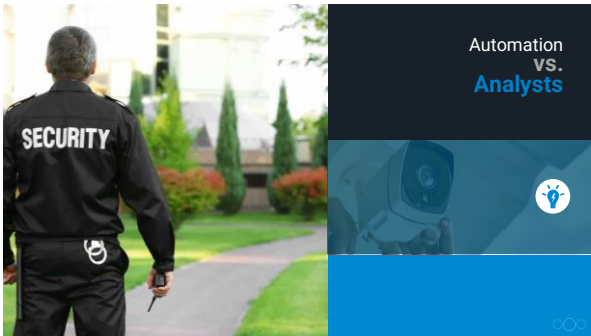
20



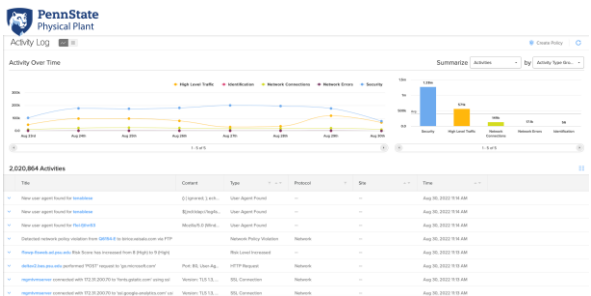
21



22



23



24

PATCHING & VULNERABILITY MANAGEMENT

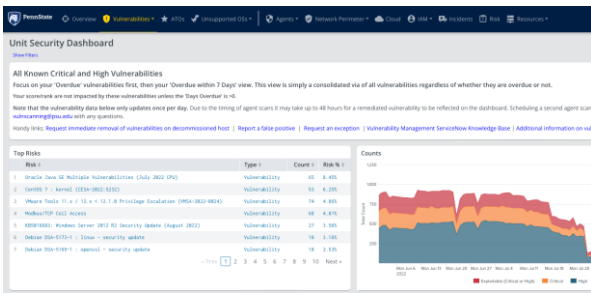
The terms patch management and vulnerability management are often used interchangeably, albeit with different meanings. While patch management and vulnerability management have a comparable relationship to the real-world processes with different goals, patch management focuses on applying software updates to correct specific flaws on which the application features rely. In contrast, vulnerability management is a much broader process that incorporates the discovery and remediation of risks of all kinds.



25



26



Unit Security Dashboard

All Known Critical and High Vulnerabilities
Focus 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 is not impacted by these vulnerabilities unless the Days Overdue is >= 6.

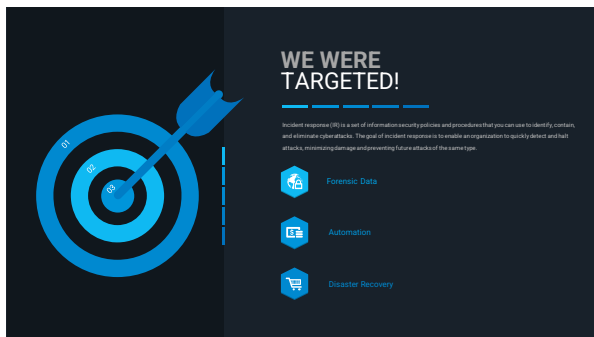
Note that the vulnerability data below only updates once per day. Due to the timing of agent scans it may take up to 48 hours for a remediated vulnerability to be reflected on the dashboard. Scheduling a second agent scan will refresh the data with any updates.

Handy links: [Request immediate removal of vulnerabilities on decommissioned host](#) | [Report a false positive](#) | [Request an exception](#) | [Vulnerability Management Service/Knowledge Base](#) | [Additional information on vuln](#)

Rank	Risk	Type	Count	Risk %
1	Oracle Java SE Multiple Vulnerabilities (July 2022 CVE)	Vulnerability	85	4.45%
2	CoreOS 7 - kernel CVE-2022-3122	Vulnerability	59	3.05%
3	Wave Suite 5.0.0 - 5.10.0 - 5.10.0 - Privilege Escalation (CVE-2022-3824)	Vulnerability	34	1.78%
4	WebkitGTK CVE-2022-3824	Vulnerability	34	1.78%
5	MSB16881 - Windows Server 2012 R2 Security Update (August 2022)	Vulnerability	27	1.42%
6	Debian 10-1070-1 - libssl - security update	Vulnerability	16	0.84%
7	Debian 10-1070-1 - openssl - security update	Vulnerability	16	0.84%

Counts: Line chart showing the number of vulnerabilities over time, categorized by risk level (Critical, High, Medium, Low).

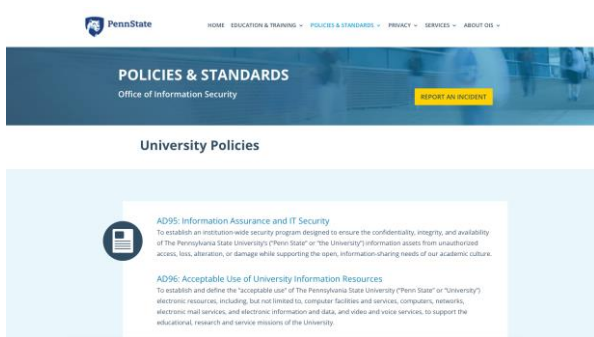
27



28



29



30



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



31

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

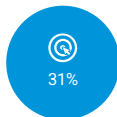
Of all attack vectors, **phishing** remains the most commonly exploited, and accounts for **90%** of all **successful** cyberattacks worldwide. Over the last year, there has been a 400% increase in phishing attacks!

32

HOW MANY HAVE BEEN REELED IN? PHISHING IS EFFECTIVE



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

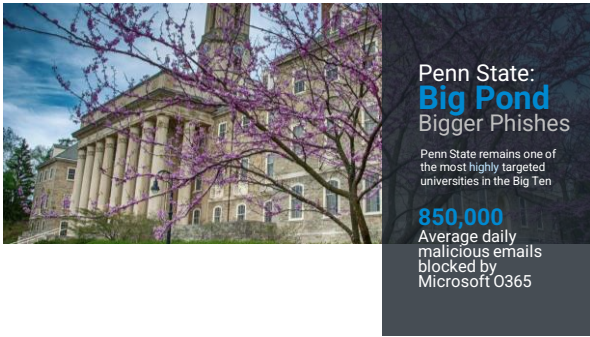


DUO saw that an average of 31% of people click the phishing links. They also saw that 17% of users enter their credentials into the phishing site



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

33



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

34

“ HOW DO I KNOW IT'S A PHISH? ”

<p>Style</p> <p>Does the writing style match the sender?</p>	<p>Action</p> <p>Is the sender asking you to visit a site you don't recognize?</p>	<p>Grammar</p> <p>Are there spelling or grammar errors, or missing words?</p>	<p>Email</p> <p>Do you recognize the sender, and does the email address match?</p>
---	---	--	---

Links

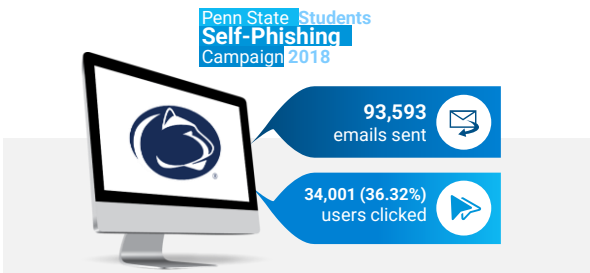
Sometimes, you can hover over links within emails to see where they're really going. Microsoft Office 365 helps protect us with Safe Links.

DON'T CLICK IF YOU AREN'T SURE!



35

Penn State Students Self-Phishing Campaign 2018







93,593 emails sent

34,001 (36.32%) users clicked

36

OK, I FELL FOR IT
“ NOW WHAT? ”

Passwords	PSU IT	Use Caution	Delete
 Change ALL your passwords, and don't use the same one for accounts.	 There's no shame in contacting us! Call immediately to limit our risk.	 In the future, if an email seems suspicious call the sender or email them directly.	 Don't "test" the email. If you click, it may already be too late. Just delete!

37



TARODGERS@PSU.EDU

38



39
