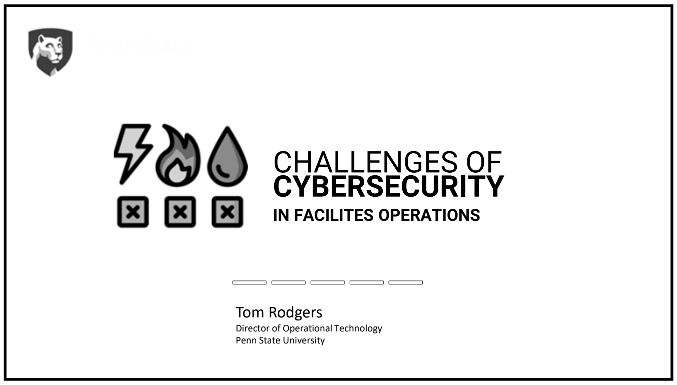
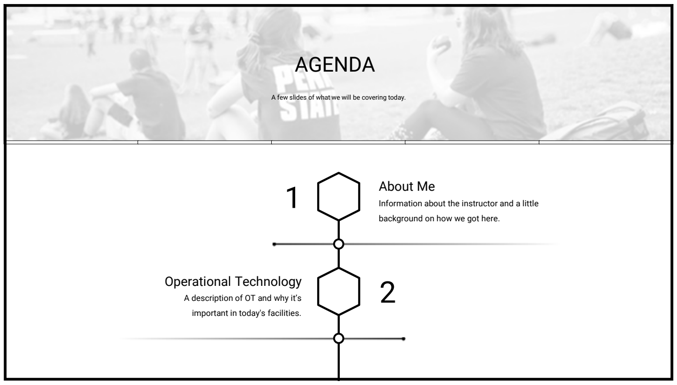


CHALLENGES OF **CYBERSECURITY**

IN FACILITES OPERATIONS

Tom Rodgers
Director of Operational Technology
Penn State University

1



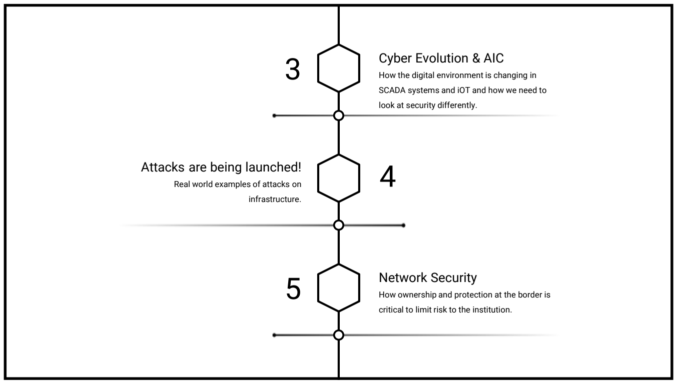
AGENDA

A few slides 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

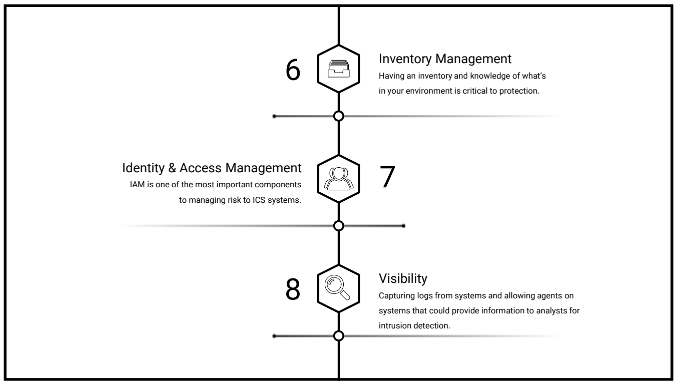


3 Cyber Evolution & AIC
How the digital environment is changing in SCADA systems and iOT and how we need to look at security differently.

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.

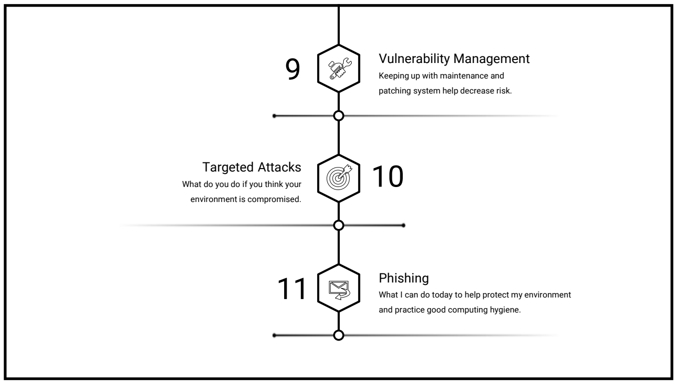
Identity & Access Management 7

IAM is one of the most important components to managing risk to ICS systems.

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 10

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
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

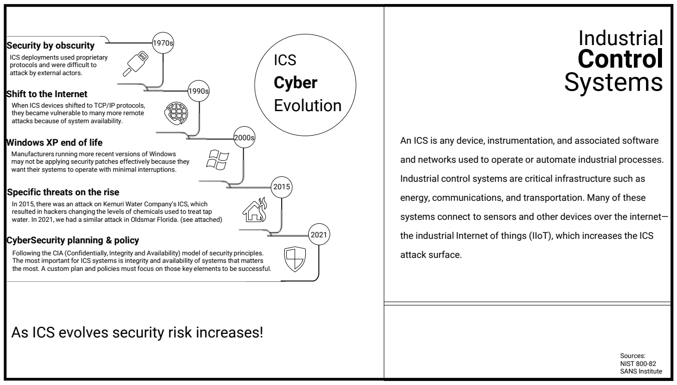
6

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



ICS **Cyber** Evolution

Security by obscurity

ICS deployments used proprietary protocols and were difficult to attack by external actors.

Shift to the Internet

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

Windows XP end of life

Manufacturers running more recent versions of Windows may not be applying security patches effectively because they want their systems to operate with minimal interruptions.

Specific threats on the rise

In 2015, there was an attack on Kemuri 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 Oldsmar Florida. (see attached)

CyberSecurity planning & policy

Following the CIA (Confidentially, Integrity and Availability) model of security principles. The most important for ICS systems is integrity and availability of systems that matters the most. A custom plan and policies must focus on those key elements to be successful.

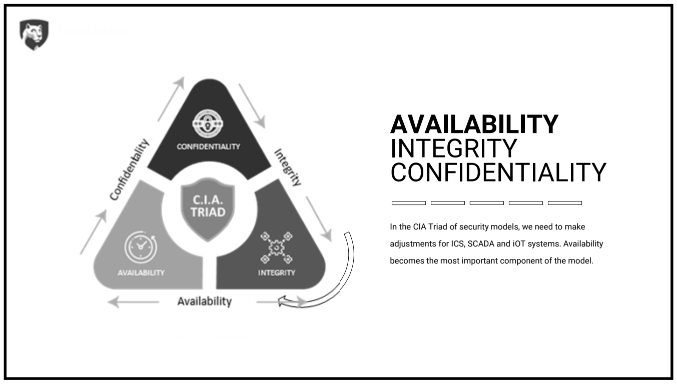
As ICS evolves security risk increases!

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.

Sources:
NIST 800-82
SANS Institute

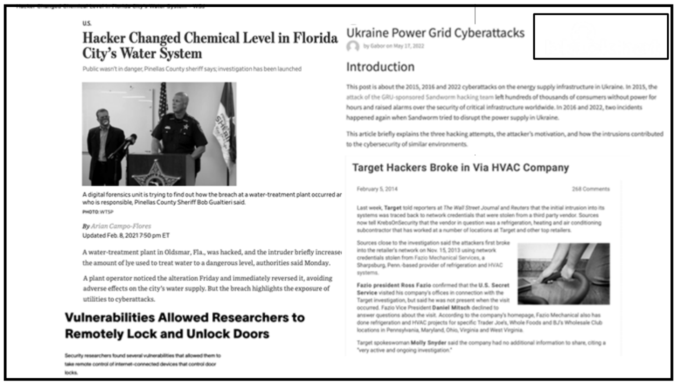
8



AVAILABILITY INTEGRITY CONFIDENTIALITY

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

9



U.S.

Hacker Changed Chemical Level in Florida City's Water System

Public wasn't in danger, Pinellas County sheriff says; investigation has been launched

A digital forensics unit is trying to find out how the breach at a water-treatment plant occurred ar who is responsible, Pinellas County Sheriff Bob Gualtieri said.

PHOTO: WTSP

By Arian Campo-Flores
Updated Feb. 8, 2021 7:50 pm ET

A water-treatment plant in Oldsmar, Fla., was hacked, and the intruder briefly increase the amount of lye used to treat water 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 take remote control of internet-connected devices that control door locks.

Ukraine Power Grid Cyberattacks

by Gabor on May 17, 2022

Introduction

This post is about the 2015, 2016 and 2022 cyberattacks on the energy supply infrastructure in Ukraine. In 2015, the attack of the GRU-sponsored Sandworm hacking team left hundreds of thousands of consumers without power for hours and raised alarms over the security of critical infrastructure worldwide. In 2016 and 2022, two incidents happened again when Sandworm tried 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 268 Comments

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Fazio president Ross Fazio confirmed that the **U.S. Secret Service** visited his company's offices in connection with the Target investigation, but said he was not present when the visit occurred. Fazio Vice President **Daniel Mitsch** declined to answer questions about the visit. According to the company's homepage, Fazio Mechanical also has done refrigeration and HVAC projects for specific Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

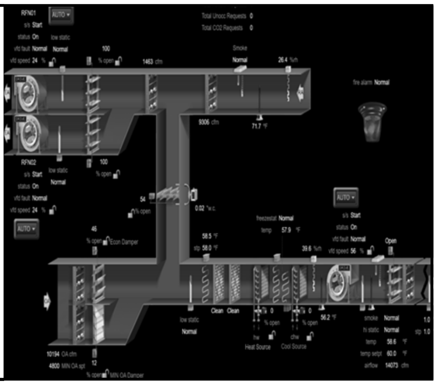
Target spokeswoman **Molly Snyder** said the company had no additional information to share, citing a "very active and ongoing investigation."

10

The **EVOLUITION** 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.

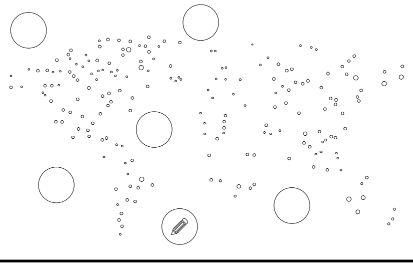


RFN01
s/s Start
status On
vfd fault Normal
vfd speed 24 %
low static Normal
100 % open
1463 cfm
Total Unocc Requests 0
Total CO2 Requests 0
Smoke Normal
26.4 %rh
fire alarm Normal
9306 cfm
71.7 °F
RFN02
s/s Start
status On
vfd fault Normal
vfd speed 24 %
low static Normal
100 % open
54 % open
0.02 "w.c.
46 % open Econ Damper
58.5 °F
stp 58.0 °F
freezestat Normal
temp 57.9 °F
39.6 %rh
s/s Start
status On
vfd fault Normal
vfd speed 56 %
Open
low static Normal
Clean Clean
0 % open hw Heat Source
0 % open chw Cool Source
56.2 °F
smoke Normal
hi static Normal
temp 58.6 °F
temp setpt 60.0 °F
airflow 14073 cfm
1.0
stp 1.0
10194 OA cfm
4800 MIN OA spt
12 % open MIN OA Damper

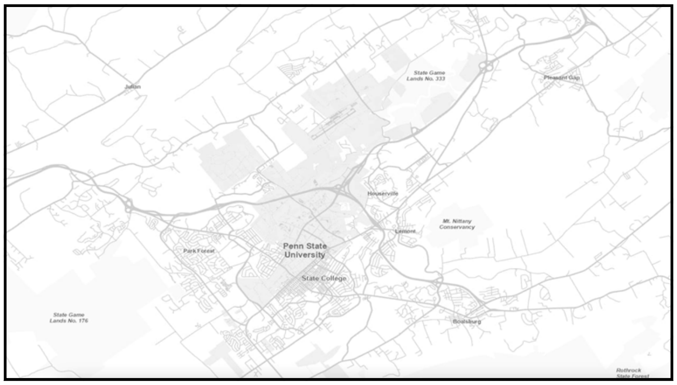
11

NETWORK SECURITY

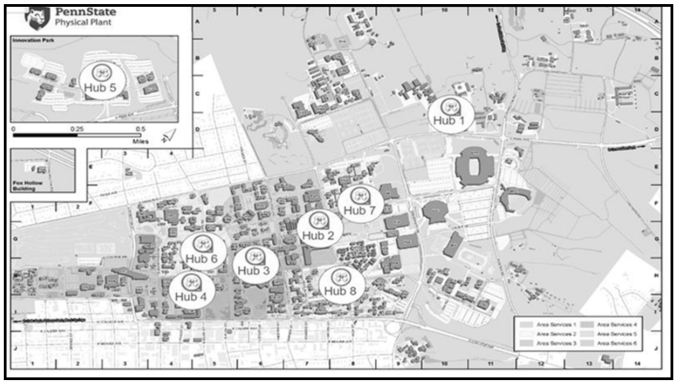
Property and facilities is very similar on how we should manage our digital environment. Many of the same principals apply in Cybersecurity!



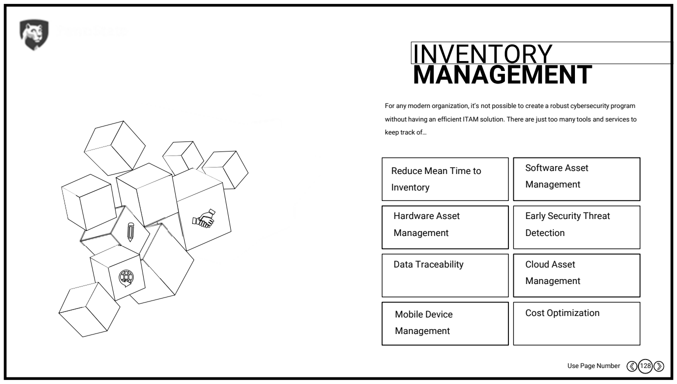
12



13



14



INVENTORY MANAGEMENT

For any modern organization, it's not possible to create a robust cybersecurity program without having an efficient ITAM solution. There 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

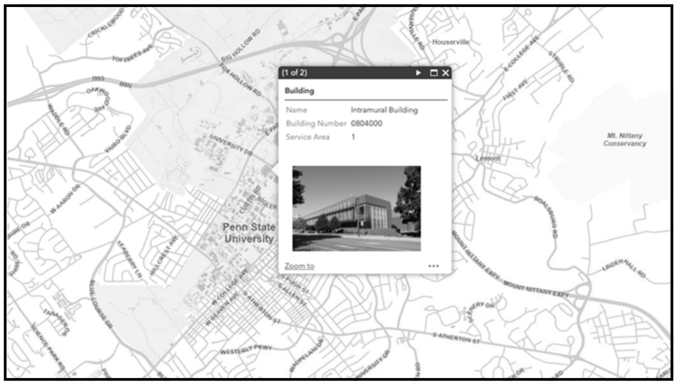
Cloud Asset Management

Mobile Device Management

Cost Optimization

Use Page Number 128

15



(1 of 2)

Building

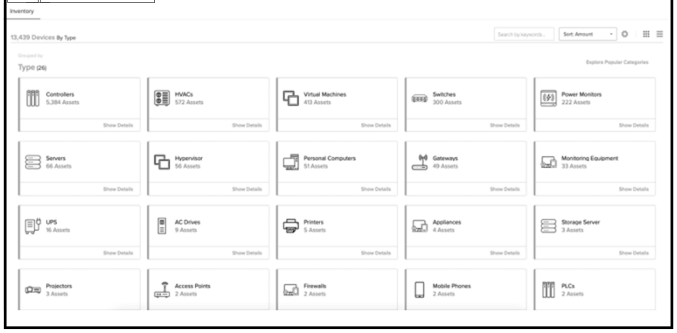
Name	Intramural Building
Building Number	0804000
Service Area	1

Zoom to

16

Look At The

INVENTORY


Inventory

13,439 Devices By Type

Grouped by

Type (26)

Controllers 5,384 Assets Show Details	HVACs 572 Assets Show Details	Virtual Machines 413 Assets Show Details	Switches 300 Assets Show Details	Power Monitors 222 Assets Show Details
Servers 66 Assets Show Details	Hypervisor 56 Assets Show Details	Personal Computers 51 Assets Show Details	Gateways 49 Assets Show Details	Monitoring Equipment 33 Assets Show Details
UPS 16 Assets Show Details	AC Drives 9 Assets Show Details	Printers 5 Assets Show Details	Appliances 4 Assets Show Details	Storage Server 3 Assets Show Details
Projectors 3 Assets	Access Points 2 Assets	Firewalls 2 Assets	Mobile Phones 2 Assets	PLCs 2 Assets

17

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.

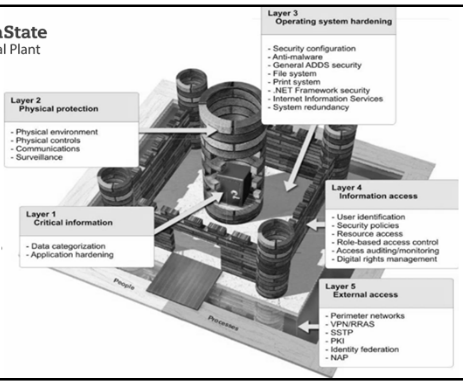
Provisioning

Multifactor Authentication (2FA)

Deprovisioning

18

PennState
Physical Plant



Layer 3
Operating system hardening

- Security configuration
- Anti-malware
- General ADDS security
- File system
- Print system
- .NET Framework security
- Internet Information Services
- System redundancy

Layer 2
Physical protection

- Physical environment
- Physical controls
- Communications
- Surveillance

Layer 4
Information access

- User identification
- Security policies
- Resource access
- Role-based access control
- Access auditing/monitoring
- Digital rights management

Layer 1
Critical information

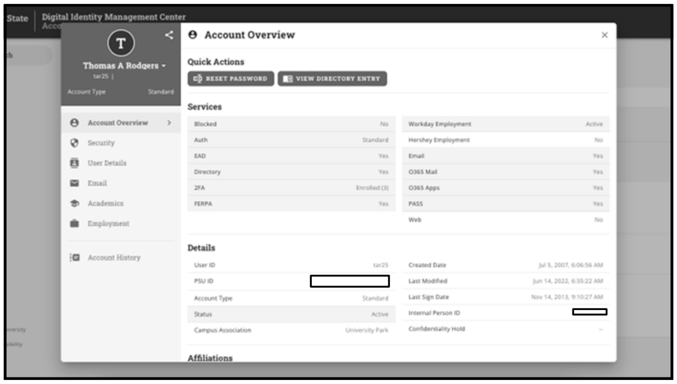
- Data categorization
- Application hardening

Layer 5
External access

- Perimeter networks
- VPN/RRAS
- SSTP
- PKI
- Identity federation
- NAP

19

20



Thomas A Rodgers
tar25 |
Account Type Standard

Account Overview

Quick Actions

Services

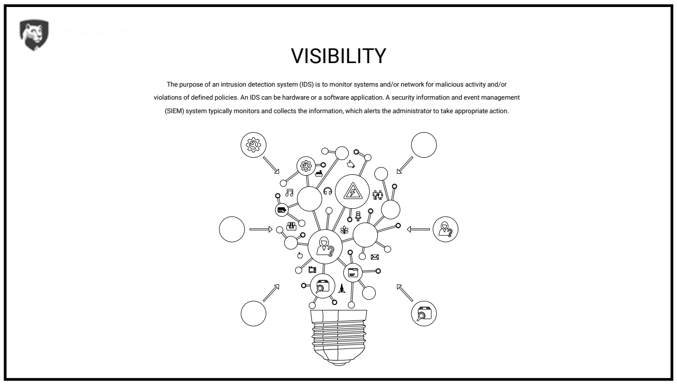
Blocked	No	Workday Employment	Active
Auth	Standard	Hershey Employment	No
EAD	Yes	Email	Yes
Directory	Yes	O365 Mail	Yes
2FA	Enrolled (3)	O365 Apps	Yes
FERPA	Yes	PASS	Yes
		Web	No

Details

User ID	tar25	Created Date	Jul 5, 2007, 6:06:56 AM
PSU ID	[redacted]	Last Modified	Jun 14, 2022, 6:35:22 AM
Account Type	Standard	Last Sign Date	Nov 14, 2013, 9:10:27 AM
Status	Active	Internal Person ID	[redacted]
Campus Association	University Park	Confidentiality Hold	--

Affiliations

21



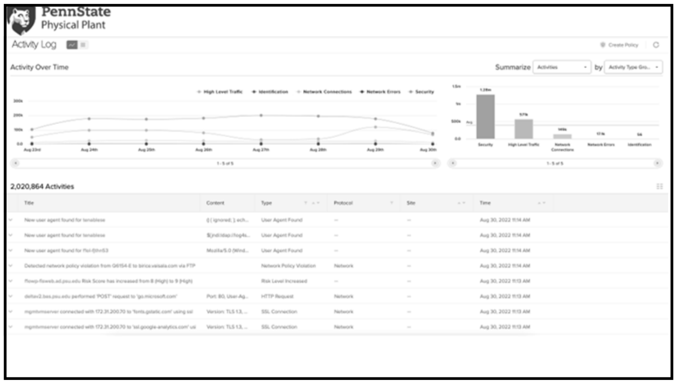
VISIBILITY

The purpose of an intrusion detection system (IDS) is to monitor systems and/or network for malicious activity and/or violations of defined policies. An IDS can be hardware or a software application. A security information and event management (SIEM) system typically monitors and collects the information, which alerts the administrator to take appropriate action.

22

Automation **vs. Analysts**

23



PennState
Physical Plant

Activity Log

Activity Over Time

Summarize Activities by Activity Type Gro...

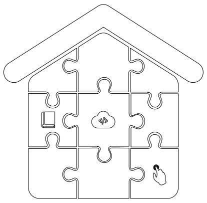
2,020,864 Activities

Title	Content	Type	Protocol	Site	Time
New user agent found for tenablese	{{ ignored; } ech...	User Agent Found	–	–	Aug 30, 2022 11:14 AM
New user agent found for tenablese	${jndi:ldap://log4s...	User Agent Found	–	–	Aug 30, 2022 11:14 AM
New user agent found for Flol-fjthn53	Mozilla/5.0 (Wind...	User Agent Found	–	–	Aug 30, 2022 11:14 AM
Detected network policy violation from G6154-E to brice.vaisala.com via FTP		Network Policy Violation	Network	–	Aug 30, 2022 11:14 AM
flowp-floweb.ad.psu.edu Risk Score has increased from 8 (High) to 9 (High)		Risk Level Increased	–	–	Aug 30, 2022 11:13 AM
deltav2.bes.psu.edu performed 'POST' request to 'go.microsoft.com'	Port: 80, User-Ag...	HTTP Request	Network	–	Aug 30, 2022 11:13 AM
mgmtvmserver connected with 172.31.200.70 to 'fonts.gstatic.com' using ssl	Version: TLS 1.3, ...	SSL Connection	Network	–	Aug 30, 2022 11:13 AM
mgmtvmserver connected with 172.31.200.70 to 'ssl.google-analytics.com' usi	Version: TLS 1.3, ...	SSL Connection	Network	–	Aug 30, 2022 11:13 AM

24

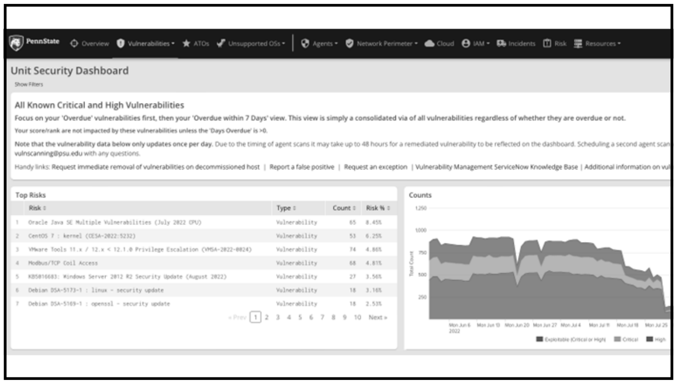
PATCHING & VULNERABLITY MANAGEMENT

The terms patch management and vulnerability management are often used interchangeably, albeit with different meanings. While patch management and vulnerability management have a compatible relationship, they are distinct processes with different goals. Patch management focuses on applying software updates to correct specific flaws or enrich the application feature sets. 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

Show Filters

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 via of all vulnerabilities regardless of whether they are overdue or not.

Your score/rank are not impacted by these vulnerabilities unless the 'Days 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
vulnscanning@psu.edu with any questions.

Handy links: Request immediate removal of vulnerabilities on decommissioned host | Report a false positive | Request an exception | Vulnerability Management ServiceNow Knowledge Base | Additional information on vul

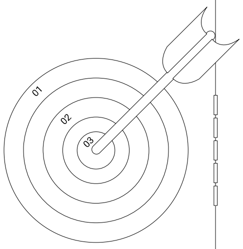
Top Risks

	Risk ⇕	Type ⇕	Count ⇕	Risk % ⇕
1	Oracle Java SE Multiple Vulnerabilities (July 2022 CPU)	Vulnerability	65	8.45%
2	CentOS 7 : kernel (CESA-2022:5232)	Vulnerability	53	6.25%
3	VMware Tools 11.x / 12.x < 12.1.0 Privilege Escalation (VMSA-2022-0024)	Vulnerability	74	4.86%
4	Modbus/TCP Coil Access	Vulnerability	68	4.81%
5	KB5016683: Windows Server 2012 R2 Security Update (August 2022)	Vulnerability	27	3.56%
6	Debian DSA-5173-1 : linux - security update	Vulnerability	18	3.16%
7	Debian DSA-5169-1 : openssl - security update	Vulnerability	18	2.53%

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Counts

27



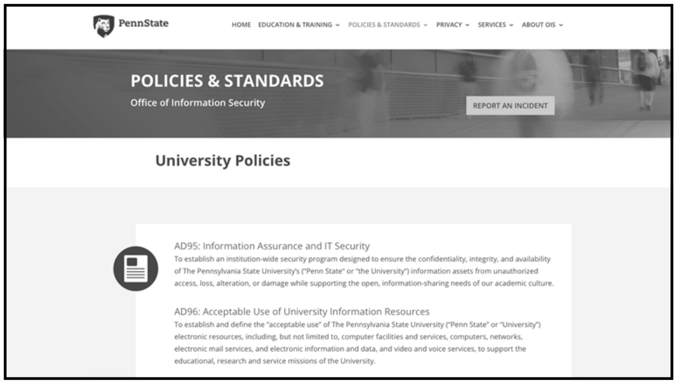
WE WERE TARGETED!

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, minimizing damage and preventing future attacks of the same type.

- Forensic Data
- Automation
- Disaster Recovery

28

29



POLICIES & STANDARDS

Office of Information Security

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

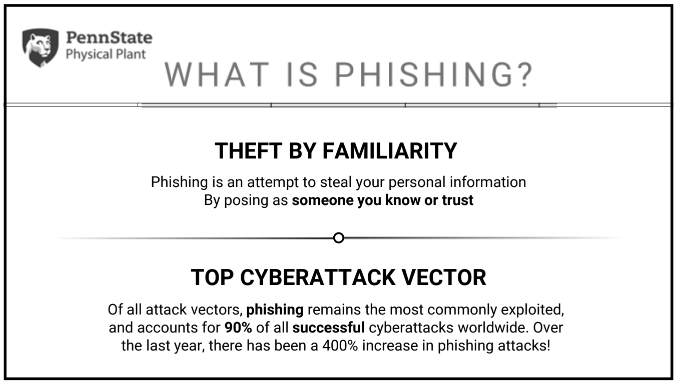
To establish and define the "acceptable use" of The Pennsylvania State University ("Penn State" or "University") electronic resources, including, but not limited to, computer facilities and services, computers, networks, electronic mail services, and electronic information and data, and video and voice services, to support the educational, research and service missions of the University.

30

PennState Physical Plant

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

31



PennState Physical Plant

WHAT IS PHISHING?

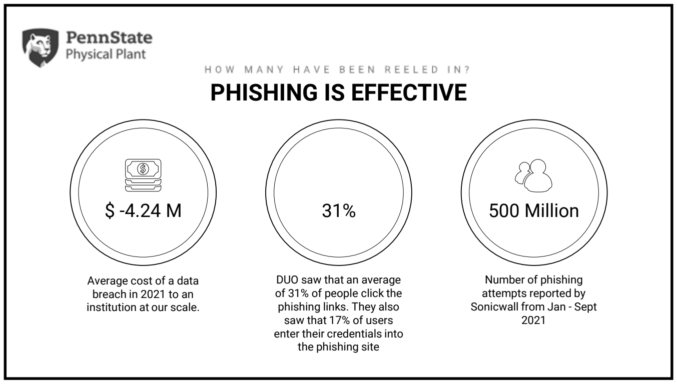
THEFT BY FAMILIARITY

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



PennState Physical Plant

HOW MANY HAVE BEEN REELED IN?

PHISHING IS EFFECTIVE

$ -4.24 M

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

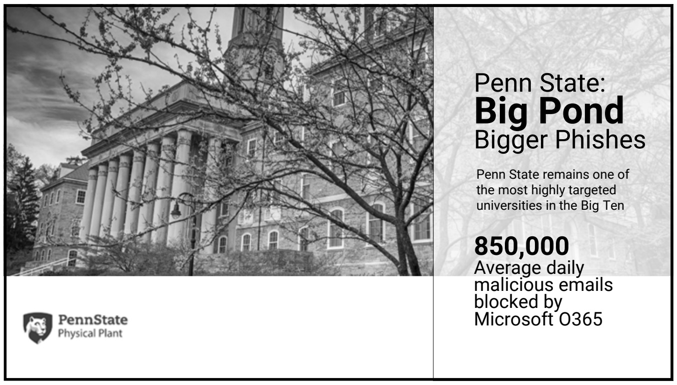
31%

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

500 Million

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

33



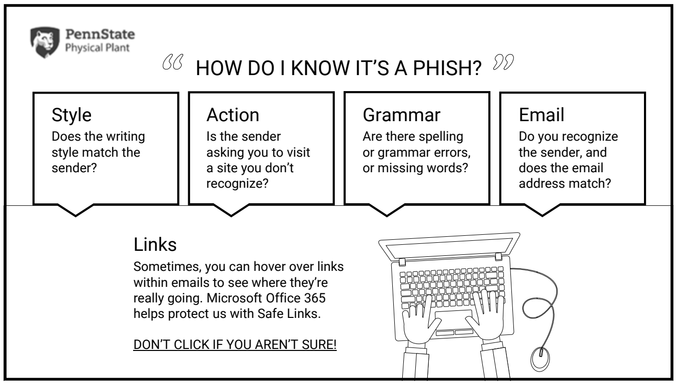
Penn State:
Big Pond
Bigger Phishes

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

850,000
Average daily malicious emails blocked by Microsoft O365

PennState Physical Plant

34



PennState Physical Plant

“ 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?

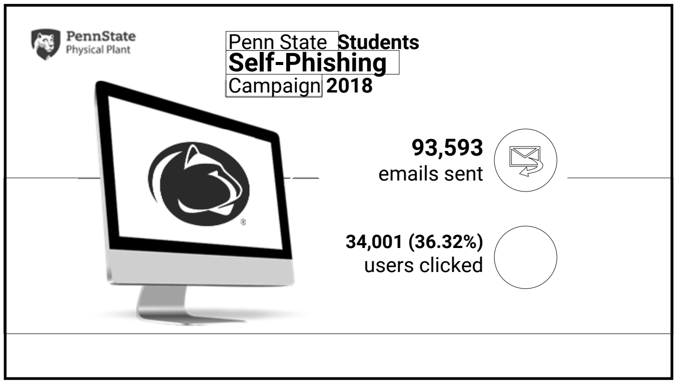
Grammar
Are there spelling or grammar errors, or missing words?

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!

35



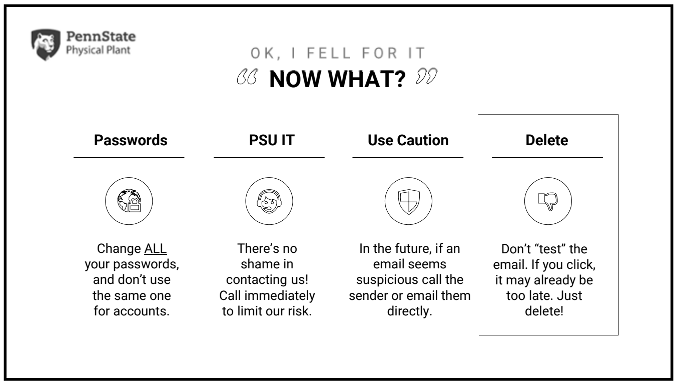
PennState Physical Plant

Penn State **Students**
Self-Phishing
Campaign **2018**

93,593
emails sent

34,001 (36.32%)
users clicked

36



PennState Physical Plant

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.

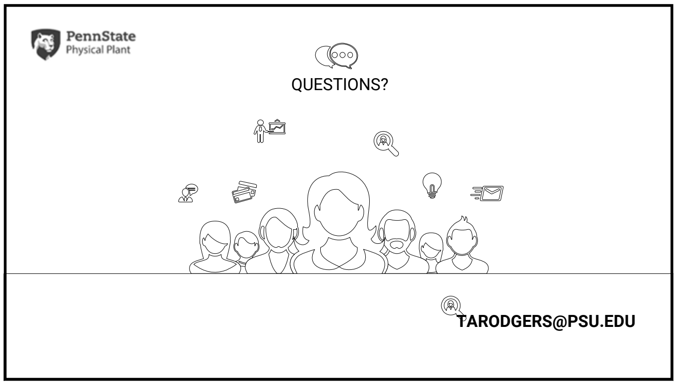
Use Caution

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!

37



PennState Physical Plant

QUESTIONS?

TARODGERS@PSU.EDU

38