

CHALLENGES OF CYBERSECURITY

IN FACILITIES OPERATIONS

Tom Rodgers
Director of Operational Technology
Penn State University

1



AGENDA

A few slides of what we will be covering today.

1



Operational Technology

A description of OT and why it's important in today's facilities.


2



About Me
Information about the instructor and a little background on how we got here.

2


3



Attacks are being launched!


Real world examples of attacks on infrastructure.

4



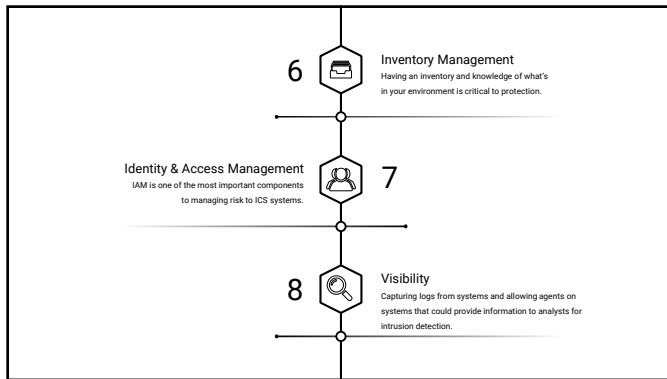
Cyber Evolution & AIC
How the digital environment is changing in SCADA systems and IOT and how we need to look at security differently.

5

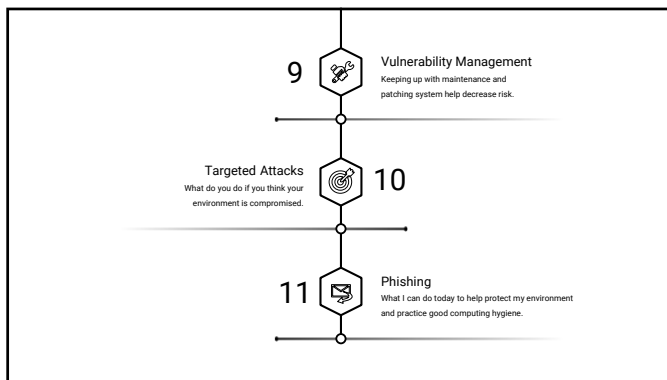


Network Security
How ownership and protection at the border is critical to limit risk to the institution.

3



4



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 W. JAGERS




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 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.

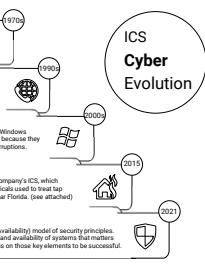
Specific threats on the rise

In 2015, there was an attack on Kenwat 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 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 that matters the most. A custom plan and policies must focus on those key elements to be successful.

ICS Cyber Evolution



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.

As ICS evolves security risk increases!

Source:
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 IIoT systems. Availability becomes the most important component of the model.

9

Hacker Changed Chemical Level in Florida City's Water System

Police wasn't in danger, Pinellas County sheriff says. Investigation has been launched.



By Adrian Campor-Flores
Updated Feb. 8, 2022 7:00 pm ET

A water-treatment plant in Oldsmar, Fla., was hacked, and the intruder briefly increased the amount of dye 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 Suben on May 17, 2022

Introduction

The goal is about the 2015, 2016 and 2022 cyberattacks on the energy supply infrastructure in Ukraine. In 2015, the attack of the GUC-sponsored Sandstorm 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 Sandstorm 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 system was traced back to network vulnerabilities that were stolen from a third-party vendor. Sources now tell InfoSecSource 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 vulnerabilities stolen from Trane Mechanical Services, a Shreveport, Penn.-based provider of refrigeration and HVAC systems.

Facis president Ross Facis 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. Facis has President Barack Obama's lockpick to answer questions about the visit. According to the company's homepage, Facis Mechanical also has done refrigeration and HVAC projects for specific Trane, York, Whalen, Trane and York Whalen Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

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

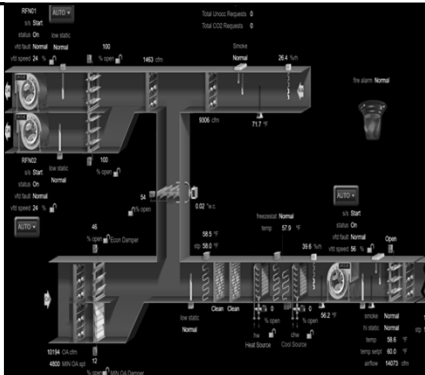
10




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.

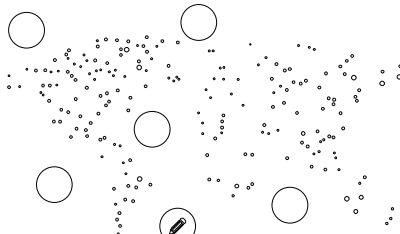


11



NETWORK SECURITY

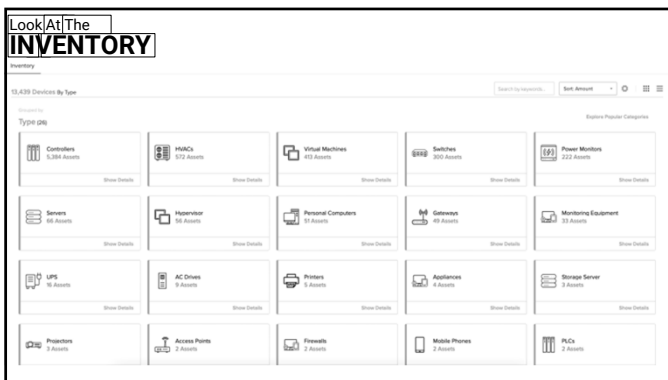
Property and facilities is very similar on how we should manage our digital environment. Many of the same principals apply in Cybersecurity!



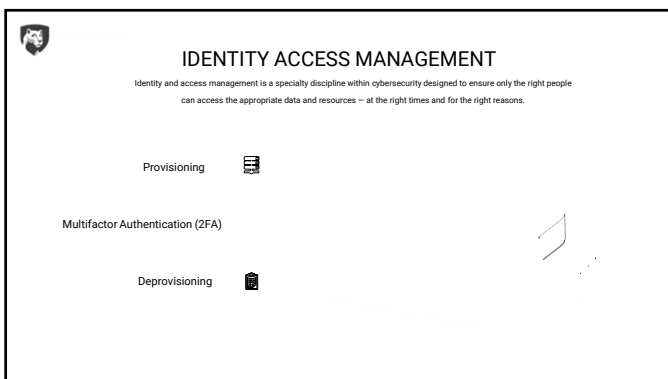
12



16




17



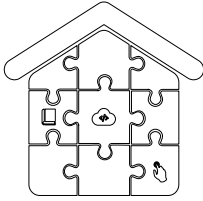
18





PATCHING & VULNERABILITY MANAGEMENT

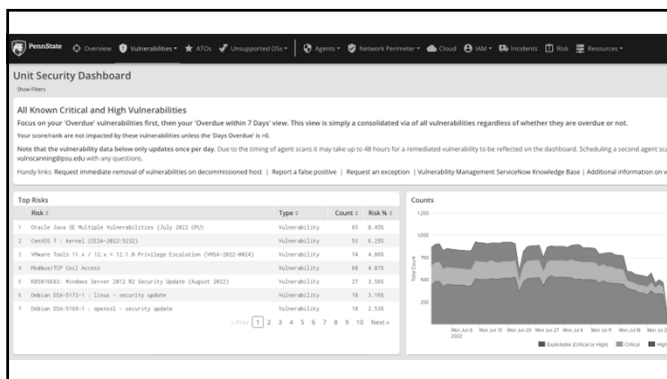
The terms patch management and vulnerability management are often used interchangeably, albeit with different meanings. While patch management and vulnerability management have a compatible relationship, they are distinct processes with different goals. Patch management focuses on applying software updates 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.



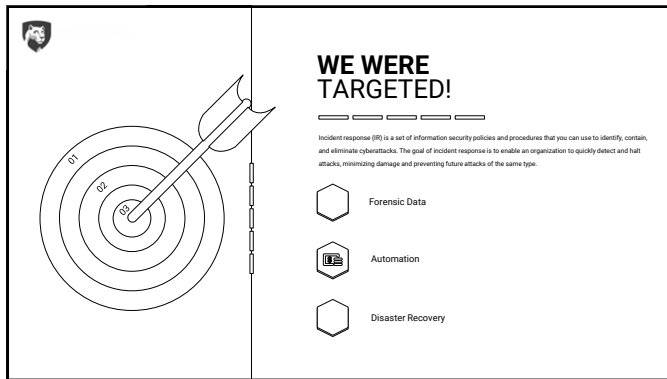
25



26



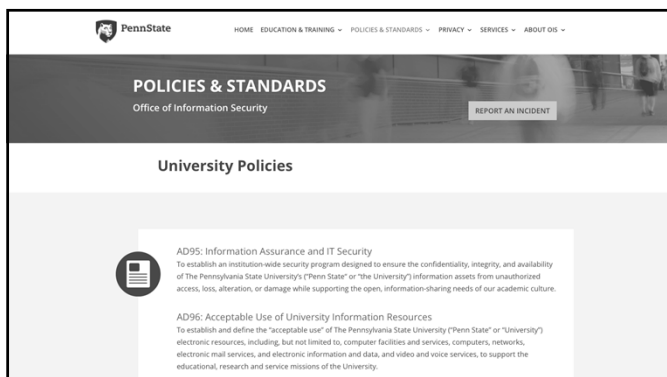
27



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

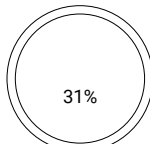


HOW MANY HAVE BEEN REELED IN?

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?


Style	Action	Grammar	Email
Does the writing style match the sender?	Is the sender asking you to visit a site you don't recognize?	Are there spelling or grammar errors, or missing words?	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




Penn State Students Self-Phishing Campaign 2018







93,593 emails sent 

34,001 (36.32%) users clicked 


36




OK, I FELL FOR IT
BB **NOW WHAT?** *DD*


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



QUESTIONS?



 **TARODGERS@PSU.EDU**

38
