United States
Department of Energy
National Nuclear Security Administration
International Nuclear Security

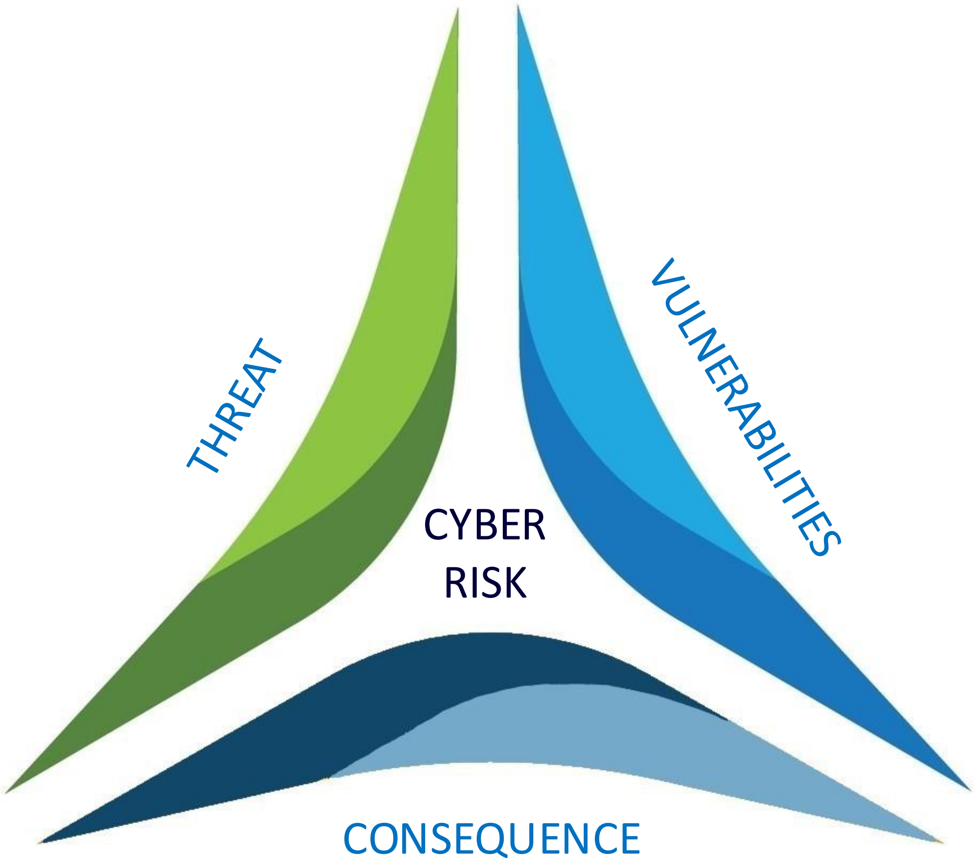
The Cyber Insider Threat

Shannon Eggers, Idaho National Laboratory

WINS International Best Practices Workshop on Mitigating Cyber Insider Threat in the Nuclear Sector
03-05 September 2024

INL/MIS-24-80002

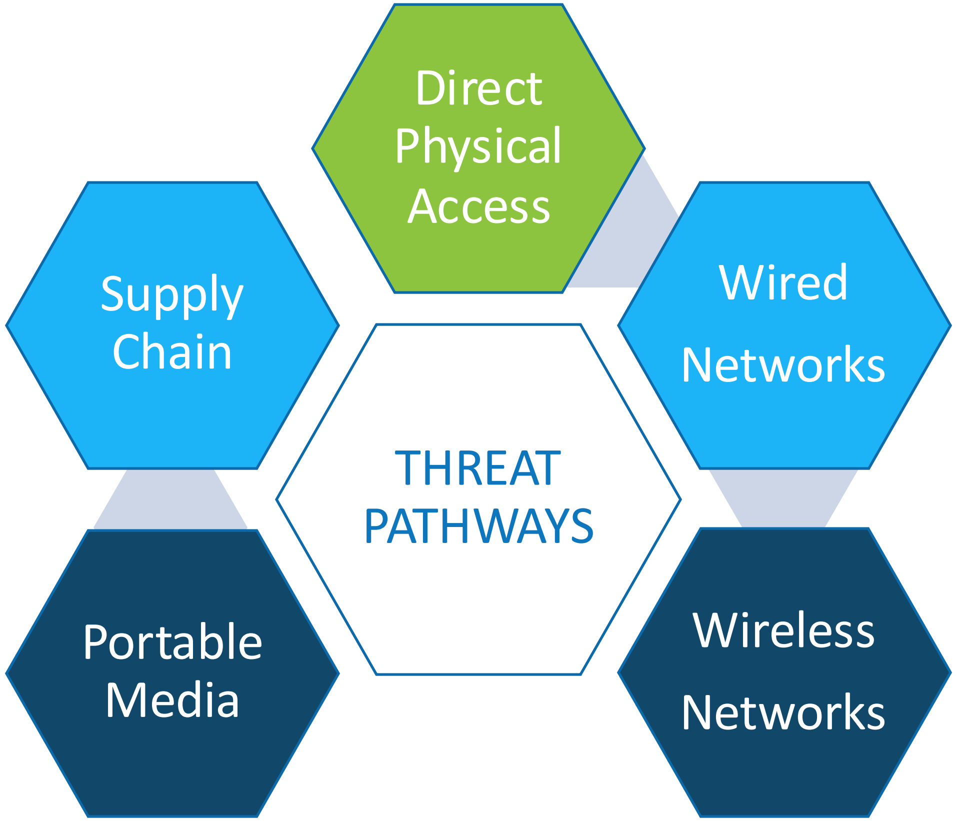
What is Cyber Risk?



CYBER RISK

The likelihood that a threat will successfully exploit a vulnerability leading to an adverse impact or consequence

CYBER THREATS



THREAT PATHWAYS

Wired networks
Wireless networks
Portable media & mobile devices
Supply chain
Direct physical access

WHERE IS THE INSIDER THREAT?

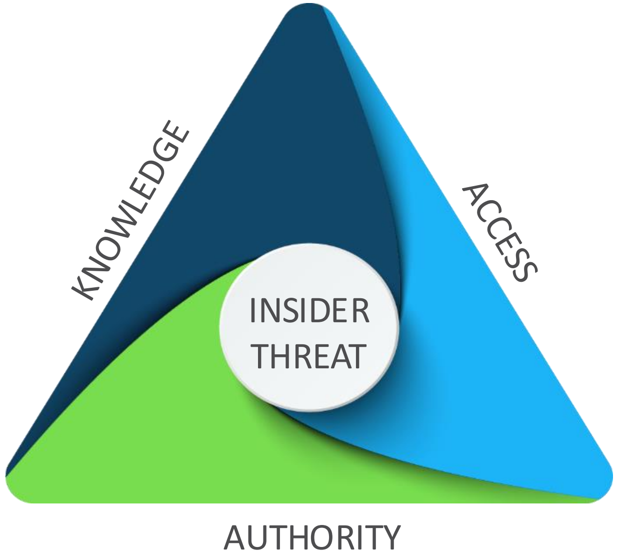
What is an Insider? (NSS 8-G, Rev. 1)

Definition:

"an individual with authorized access to [nuclear material,] associated facilities or associated activities or to sensitive information or sensitive information assets, **who could commit**, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security"

Attributes:

- Knowledge: inside knowledge of facility
- Access: authorized physical and electronic access to facility areas and computer systems
- Authority: authorization to conduct operations or direct other employees



RECRUITING INSIDERS

Finding Limits To Employee Loyalty

1 LOCKBIT RANSOMWARE

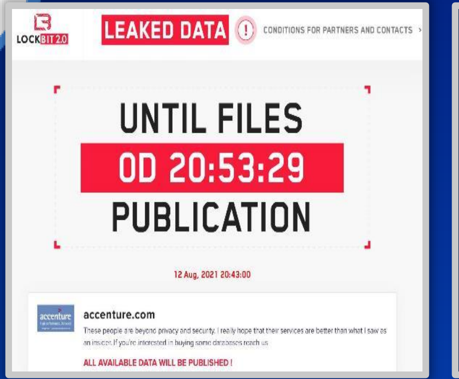
LockBit is a Ransomware-as-a-Service (RaaS) platform that uses the double extortion model. Aside from encrypting systems and data, LockBit first exfiltrates sensitive info and threatens disclosure if ransom is not paid.

2 LOCKBIT AFFILIATES

The LockBit Group sells or rents access to the LockBit RaaS platform to an affiliate or partner. The affiliate orchestrates intrusions into networks, deploys the rented ransomware, and then earns a commission from successful extortions.

3 RECRUITING AFFILIATES

On June 21, 2021, the LockBit Group initiated an affiliate recruiting campaign offering insiders $1,000,000 USD to install LockBit on "attractive systems."


LOCKBIT 2.0 LEAKED DATA CONDITIONS FOR PARTNERS AND CONTACTS ›

UNTIL FILES
0D 20:53:29
PUBLICATION

12 Aug, 2021 20:43:00

accenture.com

These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases reach us

ALL AVAILABLE DATA WILL BE PUBLISHED !

MALWARE ANALYSIS SOLUTIONS AND TECHNOLOGIES VULNERABILITIES LIST

LockBit is recruiting employees to breach corporate networks

Share

[1] BleepingComputer.com, "LockBit Ransomware Recruiting Insider To Breach Corporate Networks."

VULNERABILITIES

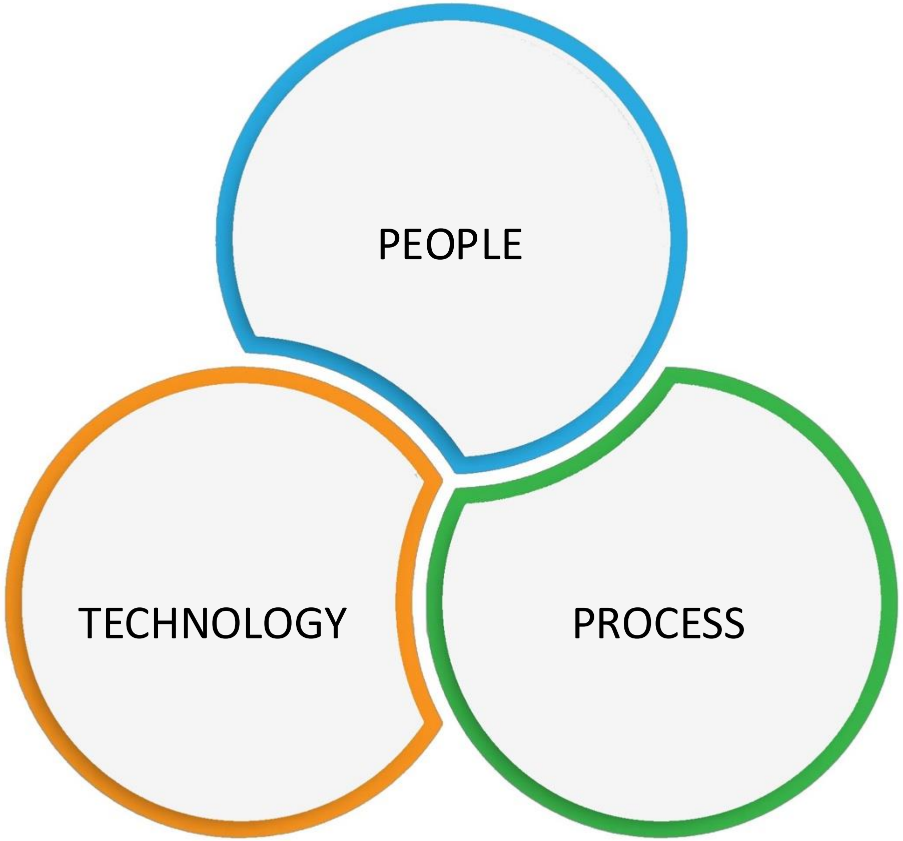
VULNERABILITY

*A weakness in **People**, Process, or Technology that can be exploited by a threat.*

UNWITTING VS. WITTING INSIDER

***Unwitting Insider:** without intent and motivation to commit malicious act who is exploited by an adversary*

***Witting Insider:** commits malicious activities with awareness, intent, and motivation*

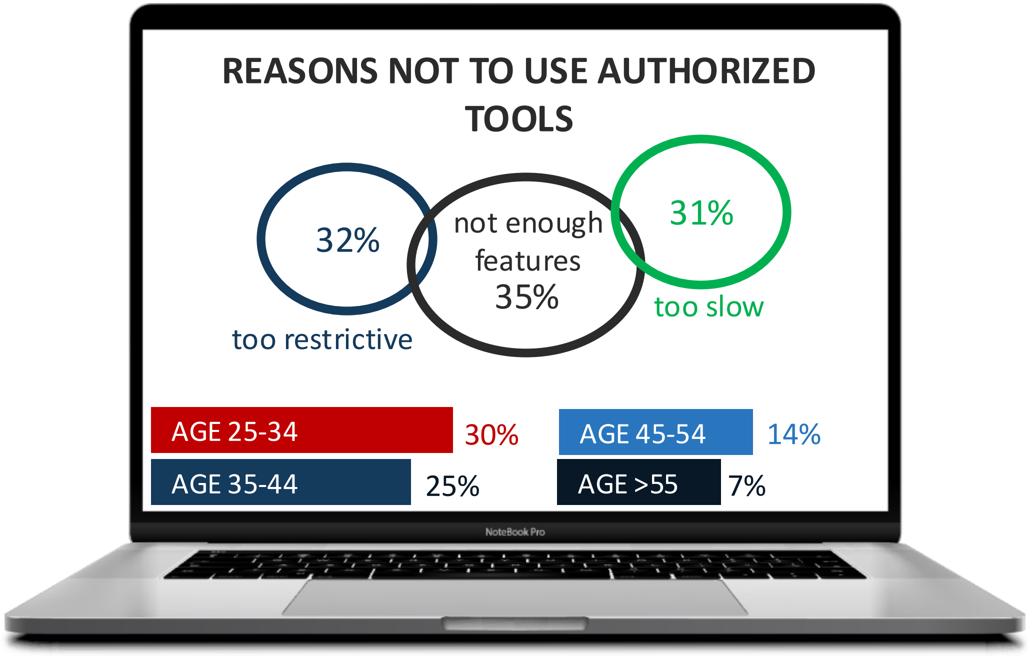


VULNERABILITIES – PEOPLE

INSIDER MOTIVATIONS

Unwitting Insiders

ANALYZING BEHAVIORS & BUILDING PROFILES



“Workers opt for unsanctioned collaboration tools” – 2020 CODE42 Data Exposure Report
https://em360tech.com/sites/default/files/2020-09/2020-Code42-DER-feb19_FINAL.pdf

DATA-USE POLICIES & TRUST

How data is created and used requires controls similar to how network access controls limit employee digital actions. Establishing these policies and monitoring compliance creates detection opportunities.

UNWITTING INSIDERS & CONFLICTING PRIORITIES

Organizational culture often puts staff in a situation where they have to choose between conflicting priorities, such as keeping their bosses happy or adhering to company security policy. This can affect you in two ways:

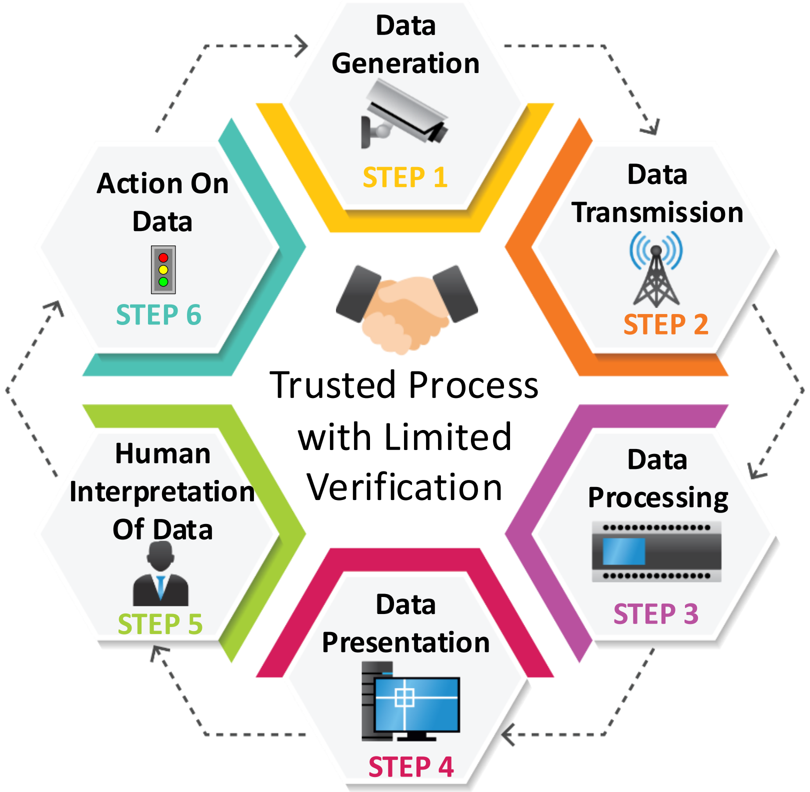
BYPASS EFFECT: To meet business objectives, employees create work-arounds to avoid frustration and missed deadlines.

ILLUSION OF SECURITY: Unaware of bypass, security leaders feel confident in policies and are blind to vulnerabilities & sidetracks investments into current insider risks.

VULNERABILITIES – PEOPLE

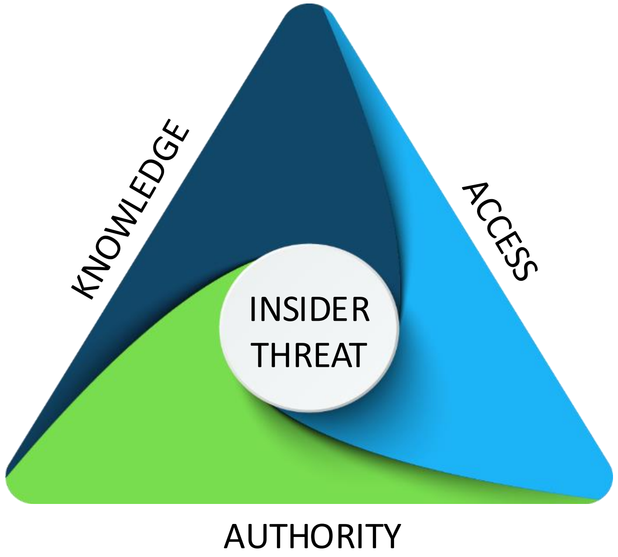
OUR BLIND SPOT

Balancing Trust With Productivity



TRUST ISSUES

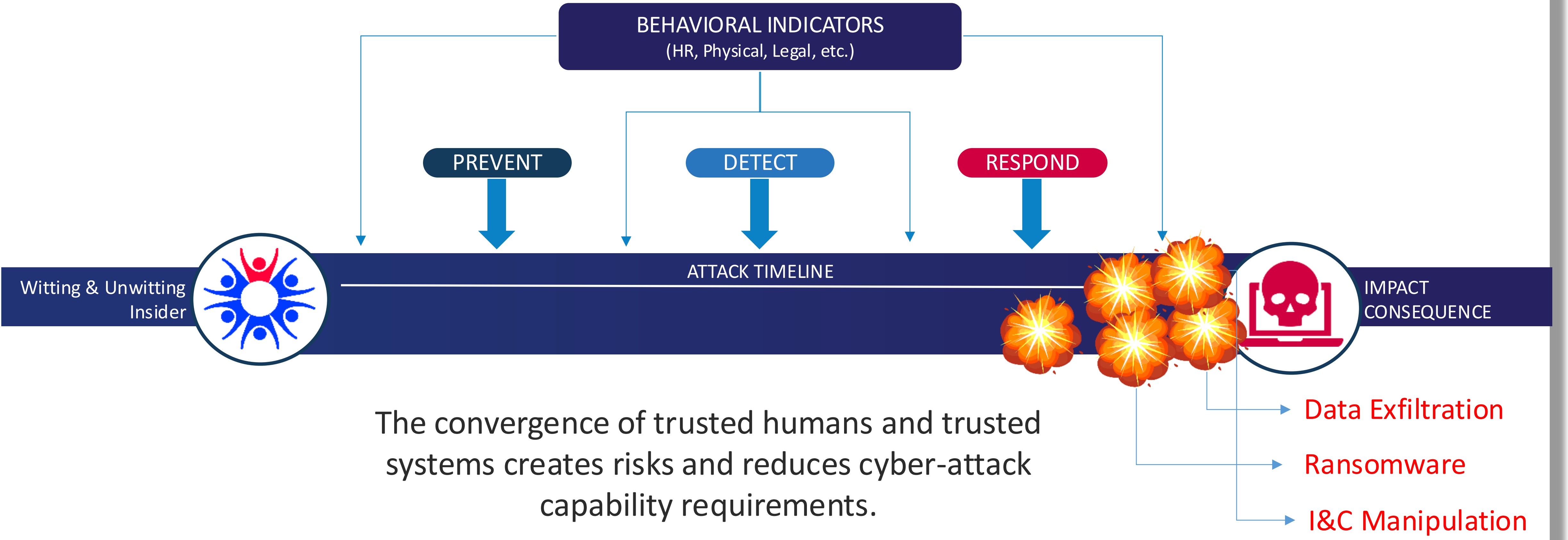
- We TRUST the Humans In the Loop through verification
- We TRUST the technology through verified design and implementation processes.
- But we inherently trust the humans to use the technology correctly.



Detection & Response Challenges

Insider Attack

Detection Comes Too Late



The convergence of trusted humans and trusted systems creates risks and reduces cyber-attack capability requirements.

Case Study 1 – Witting Insider

Water Treatment Facility

Case Study 1

1 FOOTBALL WEEKEND

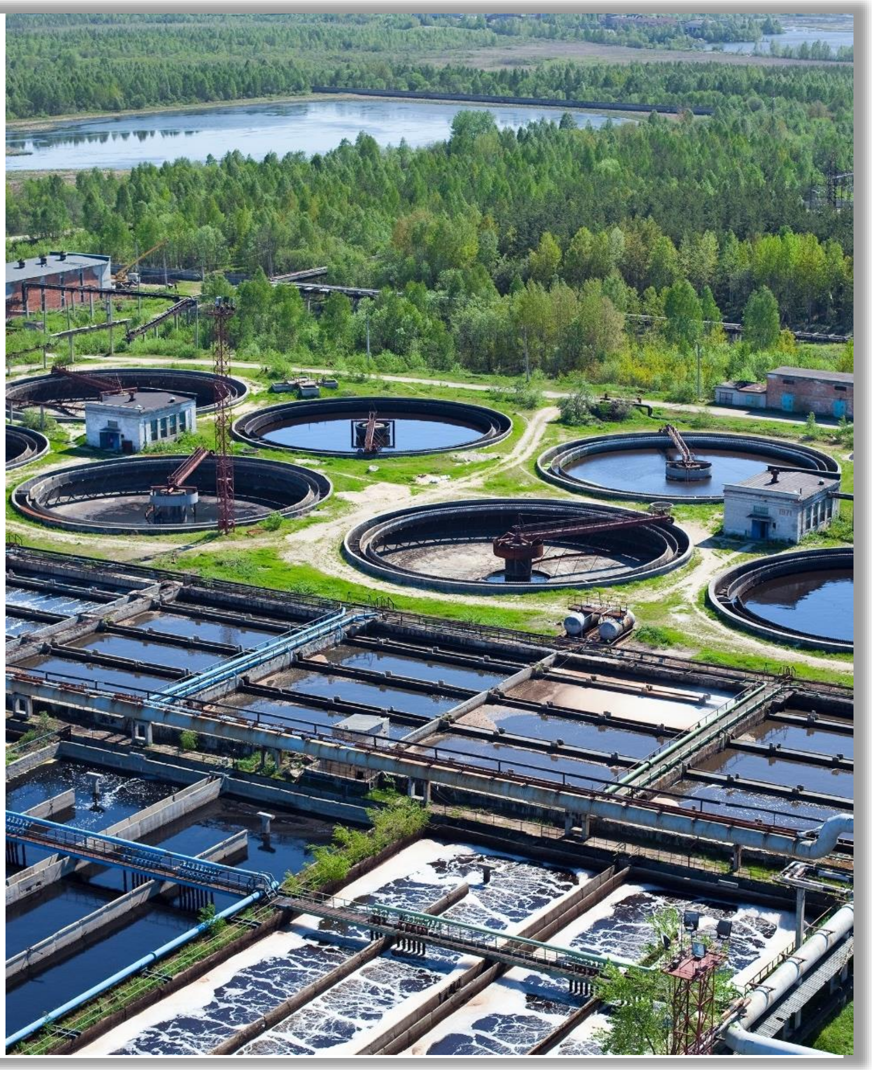
On 5 February, the city was celebrating an historic football match with a rival team. Most of the employees were not working. Only one operator was onsite.

2 CYBER INCIDENT (DEFENDER PERSPECTIVE)

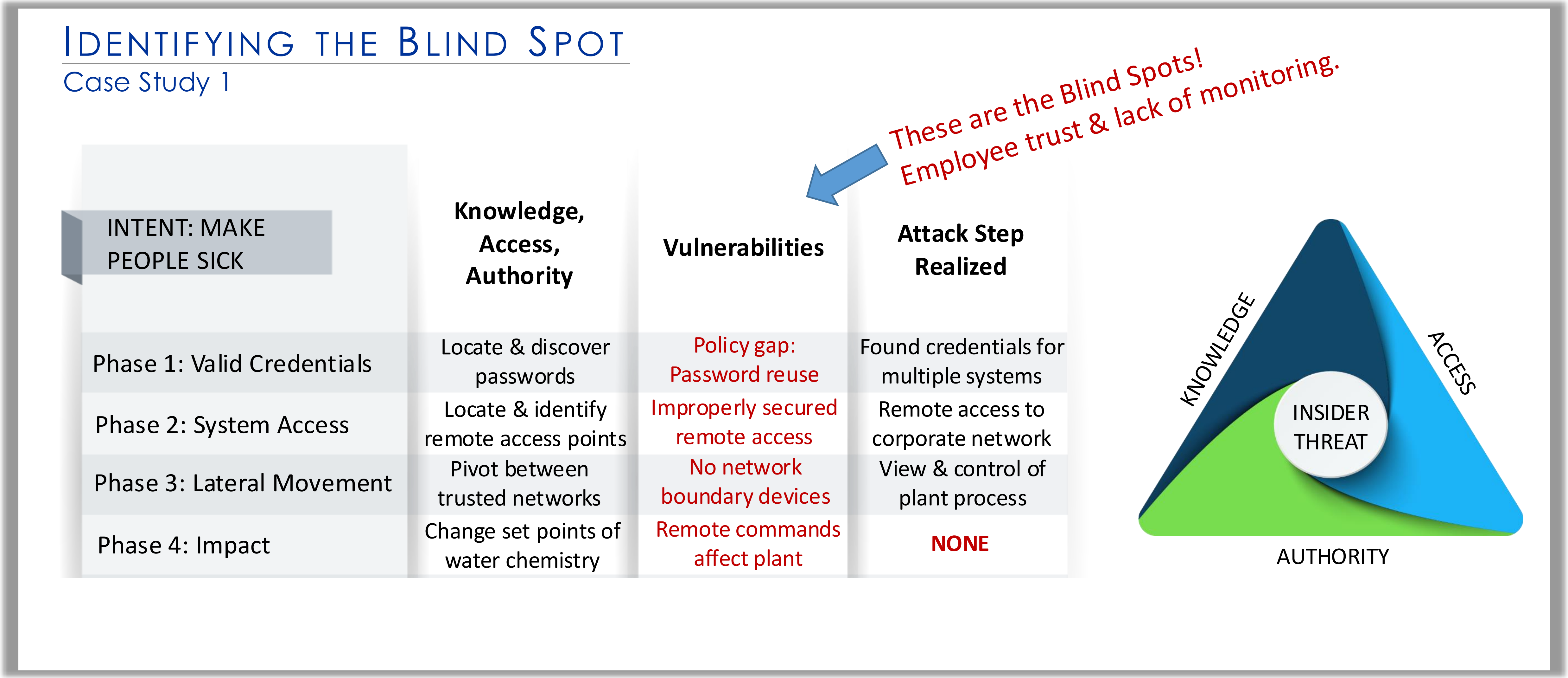
A disgruntled office employee gained remote access to the chemistry control system and increased sodium hydroxide concentrations of the water supply for the local citizens. The onsite operator noticed the mouse moving and the setting changed. While remote access to the control system was allowed, there was no prior notification when the operator noticed the abnormal operation.

3 CONSEQUENCES

Control system safety interlocks prevented the concentration change and the setting was returned to normal by the operator. If the safety system was defeated, the local population may have been poisoned.



Case Study 1 – Witting Insider



Identifying the Blind Spot

Case Study 1

These are the Blind Spots!
Employee trust & lack of monitoring.

INTENT: MAKE PEOPLE SICK	**Knowledge, Access, Authority**	**Vulnerabilities**	**Attack Step Realized**
Phase 1: Valid Credentials	Locate & discover passwords	Policy gap: Password reuse	Found credentials for multiple systems
Phase 2: System Access	Locate & identify remote access points	Improperly secured remote access	Remote access to corporate network
Phase 3: Lateral Movement	Pivot between trusted networks	No network boundary devices	View & control of plant process
Phase 4: Impact	Change set points of water chemistry	Remote commands affect plant	**NONE**

CASE STUDY 2 – UNWITTING INSIDER

Electric Grid

Case Study 2

1 HOLIDAY SEASON

There was a skeleton crew of operators working at 3 regional electric power distribution companies on 23 December 2015 due to the holiday. The power grid was built when Ukraine was part of the Soviet Union, and it was upgraded with Russian equipment.

2 CYBER INCIDENT (DEFENDER PERSPECTIVE)

Cyber attacks occurred at each company within 30 minutes of each other. Remote operation of substation breakers occurred using either remote administration tools or remote ICS software via VPN. The actors gained legitimate credentials through phishing emails infected with BlackEnergy malware.

3 CONSEQUENCES

There were widespread power outages in Western Ukraine with 225,000 customers losing power for many hours. The KillDisk malware rendered multiple systems inoperable at the end of the attack.

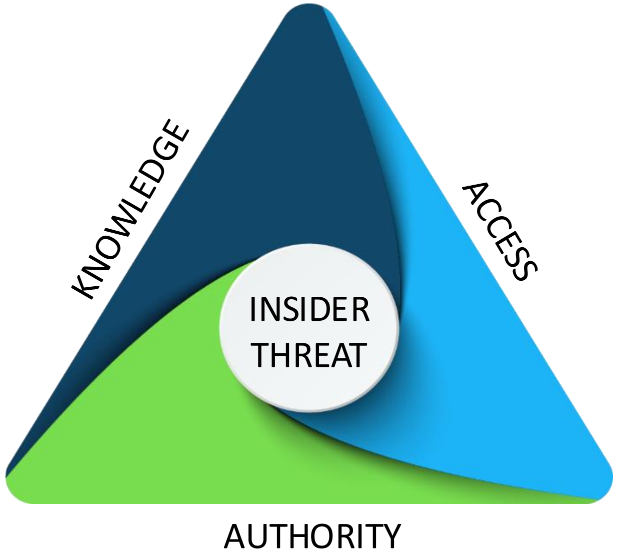
Case Study 2 – Unwitting Insider

Identifying the Blind Spot

Case Study 2

These are the Blind Spots! Employee trust, lack of monitoring, and supply chain insider.

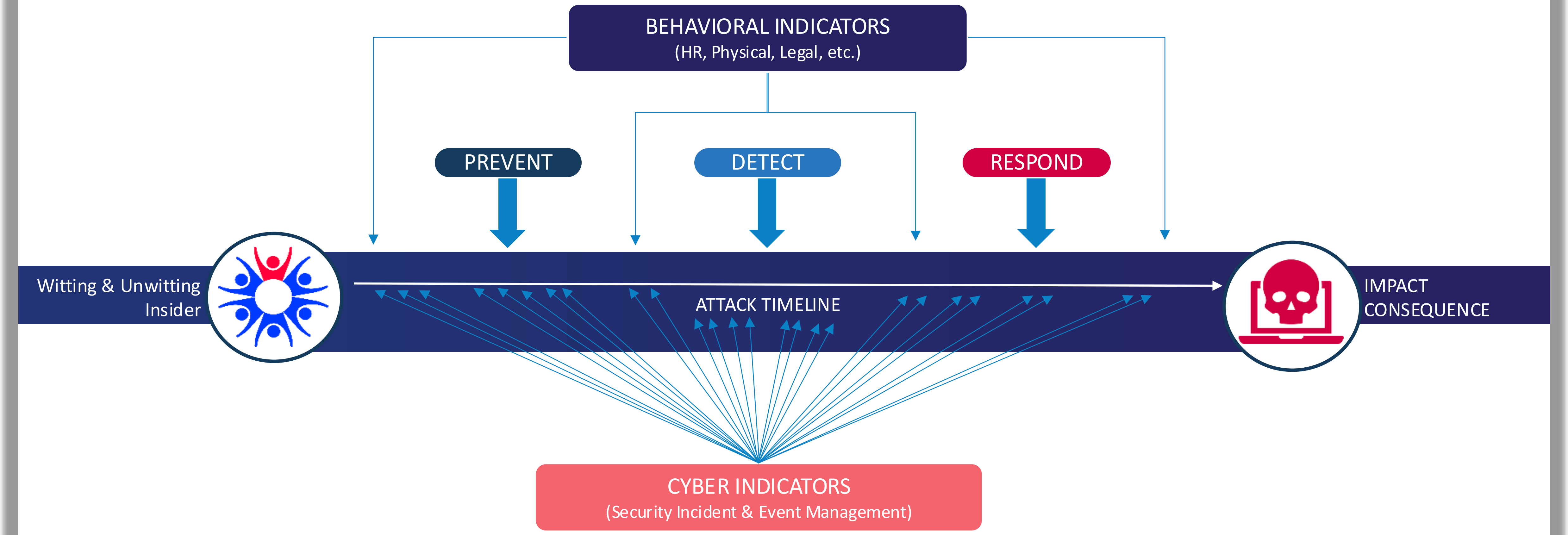
INTENT: Loss of electric grid	**Knowledge, Access, Authority**	**Vulnerabilities**	**Attack Step Realized**
Phase 1: Valid Credentials	Locate & discover passwords	Policy gap: Phishing awareness	Found valid credentials
Phase 2: System Access	Locate & identify remote access points	Improperly secured remote access	Remote access to corporate network
Phase 3: Lateral Movement	Pivot between trusted networks	No network boundary devices	View & control of SCADA
Phase 4: Impact	Open breakers at substations	Remote commands affect SCADA	**225,000 customers lose power**



Integrating Cyber With Insider Programs

Increasing Visibility

Balancing Trust With Monitoring



BEHAVIORAL INDICATORS

(HR, Physical, Legal, etc.)

PREVENT

DETECT

RESPOND

Witting & Unwitting Insider

ATTACK TIMELINE

IMPACT CONSEQUENCE

CYBER INDICATORS

(Security Incident & Event Management)

What Can we Do?

Measures Against the Insider Threat

Consider the Insider Threat in Cybersecurity Programs

Prevent

- Develop & implement a cybersecurity program
- Secure architecture
- Boundary devices
- Establish access controls
- Limit remote access
- Enforce separation of duties
- Establish IT policies
- Data Loss Prevention (DLP) practices
- Use data masking or anonymization

Detect

- Characterize, monitor, and audit networks & hosts for anomalies
- Implement cyber intrusion detection systems
- Monitor remote access
- Implement behavior monitoring tools
- Use a Security Information and Event Management (SIEM) system
- Establish rule-based alerting

Respond

- Develop & practice incident response and contingency plans
- Maintain digital asset configurations in secure location
- Keep digital asset and data backups in secure location

INS International Nuclear Security

Reducing Risk of Nuclear Terrorism