Cyber Insider Threat

Rodney Busquim | R.Busquim@iaea.org

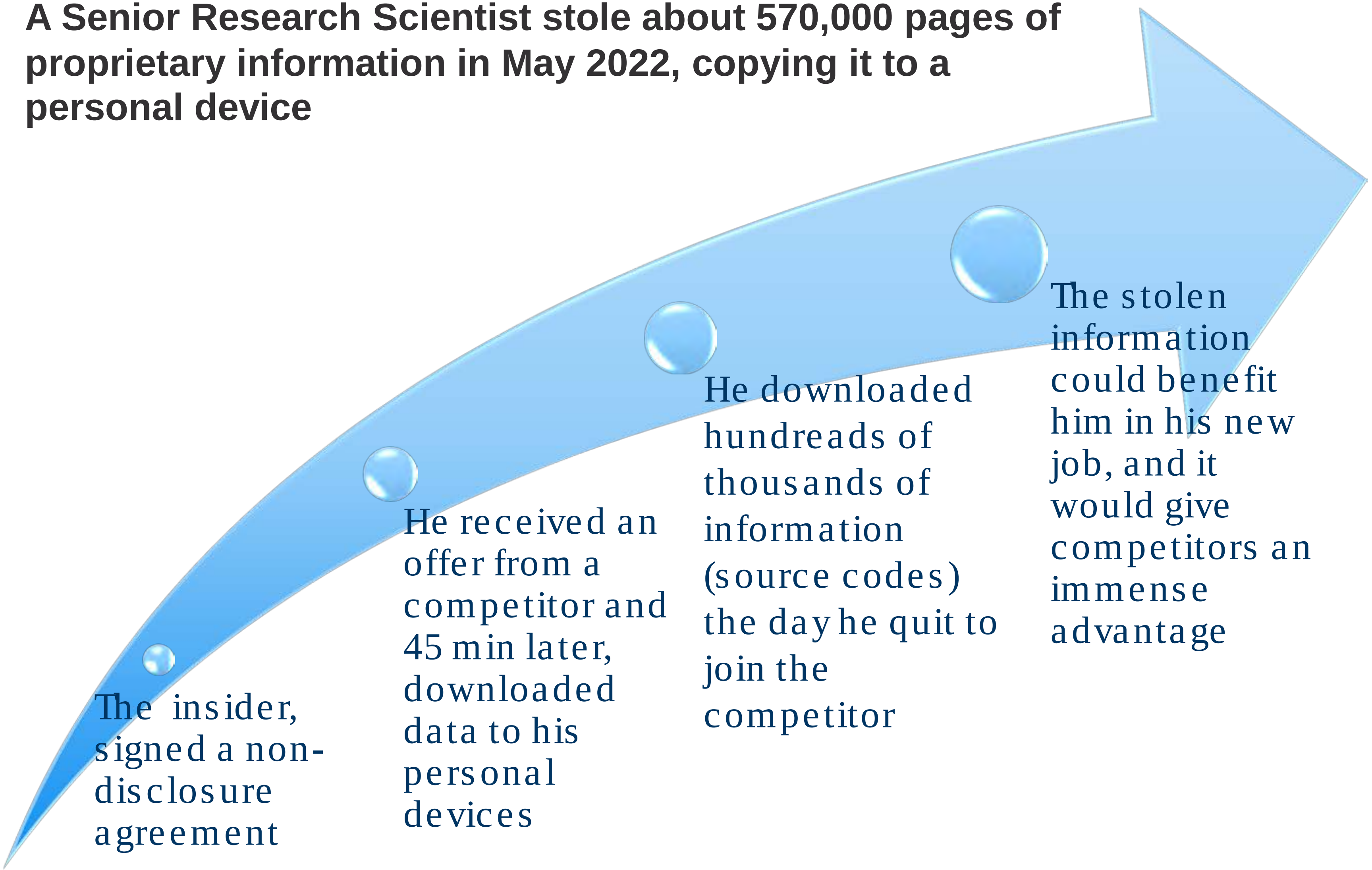
Angela Lousteau | A.Lousteau@iaea.org

Division of Nuclear Security | International Atomic Energy Agency

03 September 2024

Could this Happen to your Organization?

A Senior Research Scientist stole about 570,000 pages of proprietary information in May 2022, copying it to a personal device

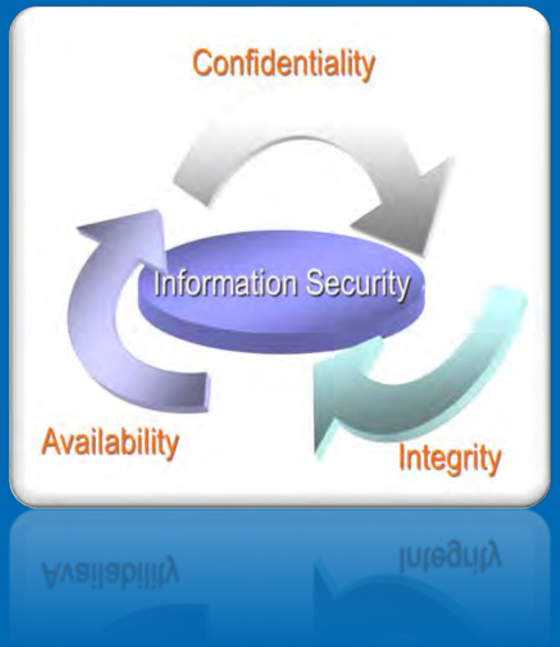


The insider, signed a non-disclosure agreement

He received an offer from a competitor and 45 min later, downloaded data to his personal devices

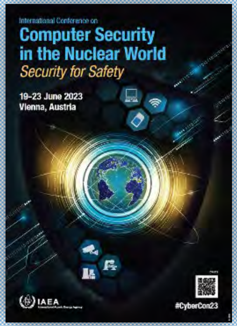
He downloaded hundreads of thousands of information (source codes) the day he quit to join the competitor

The stolen information could benefit him in his new job, and it would give competitors an immense advantage



IAEA Division of Nuclear Security (NSNS)

It provides Member States assistance to raise awareness of the threat of cyber-attacks, and their potential impact on nuclear security


International Conference on
Computer Security in the Nuclear World
Security for Safety
19–23 June 2023
Vienna, Austria
IAEA
#CyberCon23

IAEA Computer Security Activities

NSNS raises computer security awareness by:

- Developing appropriated guidance
- Providing Computer Security training courses, exercises, demonstration and workshops
- Bringing together experts to promote the exchange of information and experiences
- Coordinating computer security and insider threat-related research projects

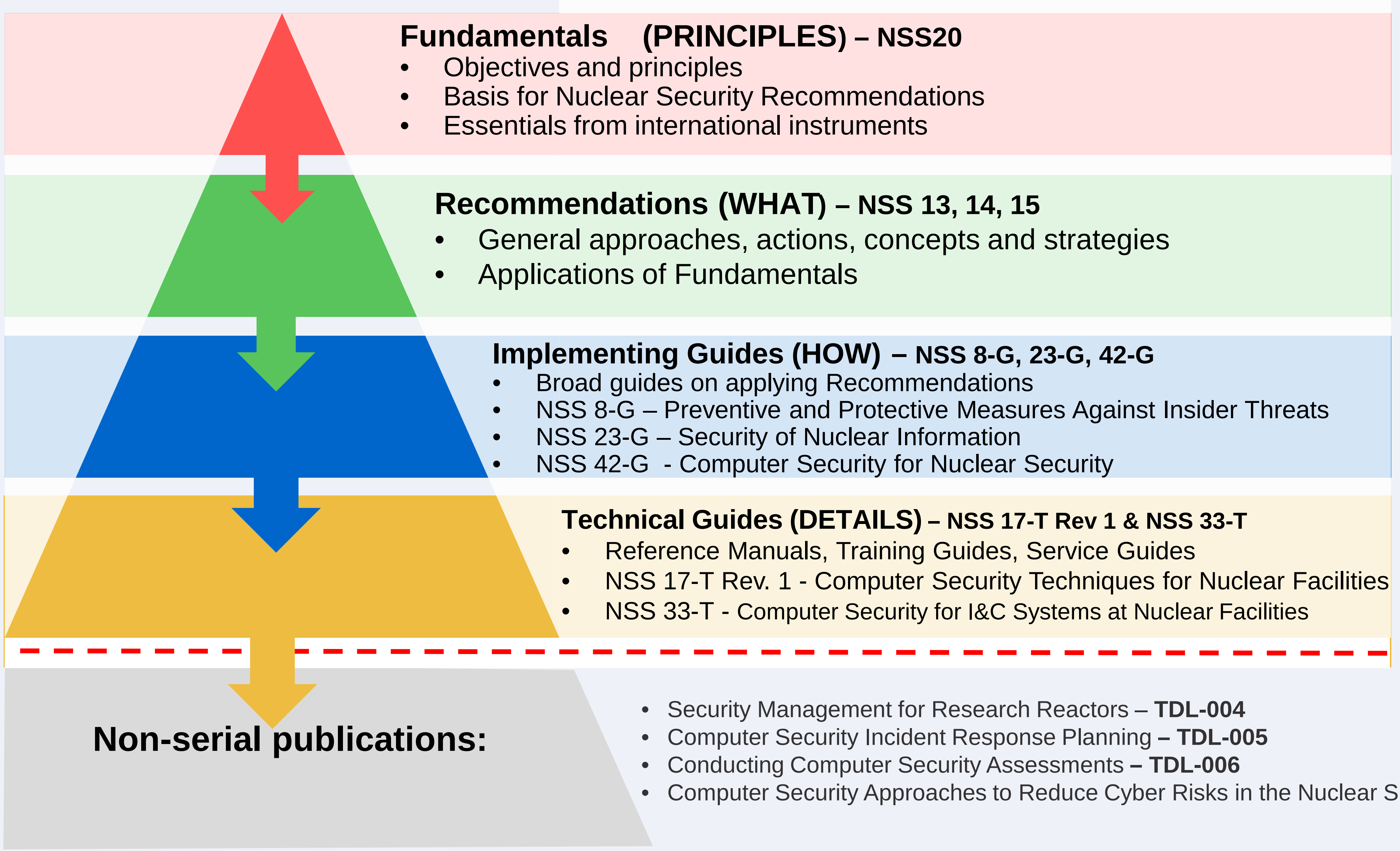
IAEA
Introduction to and overview of IAEA Nuclear Security Series Publications

IAEA
Overview of nuclear security threats and ris

IAEA
Radiation Basics and Consequences of Exposure to Radiation

IAEA
Categorization of radioactive sources

Nuclear Security Series (NSS) Publications



Fundamentals (PRINCIPLES) – NSS20

- Objectives and principles
- Basis for Nuclear Security Recommendations
- Essentials from international instruments

Recommendations (WHAT) – NSS 13, 14, 15

- General approaches, actions, concepts and strategies
- Applications of Fundamentals

Implementing Guides (HOW) – NSS 8-G, 23-G, 42-G

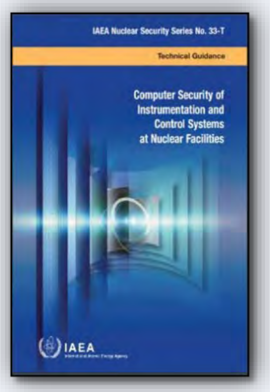
- Broad guides on applying Recommendations
- NSS 8-G – Preventive and Protective Measures Against Insider Threats
- NSS 23-G – Security of Nuclear Information
- NSS 42-G - Computer Security for Nuclear Security

Technical Guides (DETAILS) – NSS 17-T Rev 1 & NSS 33-T

- Reference Manuals, Training Guides, Service Guides
- NSS 17-T Rev. 1 - Computer Security Techniques for Nuclear Facilities
- NSS 33-T - Computer Security for I&C Systems at Nuclear Facilities

Non-serial publications:

- Security Management for Research Reactors – **TDL-004**
- Computer Security Incident Response Planning **– TDL-005**
- Conducting Computer Security Assessments **– TDL-006**
- Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain **– TDL-011**



IAEA Nuclear Security Series No. 33-T

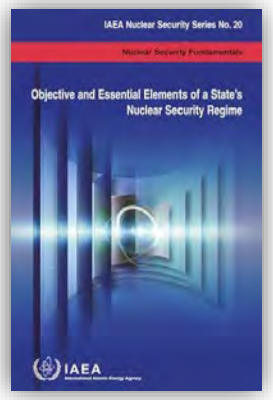
Technical Guidance

Computer Security of Instrumentation and Control Systems at Nuclear Facilities

IAEA

Cyber Insiders are not Different from other Insiders

- Motivations: ideological, financial, coercion, psychological/mental health issues, disgruntled employee, ego, revenge or embarrassment etc.
- Access, authority, and knowledge give cyber insiders unique opportunities to conduct or facilitate malicious acts
- NSS No. 20 Objective and Essential Elements of a State's Nuclear Security Regime provides a definition of insider that considers sensitive information or sensitive information assets.



IAEA Nuclear Security Series No. 20

Nuclear Security Fundamentals

Objective and Essential Elements of a State's Nuclear Security Regime

IAEA

International Atomic Energy Agency

An individual with authorized access to 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.

NSS No. 20

What Capabilities does the Cyber Insider Adversary Need?

- To access the target
  - ✓ Physical access or remote access
  - ✓ Remember, their perception of the target may differ from yours!
- To manipulate target systems
  - ✓ Perhaps technical ability
  - ✓ Perhaps external assistance
- To exfiltrate their data or develop their attack
- Also may need:
  - ✓ Equipment (e.g. electronic access to physical protection systems, NMAC systems, safety systems, process systems, control of access systems, building management systems, personnel systems)
  - ✓ An exfiltration route for data (sometimes)

Image Credit: Shutterstock 211208341

Cyber Insider Advantages

- **Computer-based environment**
  - ✓ Cyber attacks or other computer based actions might not be as readily observable
- **Time**
  - ✓ Can extend acts over long periods of time if not detected – years sometimes
  - ✓ Can infect back-up data with malicious software
  - ✓ Can complete a strategic goal within significantly shortened timelines, depending on the scenario type
- **Tools**
  - ✓ Might be able to create remote access
  - ✓ Might be able to manipulate critical code onsite or offsite via remote access
  - ✓ Can automate attacks so that the insider adversary does not have to be present
- **Tests**
  - ✓ Can test the system with normal "mistakes" and then delete evidence
- **Sequence of actions**
  - ✓ Can automate sequences of actions
- **Collusion**
  - ✓ Might collude (work together) with others (either insiders or external adversaries)

Image Credit: Shutterstock 75543914

Potential for Malicious Acts by Cyber Insider

- In cybersecurity, the unwitting adversary is a major concern

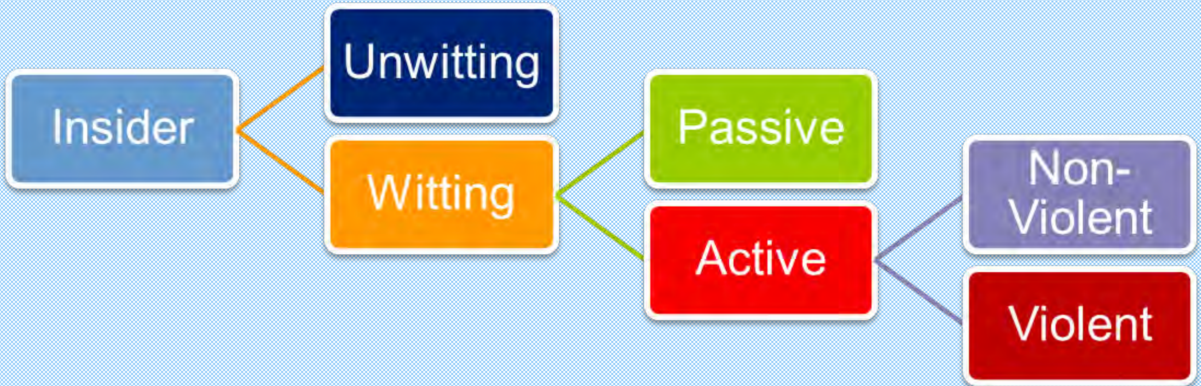
- An insider may not be aware that they are providing information or authenticated access to an adversary, and is therefore unaware of their involvement in a cyber-attack

Image Credit: Shutterstock 1315776704

Examples of Unwitting Cyber Insiders Actions

- Following instructions of a social engineer
- Visiting a malicious website
- Providing a password to someone calling pretending to be an administrator
- Opening a malicious email attachment
- Connecting an unknown thumb drive
- Sharing sensitive network information
- Sharing information about operational technology systems
- Accessing open wireless network using corporative laptop

Image Credit: Shutterstock 2238412723


Insider

Unwitting

Witting

Passive

Active

Non-Violent

Violent

Example: Electric Utility

- In 2012, a power company reported a virus infection in a turbine control system that impacted approximately ten computers on its control system network
- Analysis of the incident revealed that a third-party technician had used a USB drive to upload software updates during a scheduled outage for equipment upgrades
- Unknown to the technician, the USB drive was infected with a variant of the Mariposa botnet virus, which moved from machine to machine on the local network
- The infection resulted in downtime for the impacted systems and delayed the plant restart by approximately three weeks

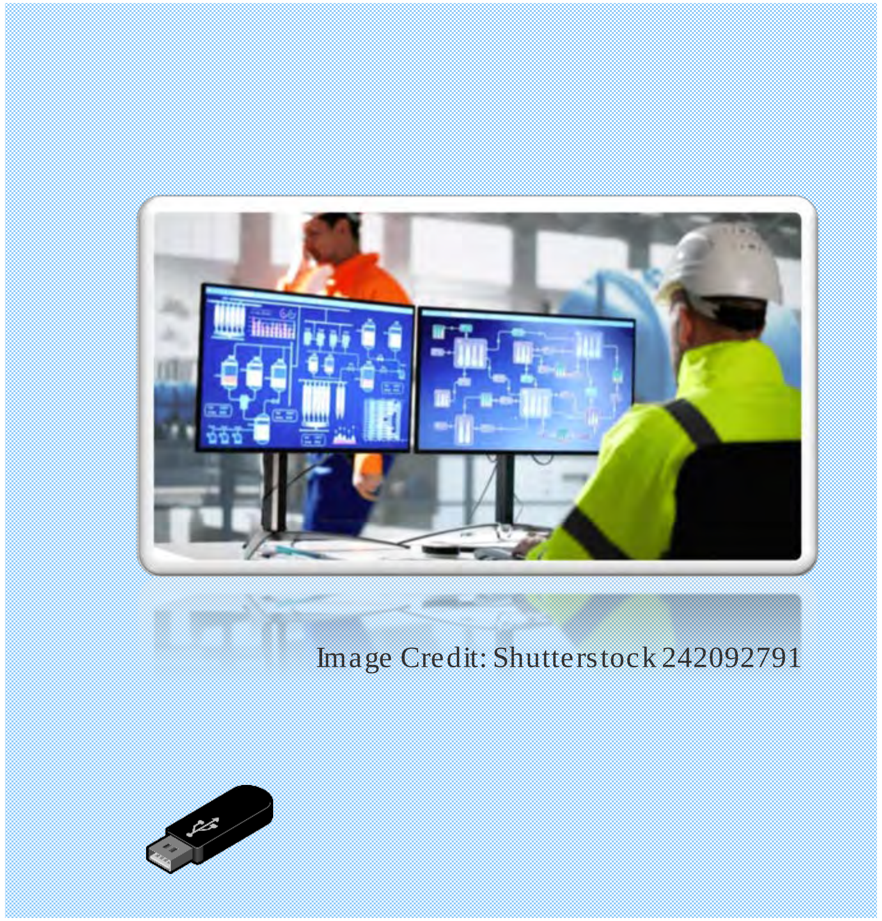


Image Credit: Shutterstock 242092791

Cyber Threats & Cyber Insider Targets

Examples of Cyber Threat Trends

Increase in sophistication

Ransomware

Spear phishing

Pretexting

Examples of Targets of Cyber Insiders

Supply chain

Detection architecture

Access control systems

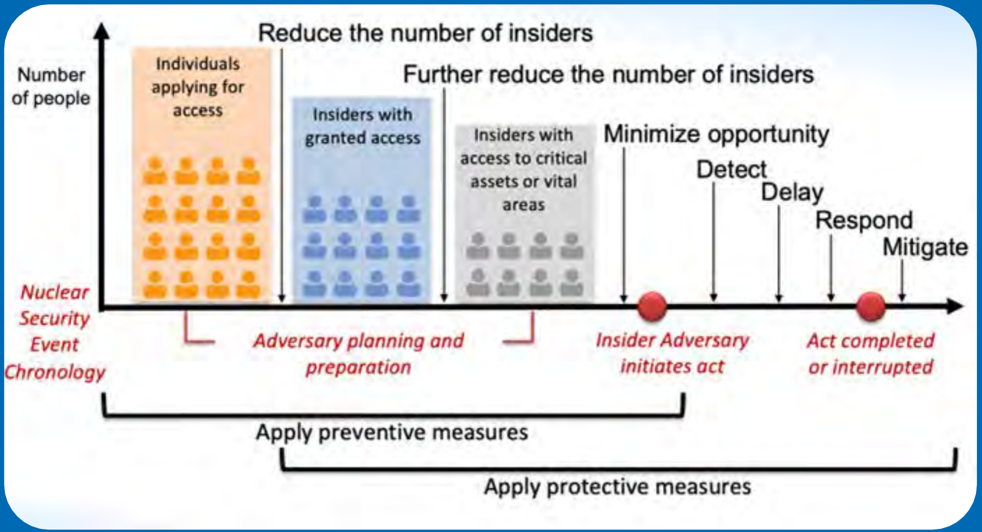
Sensitive information

Instrumentation & Control Systems

Critical infrastructure systems

Image Credit: Shutterstock 2498690647

Cyber Insider Threat Prevention, Detection and Respond


Reduce the number of insiders
Further reduce the number of insiders
Number of people
Individuals applying for access
Insiders with granted access
Insiders with access to critical assets or vital areas
Minimize opportunity
Detect
Delay
Respond
Mitigate
Nuclear Security Event Chronology
Adversary planning and preparation
Insider Adversary initiates act
Act completed or interrupted
Apply preventive measures
Apply protective measures

Preventives measures

- Screening prior to allowing access
- Observing behaviors after access is granted
- Limit opportunities for damage

Protective measures to detect, delay, and respond, and mitigate consequences:

- Administrative - policies, procedures, and practices
- Physical - physical barriers for the protection of computer and supporting assets
- Technical - computer hardware/software security controls

Examples of Key Administrative Measures in Mitigating the Cyber Insider Threat

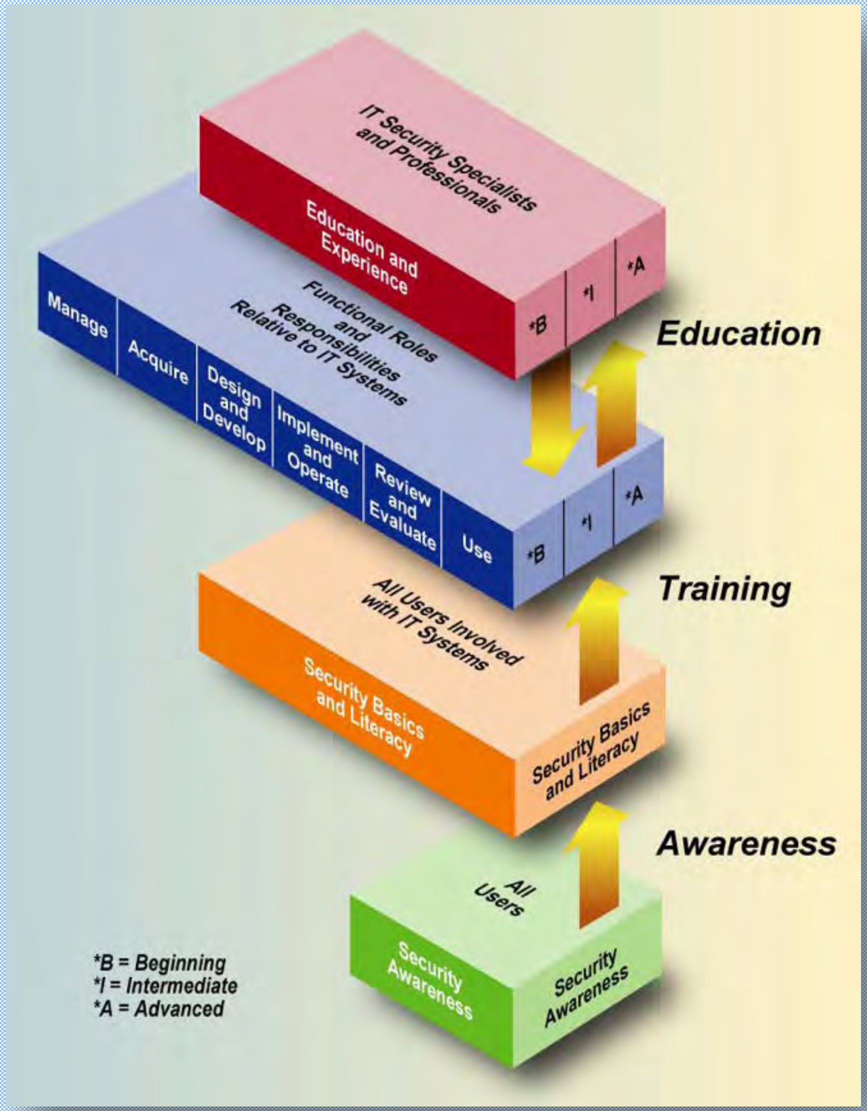
- A national strategy
- Provide and implement good governance and practice from the leadership level to the working level
- Develop a nuclear security culture with sound and practical policies through:
  - ✓Understanding computer security;
  - ✓Understanding the risk: impacts, threats, and vulnerabilities;
  - ✓Understanding computer security risk mitigations;
  - ✓Good recruitment practices, including vetting;
  - ✓Constantly applying and revising these parameters through education, exercises and training.
- Recognizing that the insider adversary can emerge at all levels of management and length of service.

Example Technical Computer Security Measures

- Inventory of authorized and unauthorized devices and software
- Secure configurations for hardware and software
- Continuous vulnerability assessment and remediation
- Controlled use of administrative privileges
- Maintenance, monitoring, and analysis of audit logs
- Email and web browser protections.
- Malware defences

- Limitation and control of network ports
- Data protection and network access control
- Controlled access based on the need-to-know
- Account monitoring and control
- Segmentation and separation of workplace networks
- Data recovery capability
- Security skills assessment and appropriate training to fill gaps
- Incident response and management.
- Cyber exercises

Awareness and Training



Computer security awareness

The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize information and computer security concerns and respond accordingly.

Computer security training

The purpose of training is to teach and instil relevant and needed security skills and competencies in practitioners of specific computer security functions.

Computer security exercises

The purpose of computer security exercises is to evaluate and enhance the effectiveness of nuclear organizations in responding to computer security threats, and also be the basis for continued improvement programmes for all organizations within the State’s nuclear security regime.

IAEA

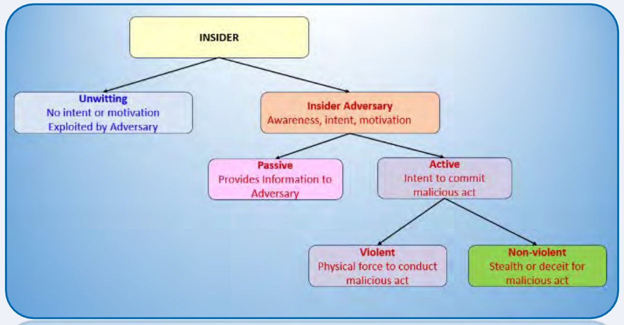
IAEA Project Concept Note (PCN) on Insider Treats

PCN on Preventive and Protective Measures Against Threats Posed by Insiders to Nuclear Material and Facilities

- Capacity building components on:
  a. Regulations
  b. Threat assessment
  c. Methodologies on system effectiveness for the threats posed by insiders
  d. Nuclear security culture
  e. Nuclear material accounting and control (NMAC)
  f. Computer security

- Requests that came through the INSSP process to capacity building to increase their awareness of preventive and protective measures against the insider threat

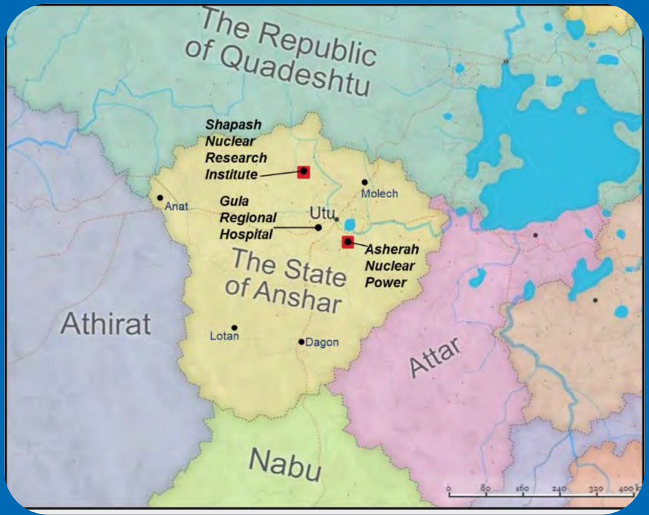
- Expected duration: 5 year


INSIDER
Unwitting
No intent or motivation
Exploited by Adversary
Insider Adversary
Awareness, intent, motivation
Passive
Provides Information to Adversary
Active
Intent to commit malicious act
Violent
Physical force to conduct malicious act
Non-violent
Stealth or deceit for malicious act

IAEA Training Course on Insider Threat Using the Shapash 3D Model

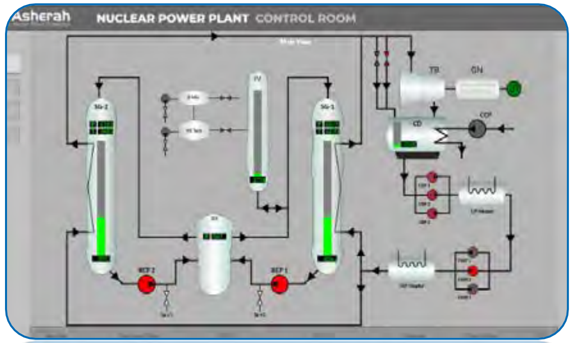
216 EMPLOYEES

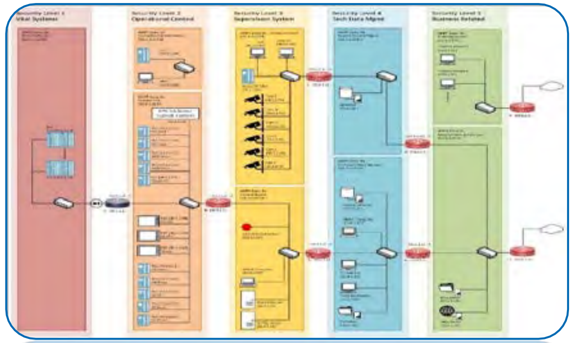
173 HAVE AUTHORIZED ACCESS TO THE PROTECTED AREA

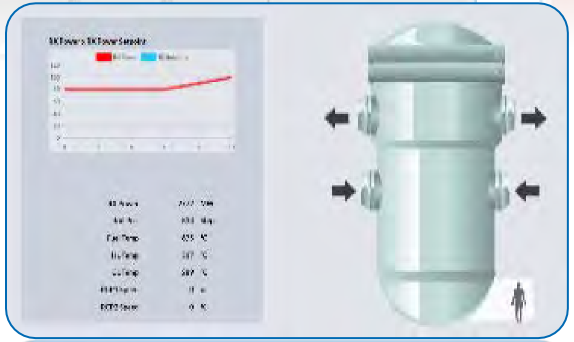


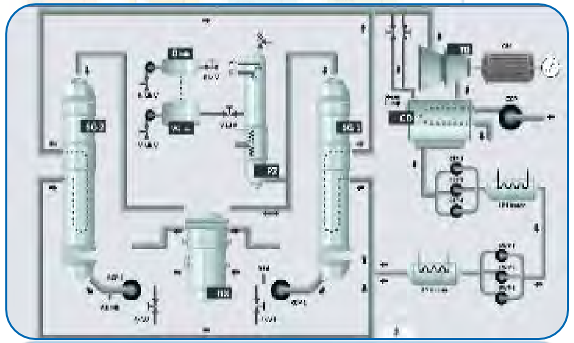
IAEA Demonstration on using Asherah Nuclear Power Plant Simulator 2.0

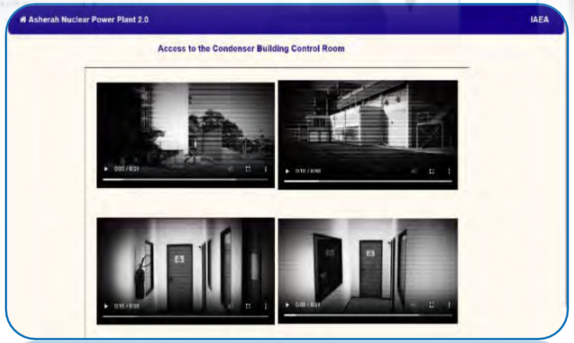
Insider Install a Malware during a Planned Outrage



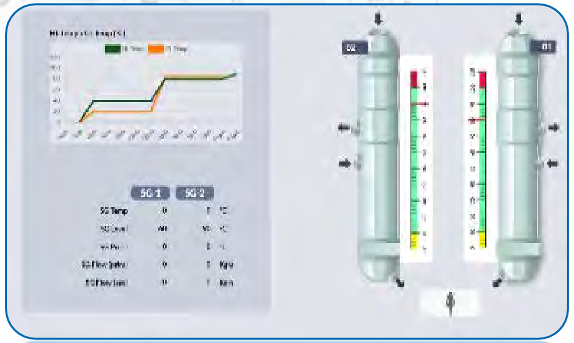








Access to the Condenser Building Control Room



Asherah
Nuclear Power Plant Simulator

Computer Security Exercises

- Key assurance activity supporting cyber security programmes
- Provide unique insight in the state of computer security preparedness and can also be the basis for continuous improvement programmes
- Testing, training, evaluating and demonstrating capabilities
- Cyber insider is part of the storyline (injects and artifacts)
- Opportunity for procedures and decision-making processes to be applied in a realistic manner

Brazilian Cyber Guardian Exercise (2018-2024)

Slovenian KIVA Exercise (2022)

Romanian Cyber Spring Exercise (2024)

Coordinated Research Project on Enhancing Computer Security of Small Modular Reactors and Micro Reactors

The objective of this CRP is to increase the computer security of digital systems, especially instrumentation and control systems, used in SMR through the application of control measures during their lifecycle.

Image Credit: IAEA

This CRP will develop a network of international research institutions to identify, develop and explore approaches, methodologies, technologies and techniques related to computer security of instrumentation and control systems to increase the resilience of small modular reactors and microreactors to cyber-attacks.

IAEA

Thank You!