Cybersecurity Risk Assessment and Management for Energy Sector

CSP003_S_E

PRESENTATION BY:

- **ARTSIOM YAUTSIUKHIN**
  CNR, ITALY
- **CRISTINA ALCARAZ**
  UNIVERSITY OF MALAGA, SPAIN
- **JAVIER LOPEZ**
  UNIVERSITY OF MALAGA, SPAIN

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Outline

Topic 1 - Threats and Vulnerabilities for Energy Sector

Topic 2 - Risk Assessment and Management Processes and Methodologies for Energy Sector

Conclusions

References and sources

Topic 1:Threats and Vulnerabilities for Energy Sector

Overview

- A Small Overview of the Energy Sector and its main components
- Overview of vulnerabilities and threats

CSP003_S_E: Cristina Alcaraz and Javier Lopez (UMA), Artsiom Yautsiukhin (CNR)

Power systems and traditional operational stages

- Electrical power systems normally follow systematic procedures, in which a set of operational equipment and devices are intended to (1) produce, (2) transmit and (3) distribute power to end users

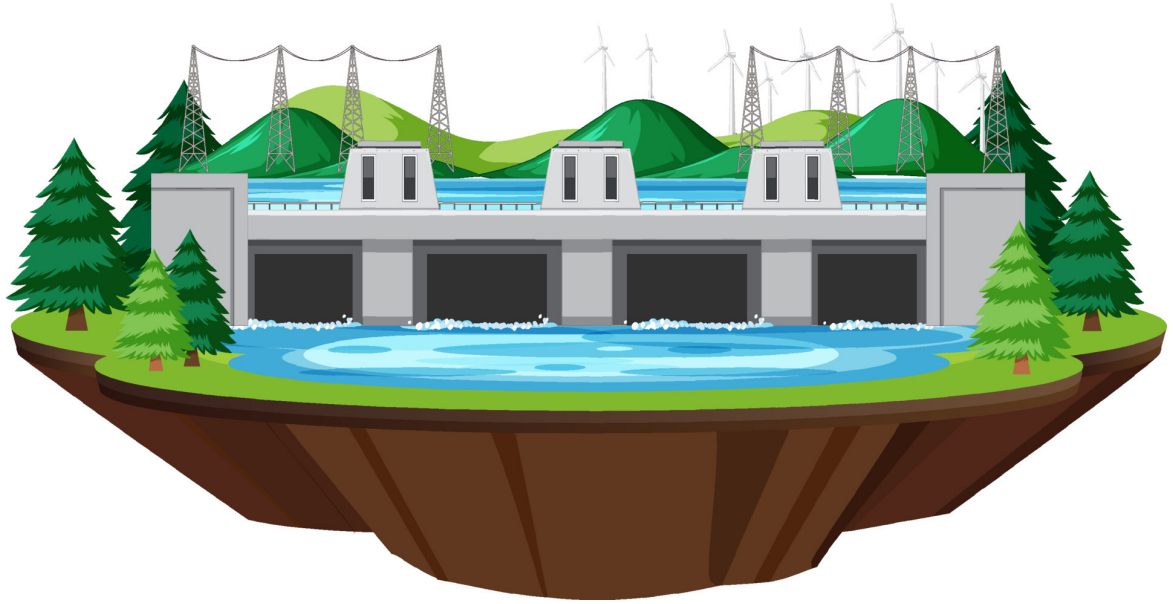


Figure source: Vecteezy
URL:https://www.vecteezy.com/vector-art/4496530-isolated-hydro-power-plants-generate-electricity

Power systems and traditional operational stages

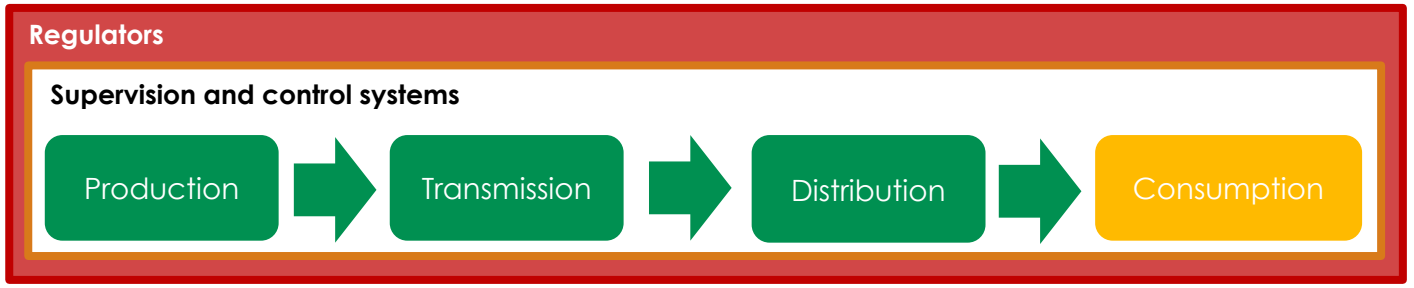
- These energy production and distribution phases are as follows:
  - **Energy production** involves the incorporation of mechanisms and components capable of generating large amounts of energy with the ability to store or distribute it via pylons
  - **Energy transmission** aims to transport large quantities of electricity with high loads over long distances (via pylons), supported by storage and generation systems at substations
  - **Energy distribution** consists of transporting electricity at an acceptable intensity for its final consumption, and probably with the support in storage and generation systems at substations close to end users

Main systems, components and stakeholders

- Beyond the typical generators and high-voltage towers, within these three phases of energy production and distribution, a number of Operational Technologies (OT) also emerge, such as:
  - **Field devices** such as sensors and actuators
  - **Controllers** such as Remote Terminal Units – RTUs
  - **Human Machine Interfaces** (HMIs)
  - **Supervisory Control And Data Acquisition (SCADA) servers** for supervision and control of control substations
- These OTs help provide constant monitoring of the operational statuses and processes of remote substations and their critical resources, which are essential for generating, transforming and distributing power
  - This is relevant to ensure the proper functioning of the underlying infrastructure and the provision of essential resources for well-being

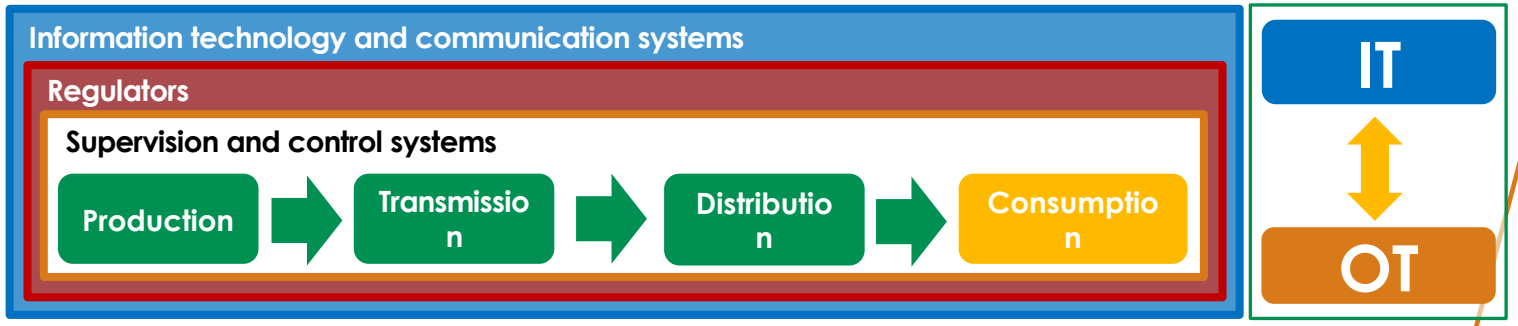
Operation stages and stakeholders

- For a coordinated production and distribution of energy, a number of stakeholders are part of the whole process, such as:
  - **Grid/system operators** responsible for generating, transmitting and distributing energy, also known as Transmission System Operators (TSO) and Distribution System Operators (DSO)
  - **Suppliers or providers** to facilitate the access to the energy
  - **Supervision and control systems**
  - **Authorities or regulators** to establish operation rules
  - **End users** such as consumers or prosumers
  - **Organizations or associations** support energy use and access



Operation stages and stakeholders

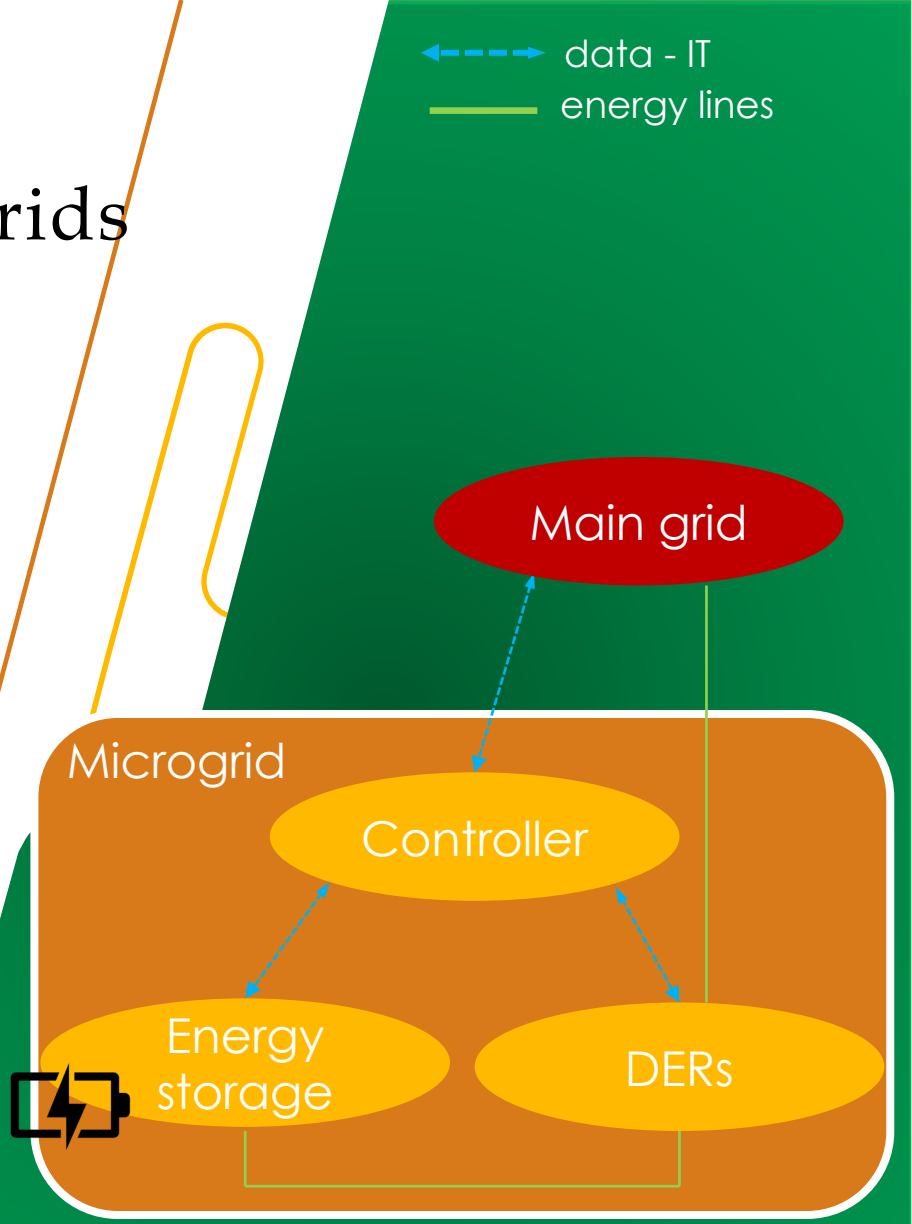
- To efficiently generate, distribute and control energy according to actual demand, it is also necessary to create hyperconnected environments based on **new Information Technologies** (ITs) **and communication systems**



- This technological convergence, IT-OT, brings with it the need to digitally transform electricity infrastructures, and create decentralized, open, and easily accessible environments for control

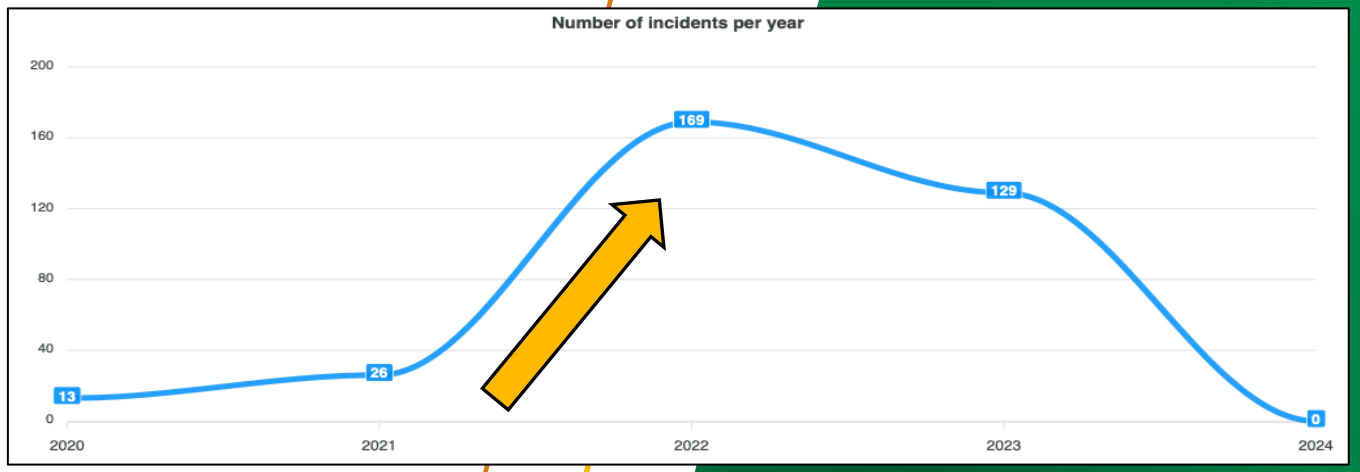
Smarter operation stages lead to Smart Grids

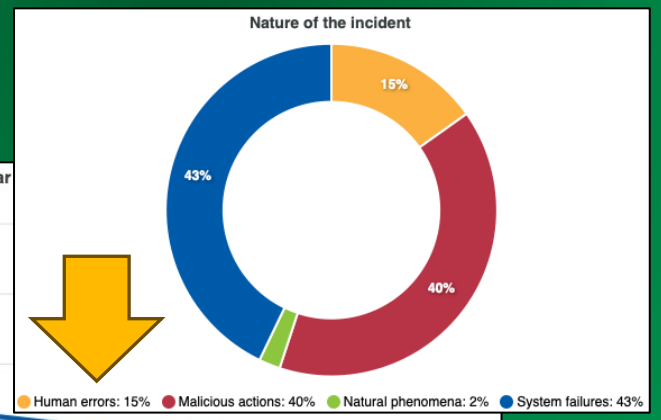
- As a result, the **Smart Grid** concept arises,
  - where different stakeholders must cooperate with each other to dynamically manage, without wasting, energy based on actual demand
- This concept can in turn be reduced in the deployment of "**Microgrids**"
  - composed of modular digitized electricity infrastructures connected to the main grid, and
  - capable of managing Distributed Energy Resources (DERs) composed of energy sources such as
    - renewable and storage systems, electrical vehicle batteries, charging stations, etc.
- This way of isolating operations through energy islands also provides **safety and resilience** against blackouts, malfunctions or cyber-attacks

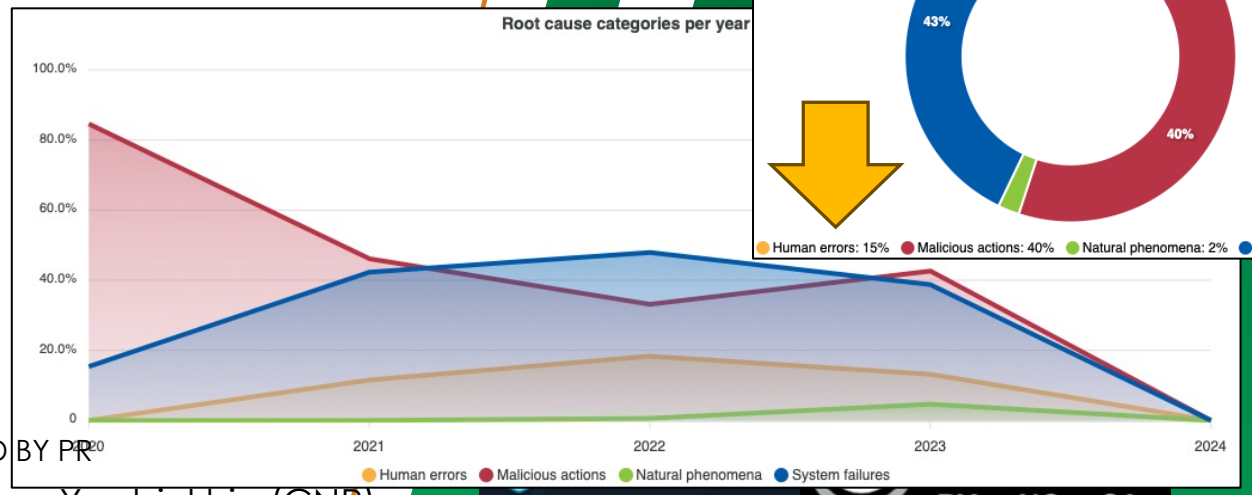


Security risks in the energy sector

- Unfortunately, the sector is very much in the crosshairs of attackers, who know the consequences of a power outage caused by:
  - **A deliberate threat**, such as a denial of service, modification of critical values or a phishing attack
  - **An unintended threat** such as a phenomenal catastrophe or human error
- According to the European Union Cybersecurity Agency (ENISA), through its CIRAS tool,
  - the number of cyber incidents in the energy sector is increasing, including the human errors







Source: ENISA, CIRAS, 2024
URL: https://ciras.enisa.europa.eu/

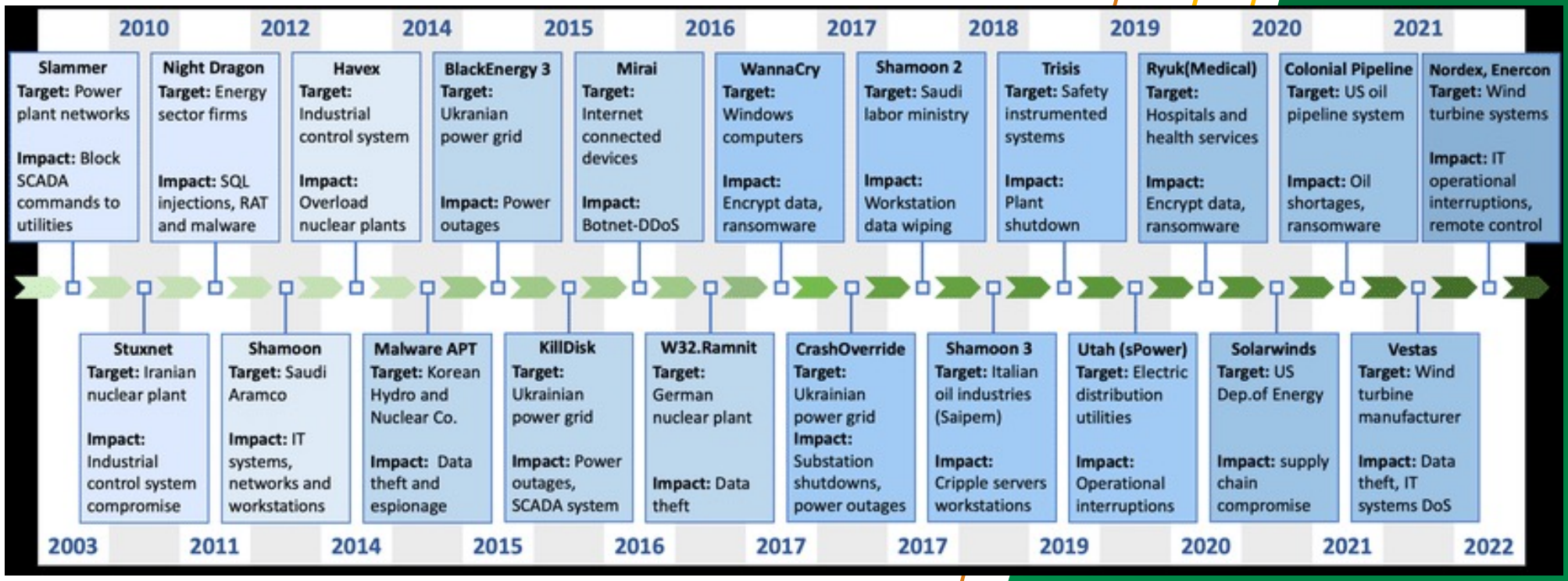
Security vulnerabilities in the energy sector

- In fact, part of these security risks are also due to **system failures**, usually caused by hardware or software errors that can be easily exploited
  - Among the vulnerabilities, the most interesting for attackers are those based on ZERO-DAYS vulnerabilities
  - These vulnerabilities are part of the main goals of the Advanced Persistent Threats (APTs)
- All vulnerabilities are publicly reported and accessible from repositories such as:
  - MITRE CVE: https://cve.mitre.org
  - NIST NVD: https://nvd.nist.gov
- As can be seen in the figure, these CVEs do not necessarily have to be based on software components
  - They may be related to OTs such as industrial protocols

Source: MITRE, MITRE CVE, 2024
URL: https://cve.mitre.org
Figure source: MITRE, MITRE CVE, 2024
URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=modbus
Source: NIST, NVD, 2024
URL: https://nvd.nist.gov

Security risks multiply in these systems

- What is more, multiple threats have emerged in recent years, where the goal is to cause as much damage as possible



Source: Zografopoulos, Ioannis, Nikos D. Hatziargyriou, and Charalambos Konstantinou. "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations." *IEEE Systems Journal* (2023).

Topic 2:Risk Assessment and Management Processes and Methodologies for Energy Sector

Overview

- Risk assessment definitions and process
- Risk analysis
- Tools for risk assessment
- Risk treatment

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

How to measure cyber security?

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

How to measure cyber security?

Goal:

- Make a rational decision about improving your cyber security.

Problems

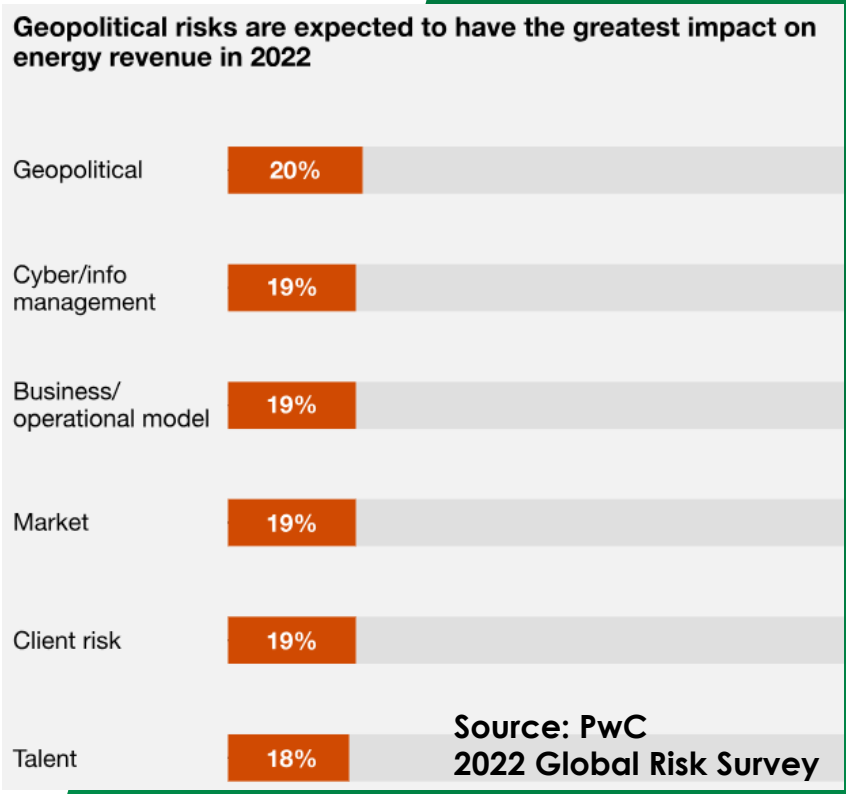
- The decision is to be done for the **whole** cyber security system;
- The decision is to be made by **managers**, not technicians;
- Security solutions (options) are **costly** and cyber security budget is **limited**;
- How to make the decision **rationally**? Which measures/metrics to use?
- Cyber security if very **heterogeneous** (includes management, policies, technical solutions, multiple small options for tech. solutions, physical and social aspects, etc.)
- Even similar IT systems **are different**
- Cyber security context **is changing**

Cyber security is not only technical issue!

CYBERSECURITY VENTURES ABOUT RESEARCH LISTS VIDEOS EVENTS JO

Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019



Risk Assessment

Risk Assessment in a nutshell:

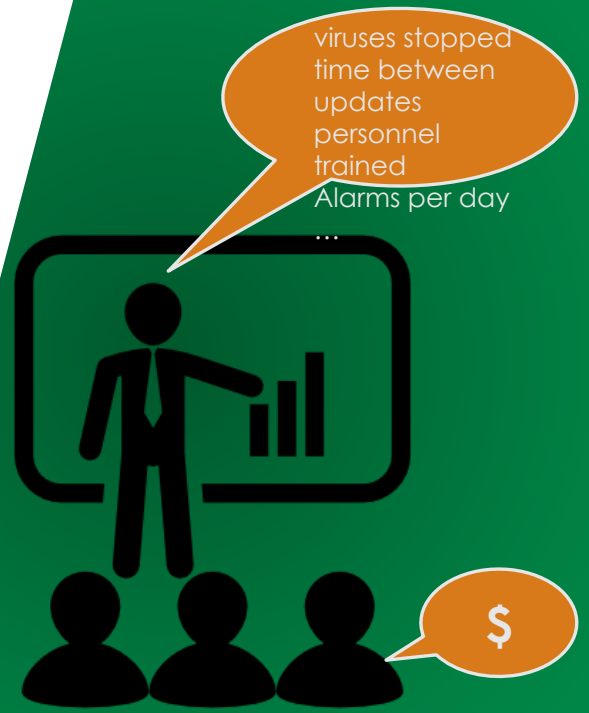
- Weight your capabilities and needs by identifying your
  - main assets
  - potential threats
  - Installed and potential security controls
- Analyse the current state, and possible improvements
  - Are you happy with the current risks?
  - What can you do to improve your risk level.

Pros:

- Addresses your needs
- Optimises decisions
- Easy to understand and use by manager
- Supports justification of the taken decisions

Cons:

- Requires good knowledge (and data) about cyber security and risk management



Risk management, Assessment and Security Management

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

What is risk?

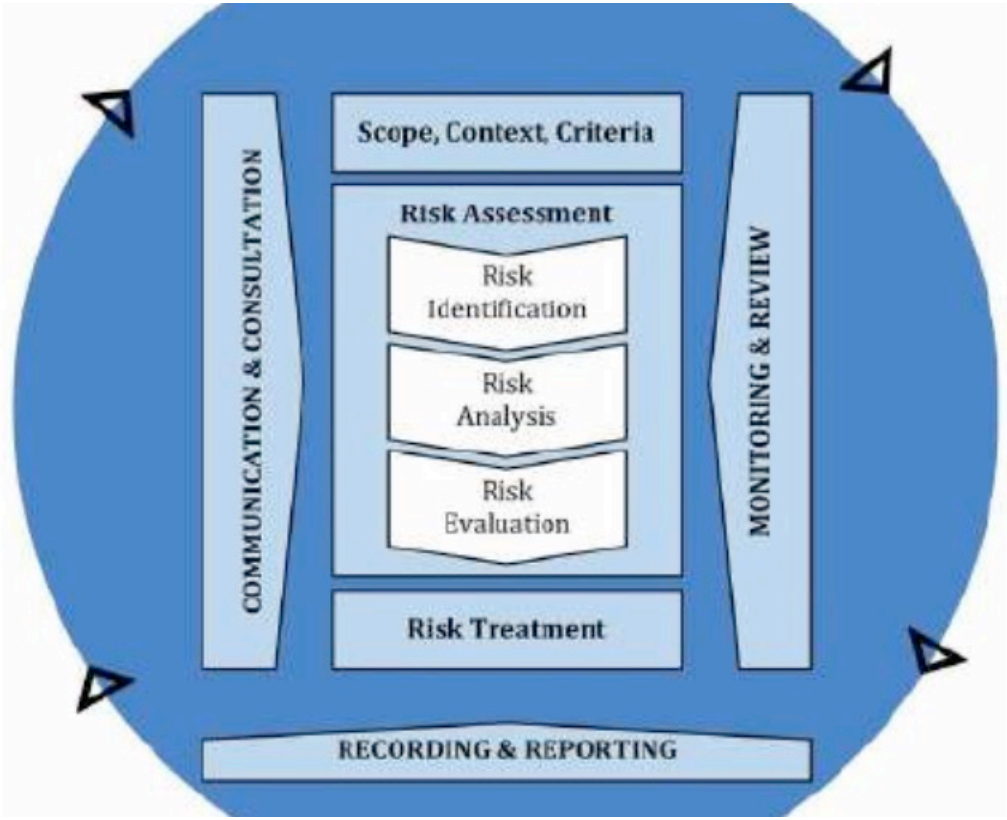
Risk is the **possibility** of suffering harm or **loss** [NIST SP800-30]

- **Threat** – cause of risk
- **Vulnerability** – existing flow or weakness
- **Impact** – possible loss

- **Asset** – something valuable
- **Incident** – threat occurrence

Risk Management

Risk Management – coordinated activities to direct and control an organization with regard to risk [ISO 31000]



Risk Assessment

Risk identification

Threats,
Vulnerabilities/controls,
Assets

Risk analysis

Threat exposure
Success probability
Impact

Risk evaluation

Compute risk
Prioritize risk
Evaluate risk

Risk Treatment

Risk assessment estimates the **current level** of risks

- Where are we?

Risk treatment helps to plan the steps to **deal with** the excessive risks

- What are we going to do?

Implementation of more or better controls is only one way (risk reduction) to treat risks!

- Risk treatment ≠ more controls
- Risk treatment ⊃ more controls

Identified problems can (and should be) solved on risk level, with other instruments (including, risk avoidance, risk transfer and risk acceptance).

Cyber Security Management

Typically, security management is focused more
- on technical aspects
- on reducing probability of a threat occurrence
- on increasing security strength.

Does not (explicitly) take possible impact into account.

Security management Is governed by risk management decisions

The difference with cyber risk management is blurred and, in practice, is not crucial
- Without going much into details, it is even possible to say that
  - security management = risk management

Risk/Security Management standards

Cyber Risk Management

- ISO 31000 – Risk management – Guidelines
- **ISO 27001 – Information security management systems — Requirements**
- NIST 800-37 – Risk Management Framework for Information Systems and Organizations

Cyber Risk Assessment

- ISO 27005 – Information security risk assessment
- NIST 800-30 – Guide for Conducting Risk Assessments
- Other risk management methodologies:
  - CIS RAM, OCTAVE, Magerit, Mehari, Microsoft, etc.

Security control lists/guidelines

General Security Control lists and guidelines:

- ISO 27002 – Code of practice for information security controls
- NIST 800-53 - Security and Privacy Controls
- CIS Controls

Cyber Security guidelines for Energy:

- NISTIR 7628 (smart grid)
- IEC 62351 (protocols)

Cyber security guidelines for Critical Infrastructure:

- NIST CSF
- NIS /NIS2
- IEC 62443
- NERC CIP
- NIST SP 800-82 Rev. 3

Cyber Risk Assessment

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Cyber risk Assessment for energy systems

Risk assessment is a universal instrument for management of any type of risk

Then, what is **cyber** risk assessment for **energy systems**?

- It is application of the generic risk assessment process to cyber domain, taking into account peculiarities of energy domain.
  - How to define **scope** of the security system?
  - What are the typical cyber **assets** for energy systems?
  - Which threats are typical for cyber **threats** for energy systems?
  - What are the cyber security **controls** for energy systems?
  - How to estimate **impact**?
  - How to estimate **probabilities and exposure**?

Typical Risk assessment process

Context establishment

Risk identification

- Assets
- Threats
- Controls

Risk estimation/analysis

- Impact
- Exposure
- Probabilities

Risk evaluation

- Risk computation
- Risk prioritization
- Risk evaluation

Context Establishment

Context Establishment. Context

It is required to understand the environment in which the IT system operates in and how much it affects the risk assessment

In particular, the following points should be taken into account:

- Organizations business objectives, strategies and policies
- Business process, function and structure
- Legal, regulatory and contractual requirements
- Organization's overall approach to risk management
- Geographical location
- Expectations of stakeholders
- Location and socio-cultural environment

Context Establishment. Scope and boundaries

Scope

- ensures that all relevant security **assets** are considered during risk assessment.

Boundaries

- helps to focus on the **threats** which could penetrate through the boundaries.

In the cyber context, it is important to pay particular attention to the scope and boundaries because of distributed nature of IT systems:

- Does cloud service is within your boundaries or not?
- Should the assets on devices connected from outside of the network be in scope of the assessment?
- Should assets on mobile devices connected to your network be in scope?
- Are all IoT devices/sensors/actuators considered?

Context Establishment. Criteria

Risk evaluation criteria

- These are the criteria for evaluating cyber security risks, which include:
  - Strategic importance of existing business processes
  - Sensitivity of cyber assets
  - Legal, regulatory, and contractual obligations
  - How confidentiality, integrity, and availability of cyber assets affect business processes
  - Expectance of stakeholders and value of trust and reputation.

Impact criteria

- These are the criteria to evaluate possible loss:
  - Breaches (loss of confidentiality, integrity, availability)
  - Halted operations
  - Missed deadlines
  - Financial loss (including loss of business opportunity)
  - Loss of Reputation
  - Inability to fulfil legal, regulatory and contractual requirements

Context Establishment. Criteria

Risk acceptance criteria

- These criteria define which risk levels are accepted
- Could have different levels
- Could be different for different risks
- Could depend on the expected profit

Risk Identification

Risk identification. Cyber Assets

Peculiarities in identification of cyber assets

- Cyber assets could be difficult to assign to a physical object (e.g., client's data are stored on a server), because they are easy to copy, modify and exchange (e.g., communicated via Intranet/Internet, processed on a desktop; backed up on a NAS or cloud, etc.).
- Cyber assets are difficult to monitor. They could be copied to a different cyber assets. They could be processed and turned in a different asset (e.g., analytics or logs).
- It is not trivial to identify and list all cyber assets. Often the value of cyber assets is too much undermined (e.g., personal identifiable information, like location or email).
- Some cyber assets are very important, but do not provoke immediate or definite loss. Example: credentials.

- There are non standard (sometimes innovative) ways for attackers to abuse your assets or use them to attacking others. For example, cryptojacking, botnets, or supply chain attacks.
- Assets could depend on each other (e.g., forging monitoring data may lead to a business process)

Risk identification. Cyber Assets

Logical
- Business processes
- Information
  - personal identifiable information,
  - personal health information,
  - financial information
  - Know-how
  - Business strategic information
  - Business relevant information
  - Credentials
  - Source code

- Containers
  - Databases
  - Files
  - Applications
  - Communication
  - E-mails
  - Development environment
  - Web Service/ Website

Physical
- Server
- Network
- Personnel
- IoT, mobile device
- Desktop
- Media (CDs, NAS, etc.)
- Cloud
- Paper

Cyber Assets for Energy sector

Personal/Financial/Billing Data
- Can be deleted/encrypted (e.g., Ransomware) [Availability]
- Stolen [Confidentiality]

Colonial Pipeline attack

Energy delivery/generation/distribution process:
- Monitoring/Personal data [Integrity/Availability]
  - Deleted/Encrypted (e.g., Ransomware)
  - Modified (False Data Injection)
    - Transmitted data (Communication Problems)
    - Physical access to sensors and IT network
- Applications (e.g., Controlling Application) [Integrity/Availability]
  - Email (Phishing)
  - Development environment/software distribution (e.g., Backdoo updates)

May 2021
Ransomware attack on French producer of renewable energy
Albioma - Paris, France

05 May 2021
Ransomware at Norwegian energy technology provider
Volue ASA is headquartered in Norway and was very open about the cyber attack.

27 November 2021
Ransomware at energy provider in Australia
CS Energy - Brisbane, Queensland, Australia

Hacker, attacco a Eni dopo il Gse. Massima allerta dell'intelligence

February 2022
Cyberattack on a power company in Italy
Gruppo Dolomiti energia - Rovereto, Trentino, Italy

The 2015 Ukraine Blackout

Risk Identification. Threats

Cyber threats are, in grand part, are intentional. Which means that we fight against other humans:

- Adaptable
- Inventive
- Collaborating
- Planning
- Patient
- Could be persistent

Cyber threats are heterogeneous and dynamic

- New threats appear
- Existing threats evolve
- Old threats re-appear.

Risk Identification. Threats

Cyber attacks often requires several steps to obtain the result.

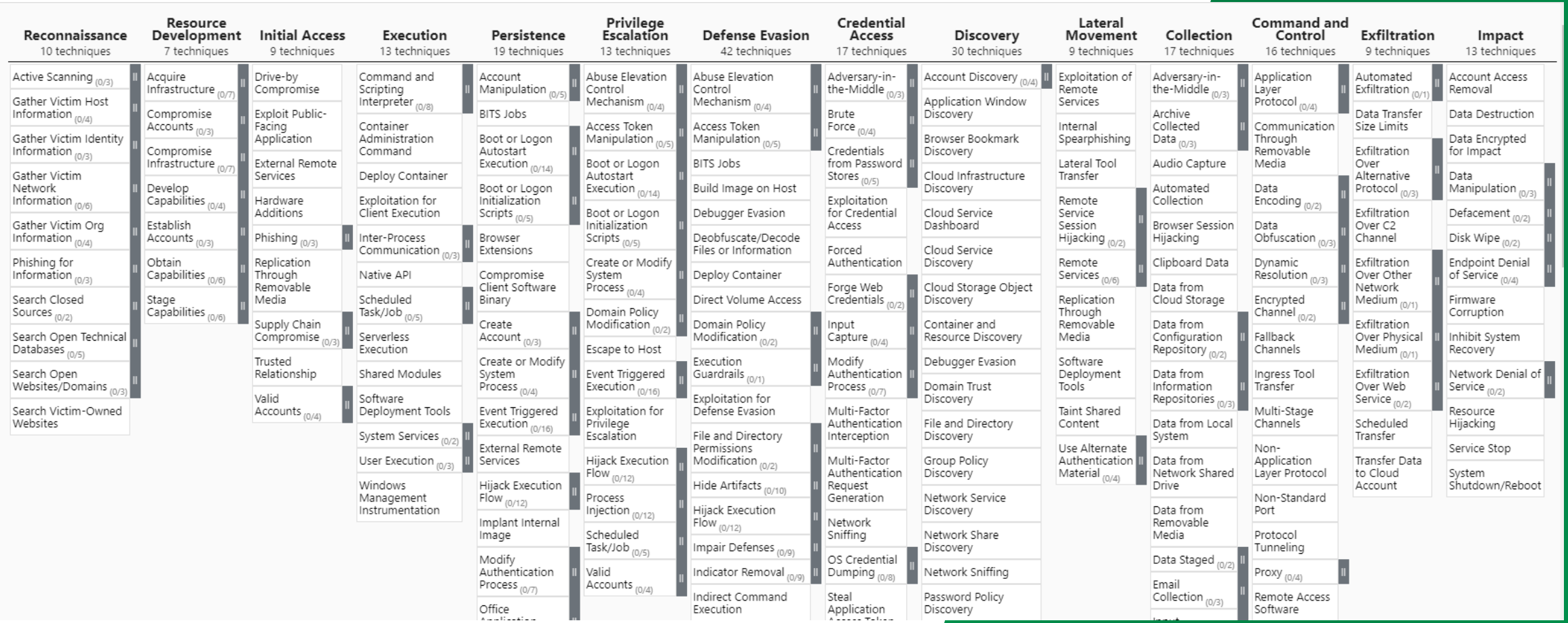
- A user opens a fraudulent e-mail with a virus attached.
- A virus runs on a victim's device. A backdoor is installed
- An attacker gets access to the system and runs an exploit to gain higher level access
- And…
  - Steal data?
  - Implement a bot? cryptojacker?
  - Get access to a server?
  - Plant a ransomware?

Several vulnerabilities are used

Several threats occur

Final outcome (impact) is uncertain

MITTRE ATT&CK Matrix



Risk Identification. Scenarios

A possible solution: define scenarios.

A scenario is a specific way to attack a system and obtain certain result. Helps to make clear:

- Who is the attacker
- Which vulnerabilities are exploited
- What is the expected impact.

In this case it is possible to understand

- Which controls can prevent it
- Which assets are affected and in which way.

But

- There is (almost) infinite amount of scenarios
- There is (almost) no statistics available for scenarios
  - Most statistical data available are focused on threats.

Risk Identification. Attackers

External attacker
- Cyber criminal
- Cyber terrorist
- Vandal
- Nation sponsored
- Virus/worm
- Hacktivist
- Industrial spy

Internal attacker
- Abuser
- Hacker

Malicious client

Physical attacker

Partner

Negligent user

Failures

Environment
- Local (pollution, heating, etc.)
- Global (earthquake, flood, etc.)

Typical Cyber threats

Virus, Worm and Ransomware

Virus and **worm** are malicious programs that can change the way your computer runs and behaves. Viruses and Worms have independent propagation mechanisms.

- Virus. A user should allow a virus to be executed. For example,
  - Open malicious mail attachment
  - Allow installation of an infected program
  - Download and run an infected file
- Worm propagates autonomously exploiting vulnerabilities in network services.

Ransomware is a malware that encrypts data of the compromised computer, making the files and the system unusable. Usually, after that a ransom is requested from the user.

- Distributed in different ways, including viruses and worms, but also can be planted by an attacker who has enough access rights on the computer.

Web-based attacks, Web-application attacks

Web application attacks – a wide set of attacks aiming at exploiting vulnerabilities in service GUI and APIs (e.g., SQL injection attacks, Cross-Site scripting XSS). Aims at compromising web applications.

Web-based attack – a wide set of attacks during which attackers exploit vulnerabilities in coding to gain access to a server or computer. Aims at compromising a system connected to the Internet.

Communication attack D(Dos)

(D)DoS –Denial of Service threat aims to bombard the selected service with a huge number of requests that make the service unavailable for legitimate users

- (Distributed) Denial of Service uses multitude of sources (bots) sending requests to the service.

Communication attack - this threat aims to eavesdrop or tamper the communication between a victims. The attacker may find a way to decipher the communication (with no or weak encryption) or exploit vulnerabilities of the non-secure protocols

- Man in the middle attacks – an attacker breaks the communication between two victims and forces the traffic to flow through him, with a potential to read or modify the communication.

Social engineering attacks
Physical attacks

Social Engineering – is a set of threats aiming to manipulate, influence and deceive a victim in order to make him/her to act in a certain way (e.g., grant access to a computer system, share secrete information or credentials.

- **Phishing** – a typical social engineering threat communicating with a used through an email, messenger or other means of communication.
- Social Engineering attacks required physical presence
  - *Shoulder surfing* – peep the password typing
  - *Dumpster diving* – look for passwords in the litter
  - *USB drop* – leaving an infected USB stick to be picked up and used by an employee

Physical attacks – intentional damage to hardware done by attackers (internal or external)

Tampering – physical modification of a hardware to alter its functionality it or get access to the network.

Insider

Abuser – an employee uses his/her access rights to compromise the system. Typically, copy data outside of the enterprise premises.

Insider attacker – an attacker who benefits from the initial access to system but aims to increase its privileges through compromising the system.

Former employee – a former employee, who uses his/her knowledge about the system, still valid credentials and/or previously installed backdoor to compromise it.

Malicious client
Partner problem

Malicious attacker: a client, that uses the bought services to launch an attack on you or you clients

Illegal client: a client that uses your service for illegal purposes (e.g., sending spam, host illegal content, provide malicious services, etc.).

Partner – a partner attacking the system, using its privileges in your system

A **partner** could be **compromised**. The hacker may aim to attack your partner to use it as a foothold for attacking you – supply chain attack.

Employee Negligence

Hardware loss or **theft** – a threat related to physical loss of a hardware. This threat is typically, results in potential loss of sensitive information contained on a mobile device (e.g., laptop or cellphone).

Incidental physical damage – an incidental action of an employee causing physical damage to hardware. E.g., spilled coffee on a laptop.

Incidental logical error – an incidental error or benign action leading to compromising the system. A typical error is sharing sensitive data (e.g., by granting access to sensitive data to public or sharing information not knowing that it is private).

Typical Threats for Energy sector

Ransomware

May 2021
Ransomware attack on French producer of renewable energy
Albioma - Paris, France

27 November 2021
Ransomware at energy provider in Australia
CS Energy - Brisbane, Queensland, Australia

05 May 2021
Ransomware at Norwegian energy technology provider
Volue ASA is headquartered in Norway and was very open about the cyber attack.

Hacker, attacco a Eni dopo il Gse. Massima allerta dell'intelligence

False Data Injection
- reporting wrong/modified data

The 2015 Ukraine Blackout

Data Breach

Colonial Pipeline attack

March 15, 2022
Cyberattack on an energy provider in Spain
Iberdrola / I-DE Redes Eléctricas Inteligentes - Bilbao, Spain
This resulted in a breach of 1.3 million customer records.

April 25, 2022
1.1 million emails of a Russian service provider for the energy industry leaked
АЛЕТ (ALET) - Moscow, Russia

Phishing and other Account Hijacking techniques
- IT system/Application (e.g., SCADA) access
- Data Access

The 2015 Ukraine Blackout

Malware

Stuxnet

March 2022
Hacker attacks on the power grid in the north of India
Ladakh, India
Affected are systems in the Ladakh region in the north of India.

Energy Threats for AIC

Threat	Data			Process		
	Avail.	Integrity	Conf.	Avail.	Integrity	Conf.
Virus, worm, Ransomw.						
Web-based attacks						
Web-application att.						
Communication att.						
(D)Dos						
Social Engineering (phishing)						
Physical attack						
Tampering						

Energy Threats for AIC

Threat	Data			Process		
	Avail.	Integrity	Conf.	Avail.	Integrity	Conf.
Abuser						
Insider/ Former employee						
Malicious client						
Illegal client						
Partner						
Loss or theft						
Incidental damage						
Incidental error (glitch)						

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Vulnerabilities and Security controls

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Vulnerabilities vs. Security controls

Simplification of vulnerability identification:

- Lack of security controls = a vulnerability

included

prevents

Specific bug

Low level
Technical
Difficult to reasoning

Bug type

High level
Generic
Simpler reasoning

Security control

"Easy" to identify
Generic
Listed in standards
(ISO 27002, CSF, CIS)

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Security controls. ISO 27002

ISO (CIS)

Organisation

Policies

Asset management

Compliance

Supplier relationships

Physical and environmental protection

Human Resources

Access control

Cryptography

Communication security

Operations security,

System acquisition, development and maintenance

Incident management

Business continuity

Security controls. NIST CSF

NIST CSF

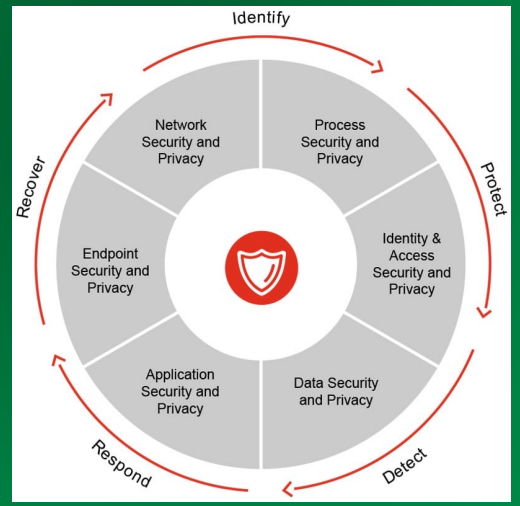
Identify
- Asset Management, Organisation, Policies, Supplier relationships, Compliance

Protect
- Physical and environmental protection, Human Resources, Access Control, Operations security, Cryptography, Communication security, System acquisition, development and maintenance

Detect
- System Protection

Respond
- Incident management
- Business continuity

Recover
- Incident management



Policies

A set of policies for cyber security should be:

- Defined
- Approved (by management)
- Published
- Communicated to employees and external parties
- Regularly reviewed

Organisation

Define roles and responsibilities

Establish contacts with authorities

Define policies for use of mobile devices and teleworking

Human resources

Perform screening of the candidates

Define contractually terms and condition regarding cyber security

Make the management to ensure that security policies are followed

Educate and train employees

Establish a disciplinary process

Ensure that contract termination procedure includes required security actions

Asset management

Create, maintain, and update inventory of assets

Define the owner of the assets

Classify assets

Manage removable media

Secure disposal of media

Secure physical media transition

Access Control

Define policies for access control (especially, access to your IT network)

Define how to register de-register a user

Define how formally access is granted or revoked

Special management of privileged access rights

Special a formal management process for managing secrete authentication information and make sure that users follow it.

Define formal rules for removal or change of access rights

Make sure that access is granted according to the access control policies

Establish secure log-on procedures and password management systems

Restrict access to source code.

Cryptography

Define policies for using cryptographic controls

Define policies for key management

- How to use
- How to protect
- Lifetime of cryptographic keys

Physical and Environmental protection

Establish and secure physical perimeter

Establish physical controls

- Secure offices and other facilities

Establish procedures for working in secure areas

Define and implement procedures for delivery and loading

Deploy protections against natural disasters, malicious attacks and incidents.

Protect and maintain equipment, utilities, cables, etc.

Define and follow procedures for equipment disposal and removal.

Define clear desk and screen policies

Operations security

Define operational procedures and responsibilities

Implement malware protection

Implement back-up procedures

Implement logging and monitoring procedures

Defined procedures for installation of a software

Implement vulnerability management procedures

Plan audit activities

Communication security

Define management procedures for network control

Implement and maintain network security mechanisms (e.g., firewall, IDS/IPS, etc.)

Segregate networks (if necessary).

Define how and which information can be transferred

Define rules for electronic messaging

Define requirements for confidentiality and non-disclosure agreements for information exchange.

System acquisition and development

Define and implement security requirements for new information systems (especially, how applications exchange information in public networks)

Define rules for secure development

Define and implement control over changes to systems

Use secure system engineering principles

Secure development environment

Define rules for outsourced development

Use security and system acceptance testing

Supplier relationships

Define security policies for suppliers

Ensure that security requirements are negotiated, agreed with and followed by the supplier

Review and monitor fulfilment of security requirements by the supplier.

Information security incident management

Define responsibilities and procedures for incidence response and ensure their execution

Establish reporting procedures for events and weaknesses

Ensure that security events are analysed and assessed.

Ensure execution of procedures for incident response

Analyse occurred events and apply actions to reduce similar risk it in the future

Store information about occurred events.

Business continuity

Define requirements for, plan, implement, review business continuity procedures.

Compliance

Identify legislations and contractual agreement required to comply with

Identify intellectual property rights and protect them

Protect third party data in accordance with the law (e.g., GDPR)

Follow regulations on cryptographic controls

Audit

Organise independent review of your cyber security system

Ensure compliance with security policies or standards

Tools and methods

Desktop Research

Analysis of company's documents

- Business strategy, Company strategy, Flow charts, Roles assignment,…
- Asset Inventory
- Logs analysis, past event analysis, reports (including audit reports)…
- Vulnerability scanning reports (Nessus, OpenVas)

External sources

- Statistical analysis (ENISA, IBM/Ponemon, Verizon, Accenture, NetDilligence, McAffee, Semantec, Deloitte, PwC, etc…)
- Information sharing centres (e.g., CERT ISACs) reports, bulletins

Talking to people

- Interviews – individual discussions with key stakeholders about the current state of practice (security managers, HR, resource owners, etc.)
- Workshops – group discussion with people involved in the risk assessment

  Delphi method - a systematic, interactive forecasting method which relies on a taking into account opinion of several experts
  - Experts answer a questionnaire (providing explanations)
  - The answers are anonymously reported to others (with explanations)
  - The experts answer the questionnaire again (correcting their answers)
  - Stop at a predefined criteria (e.g., fixed number of rounds) and mean or medina score is used.

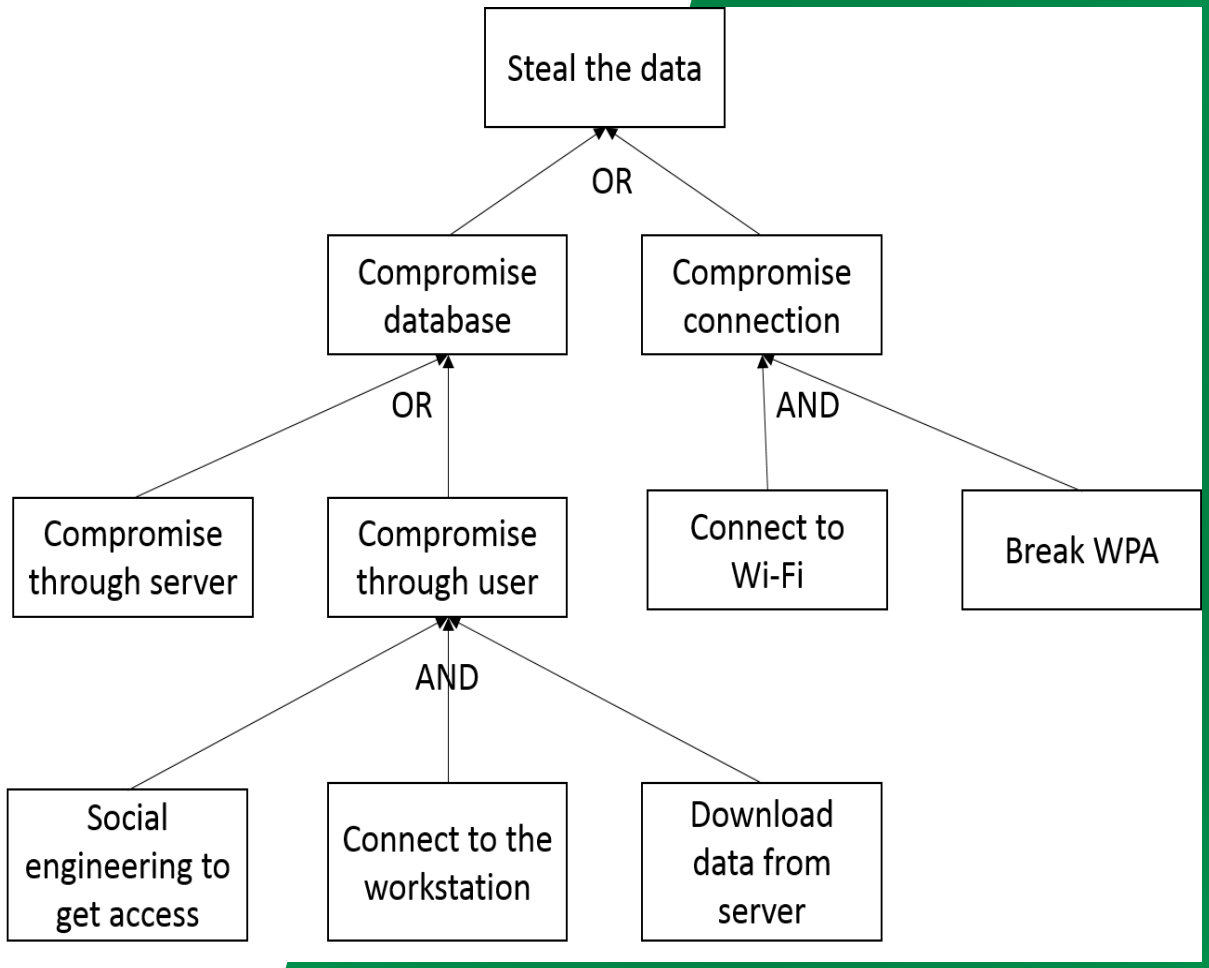
Attack Tree

Attack tree is a useful technique for a structured way to analyse and detail a threat

Start with a possible unwanted consequence (top node)

Break it down using AND and OR operators into more detailed steps

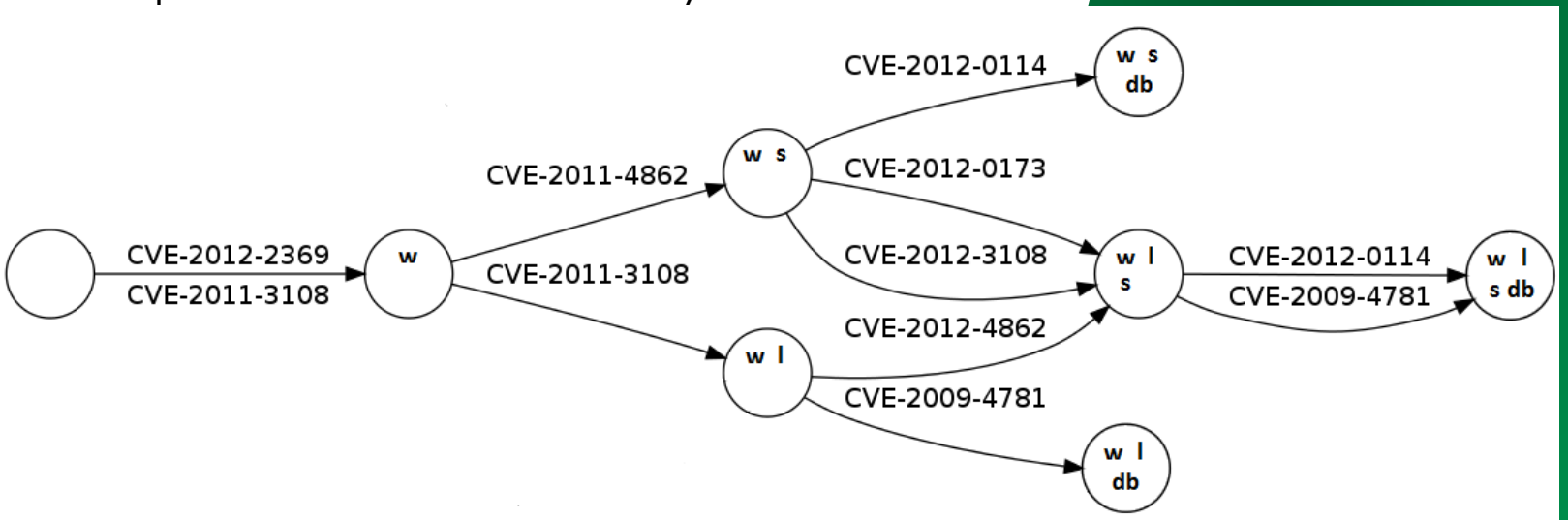
Repeat until the required level of details is reached.



Attack graph

Attack graph is a technique aiming to represent all paths (a sequence of existing vulnerabilities to exploit) through a system which an attacker may follow to achieve its final goal.

After vulnerability scanning, the attack graph building tool links them in a graph based on pre and post conditions for every detected vulnerability.



Risk Analysis and Evaluation

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Quantitative or Qualitative Risk Analysis

Quantitative

- Operates with (real) **meaningful** values!
- Operations on values are defined.
- Provide monetary results (suitable for further analysis and re-use)
- Difficult to use

Loss – measured in euro [dollars, tugrik, etc.]

Likelihood – positive real value

Qualitative

- Easy to work with
- Widely used
- Needs the definition of value
- Needs the definition of operations

Loss – {very low, low, medium, high, very high}

Likelihood – {very low, low, medium, high, very high}

Risk analysis. Impact

A compromised asset causes impact.

- Impact is estimated as an expected loss from a single threat occurrence

Take into account:

- Disruption of business activities
- Direct loss
- Violation of a legislation
- Violation of a contract
- Reputation loss
- Customer loss
- Notification cost
- Impact to personnel/user
- Investigation/recover loss
- Loss of competitive advantage

Do not forget about asset dependency!

Risk Analysis. Impact

From security perspective it is important to evaluate losses due to impact to a specific security aspect:

- Confidentiality
- Integrity
- Availability

Risk analysis. Likelihood

Likelihood = Exposure × Probability[Success]

- Threat sources and context of organization
- Controls and vulnerabilities
- Expertise and statistics

Exposure is mostly external

- Affected by global trends and type of your organisation

Probability is mostly internal

- Affected by your protection

Risk Estimation. Compute

General formula:

- Risk = Likelihood × Impact

Multiple threats (t) and assets (a):

- Per asset: $Risk_{CIA}^{a} = \sum_{\forall\, t} Likelihood^{t} \times Impact_{CIA}^{a}$
- Per threat: $Risk_{CIA}^{t} = \sum_{\forall\, a} Likelihood^{t} \times Impact_{CIA}^{a}$

Risk Estimation. Compute risk. Qualitative

	Likelihood	**Very low**	**low**	**medium**	**high**	**Very high**
Impact	**Very low**	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very high	4	5	6	7	8

Prioritise risk

Prioritise risks according to evaluation criteria.

Threats	Impact	Likelihood	Risk	Rank
Threat A	Very low	Very low	0	5
Threat B	Very high	Medium	6	1
Threat C	Low	Low	2	4
Threat D	Very low	High	4	2
Threat E	Medium	Low	3	3
Threat F	High	Low	4	2

Simple Example

Consider a system (SCADA) that manages power transmission process.

In this scenario a large amount of power transmission points receives power by power lines, process it and directs it further. All these points collect various information.

The collected data is then communicated to the management centre, where the data is used to evaluate the state of the power transmission system, re-direct power according to needs, avoid dangerous situations (e.g., transmitting too much power through a specific power line). Some of this data is stored in the database for history-based analysis.

The controlling signal is sent back to power transmission point, where actuators adjust the operation of the point.

The operators interact with the management centre only through GUI locally.

The scope of the risk assessment: the management centre + all transmitting points

Risk acceptance threshold: 3

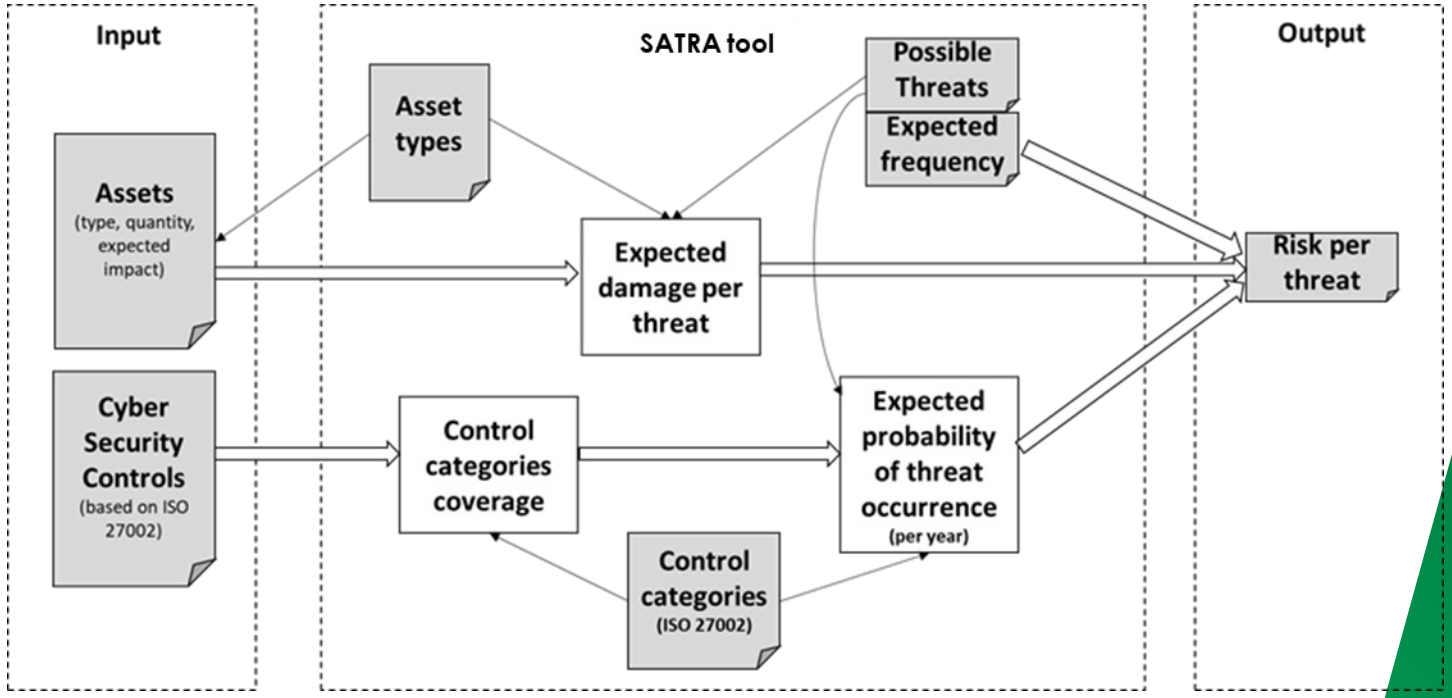
Simple example. Risk Analysis

	Value
Threat description	Communication problem: Man-In-The-Middle. An attacker physically approaches the area of a power re-direction points and starts sending fake monitoring data to the central station (blocking genuine messages), forcing it to direct excessively large amount of power though this part of the power network and damage the equipment.
Attacker	Vandal / Nation sponsored / Cyber Terrorist
Vulnerability	Absent or poor cryptographic protection of the communication channels
Likelihood level	**medium**
Impacted Assets	Control data - blocked / modified in transmission Control Process – incorrectly operating because of fake data Power transmission process – impacted efficiency or prevention of power transmission in case of equipment damage
Impact level	**medium**
Risk	4
Accepted risk?	No
Suggested controls	Communicate data only in an encrypted form. Use secure protocols which have secure mechanisms for authentication of data senders and receivers. Implement safeguarding mechanisms preventing potentially dangerous power distribution.

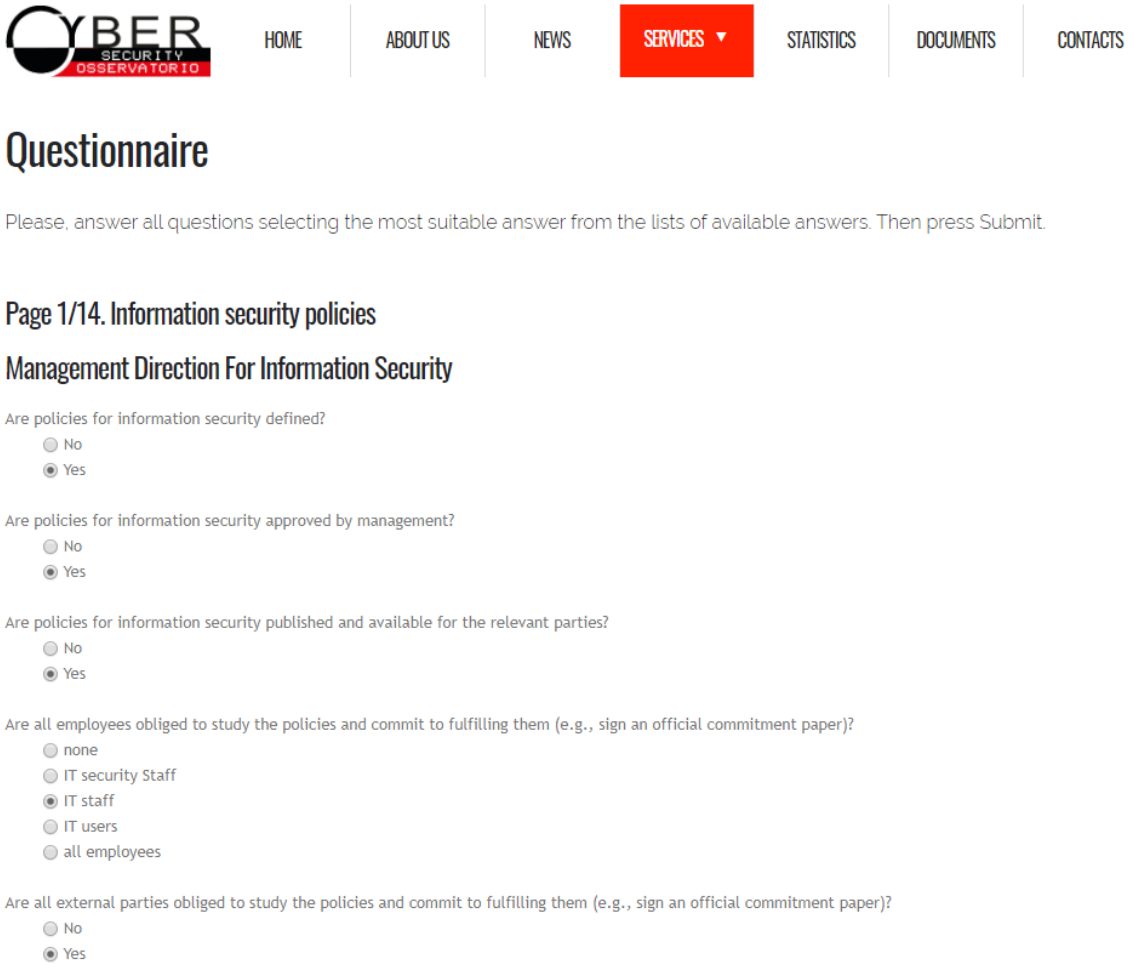
SATRA

SATRA – Self-Assessment Tool for Risk Analysis

The main goal is to offer a simple and fast way for cyber risk self-assessment and mitigation planning.

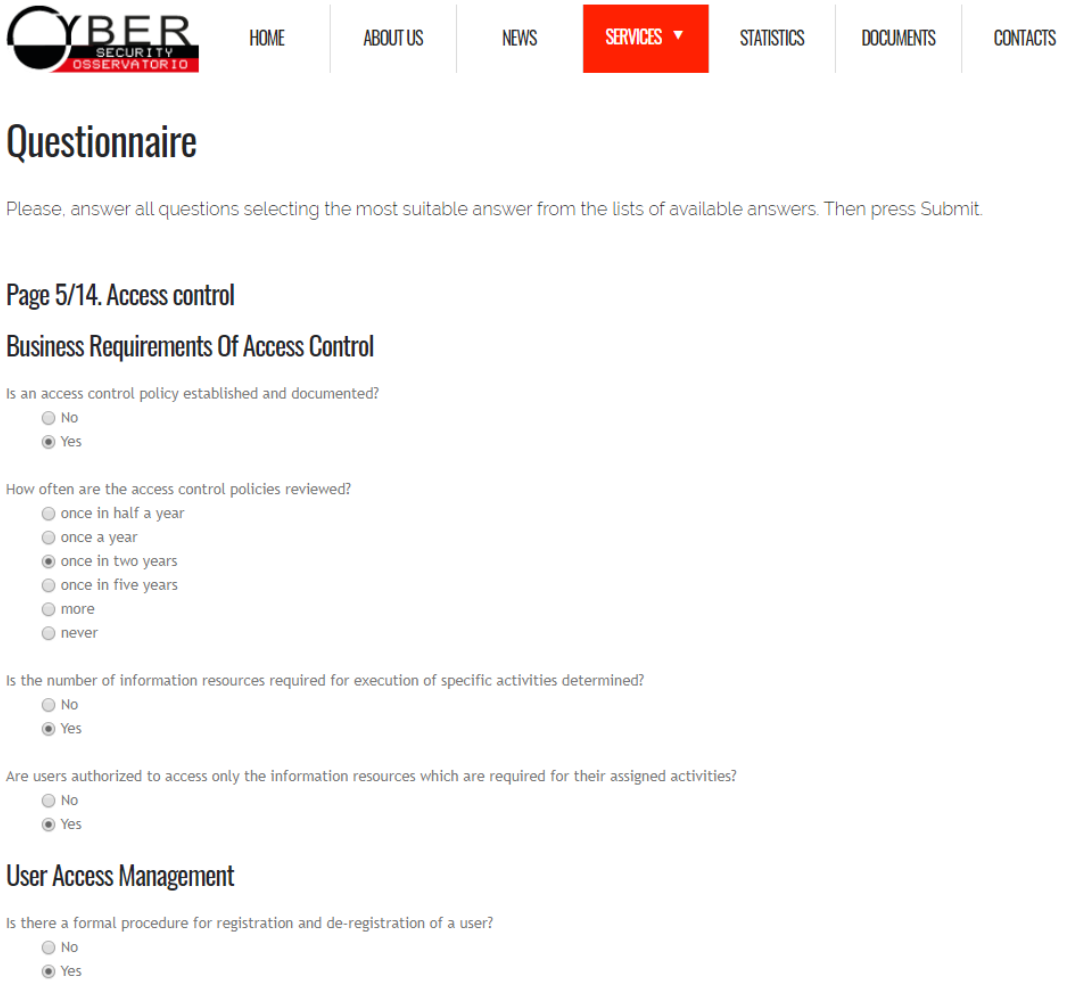


SATRA. Security Controls



CSP TRAINING MODULE NAME: PRESENTATION TEMPLATE CREATED BY PR

SATRA. Security Controls



SATRA. Assets

Asset Identification

ID	Asset	Asset Type	Number of Units	Confidentiality Damage (€)	Integrity Damage (€)	Availability Damage (€)
A1	VMWare	Critical Applications	1	0.0	10000.0	5000.0
A2	Management configuration	Technical documentation	1	500.0	50.0	50.0
A3	Private data of employees	Private records	20	100.0	10.0	20.0
A4	Router Cisco ASR 9k	Auxiliary equipment	1	1000.0	500.0	2000.0
A5	Financial documents	Private records	1	1000.0	500.0	200.0
A6	Contracts	Private records	100	40.0	10.0	10.0
A7	VM OSs	Critical Applications	75	0.0	200.0	200.0
A8	firmware firewall	Private records	1	1000.0	2000.0	3000.0
A9	Services	Web Applications	75	0.0	1000.0	2000.0
A10	Logs DB	Audit/logs	1	1000.0	500.0	200.0
A11	Firmware routers and switches	Auxiliary equipment	6	0.0	500.0	2000.0
A12	Firewall cisco ASA	Private records	1	1000.0	2000.0	3000.0
A13	Service configuration info	Technical documentation	75	200.0	50.0	50.0
A14	Operational data	Private records	20	10.0	40.0	10.0

CREATE ROW DELETE ROW SUBMIT

SATRA. Results

Overall Risk

104055.34€

GO TO MITIGATIONS PAGE

Threat title	Risk
web application attacks	25549.72
malware	6643.02
Environmental damage	1191.74
Phishing	4601.79
Physical damage	520.04
System glitch	635.2
Onsite penetration/tempering	4721.53
Communication break	6650.44
Malicious client	5039.01
(D)Dos	8161.62
Employee Negligence	7781.87
Insider Threat	2425.3
System inappropriateness	2050.59
Social engineering attacks	5161.09
Mechanical failure	1702.56
Hardware theft	2120.93
Third Party Problems	6101.59
web based attacks	1672.02
Spam/Infected email	4213.03
ransomware	7112.17

SATRA

Short demo

Cyber Risk Treatment

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

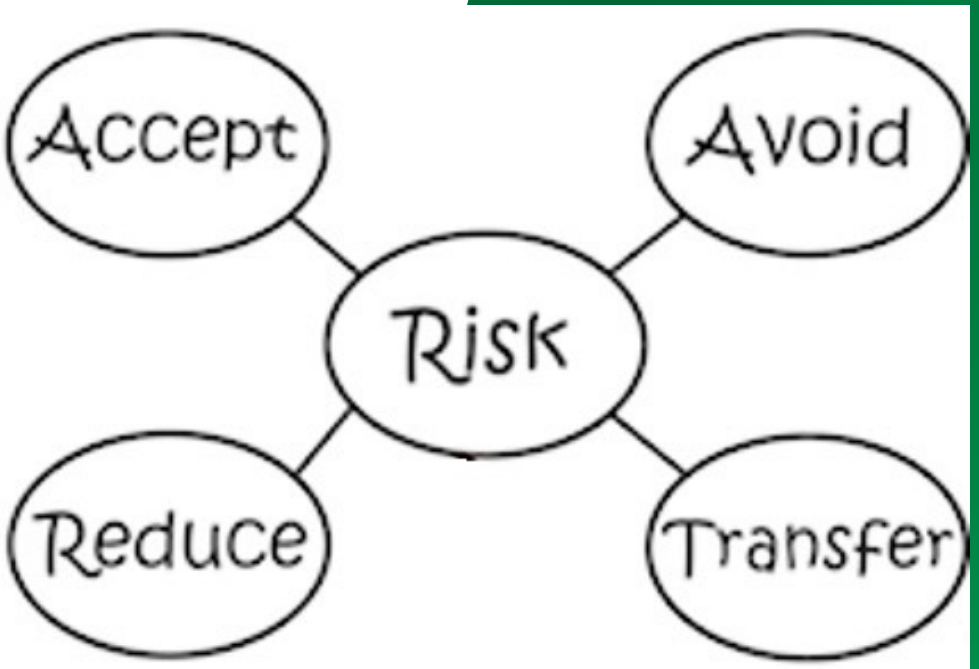
Risk Treatment

Risk avoidance
- do not perform risky activity

Risk mitigation (reduction)
- Prevent/reduce threat occurrence or loss

Risk transfer
- Insurance

Risk acceptance (retention/tolerance)
- Well… ok.



Risk Treatment. Reduction

Risk can be reduced in 3 ways:

- Reduce threat exposure
  - Very difficult!
  - Do not irritate people.
- Reduce threat likelihood
  - Malware protection, Network protection, Cryptography, Incident management
- Reduce threat impact
  - Business continuity plan, Back-up, Incident management

Risk Treatment. Cost-Benefit Analysis

Cost benefit analysis

- $Benefit = Risk_{before} - Risk_{after} - Cost$

Return on (security) investment

- $ROSI = \frac{Risk_{before} - Risk_{after}}{Cost}$
- For greedy approach

Multiple choices? Possible solution: solution to a knapsack-like problem:

- Select a set of possible controls to
  1. Minimise risk
  2. Keep cost within budget

Risk Treatment. Trade-off analysis. Semi-quantitative

		Tradeoff Attributes				
		Ease of Maintenance	Purchase Cost	Vulnerability	Productivity Impact	Tradeoff Ranking
Security Technology	Rank	w = .10	w = .25	w = .35	w = .30	$\Sigma w_i v_i(x_i)$
	Vulnerability Assessment Scanner	25	25	40	0	.20
	Secure Email	40	35	20	0	.24
	Smart Card	25	15	30	60	.34
	E-Signature	10	25	10	40	.22

S. Butler "Security attribute evaluation method: a cost-benefit approach". International Conference on Software Engineering, 20

Risk Treatment. Risk Avoidance

Try to reduce risk

Try to transfer it

If risk is still too high to accept it…

Close the activity which prone to this risk.

For example,

- do not use a cloud system (e.g., if you have not skills to configure it correctly) or
- do not outsource coding to unknown developers

Risk Treatment. Risk Transfer

Shift the activity to another entity (that is responsible for handling risk)

- Managed security
- Cloud
- Outsource development

But, it is difficult to transfer liability

Insurance

- Buy insurance to cover those risks that you cannot accept

Risk Treatment. Risk acceptance

Default option, but you must be aware about this decision

Driven by acceptance criteria

Can we be covered by self-insurance

If you cannot accept risk – re-plan the risk treatment plan

Risk Management. Other activities

Communication and Consultation

- Communicate with stakeholders
- Consult with external experts

Monitoring and review

- Monitor defined values
- Review risk assessment results regularly (or when serious errors detected)

Recording and reporting

- Record the results for the future use
- Report risk assessment results

Conclusions

CSP003_S_E: Artsiom Yautsiukhin (CNR),
Cristina Alcaraz (UMA)

Conclusion

- Risk assessment is an important practice for securing an IT system
- Risk assessment requires:
  - Good planning
  - Time
  - Effort
  - Good knowledge about the IT system
  - Very good knowledge of cyber security
  - Experience in risk management
- There are other ways to treat risks
  - Not only risk reduction

References and sources

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

References and sources

1. Some figures are attributed from Vecteezy,
   URL: https://www.vecteezy.com/ - thanks !
2. DeepL Translator for proofreading.
   URL: https://www.deepl.com/translator
3. ENISA, CIRAS, 2024
   URL: https://ciras.enisa.europa.eu
4. MITRE, MITRE CVE, 2024
   URL: https://cve.mitre.org
5. Figure source: MITRE, MITRE CVE, 2024
   URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=modbus
6. Source: NIST, NVD, 2024
   URL: https://nvd.nist.gov
7. Zografopoulos, Ioannis, Nikos D. Hatziargyriou, and Charalambos Konstantinou. "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations", IEEE Systems Journal (2023)

Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

If you have any questions, please do not hesitate to contact us:

- Artsiom Yautsiukhin
  artsiom.yautsiukhin@iit.cnr.it
- Cristina Alcaraz
  alcaraz@uma.es
- Javier Lopez
  javierlopez@uma.es