Cyber Risk Assessment, IT Asset Management and… AI obviously

Let’s talk about…

Who am I
Cybersecurity 101
Why we are talking about these fascinating arguments
Cyber Risk Management : What it is & How to
IT Asset Management & Cybersecurity
The fast growth of Artificial Intelligence
    Threats and Opportunities
Useful Resources

$ whoami

Graziano Specchierla

I have worked in IT since 1996
Now I'm a Senior Security Consultant
in the Exprivia Cybersecurity Business Unit

Interests & Hobbies:
Technology, Books,
Photography, Travel, Motorbikes,
Cinema, be part of interesting
associations, Personal Growth

https://www.linkedin.com/in/grazianospecchierla/

A well-chosen book saves you from anything, even from yourself.

Daniel Pennac

Cybersecurity 101

Information Security, is 'The degree of resilience of information from damage'.

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, theft, and damage.

«Security Information Management is the art to decide how to spend 0.01$ to minimize the possibility to be a victim of a cyberthreat»

AI

Confidentiality

Only restricted parties (identified, authenticated and authorized) can access the information (read and/or write).

Integrity

Ensure data remains accurate, consistent, and unaltered by unauthorized actions throughout its lifecycle.

Availability

Information is readily available. This requirement primarily concerns storage and data transmission systems, but also privacy regulations

Why we are talking about Cyber Risk & C. : NIS 2

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Article 21

Cybersecurity risk-management measures

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) **policies on risk analysis and information system security**;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) **policies and procedures to assess the effectiveness of cybersecurity risk-management measures**;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Cyber Risk Management: what is it?

Cyber Risk Management

Process for the overall management of cyber risk

It support the evaluation of risk associated with the loss of integrity, confidentiality, availability of information.
The main goal is to reduce the probability and impact of a cyber attack to an acceptable level for the organization.

It is one of the core processes for the cybersecurity
Organizations needs that process to ***understand how to protect the business***, and other processes need Risk Management (continuity, recovery, mitigation plans)

It has to be repeated at least once a year, and partially revised in case of incident or relevant changes in the organization or in the IT

…But Risk Management relies on other aspects that have to be well defined: one of the most important is the IT Asset Management

Standard and Framework
There are many references to help in performing cyber risk management process

ISO 27001 (27005) ("Information security, cybersecurity and privacy protection — Guidance on managing information security risks")
ISO 31000 (Generic)
NIST RMF (Risk Management Framework)
EBIOS (ANSSI)

Good to Know: Glossary

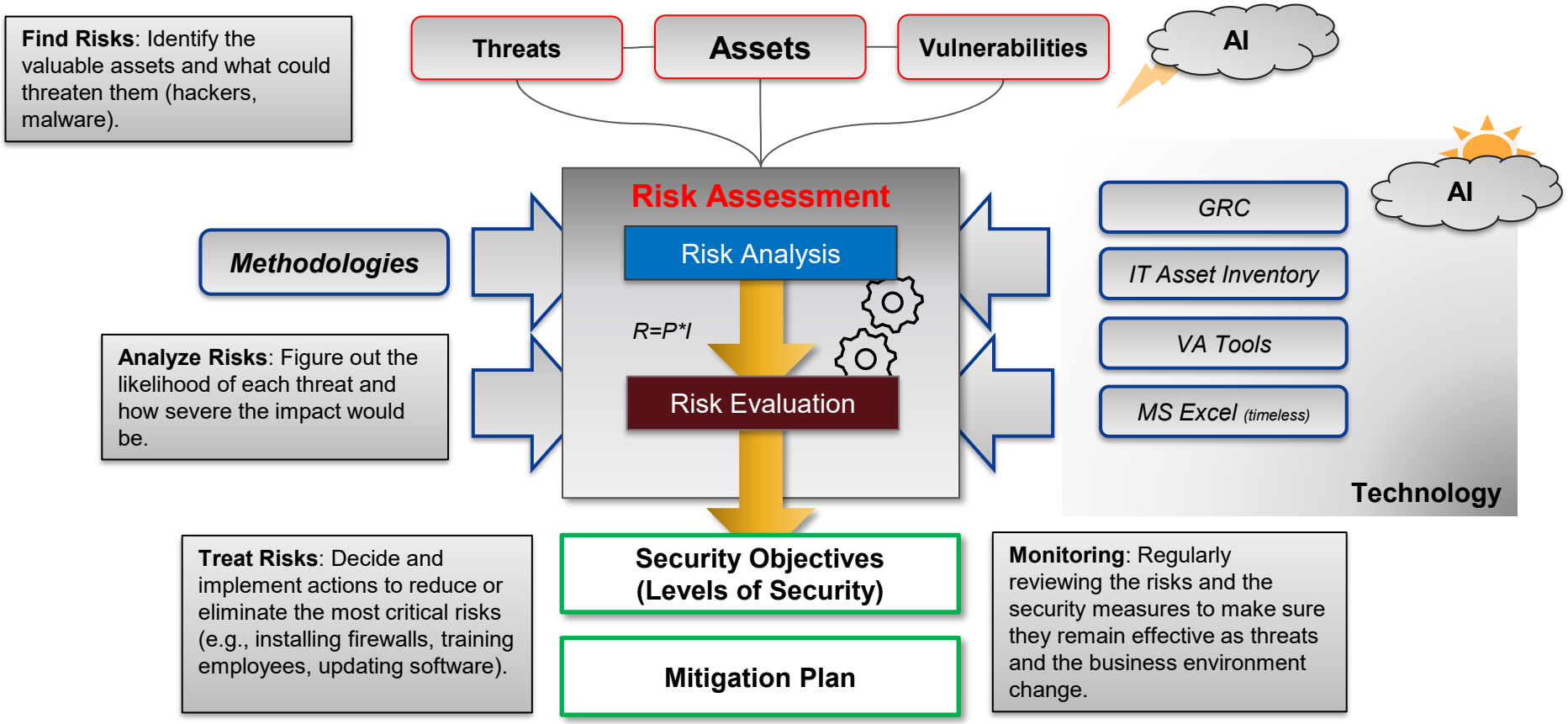
Inherent Risk:
- Risk in absence of controls/measures

Residual Risk:
- Risk that remains out of controls / measures

Risk Appetite :
- The willingness to take risks

Risk Tolerance :
- Boundary limit for cyber risks

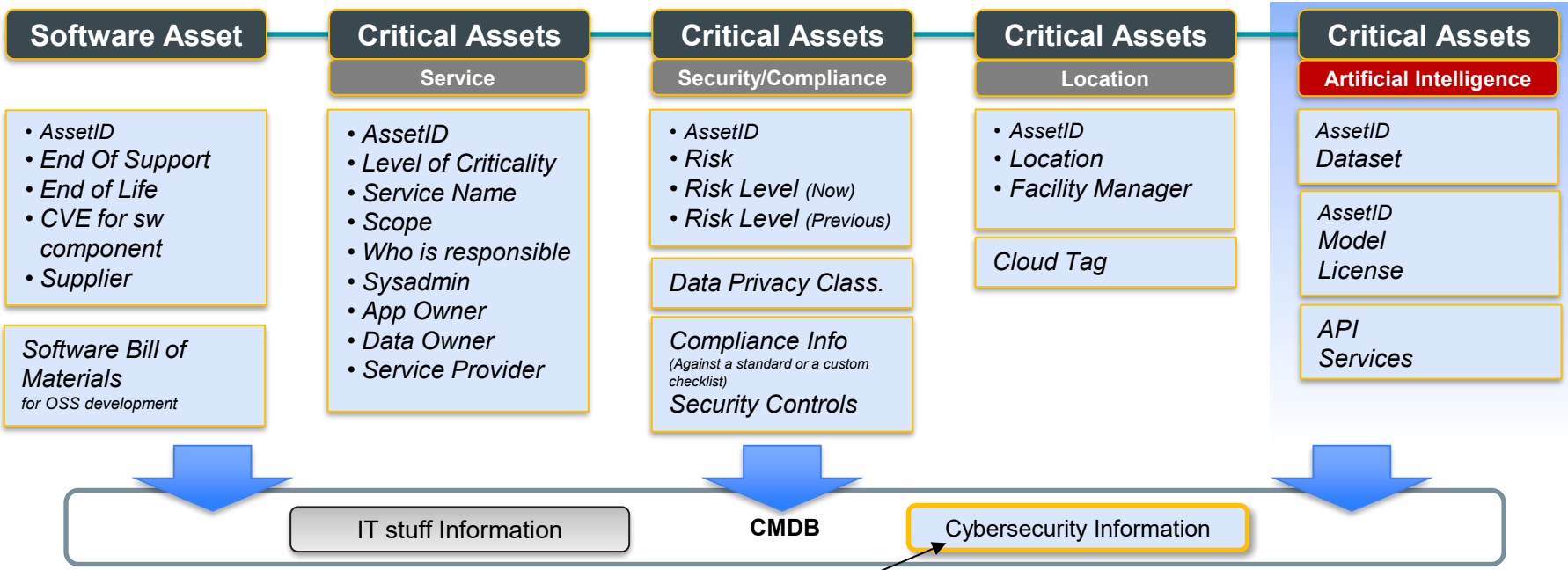
Cyber Risk Management: How To



IT Asset Inventory for Cybersecurity

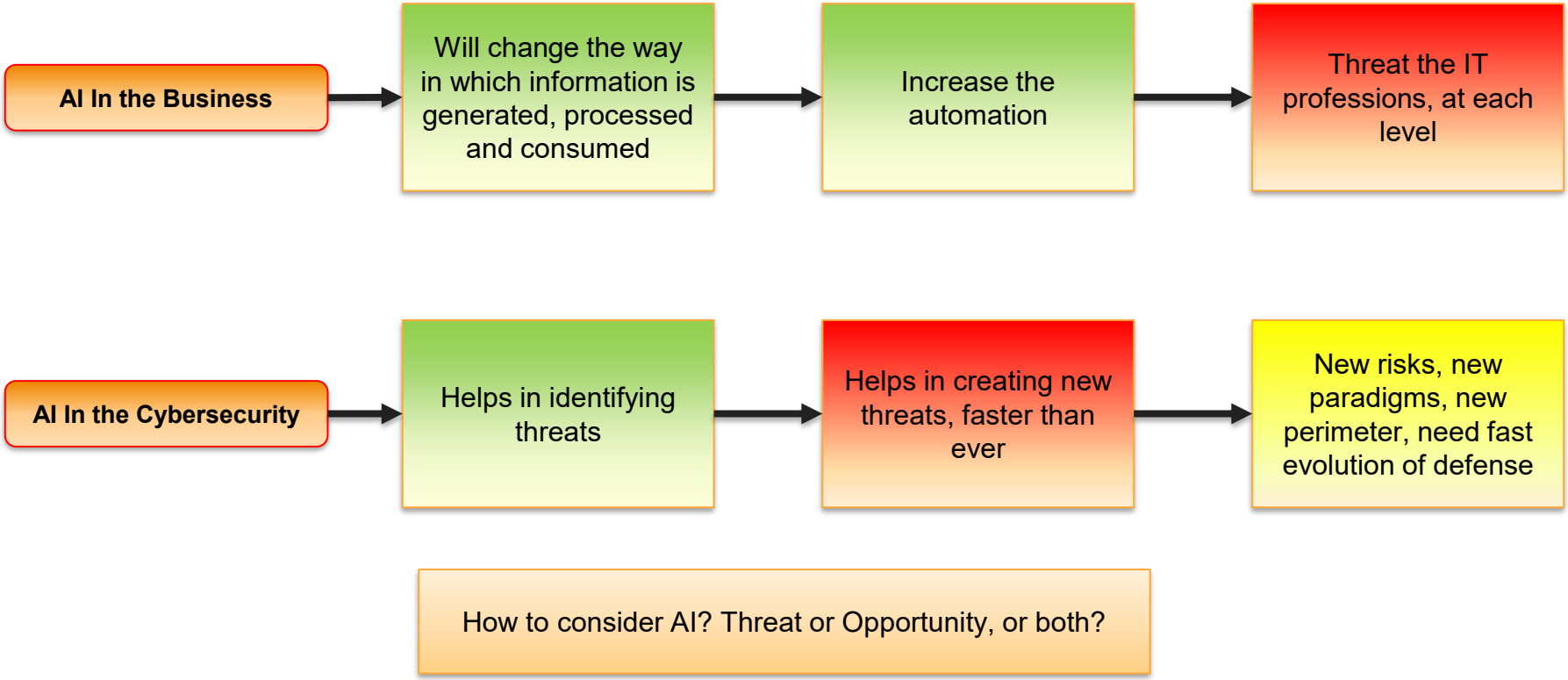
Asset management is crucial: just as it is necessary to know the threats we need to defend against, it is necessary to know **what we need to protect**, to do it in the best possible way.

In order to effectively implement Cybersecurity processes, it is therefore recommended to add and maintain some **additional information** in a “Configuration Management Database”

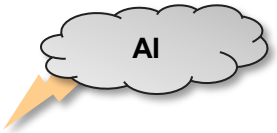


The «need to know» principle has to be applied: the information is only visible to specific parties

The growth of Artificial Intelligence



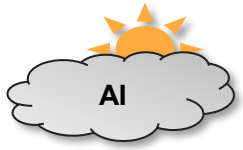
The growth of Artificial Intelligence



Threats

- High expectations, high delusions?
- Answer are calculated, not known. It's probability. So the truth? Poisoned data is a problem.
- Take a lot to segregate and classify data. So put it all together to train the model and… you can query data not in your scope. How to segregate again for role and need to know?
- High costs, high power consumption, where is the cost/benefit? Could be difficult to calculate it.

Opportunities



- Does it works or not for my use case? This could be a good question to start use it.
- In Cybersecurity , could be good for due diligence in documents, policies, procedures
- Automation is more powerful than ever, due to agentic AI and MCP protocol. The digitalization runs faster.
- This is another wave of progress in the information technology. LLM is a step forward, not the last step
- AI needs governance

Private is better

Open Source is better

Has to be managed (ISO 42000)

Has to be secured (Risk Assessment)

Useful Resources

First steps in automating cybersecurity

There are large language models trained and specialized for cybersecurity, a couple of examples:

CybersecurityRiskAnalyst
Custom fine-tuned Large Language Model (LLM) designed to act as a senior cybersecurity risk assessor and strategist.

https://ollama.com/saki007ster/CybersecurityRiskAnalyst

Room-research
Ideal for cyber security researchers who need a reliable assistant for various tasks such as analyzing security logs, generating reports, or providing recommendations on security practices.

https://ollama.com/kangali/room-research

GRC Tools
Eramba (eramba.org)
CISO Assistant (intuitem.com)

By ANSSI, ACN and various

https://cyber.gouv.fr/en/publications/building-trust-ai-through-cyber-risk-based-approach

Grazie!

graziano.specchierla@gmail.com
graziano.specchierla@exprivia.com
graziano.specchierla@sec-ops.it

exprivia CyberSecurity

The art of optimizing Investments reducing risks

BOF

NIS2 is here to stay

17:00
40 mins
07/11/2025

Deepdive in the norm with an opensouce perspective

Crane Hall