Cyber Security obsolete ?
Speak about Cyber Resilience Now !

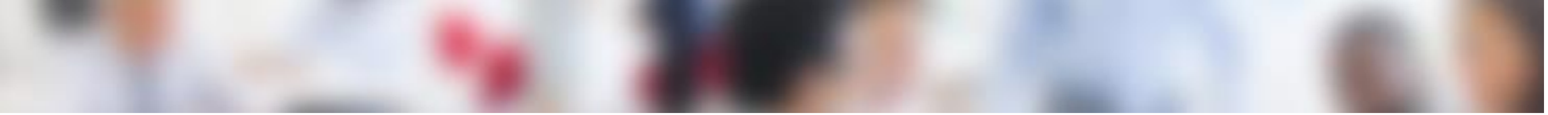
INDUSTRIAL CYBERSEC FORUM

09/02/2023

Embracing technology
Embracing ambition

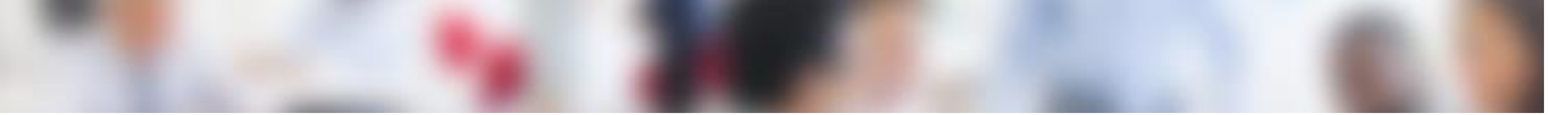
Eric Van Cangh
Senior Business Group Leader Cyber Security

.AGORIA



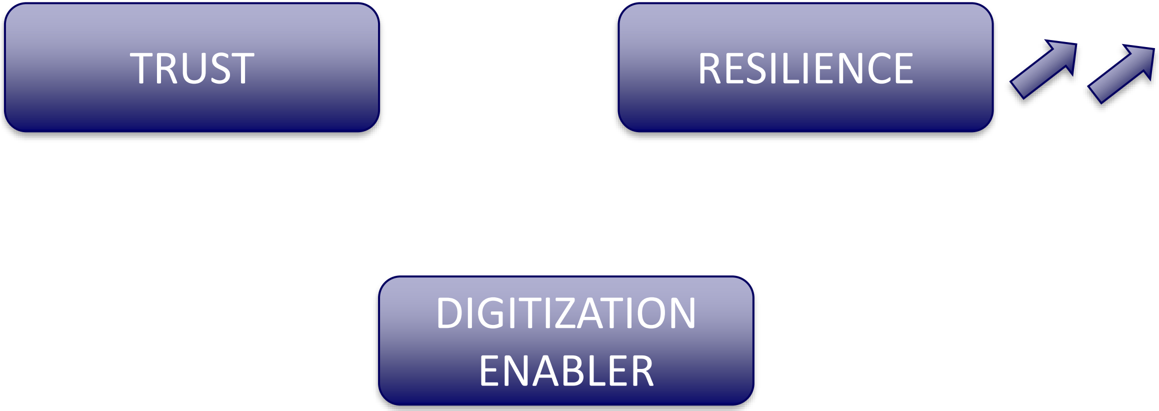
Agenda

- **Introduction**
  - Value proposition
- **Cyber Security Basics**
  - Set the scene
  - Understand the specificities of IT / OT world
- **Importance of Cyber Resilience**
  - Definition
  - Why is CS obsolete ?
- **How to achieve Cyber Resilience ? The Building Blocks**
  - Strategic level – ABC for Executive
  - Tactic level – ICD processes
  - Operational Level – AOA Matrix
- **Conclusion**



Introduction – Value Proposition

- **The Value proposition of Cyber Security**

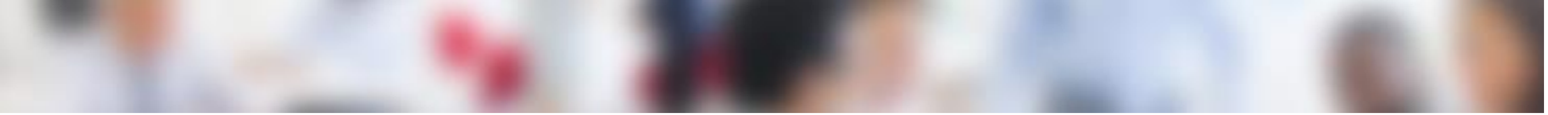


TRUST

RESILIENCE

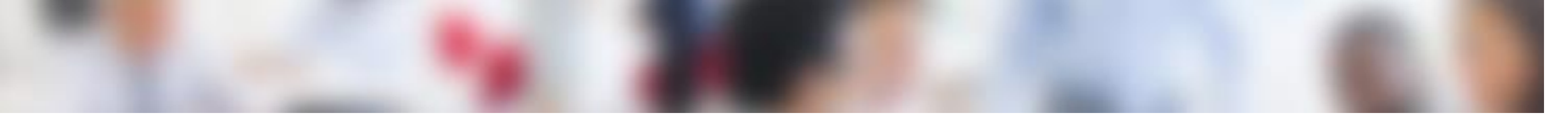
DIGITIZATION ENABLER

https://en.wikipedia.org/wiki/Digitization

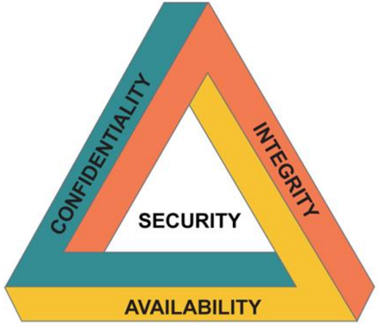


Agenda

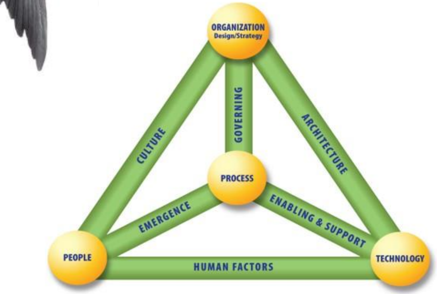
- **Introduction**
  - Value proposition
- **Cyber Security Basics**
  - Set the scene
  - Understand the specificities of IT / OT world
- **Importance of Cyber Resilience**
  - Definition
  - Why is CS obsolete ?
- **How to achieve Cyber Resilience ? The Building Blocks**
  - Strategic level – ABC for Executive
  - Tactic level – ICD processes
  - Operational Level – AOA Matrix
- **Conclusion**



Set the scene – CyberSecurity ?

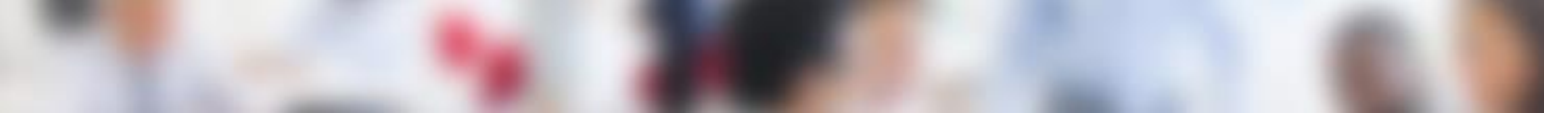


The Security triad
Confidentiality , Integrity , Availability



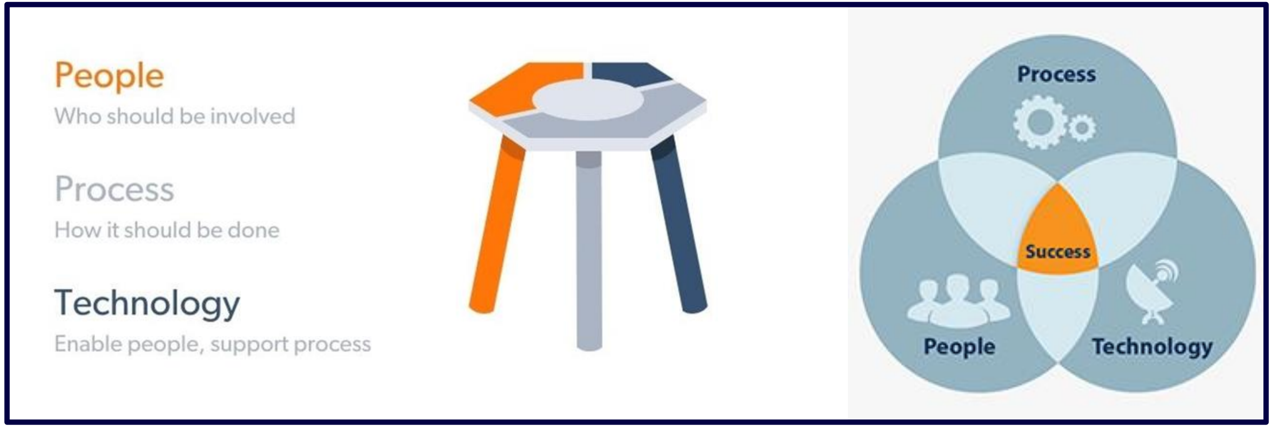
All the <u>means</u> to secure/protect the information at People, Process and Technology level

https://cio-wiki.org/wiki/Business_Model_for_Information_Security_(BMIS)



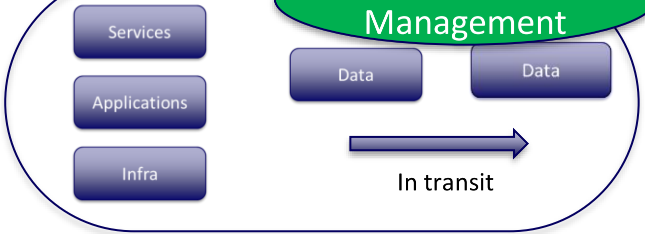
How to implement CS activities?

“The 3-legged stool of People-Process-Technology”

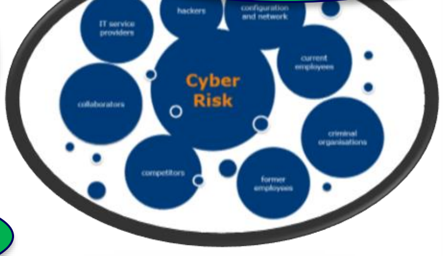


Set the scene - Context

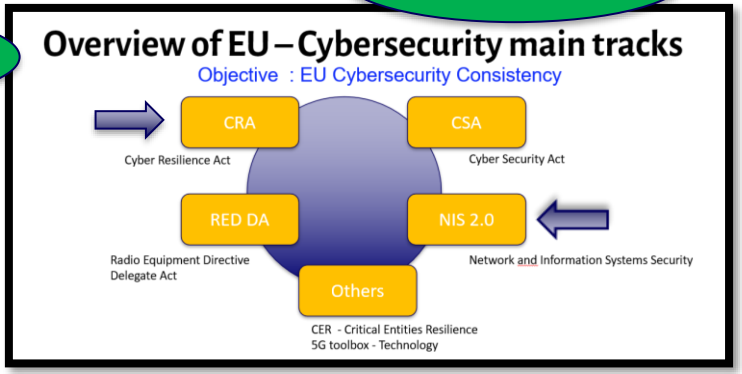
Asset Management



Risk



Compliance



Overview of EU – Cybersecurity main tracks

Objective : EU Cybersecurity Consistency

CRA
Cyber Resilience Act
CSA
Cyber Security Act
RED DA
Radio Equipment Directive Delegate Act
NIS 2.0
Network and Information Systems Security
Others
CER - Critical Entities Resilience
5G toolbox - Technology

Ownership

Attributs de Sécurité	Besoin en Sécurit			
C rating	Correctement classifié			
I rating	Correctement classifié			
A rating	Correctement classifié	I	A	R
Business Owner	Correctement Inventorié	I	A	R
Technical Owner	Correctement Inventorié	I	A	R
Subject Matter Expert (SME) Owner	Correctement Inventorié	I	A	R
CMDB owner	Correctement Inventorié	I	A	R
ENV Environment	Correctement Inventorié	I	A	R
RTO	Besoin en Continuité	C	A	R
RPO	Besoin en Continuité	C	A	R
Web facing	Protégés (gérer risques)	R	R	A
OS (operating system)	Complétude des attributs de sécurité	I	A	R
Config admin group	protégés (accès)	A	R	C
CI Status	Décommissionné en fin de vie	R	A	I
Security OPERATIONAL STATUS	Correctement Inventorié	I	A	R
Classe = CI Type	Correctement Inventorié	I	A	R
Asset type	Correctement Inventorié	I	A	R
Asset subtype	Correctement Inventorié	I	A	R
Last review date	Complétude des attributs de sécurité	I	A	R
Creation date	Demande création actif	R	A	C
Antimalware (installed)	Protégés (gérer risques)			
ISO_SEC_location	Besoin en Continuité			
CMDB field properties	Complétude des attributs de sécurité			
Security Impact (yes/no)	Protégés (gérer risques)	R		

Attributes

Confidentiality

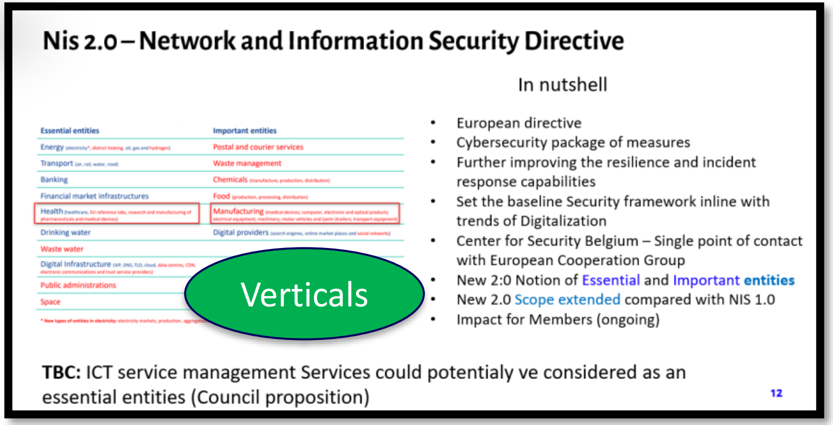
Integrity

Availability

Privacy

Safety

Verticals



Nis 2.0 – Network and Information Security Directive

In nutshell

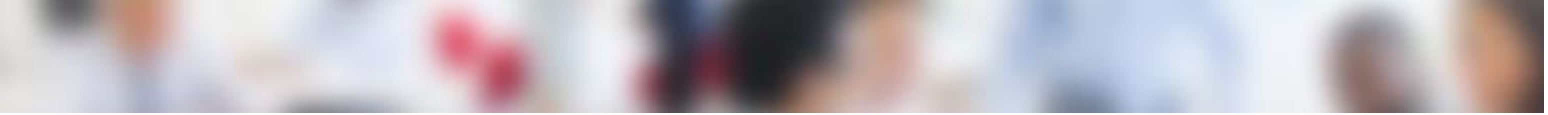
Essential entities	Important entities
Energy (electricity*, district heating, oil, gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)	
Public administrations	
Space	

* New types of entities in electricity: electricity markets, production, aggreg

- European directive
- Cybersecurity package of measures
- Further improving the resilience and incident response capabilities
- Set the baseline Security framework inline with trends of Digitalization
- Center for Security Belgium – Single point of contact with European Cooperation Group
- New 2:0 Notion of Essential and Important entities
- New 2.0 Scope extended compared with NIS 1.0
- Impact for Members (ongoing)

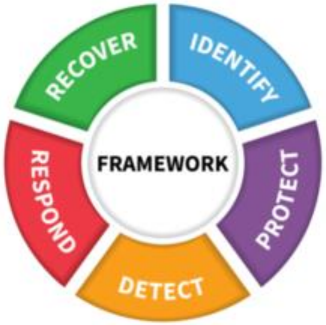
TBC: ICT service management Services could potentialy ve considered as an essential entities (Council proposition)

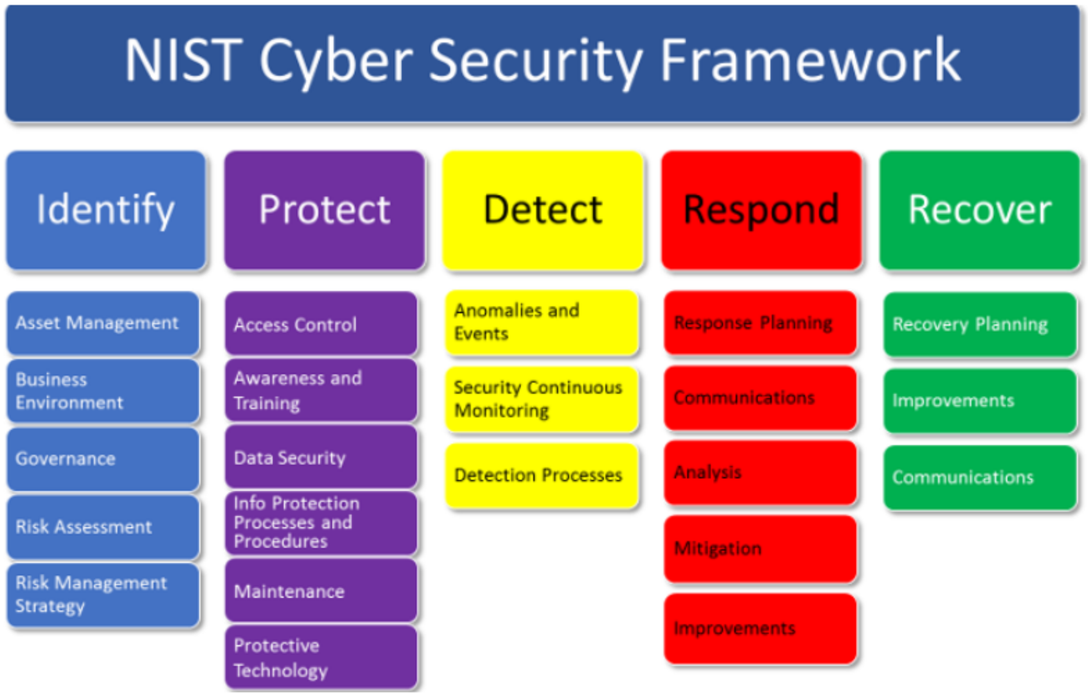
12



National Institute of Standards and Technology

NIST – the 5 Cyber Security functions





NIST Cyber Security Framework

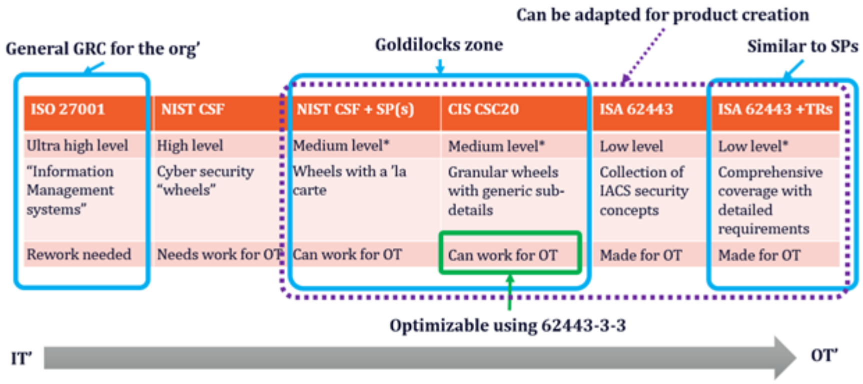
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

https://www.nist.gov/cyberframework/online-learning/five-functions

IT/OT World

Blending IEC 62443 with other frameworks and standards

IEC 62443 standards are fully compatible and mostly map directly with other well-known guidance such as the NIST CSF. There can be, however, substantial differences in language and application that require the use of OT-specific overlays and adaptation of IT variations in order to manage exceptions in a converged OT/IT environment. Getting the best of both worlds requires organizations to get a little creative.



Can be adapted for product creation

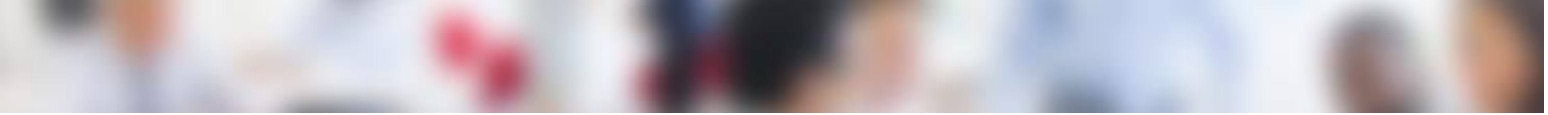
General GRC for the org’

Goldilocks zone

Similar to SPs

ISO 27001	NIST CSF	NIST CSF + SP(s)	CIS CSC20	ISA 62443	ISA 62443 +TRs
Ultra high level	High level	Medium level*	Medium level*	Low level	Low level*
“Information Management systems”	Cyber security “wheels”	Wheels with a ’la carte	Granular wheels with generic sub-details	Collection of IACS security concepts	Comprehensive coverage with detailed requirements
Rework needed	Needs work for OT	Can work for OT	Can work for OT	Made for OT	Made for OT

Optimizable using 62443-3-3



Understand the specificities of IT / OT world

ANSI ISA/IEC 62443

Security Challenges in IACS / OT are

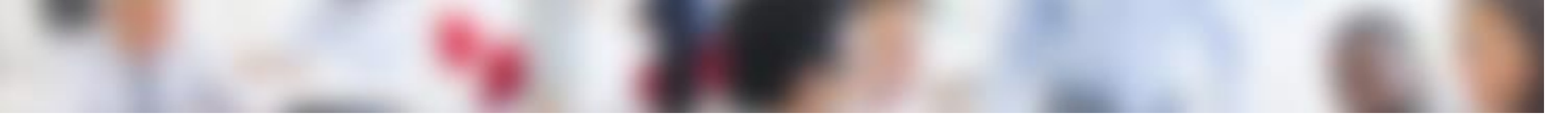
- The relative criticality of data confidentiality in facility operations or functions.
- Unique approaches to ensure systems reliability and integrity in industrial environments.
- Potential dangers to personnel, the environment, and society in the event of cyber-physical failures. = SAFETY
- The increased need for compensating controls to protect legacy IACS/OT systems.
- The relative difficulty of applying common IT security techniques without severe systems modifications.
- Prospects for financial loss due to an incident-related drop in productivity.

AVAILABILITY

SAFETY

LEGACY

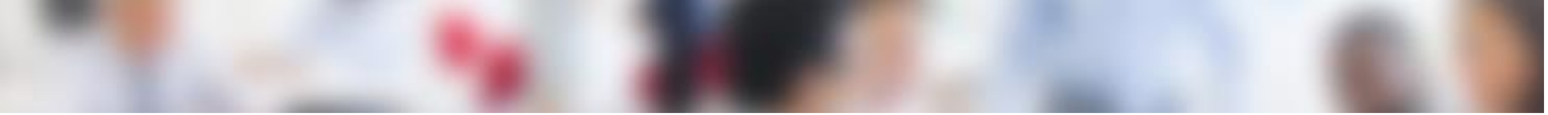
DIFFICULTY



.AGORIA

Agenda

- **Introduction**
  - Value proposition
- **Cyber Security Basics**
  - Set the scene
  - Understand the specificities of IT / OT world
- **Importance of Cyber Resilience**
  - Definition
  - Why is CS obsolete ?
- **How to achieve Cyber Resilience ? The Building Blocks**
  - Strategic level – ABC for Executive
  - Tactic level – ICD processes
  - Operational Level – AOA Matrix
- **Conclusion**



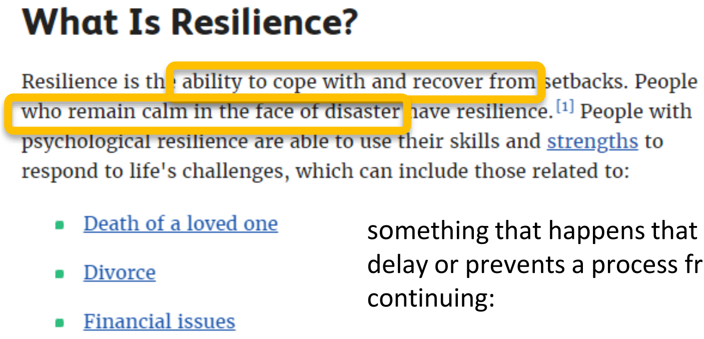
RESILIENCE DEFINITION

“Resilience is the process and outcome of successfully adapting to difficult or challenging life experiences, especially through mental, emotional, and behavioral flexibility and adjustment to external and internal demands.”

AMERICAN PSYCHOLOGICAL ASSOCIATION

erhui1979 | Getty Images (*)

https://www.entrepreneur.com/leadership/7-keys-to-developing-resilience/329053



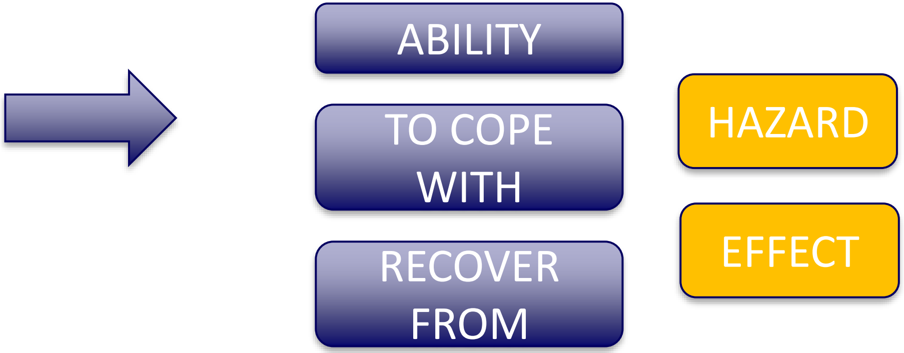
What Is Resilience?

Resilience is the ability to cope with and recover from setbacks. People who remain calm in the face of disaster have resilience.[1] People with psychological resilience are able to use their skills and strengths to respond to life's challenges, which can include those related to:

- Death of a loved one
- Divorce
- Financial issues

something that happens that causes a delay or prevents a process from continuing:

https://www.verywellmind.com/what-is-resilience-2795059



ABILITY

TO COPE WITH

RECOVER FROM

HAZARD

EFFECT

Why is CS obsolete ?

- You need to understand the context

4000 openstaande vacatures, 100 cyberaanvallen per dag

Eric Van Cangh (Agoria), Dominique Demonte (Agoria), Ludivine Dedonder (MOD), Kolonel Pierre Ciparisse (Defensie), Miguel Debruycker (CCB), Filip Verstockt (Orange Cyberdefense)

https://www.tijd.be/

First socio-economic study on the cyber security sector in Belgium

November 2022

Embracing technology
Embracing ambition

.AGORIA

.AGORIA

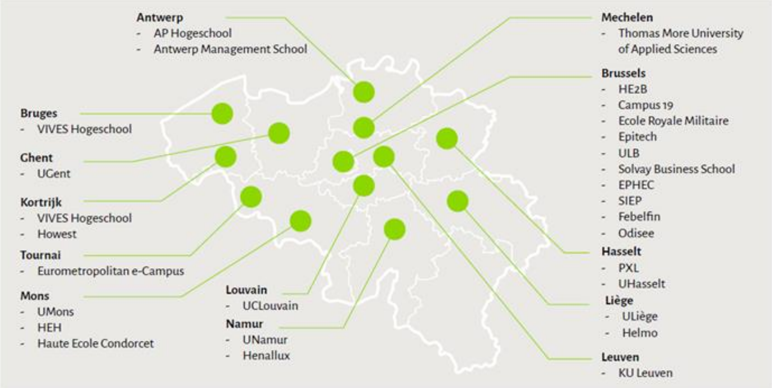
Belgium’s cyber security ecosystem

Cyber security providers and services

* Cyber security providers	
Generalists	Organisations that offer multiple cyber services
Consultants	Consultants regarding cyber security services
Integrators	Organisations that integrate products and components in industrial environments
Specialists (Pure players)	Organisations that focus on one specific cyber domain
Specialists (Niche players)	Organisations that focus on one specific sector or vertical (e.g., telecom, public services, insurance)
Training, education and certification entities	Organisations that mainly offer cyber education and certifications
Innovators	Start-ups and scale-ups that focus on an innovative product or service

** Cyber security services
Consulting and audits
Certification and accreditation
Security products (SW, HW, SECaaS, Insurance)
Security solutions (Integrations & Engineering)
Managed security services (Monitoring, Detection & Response)
Forensics and incident handling (CIRT, CERT)
Security training, education and certification
Research, development and innovation

Overview: main schools that offer cyber courses (excl. online programmes)



Antwerp
- AP Hogeschool
- Antwerp Management School

Bruges
- VIVES Hogeschool

Ghent
- UGent

Kortrijk
- VIVES Hogeschool
- Howest

Tournai
- Eurometropolitan e-Campus

Mons
- UMons
- HEH
- Haute Ecole Condorcet

Louvain
- UCLouvain

Namur
- UNamur
- Henallux

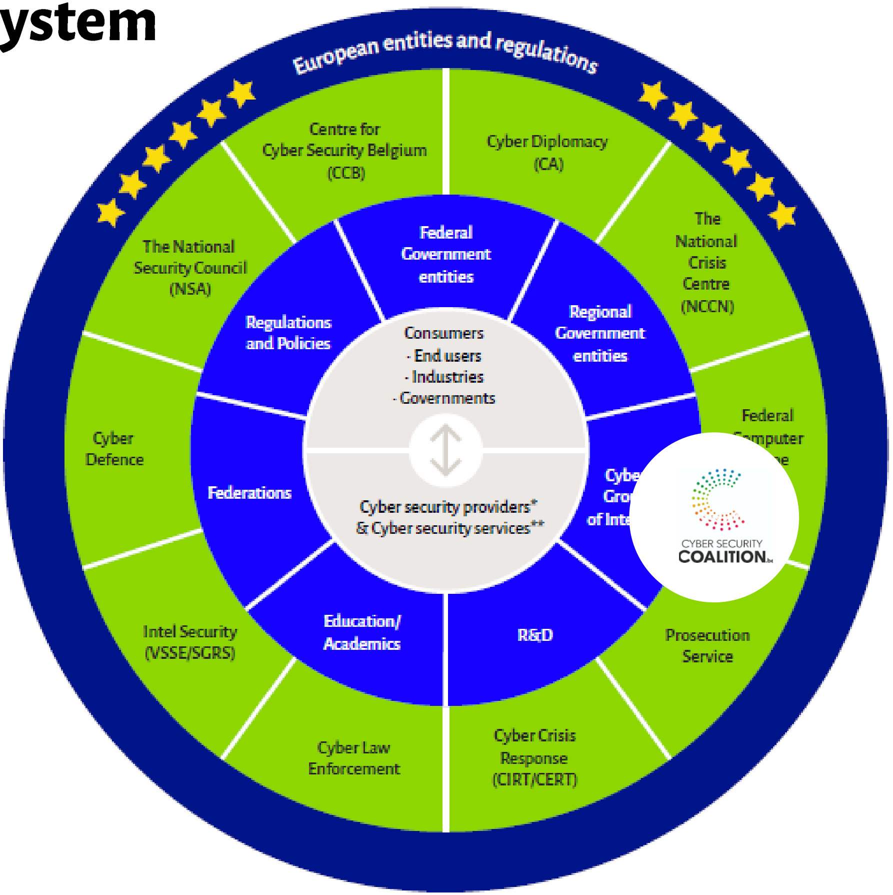
Mechelen
- Thomas More University of Applied Sciences

Brussels
- HE2B
- Campus 19
- Ecole Royale Militaire
- Epitech
- ULB
- Solvay Business School
- EPHEC
- SIEP
- Febelfin
- Odisee

Hasselt
- PXL
- UHasselt

Liège
- ULiège
- Helmo

Leuven
- KU Leuven



European entities and regulations

Centre for Cyber Security Belgium (CCB)

Cyber Diplomacy (CA)

The National Crisis Centre (NCCN)

Federal
mputer
e

Prosecution Service

Cyber Crisis Response (CIRT/CERT)

Cyber Law Enforcement

Intel Security (VSSE/SGRS)

Cyber Defence

The National Security Council (NSA)

Federal Government entities

Regional Government entities

Cybe
Gro
of Inte

R&D

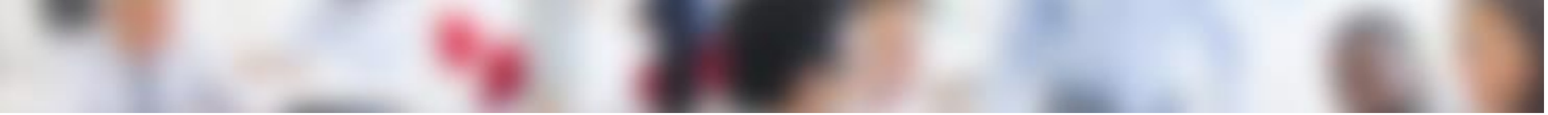
Education/ Academics

Federations

Regulations and Policies

Consumers
- End users
- Industries
- Governments

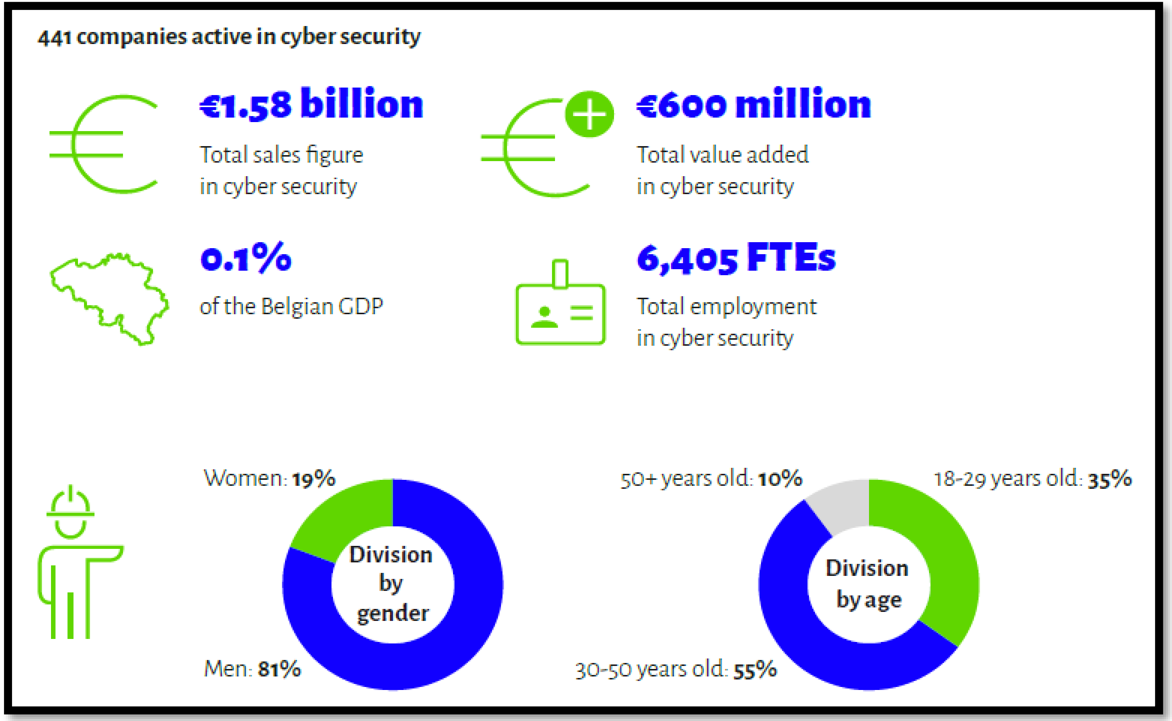
Cyber security providers*
& Cyber security services**



.AGORIA

The Belgian cyber security landscape (2021)

441 Companies



441 companies active in cyber security

€1.58 billion
Total sales figure
in cyber security

€600 million
Total value added
in cyber security

0.1%
of the Belgian GDP

6,405 FTEs
Total employment
in cyber security

Division by gender

Women: **19%**

Men: **81%**

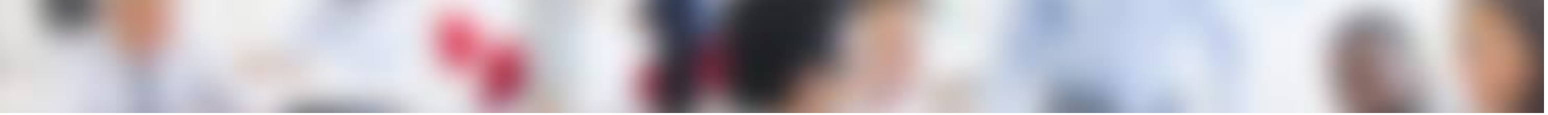
Division by age

50+ years old: **10%**

18-29 years old: **35%**

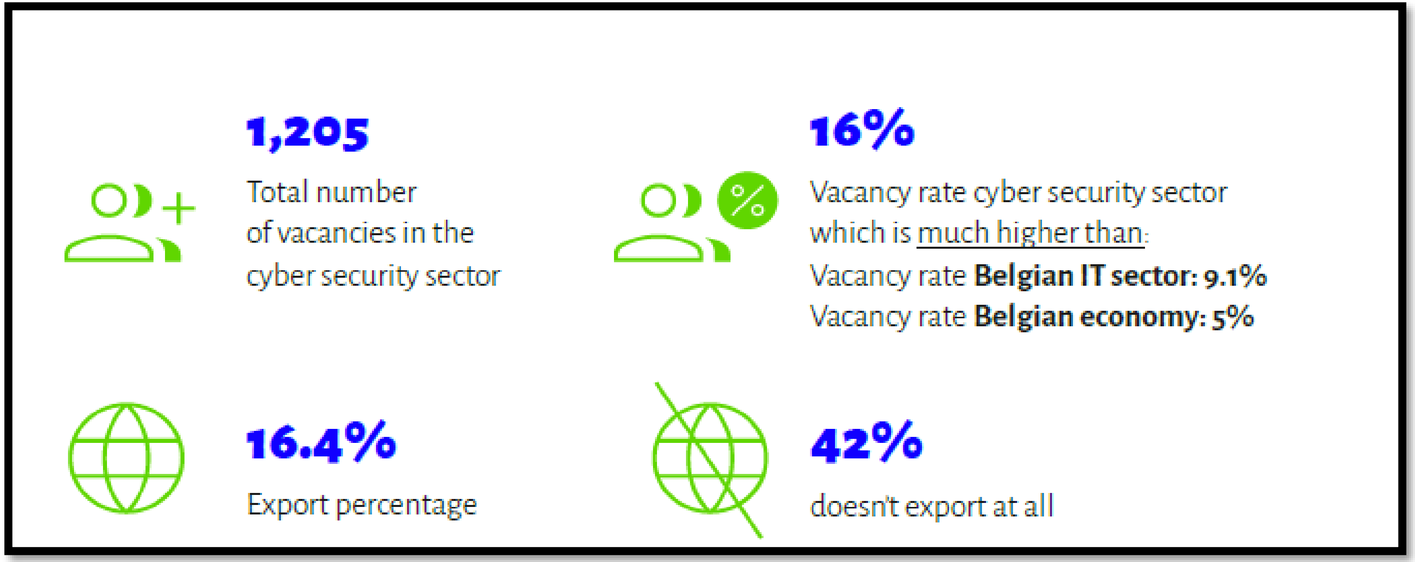
30-50 years old: **55%**

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION



.AGORIA

The Belgian cyber security landscape (2021)



1,205

Total number of vacancies in the cyber security sector

16%

Vacancy rate cyber security sector which is much higher than:

Vacancy rate **Belgian IT sector: 9.1%**

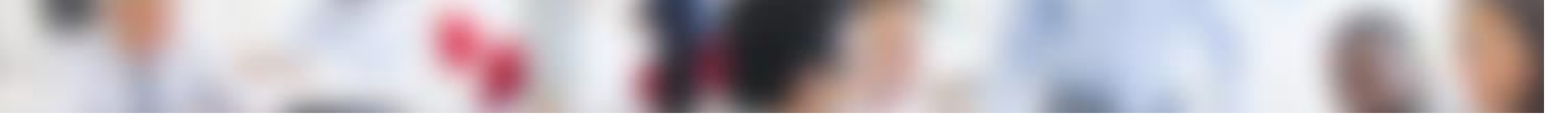
Vacancy rate **Belgian economy: 5%**

16.4%

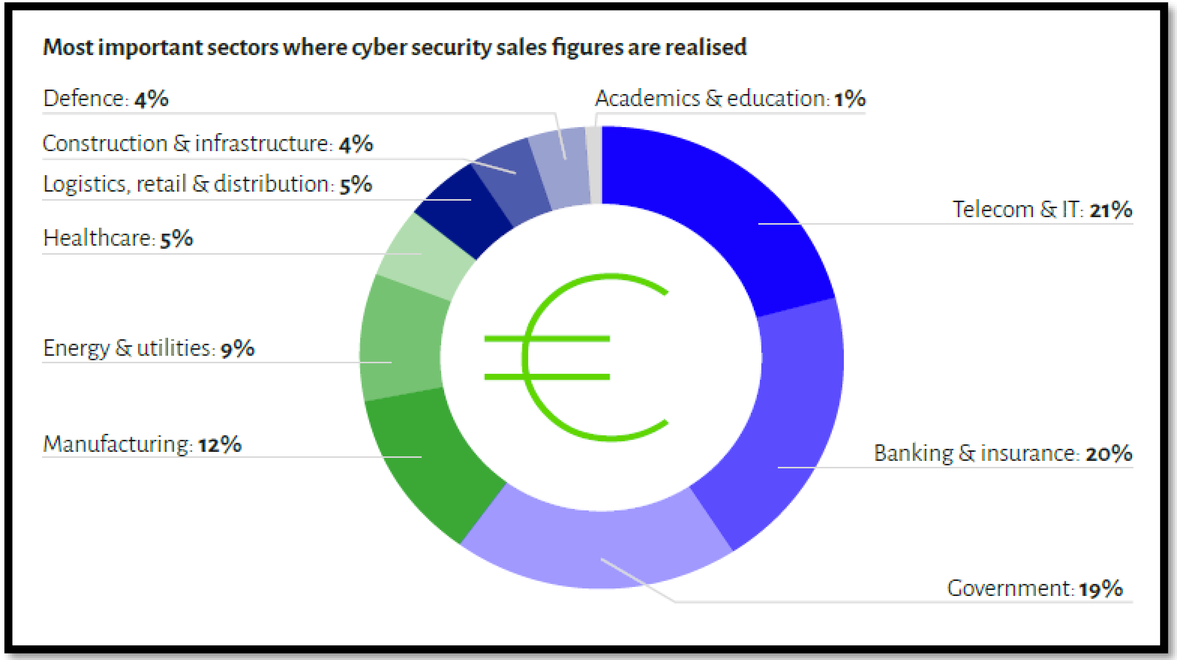
Export percentage

42%

doesn't export at all

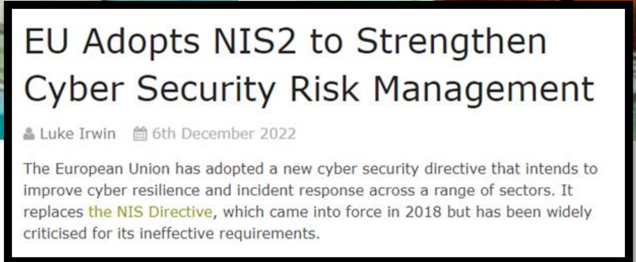


The Belgian cyber security landscape (2021)



Most important sectors where cyber security sales figures are realised

Cyber Security is based on risk



EU Adopts NIS2 to Strengthen Cyber Security Risk Management

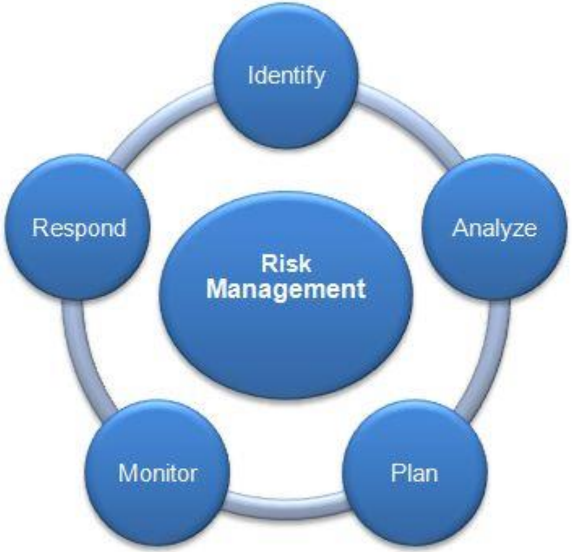
Luke Irwin 6th December 2022

The European Union has adopted a new cyber security directive that intends to improve cyber resilience and incident response across a range of sectors. It replaces the NIS Directive, which came into force in 2018 but has been widely criticised for its ineffective requirements.

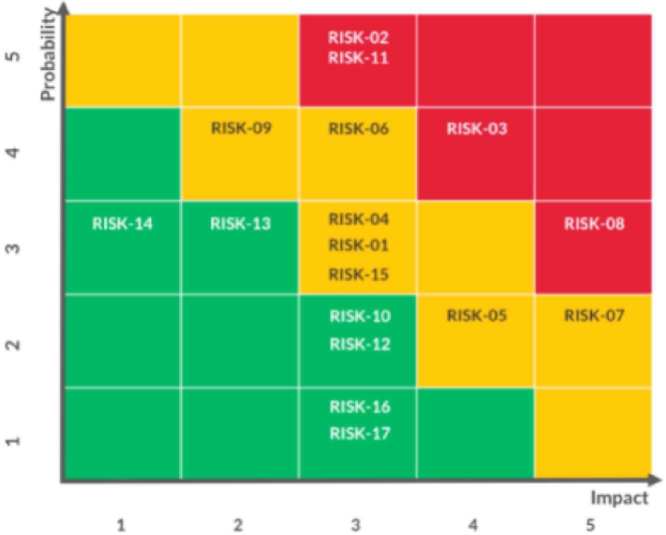
https://www.itgovernance.eu/blog/en/eu-adopts-nis2-to-strengthen-cyber-security-risk-management

What is a risk? – in a nutshell

- R = P x I
- “FROC” risks (*)
- Quantitative
- Qualitative
- Risk appetite
- Risk tolerance



(*) Financial,Reputational,Organizational, Compliance

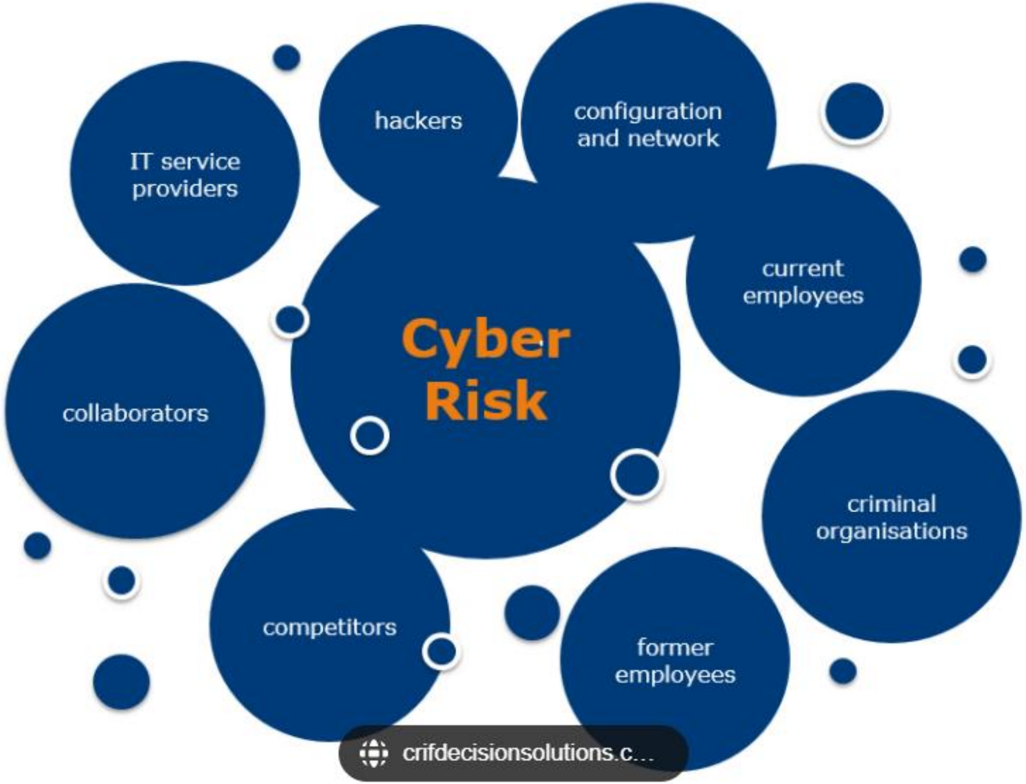


Probability \ Impact	1	2	3	4	5
5	🟨	🟨	🟥 RISK-02 RISK-11	🟥	🟥
4	🟩	🟨 RISK-09	🟨 RISK-06	🟥 RISK-03	🟥
3	🟩 RISK-14	🟩 RISK-13	🟨 RISK-04 RISK-01 RISK-15	🟨	🟥 RISK-08
2	🟩	🟩	🟩 RISK-10 RISK-12	🟨 RISK-05	🟨 RISK-07
1	🟩	🟩	🟩 RISK-16 RISK-17	🟩	🟨

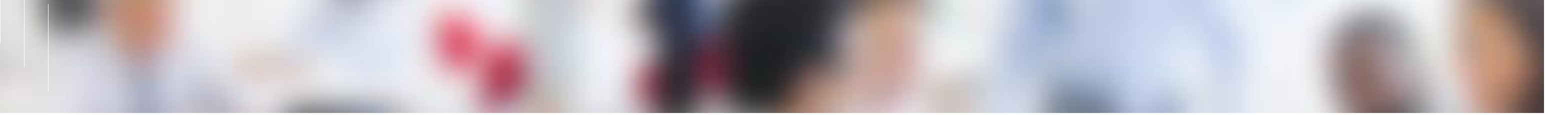
If you are not familiar with risks , adress this point quickly

https://firebrand.training/uk/learn/pmp/course-material/project-risk-management/qualitative-risk-analysis

Cyber risks ?

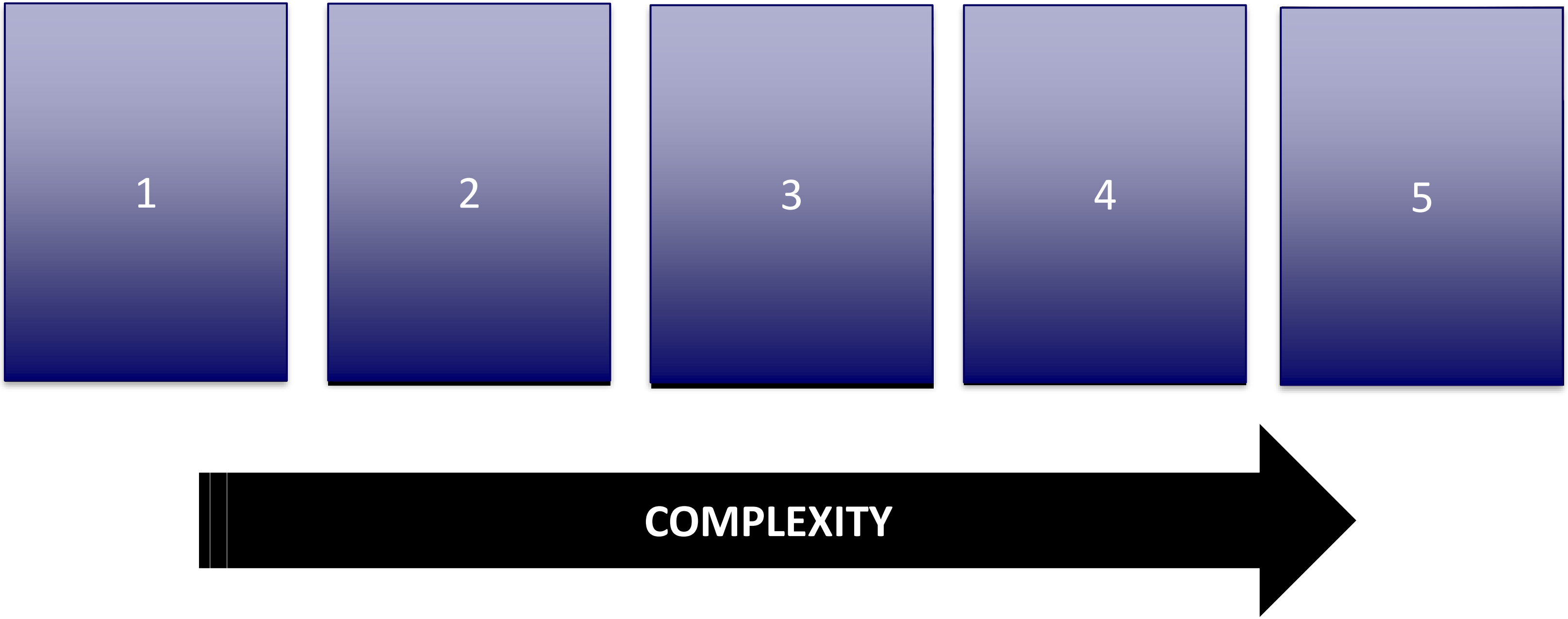


crifdecisionsolutions.c...



Who’s attacking ?

- Main attacks actors



1

2

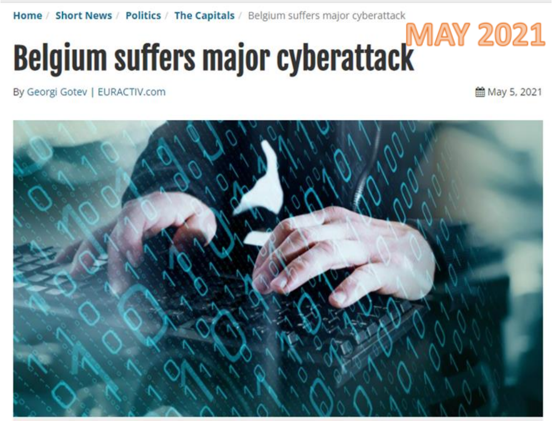
3

4

5

COMPLEXITY

Cyber risks – Belgium as a target?



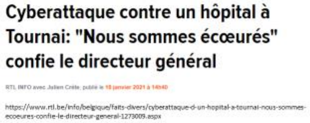
MAY 2021

Home / Short News / Politics / The Capitals / Belgium suffers major cyberattack

Belgium suffers major cyberattack

By Georgi Gotev | EURACTIV.com — May 5, 2021

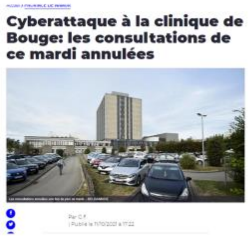
January 2021



Cyberattaque contre un hôpital à Tournai: "Nous sommes écœurés" confie le directeur général

RTL INFO avec Julien Crète, publié le 18 janvier 2021 à 14h40

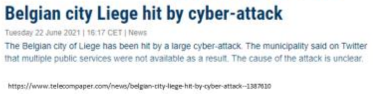
https://www.rtl.be/info/belgique/faits-divers/cyberattaque-d-un-hopital-a-tournai-nous-sommes-ecoeures-confie-le-directeur-general-1273009.aspx



Cyberattaque à la clinique de Bouge: les consultations de ce mardi annulées

Par C.F. | Publié le 11/10/2021 à 17:22

June 2021



Belgian city Liege hit by cyber-attack

Tuesday 22 June 2021 | 16:17 CET | News

The Belgian city of Liege has been hit by a large cyber-attack. The municipality said on Twitter that multiple public services were not available as a result. The cause of the attack is unclear.

https://www.telecompaper.com/news/belgian-city-liege-hit-by-cyber-attack--1387610

October 2021

Ce samedi, la clinique Saint-Luc de Bouge a été la proie d'une cyberattaque. Ce lundi matin, les experts fédéraux ainsi que le service informatique de l'hôpital ont analysé la situation. La décision a été prise d'annuler les consultations de ce mardi. La situation sera réévaluée par la suite.

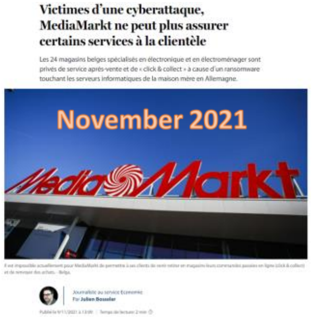
[Cyberattaque à la clinique de Bouge: les consultations de ce mardi annulées - Édition digitale de Namur (sudinfo.be)]

European Oil Port Terminals Hit by Cyberattack

February 2022

Antwerp, Belgium's main port, was one of those where oil trading firms systems were hacked by suspected ransomware attackers.

Credit: EMMANUEL DUNAND/AFP



Victimes d'une cyberattaque, MediaMarkt ne peut plus assurer certains services à la clientèle

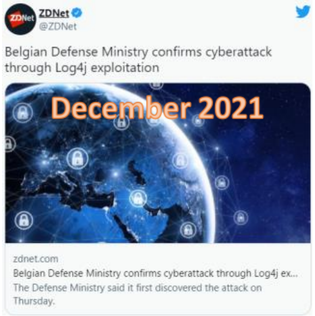
Les 24 magasins belges spécialisés en électronique et en électroménager sont privés de service après-vente et de « click & collect » à cause d'un ransomware touchant les serveurs informatiques de la maison mère en Allemagne.

November 2021

Il est impossible actuellement pour MediaMarkt de permettre à ses clients de venir retirer en magasins leurs commandes passées en ligne (click & collect) et de renvoyer des achats. - Belga.

Journaliste au service Économie
Par Julien Bosseler

Publié le 9/11/2021 à 13:00 | Temps de lecture: 2 min

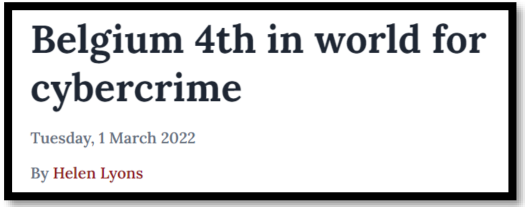


ZDNet
@ZDNet

Belgian Defense Ministry confirms cyberattack through Log4j exploitation

December 2021

zdnet.com
Belgian Defense Ministry confirms cyberattack through Log4j ex...
The Defense Ministry said it first discovered the attack on Thursday.

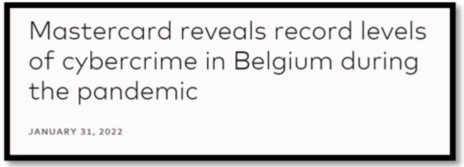


Belgium 4th in world for cybercrime

Tuesday, 1 March 2022

By Helen Lyons

https://www.brusselstimes.com/justice-belgium/208033/belgium-4th-in-world-for-cybercrime



Mastercard reveals record levels of cybercrime in Belgium during the pandemic

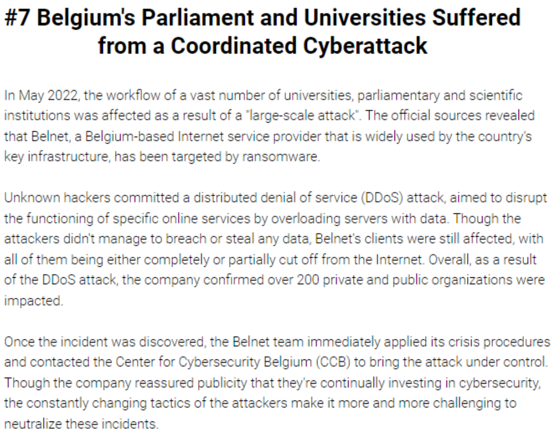
JANUARY 31, 2022

https://www.mastercard.com/news/europe/en/newsroom/press-releases/en/2022/january/mastercard-reveals-record-levels-of-cybercrime-in-belgium-during-the-pandemic/

Cyber risks – Belgium as a target?

https://www.cyberlands.io/topsecuritybreachesbelgium

May 2022

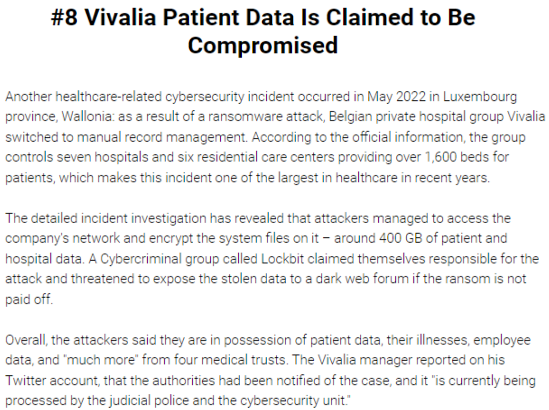


#7 Belgium's Parliament and Universities Suffered from a Coordinated Cyberattack

In May 2022, the workflow of a vast number of universities, parliamentary and scientific institutions was affected as a result of a "large-scale attack". The official sources revealed that Belnet, a Belgium-based Internet service provider that is widely used by the country's key infrastructure, has been targeted by ransomware.

Unknown hackers committed a distributed denial of service (DDoS) attack, aimed to disrupt the functioning of specific online services by overloading servers with data. Though the attackers didn't manage to breach or steal any data, Belnet's clients were still affected, with all of them being either completely or partially cut off from the Internet. Overall, as a result of the DDoS attack, the company confirmed over 200 private and public organizations were impacted.

Once the incident was discovered, the Belnet team immediately applied its crisis procedures and contacted the Center for Cybersecurity Belgium (CCB) to bring the attack under control. Though the company reassured publicity that they're continually investing in cybersecurity, the constantly changing tactics of the attackers make it more and more challenging to neutralize these incidents.



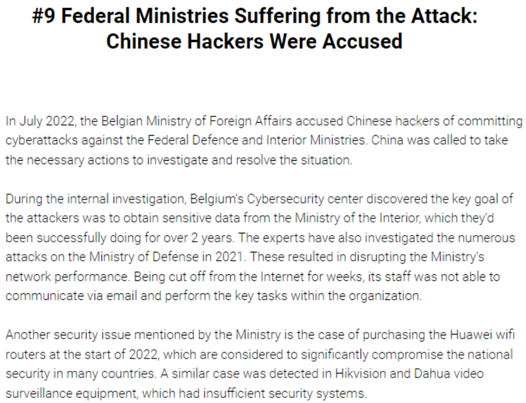
#8 Vivalia Patient Data Is Claimed to Be Compromised

Another healthcare-related cybersecurity incident occurred in May 2022 in Luxembourg province, Wallonia: as a result of a ransomware attack, Belgian private hospital group Vivalia switched to manual record management. According to the official information, the group controls seven hospitals and six residential care centers providing over 1,600 beds for patients, which makes this incident one of the largest in healthcare in recent years.

The detailed incident investigation has revealed that attackers managed to access the company's network and encrypt the system files on it – around 400 GB of patient and hospital data. A Cybercriminal group called Lockbit claimed themselves responsible for the attack and threatened to expose the stolen data to a dark web forum if the ransom is not paid off.

Overall, the attackers said they are in possession of patient data, their illnesses, employee data, and "much more" from four medical trusts. The Vivalia manager reported on his Twitter account, that the authorities had been notified of the case, and it "is currently being processed by the judicial police and the cybersecurity unit."

July 2022



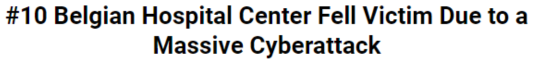
#9 Federal Ministries Suffering from the Attack: Chinese Hackers Were Accused

In July 2022, the Belgian Ministry of Foreign Affairs accused Chinese hackers of committing cyberattacks against the Federal Defence and Interior Ministries. China was called to take the necessary actions to investigate and resolve the situation.

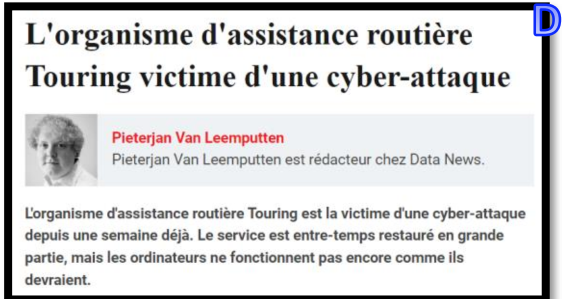
During the internal investigation, Belgium's Cybersecurity center discovered the key goal of the attackers was to obtain sensitive data from the Ministry of the Interior, which they'd been successfully doing for over 2 years. The experts have also investigated the numerous attacks on the Ministry of Defense in 2021. These resulted in disrupting the Ministry's network performance. Being cut off from the Internet for weeks, its staff was not able to communicate via email and perform the key tasks within the organization.

Another security issue mentioned by the Ministry is the case of purchasing the Huawei wifi routers at the start of 2022, which are considered to significantly compromise the national security in many countries. A similar case was detected in Hikvision and Dahua video surveillance equipment, which had insufficient security systems.

Sept 2022



#10 Belgian Hospital Center Fell Victim Due to a Massive Cyberattack

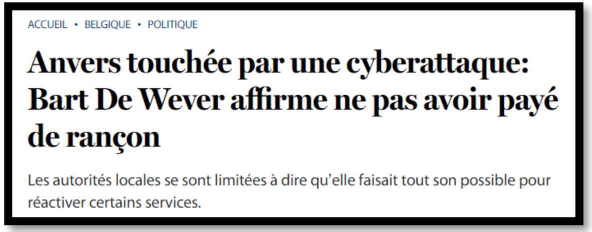


L'organisme d'assistance routière Touring victime d'une cyber-attaque

Pieterjan Van Leemputten
Pieterjan Van Leemputten est rédacteur chez Data News.

L'organisme d'assistance routière Touring est la victime d'une cyber-attaque depuis une semaine déjà. Le service est entre-temps restauré en grande partie, mais les ordinateurs ne fonctionnent pas encore comme ils devraient.

Dec 2022



ACCUEIL • BELGIQUE • POLITIQUE

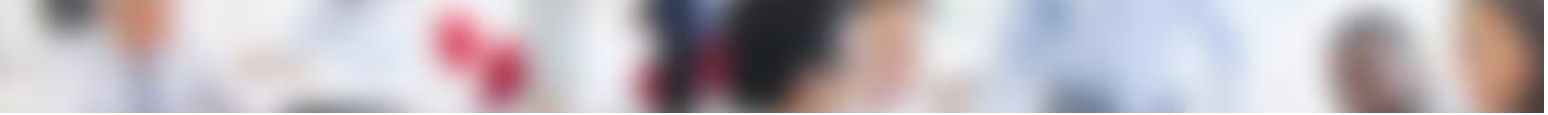
Anvers touchée par une cyberattaque: Bart De Wever affirme ne pas avoir payé de rançon

Les autorités locales se sont limitées à dire qu'elle faisait tout son possible pour réactiver certains services.

Belgian Prime Minister, Mr Decroo November 2022

« Nous devons sensibiliser nos entreprises et surtout les rendre résilientes »

« La question n’est plus aujourd’hui de savoir SI votre entreprise ou votre organisation va être touchée mais QUAND cela va se passer »



New threats

AVAILABILITY

SAFETY

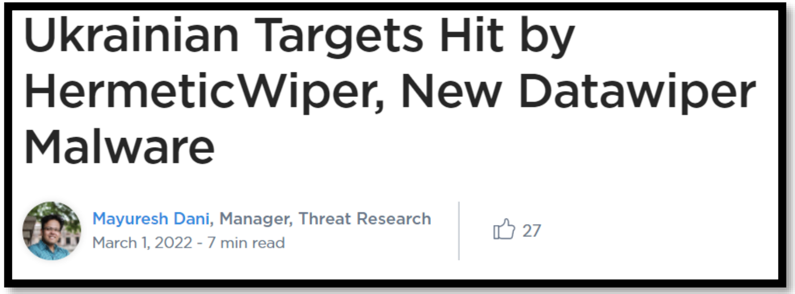
LEGACY

DIFFICULTY

- **Phishing -> Ransomware –> Wiperware -> Killware**

- Not simply to encrypt the victim’s data
- but rather to render a system essentially **unusable**. (no more protection)

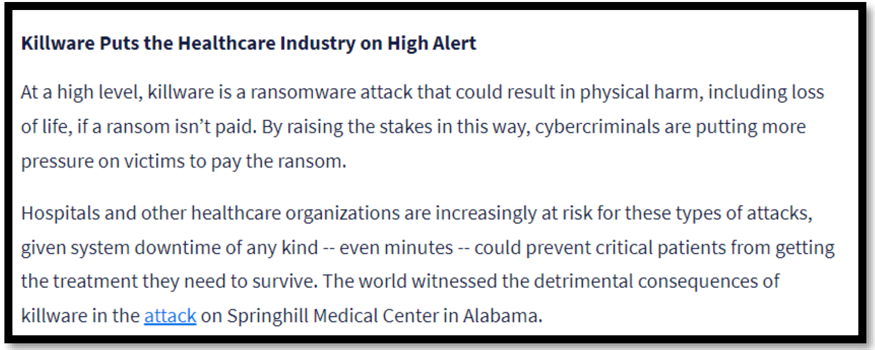
Primary Objective -> Destroy the Master Boot Record (MBR)



Ukrainian Targets Hit by HermeticWiper, New Datawiper Malware

Mayuresh Dani, Manager, Threat Research
March 1, 2022 - 7 min read

https://blog.qualys.com/vulnerabilities-threat-research/2022/03/01/ukrainian-targets-hit-by-hermeticwiper-new-datawiper-malware

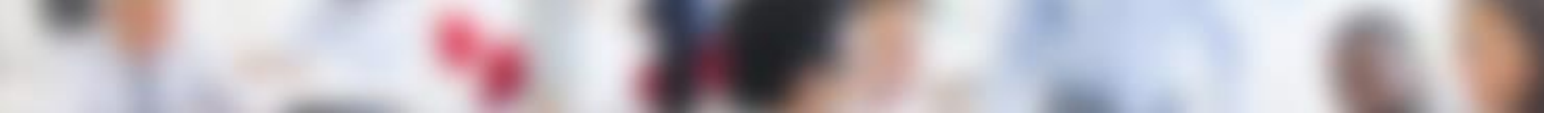


Killware Puts the Healthcare Industry on High Alert

At a high level, killware is a ransomware attack that could result in physical harm, including loss of life, if a ransom isn’t paid. By raising the stakes in this way, cybercriminals are putting more pressure on victims to pay the ransom.

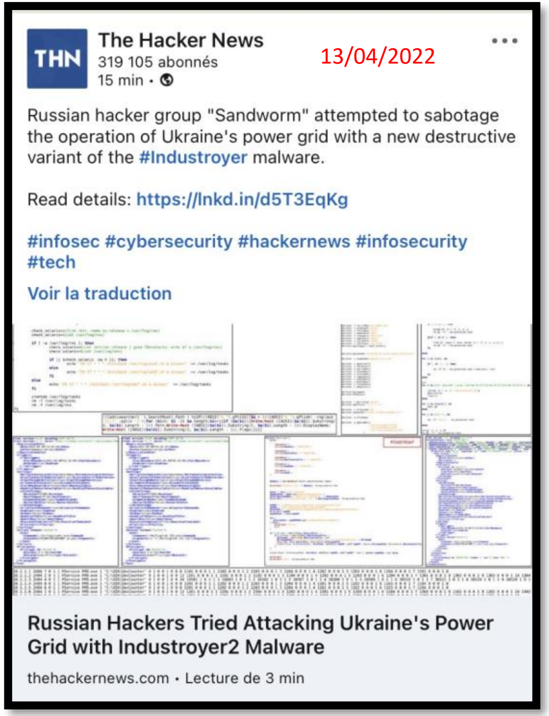
Hospitals and other healthcare organizations are increasingly at risk for these types of attacks, given system downtime of any kind -- even minutes -- could prevent critical patients from getting the treatment they need to survive. The world witnessed the detrimental consequences of killware in the attack on Springhill Medical Center in Alabama.

https://www.informationweek.com/security-and-risk-strategy/killware-the-most-dangerous-evolution-of-ransomware-



.AGORIA

ICS / OT cyber risk



THN The Hacker News
319 105 abonnés
15 min •

13/04/2022

Russian hacker group "Sandworm" attempted to sabotage the operation of Ukraine's power grid with a new destructive variant of the #Industroyer malware.

Read details: https://lnkd.in/d5T3EqKg

#infosec #cybersecurity #hackernews #infosecurity #tech

Voir la traduction

Russian Hackers Tried Attacking Ukraine's Power Grid with Industroyer2 Malware

thehackernews.com • Lecture de 3 min

“The attackers deployed Industroyer2 in the ICS network alongside another version of the CaddyWiper sabotage malware, presumably to slow down the recovery process and prevent the utility operators from regaining control of the ICS consoles. ESET first discovered CaddyWiper in Ukraine on March 14, when it was deployed in a bank's network.

In addition, ESET also discovered Wiper malware for Linux and Solaris called ORCSHRED, SOLOSHRED and AWFULSHRED on the target electricity provider's network.”

lemondeinformatique.fr/actualites/lire-ember-bear-un-groupe-de-cybercriminels-russe-tres-actif-86402.html

AVAILABILITY

SAFETY

LEGACY

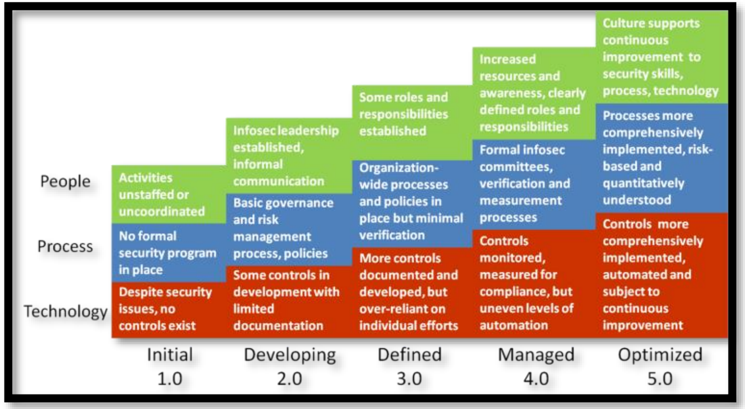
DIFFICULTY

- More and more sophisticated attacks
- Can combine different techniques (Wiper/DDOS)
- Can attack multiple layers/techno at same time

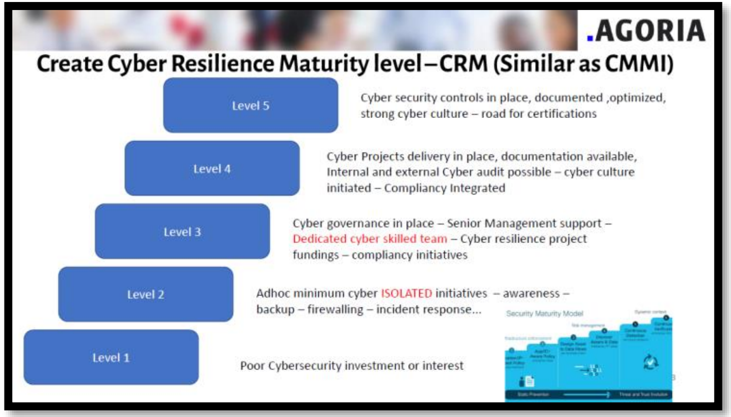
Move cyber security to cyber resilience

- Cyber Security is not enough anymore (focus on TRUST)
- Speak about Cyber Resilience -> limit the impact of CyberCrime (FROC)

GOAL : to ensure operational and business continuity with minimal impact.



	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
People	Activities unstaffed or uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
Process	No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
Technology	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement



.AGORIA

Create Cyber Resilience Maturity level – CRM (Similar as CMMI)

Level 5 – Cyber security controls in place, documented ,optimized, strong cyber culture – road for certifications

Level 4 – Cyber Projects delivery in place, documentation available, Internal and external Cyber audit possible – cyber culture initiated – Compliancy Integrated

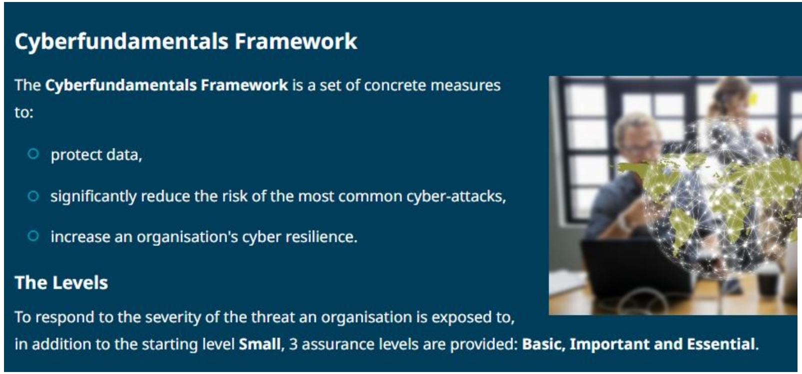
Level 3 – Cyber governance in place – Senior Management support – Dedicated cyber skilled team – Cyber resilience project fundings – compliancy initiatives

Level 2 – Adhoc minimum cyber ISOLATED initiatives – awareness – backup – firewalling – incident response...

Level 1 – Poor Cybersecurity investment or interest

Examples of Resilience Maturity level

Move cyber security to cyber resilience



Cyberfundamentals Framework

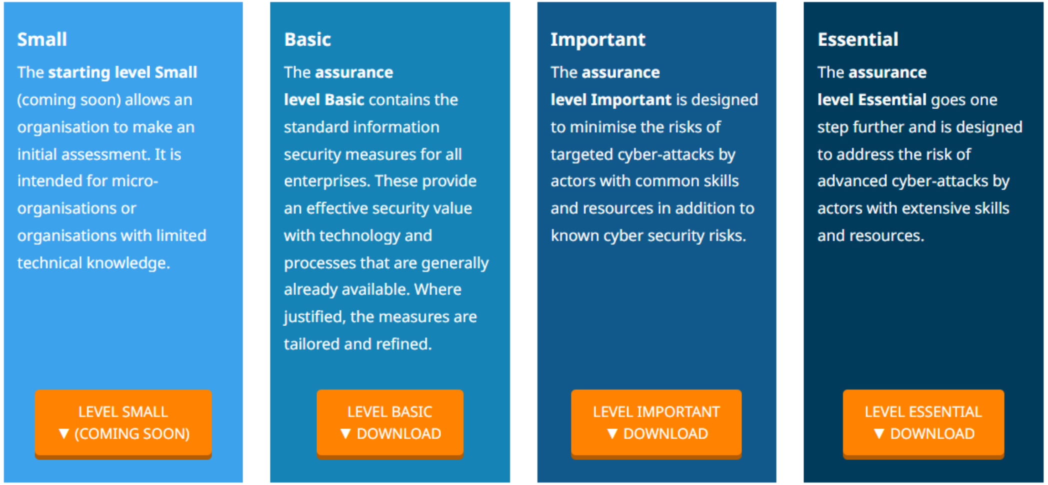
The **Cyberfundamentals Framework** is a set of concrete measures to:

- protect data,
- significantly reduce the risk of the most common cyber-attacks,
- increase an organisation's cyber resilience.

The Levels

To respond to the severity of the threat an organisation is exposed to, in addition to the starting level **Small**, 3 assurance levels are provided: **Basic, Important and Essential**.

CENTRE FOR CYBER SECURITY BELGIUM



Small

The **starting level Small** (coming soon) allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.

LEVEL SMALL ▼ (COMING SOON)

Basic

The **assurance level Basic** contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.

LEVEL BASIC ▼ DOWNLOAD

Important

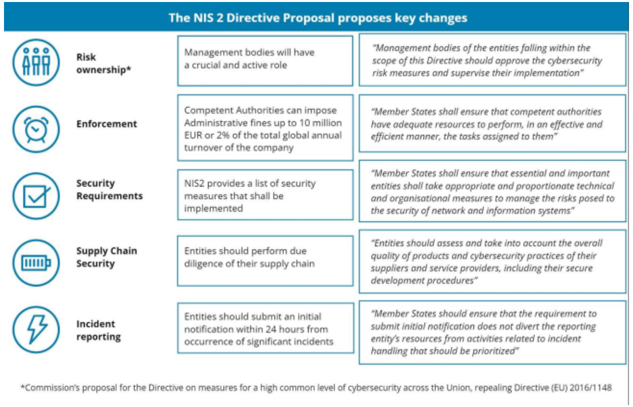
The **assurance level Important** is designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.

LEVEL IMPORTANT ▼ DOWNLOAD

Essential

The **assurance level Essential** goes one step further and is designed to address the risk of advanced cyber-attacks by actors with extensive skills and resources.

LEVEL ESSENTIAL ▼ DOWNLOAD



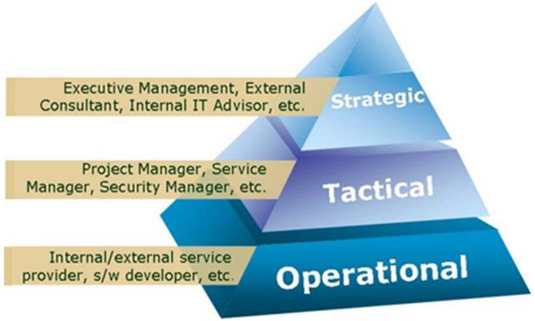
The NIS 2 Directive Proposal proposes key changes

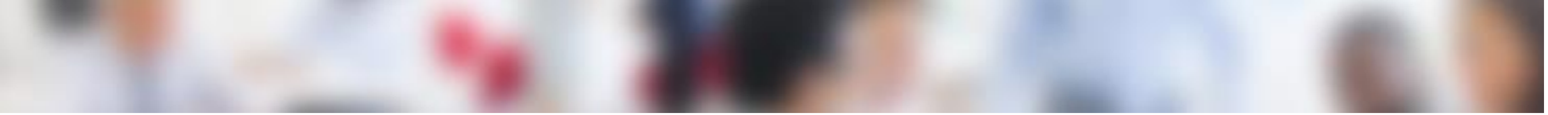
Risk ownership*	Management bodies will have a crucial and active role	*"Management bodies of the entities falling within the scope of this Directive should approve the cybersecurity risk measures and supervise their implementation"*
Enforcement	Competent Authorities can impose Administrative fines up to 10 million EUR or 2% of the total global annual turnover of the company	*"Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them"*
Security Requirements	NIS2 provides a list of security measures that shall be implemented	*"Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems"*
Supply Chain Security	Entities should perform due diligence of their supply chain	*"Entities should assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures"*
Incident reporting	Entities should submit an initial notification within 24 hours from occurrence of significant incidents	*"Member States should ensure that the requirement to submit initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritized"*

*Commission's proposal for the Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

Agenda

- **Introduction**
  - Value proposition
- **Cyber Security Basics**
  - Set the scene
  - Understand the specificities of IT / OT world
- **Importance of Cyber Resilience**
  - Definition
  - Why is CS obsolete ?
- **How to achieve Cyber Resilience ? The Building Blocks**
  - Strategic level – « ABC for Executive »
  - Tactic level – « iCD processes »
  - Operational Level – « AOA Matrix »
- **Conclusion**


Executive Management, External Consultant, Internal IT Advisor, etc.
Strategic
Project Manager, Service Manager, Security Manager, etc.
Tactical
Internal/external service provider, s/w developer, etc.
Operational



STRATEGIC LEVEL – ABC FOR EXECUTIVE

Asset Management

What are my assets that I need to protect?
Identify your critical processes -> BIA (Business impact Analysis)

Business Modelling

How my customer value proposition are depicted under services, supported by applications , hosted on servers , based on specific network segmentation , in specific Data center/cloud location

Continuity

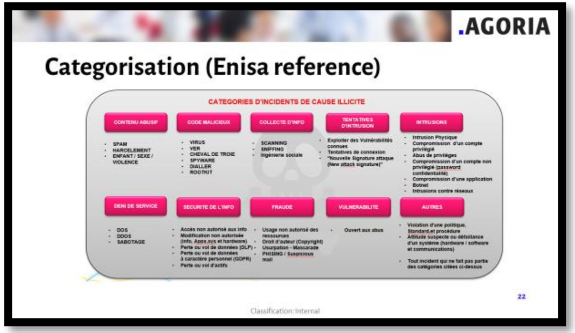
How my BIA (Business impact Analysis) will be transposed to a BCP/DRP process / Exercise ?
Business Continuity / Disaster Recovery Processes

TACTICAL LEVEL – iCD processes

Incident Management

Crisis Management

Disaster BCP management



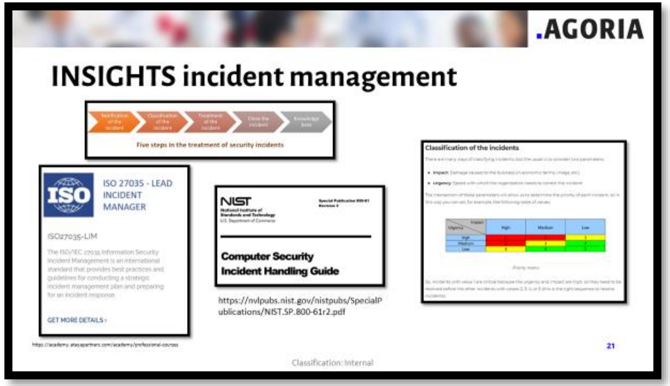
Categorisation (Enisa reference)

CATEGORIES D'INCIDENTS DE CAUSE ILLICITE

CONTENU ABUSIF	CODE MALICIEUX	COLLECTE D'INFO	TENTATIVES D'INTRUSION	INTRUSIONS
SPAM HARCELEMENT ENFANT / SEXE / VIOLENCE	VIRUS VER CHEVAL DE TROIE SPYWARE DIALLER ROOTKIT	SCANNING SNIFFING Ingénierie sociale	Exploiter des Vulnérabilités connues Tentatives de connexion "Nouvelle Signature attaque (New attack signature)"	Intrusion Physique Compromission d'un compte privilégié Abus de privilèges Compromission d'un compte non privilégié (password confidentialité) Compromission d'une application Botnet Intrusions contre réseaux
DENI DE SERVICE	**SECURITE DE L'INFO**	**FRAUDE**	**VULNERABILITE**	**AUTRES**
DOS DDOS SABOTAGE	Accès non autorisé aux info Modification non autorisée (info, Apps,sys et hardware) Perte ou vol de données (DLP) Perte ou vol de données à caractère personnel (GDPR) Perte ou vol d'actifs	Usage non autorisé des ressources Droit d'auteur (Copyright) Usurpation - Mascarade PHISING / Suspicious mail	Ouvert aux abus	Violation d'une politique, Standard,et procédure Attitude suspecte ou défaillance d'un système (hardware / software et communications) Tout incident qui ne fait pas partie des catégories citées ci-dessus

22

Classification: Internal



INSIGHTS incident management

Notification of the incident
Classification of the incident
Treatment of the incident
Close the incident
Knowledge base

Five steps in the treatment of security incidents

ISO 27035 - LEAD INCIDENT MANAGER

ISO27035-LIM

The ISO/IEC 27035 Information Security Incident Management is an international standard that provides best practices and guidelines for conducting a strategic incident management plan and preparing for an incident response.

GET MORE DETAILS ›

https://academy.atayapartners.com/academy/professional-courses

NIST National Institute of Standards and Technology U.S. Department of Commerce

Special Publication 800-61 Revision 2

Computer Security Incident Handling Guide

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Classification of the incidents

[illegible]

- Impact: [illegible]
- Urgency: [illegible]

[illegible]

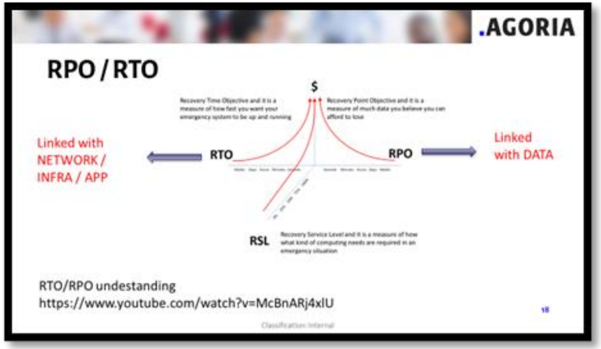
Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

[illegible]

[illegible]

21

Classification: Internal



RPO / RTO

Recovery Time Objective and it is a measure of how fast you want your emergency system to be up and running

Recovery Point Objective and it is a measure of much data you believe you can afford to lose

Recovery Service Level and it is a measure of how what kind of computing needs are required in an emergency situation

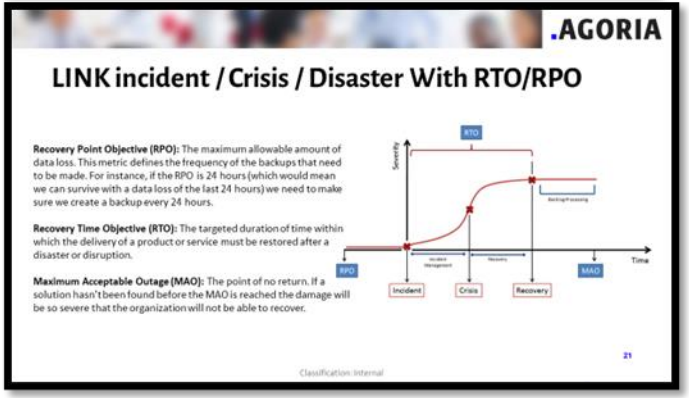
Linked with NETWORK / INFRA / APP

Linked with DATA

RTO/RPO undestanding
https://www.youtube.com/watch?v=McBnARj4xlU

18

Classification: Internal



LINK incident / Crisis / Disaster With RTO/RPO

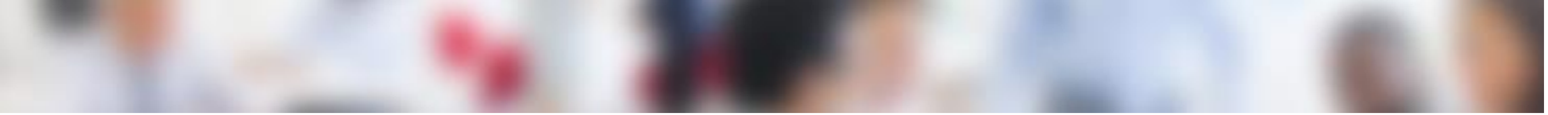
Recovery Point Objective (RPO): The maximum allowable amount of data loss. This metric defines the frequency of the backups that need to be made. For instance, if the RPO is 24 hours (which would mean we can survive with a data loss of the last 24 hours) we need to make sure we create a backup every 24 hours.

Recovery Time Objective (RTO): The targeted duration of time within which the delivery of a product or service must be restored after a disaster or disruption.

Maximum Acceptable Outage (MAO): The point of no return. If a solution hasn't been found before the MAO is reached the damage will be so severe that the organization will not be able to recover.

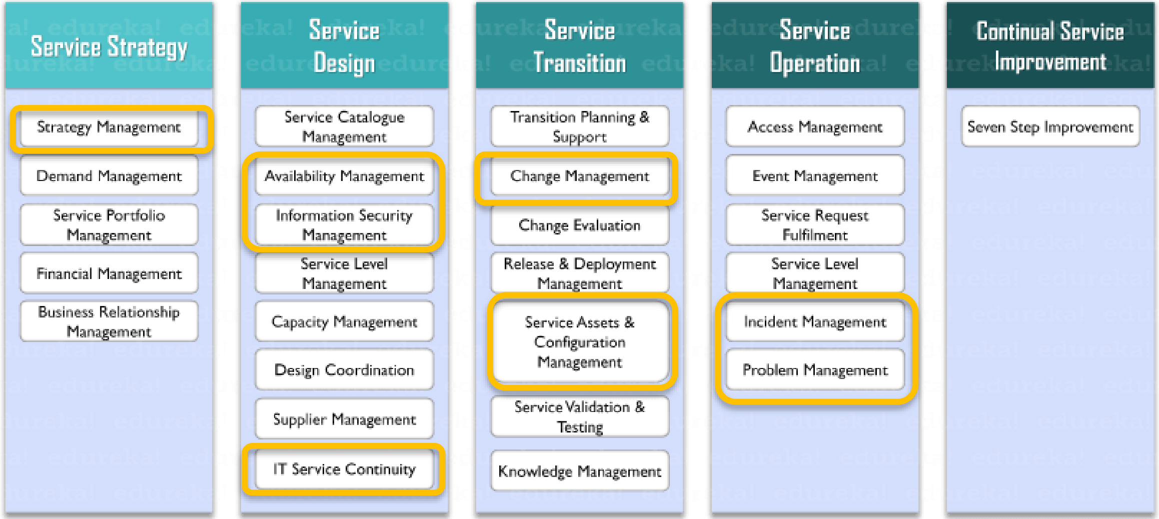
21

Classification: Internal

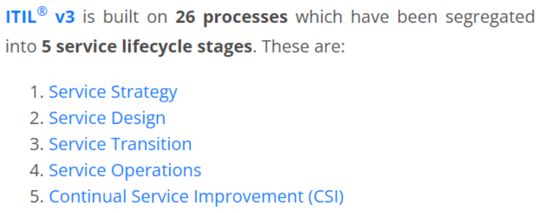


.AGORIA

ITIL v3 (*) illustrate importance of some Cyber Security Processes

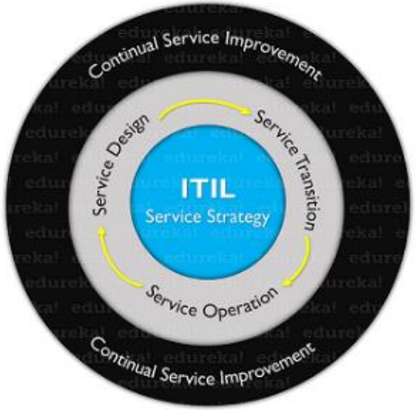


Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement
Strategy Management	Service Catalogue Management	Transition Planning & Support	Access Management	Seven Step Improvement
Demand Management	Availability Management	Change Management	Event Management	
Service Portfolio Management	Information Security Management	Change Evaluation	Service Request Fulfilment	
Financial Management	Service Level Management	Release & Deployment Management	Service Level Management	
Business Relationship Management	Capacity Management	Service Assets & Configuration Management	Incident Management	
	Design Coordination	Service Validation & Testing	Problem Management	
	Supplier Management	Knowledge Management		
	IT Service Continuity			



ITIL® v3 is built on **26 processes** which have been segregated into **5 service lifecycle stages**. These are:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operations
5. Continual Service Improvement (CSI)



ITIL® is one of the most heavily used ITSM (**) frameworks

(*) v4 is out in 2020
(**) IT Service Management

Operational LEVEL – « AOA Matrix »

Attributes

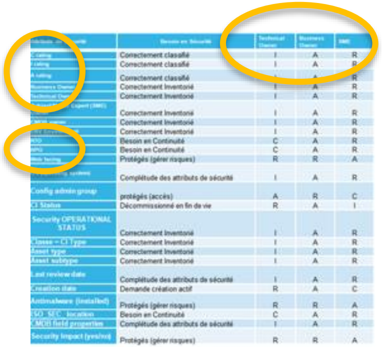
Ownership

Alignment

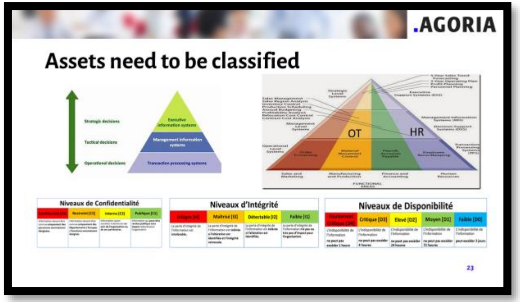
CIA RATING

RTO / RPO

BO / TO / SME



Attributs de sécurité	Besoin en Sécurité	Technical Owner	Business Owner	SME
C rating	Correctement classifié	I	A	R
I rating	Correctement classifié	I	A	R
A rating	Correctement classifié	I	A	R
Business Owner	Correctement Inventorié	I	A	R
Technical Owner	Correctement Inventorié	I	A	R
Subject Matter Expert (SME) [illegible]	Correctement Inventorié	I	A	R
CMDB owner	Correctement Inventorié	I	A	R
[illegible]	Correctement Inventorié	I	A	R
RTO	Besoin en Continuité	C	A	R
RPO	Besoin en Continuité	C	A	R
Web facing	Protégés (gérer risques)	R	R	A
Operating system	Complétude des attributs de sécurité	I	A	R
Config admin group	protégés (accès)	A	R	C
CI Status	Décommissionné en fin de vie	R	A	I
Security OPERATIONAL STATUS	Correctement Inventorié	I	A	R
Classe – CI Type	Correctement Inventorié	I	A	R
Asset type	Correctement Inventorié	I	A	R
Asset subtype	Correctement Inventorié	I	A	R
Last review date	Complétude des attributs de sécurité	I	A	R
Creation date	Demande création actif	R	A	C
Antimalware (installed)	Protégés (gérer risques)	R	R	A
ISO_SEC_location	Besoin en Continuité	C	A	R
CMDB field properties	Complétude des attributs de sécurité	I	A	R
Security Impact (yes/no)	Protégés (gérer risques)	R	R	A



.AGORIA

Assets need to be classified

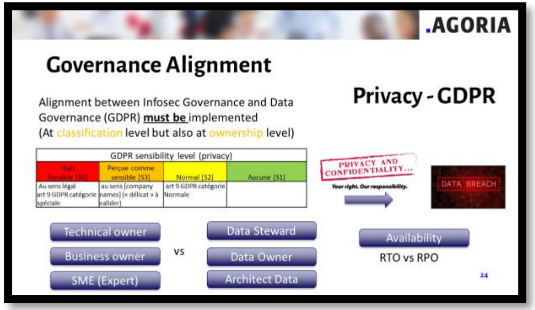
Strategic decisions
Tactical decisions
Operational decisions
Executive information systems
Management information systems
Transaction processing systems
OT
HR

Niveaux de Confidentialité			
[illegible] [C4]	Restreint [C3]	Interne [C2]	Publique [C1]
[illegible]	[illegible]	[illegible]	[illegible]

Niveaux d'Intégrité			
Intègre [I4]	Maîtrisé [I3]	Détectable [I2]	Faible [I1]
[illegible]	[illegible]	[illegible]	[illegible]

Niveaux de Disponibilité				
Hautement Critique [D4]	Critique [D3]	Elevé [D2]	Moyen [D1]	Faible [D0]
L'indisponibilité de l'information ne peut pas excéder 1 heure	L'indisponibilité de l'information ne peut pas excéder 4 heures	L'indisponibilité de l'information ne peut pas excéder 24 heures	L'indisponibilité de l'information ne peut pas excéder 72 heures	L'indisponibilité de l'information peut excéder 3 jours

23



.AGORIA

Governance Alignment

Alignment between Infosec Governance and Data Governance (GDPR) **must be** implemented
(At classification level but also at ownership level)

GDPR sensibility level (privacy)			
High Sensible [S4]	Perçue comme sensible [S3]	Normal [S2]	Aucune [S1]
Au sens légal art 9 GDPR catégorie spéciale	au sens [company names] (« délicat » à valider)	art 9 GDPR catégorie Normale	

Privacy - GDPR

PRIVACY AND CONFIDENTIALITY...
Your right. Our responsibility.
DATA BREACH

Technical owner | Business owner | SME (Expert)

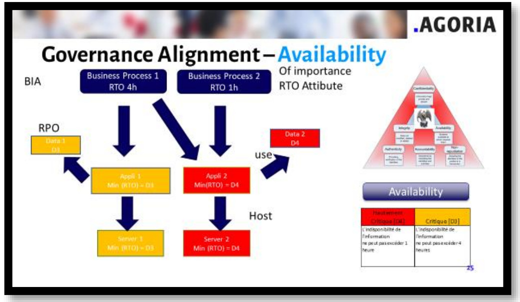
vs

Data Steward | Data Owner | Architect Data

Availability

RTO vs RPO

24



.AGORIA

Governance Alignment – Availability

Hautement Critique [D4]	Critique [D3]
L'indisponibilité de l'information ne peut pas excéder 1 heure	L'indisponibilité de l'information ne peut pas excéder 4 heures

25

Scoop – Resilience in human centric

VOLUME 8 (2022) ISSUE 1

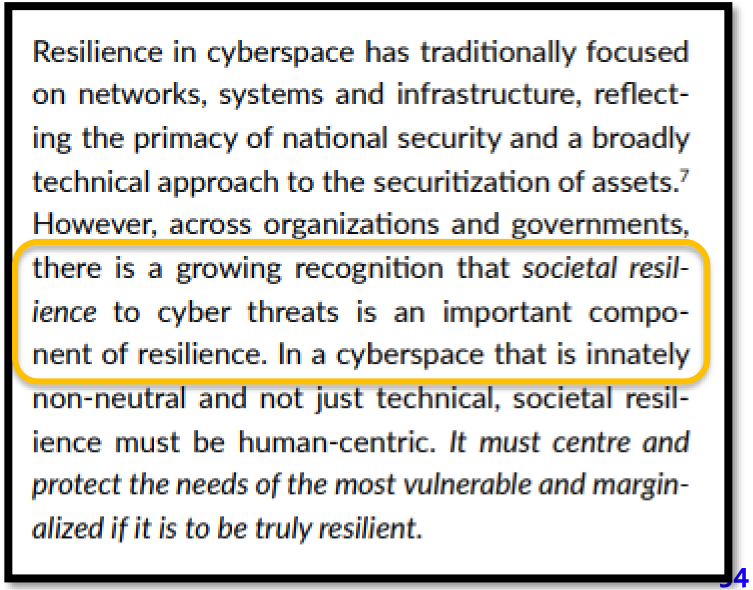
European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

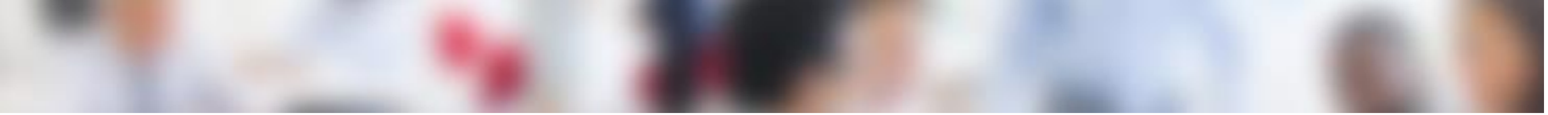
VOLUME 8 (2022) ISSUE 1

OPINION

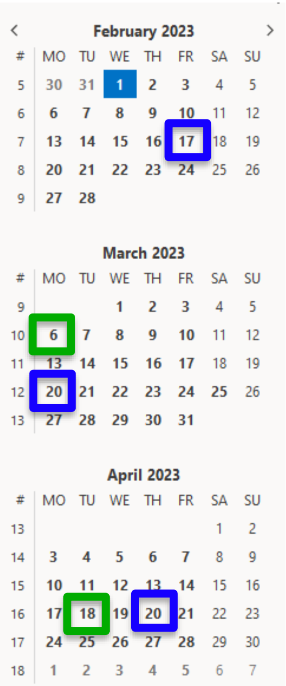
Gender and Cyber Resilience: Challenging Assumptions and Broadening Commitments



Resilience in cyberspace has traditionally focused on networks, systems and infrastructure, reflecting the primacy of national security and a broadly technical approach to the securitization of assets.[7] However, across organizations and governments, there is a growing recognition that *societal resilience* to cyber threats is an important component of resilience. In a cyberspace that is innately non-neutral and not just technical, societal resilience must be human-centric. *It must centre and protect the needs of the most vulnerable and marginalized if it is to be truly resilient.*



How to achieve Cyber resilience ?



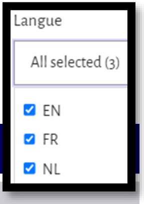
	<		February 2023				>
#	MO	TU	WE	TH	FR	SA	SU
5	30	31	1	2	3	4	5
6	6	7	8	9	10	11	12
7	13	14	15	16	17	18	19
8	20	21	22	23	24	25	26
9	27	28					

			March 2023				
#	MO	TU	WE	TH	FR	SA	SU
9			1	2	3	4	5
10	6	7	8	9	10	11	12
11	13	14	15	16	17	18	19
12	20	21	22	23	24	25	26
13	27	28	29	30	31		

			April 2023				
#	MO	TU	WE	TH	FR	SA	SU
13						1	2
14	3	4	5	6	7	8	9
15	10	11	12	13	14	15	16
16	17	18	19	20	21	22	23
17	24	25	26	27	28	29	30
18	1	2	3	4	5	6	7

🟩 FR 🟦 NL

www.agoria.be/agenda



Langue

All selected (3)

☑ EN
☑ FR
☑ NL

Lang	Date	Location
NL	12/01	Leuven
FR	20/01	Louvain-la-Neuve
NL	17/02	Brugge
FR	06/03	Nivelles
NL	20/03	Aalst
FR	18/04	Louvain-la-Neuve
NL	20/04	Mechelen
NL	11/05	Leuven
FR	June	Namur (TBC)
NL	08/06	Kortrijk

La cybersécurité en 30 étapes

Cyber Security Foundations

20/01/2023

Eric VAN CANGH

Embracing technology
Embracing ambition

Eric Van Cangh
Senior Business Group Leader Digital
Cybersecurity
eric.vancangh@agoria.be
.AGORIA
www.agoria.be
.AGORIA

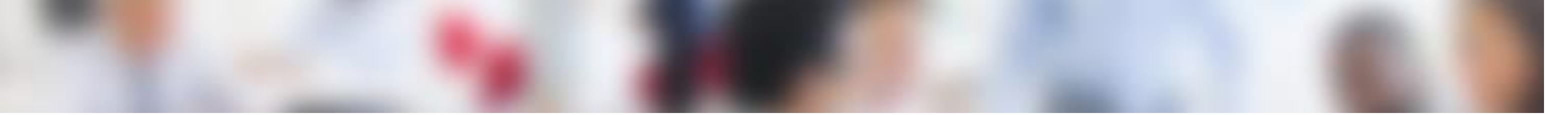
#industriepartnerschap

Patrick Coomans
Expert (Consultant) Digital products & Entrepreneurship

Cyberveilig in 30 stappen

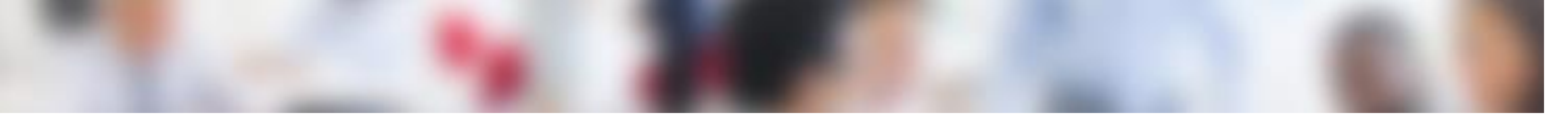
Cybersecurity Foundations
Patrick Coomans

AGENTSCHAP INNOVEREN & ONDERNEMEN
.AGORIA
sirris
samen voor #sterkondernemen



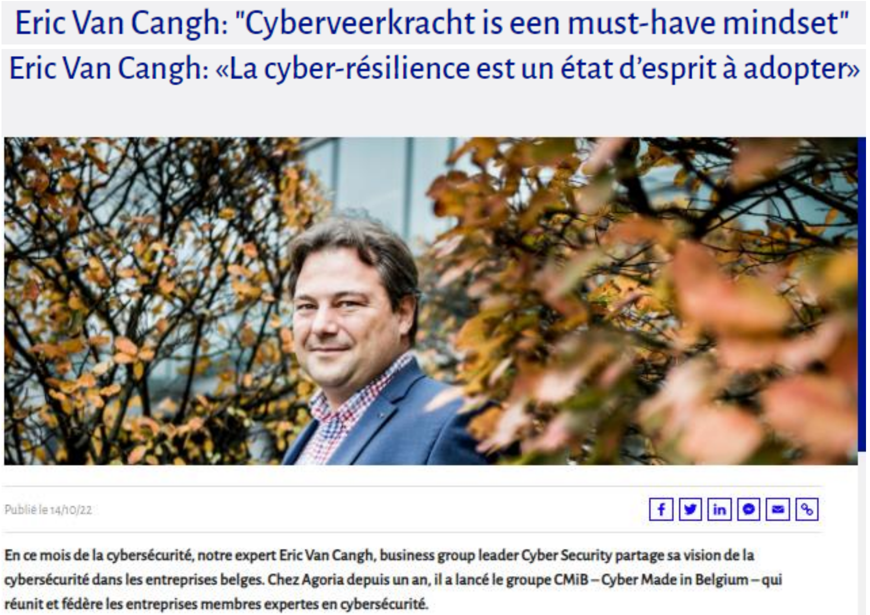
Agenda

- **Introduction**
  - Value proposition
- **Cyber Security Basics**
  - Set the scene
  - Understand the specificities of IT / OT world
- **Importance of Cyber Resilience**
  - Definition
  - Why CS is obsolete ?
- **How to achieve Cyber Resilience ? The Building Blocks**
  - Strategic level – « ABC for Executive »
  - Tactic level – « iCD processes »
  - Operational Level – « AOA Matrix »
- **Conclusion**



Conclusion

“Cyber resilience is a mindset to adopt”



Eric Van Cangh: "Cyberveerkracht is een must-have mindset"

Eric Van Cangh: «La cyber-résilience est un état d’esprit à adopter»

Publié le 14/10/22

En ce mois de la cybersécurité, notre expert Eric Van Cangh, business group leader Cyber Security partage sa vision de la cybersécurité dans les entreprises belges. Chez Agoria depuis un an, il a lancé le groupe CMiB – Cyber Made in Belgium – qui réunit et fédère les entreprises membres expertes en cybersécurité.

https://www.agoria.be/fr/digitalisation/cybersecurite/nouvelles

https://www.agoria.be/nl/digitalisering/cybersecurity/nieuws

« It is not anymore a question of IF but WHEN »

« Focus on the Value proposition »

« Everybody within an organization has a role to play in the cyber resilience process »

« Overall Belgium has all the Assets to become on a top Cyber resilience Nation »

Questions & Answers

Thank you for your attention

Eric Van Cangh
Senior Business Group Leader Digital
Cyber Security

T: +32 2 706 78 25
M:+32492.23.24.34
Eric.Vancangh@agoria.be