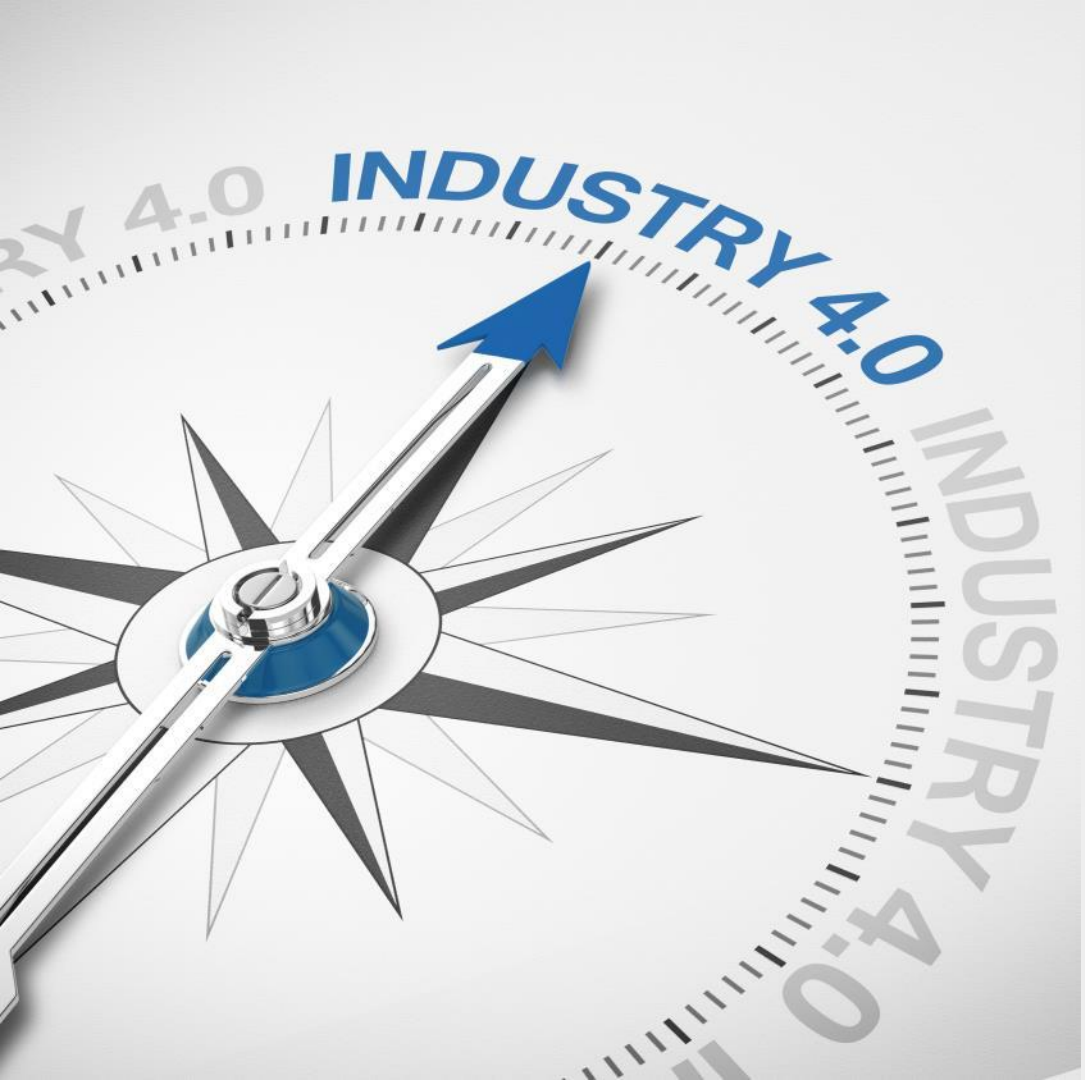


La governance della cybersecurity in Solvay

Antonio Giustino
-IS Industrial Risk Manager-

Organizzato da

We are a world leader in the chemical industry

24,500 employees

115 industrial sites

21 major R&I centers

61 countries

€ 10.3 billion of net sales

€ 2.2 billion of EBITDA

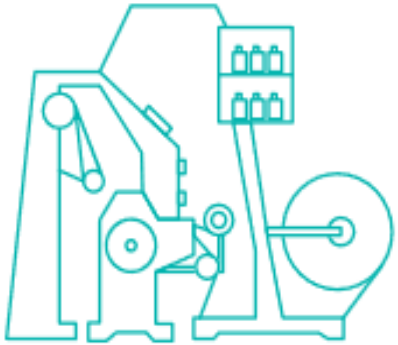
Agenda

1. Industry 4.0-background
2. La minaccia cyber per l'industria e sue attuali vulnerabilità
3. *Differenze e convergenza OT-IT*
4. La governance olistica in Solvay
5. L'approccio per la cybersecurity in Solvay
6. Il Security Profile assessment – un esempio di benchmark

Agenda

1. Industry 4.0-background
2. La minaccia cyber per l'industria e sue attuali vulnerabilità
3. *Differenze e convergenza OT-IT*
4. La governance olistica in Solvay
5. L'approccio per la cybersecurity in Solvay
6. Il Security Profile assessment – un esempio di benchmark in OT -

.....-> Industry 4.0

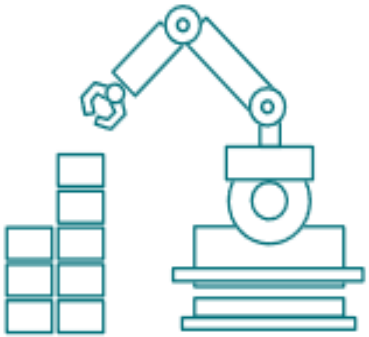


Late 18th–19th century

First Industrial revolution:
Power generation

Beginning of 20th century

Second Industrial revolution:
Industrialization



1970s–2000s

Third Industrial revolution:
Electronic automation

2010 onward

Fourth Industrial revolution:
Smart automation...and exponential change

Source: Deloitte Insights, *Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises*

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

Le 9 componenti dell' Industry 4.0

DIGITAL TRANSFORMATION OF OPERATIONAL TECHNOLOGY

- **Smarter devices**, better connected, always on
- **Continuous data collection** shared across applications, reporting tools and the supply chain
- **Automation driving down costs**, increasing production
- **Constant change** with winners and losers

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il Security Profile assessment – un esempio di benchmark in OT -

La minaccia *cyber* per l'industria e sue attuali vulnerabilità [1/4]

+ Profitable

+ Organized

+ Sophisticated

+ Aimed to the target

+ Frequent and Severity

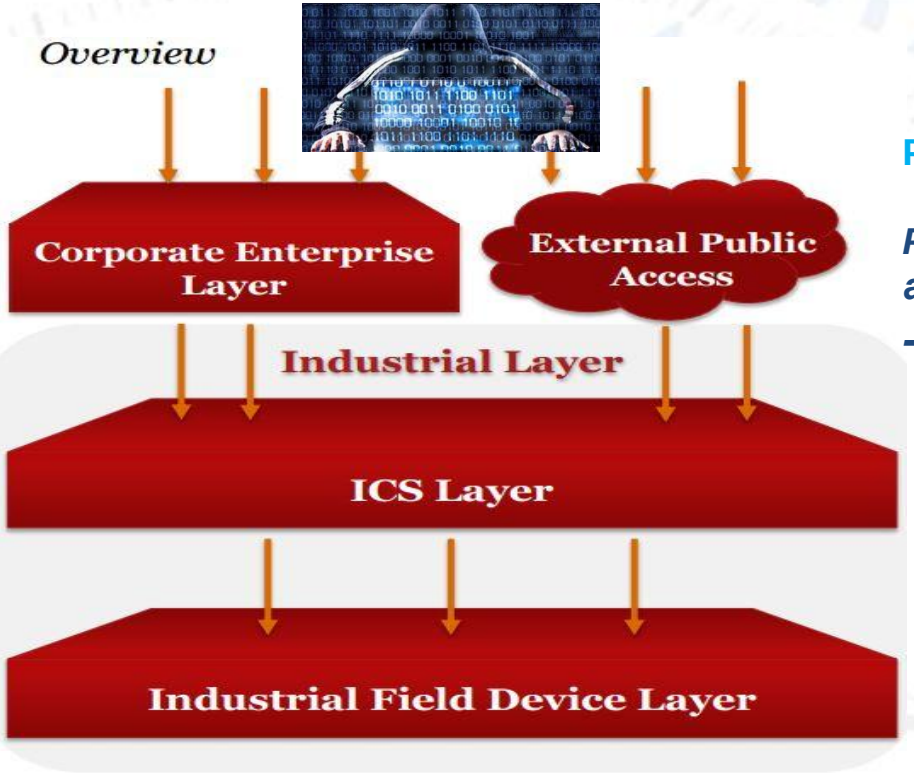
-> new technologies, skills, processes are required continuously for risk mitigation ..

La minaccia *cyber* per l'industria e sue attuali vulnerabilità [2/4]

IT:
corp.network,WEB, ERP, email ,file servers,collaboration ...

OT :
PLC,HMI,SIS,DCS, SCADA …

Field devices (sensori,attuatori..)



Source : PWC

PRINCIPALI MINACCE:

Furto di informazioni, danni all'operatività del business,..

Danni alla produzione, agli impianti e possibili conseguenze HSE,..

La minaccia *cyber* per l'industria e sue attuali vulnerabilità [3/4]

- **In ICS gli attacchi sono principalmente di tipo cyber «fisico» :**

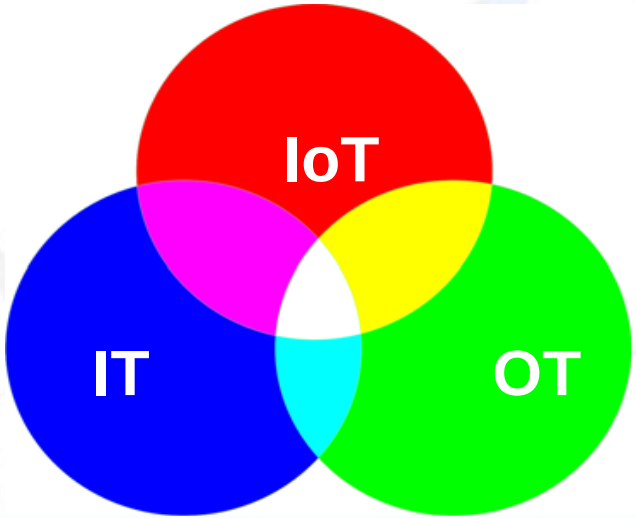
Equipment Damage	Production Damage	Compliance Violation
- *Equipment overstress* - *Safety limits violation*	- *Product quality* - *Production rate* - *Operating costs* - *Maintenance efforts*	- *Safety* - *Pollution* - *Contractual treatles*

La minaccia *cyber* per l'industria e sue attuali vulnerabilità [4/4]

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

IT-IoT-OT : complexity & risk are increasing …



Some new threats in progress:

- A.I. and M.L.
- Mobile devices
- Robotic and AGV
- Unsecure coding
- Multi-clouds environment
- Drones
- Digital & connection with stakeholders
- ..

IoT report (tbc): 2018/17:

Turnover = 40%

Declared incidents = + 280%

WHY ?

.Customer demands fast solution at lo e:

-> IoT producer/vendor priority i

low price and short ti

most IoT h

-> ough of the current h eclared incidents are in g ! ..

The new EU 'Cybersecurity ACT' regulation is coming ! ..

AUJAS

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica in Solvay

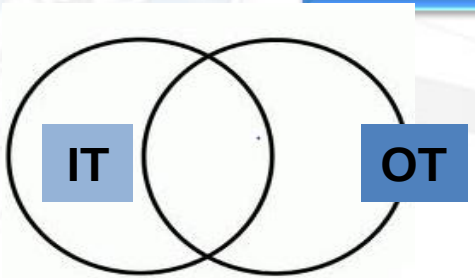
5. L'approccio per la cybersecurity in Solvay

6. Il Security Profile assessment – un esempio di benchmark in OT -

Differenti priorità rispetto alla security

+ SAFETY

L'ingresso del *Safety* è divenuto fattore aggregante dell'IT con l'OT per meglio fronteggiare la minaccia Cyber..



Principali differenze operative IT vs OT

	IT	OT
- CICLO DI VITA	- 3-5 anni	- 10-20 anni
- RISCHIO PIU TEMUTO	- Perdita dati/info	- Vita,assets,ambiente
- REBOOT	- Accettato	- Non accettato
- CHANGE MANAGEMENT	- Frequente/automatico	- Raro/accurato
- SISTEMI	- Standard	- Prorietari
- TEMPI DI RISPOSTA	- Ammesso ritardo	- Real time
- COMUNICAZIONE..	- Protocolli std	- Protocolli prop. + std

OT SECURITY VULNERABILITIES

SAFETY IS PARAMOUNT

As Safety is paramount to ICS clients, targeted polymorphic malware is a major concern in 2019 (Triton).

SECURITY NOT DESIGNED

Security not designed into ICS endpoints, controllers, and communication protocols

OUTDATED LEGACY OPERATING SYSTEMS

ICS devices are running outdated legacy Operating Systems

VISIBILITY

Lack of Visibility

Lack of Control

IT vs OT – diverse prospettive e competenze : qualche raccomandazione preliminare per favorirne la convergenza [1/2]

@IT:

- evitare di voler risolvere problemi OT che non si conoscono
- condividere i rischi cyber con OT ed indirizzarli per prevenirli
- policy,tools e procedure della sicurezza IT non vanno bene per la sicurezza OT; sono tuttavia necessarie verifiche per evitare reciproche aree grigie o sovrapposizioni all'interno del processo globale IT+OT oltre che possibili rischi di inconsistenza …

IT vs OT – diverse prospettive e competenze : qualche raccomandazione preliminare per favorirne la convergenza [2/2]

@OT :

- evitare soluzioni innovative ignare dei rischi cyber
- no alle reti “piatte”,ove tutti “vedono” tutto; segmentiamo e segreghiamo secondo gli standard ISA99/IEC62443
- proteggere reti e sistemi di fabbrica con strumenti adeguati
- controllare periodicamente HW e SW per eventuali necessità di aggiornamenti
- aggiornare documentazione e back-up non sono perdite di tempo
- censire tutti i possibili accessi e proteggiamoli sistematicamente
- …

La convergenza IT-OT è un processo: qualche suggerimento finale per favorire la cooperazione a regime ..

@ IT & OT :

. Comprendere il cyber risk “tollerato” definito dalla strategia aziendale
. Definire e condividere le politiche di cybersecurity e le architetture
. Concordare gli obiettivi/priorità/piano operativo comune
. Condividere/prevenire gli impatti reciproci delle attività
. Rendere visibili tutte le componenti in gioco e verificare le competenze
. Lavorare per processo rispettando ruoli/responsabilità
. Dotarsi di tools adeguati ad uso trasversale (monitoraggio,work-flow,..)
. Definire regole di controllo, intercettazione anomalie ed azioni conseguenti di tipo tecnico ed organizzativo (SOC,SIEM,Sonde OT, IRP,..)
. Simulare scenari di crisi e relativa escalation,..

Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il Security Profile assessment – un esempio di benchmark in OT -

La governance olistica in Solvay

Solvay Responsible Care policy commits us to ensure adequate protection of people, property, products, plants, transport, information and information systems against security threats: criminal, malicious and cyber acts.

y commits us to ensure adequate
roducts, plants, transport,
ystems against security threats:
cyber acts.

Solvay's Security Code

Our Security Code defines the management principles that we strive to implement to continuously enhance security using a threat- and risk-based approach to identify, to assess and address vulnerabilities, to enhance response capabilities and to maintain and improve relationships with key stakeholders.

1. Leadership Commitment.
Solvay leadership commits to continuous security improvement through published policies, provision of sufficient and qualified resources and established accountability.

2. Analysis of Threats, Vulnerabilities and Consequences.
Potential security threats, vulnerabilities and consequences are to be prioritized against accepted criteria and regularly analyzed.

3. Implementation of Security Measures.
Security measures are to be developed and implemented commensurate with risks, and taking into account inherently safer approaches to process design, engineering and administrative controls, and prevention and mitigation measures.

4. Information and Cyber-Security.
Protecting information and information systems is recognized as a critical component of a sound security management system, and security measures are developed and implemented accordingly.

5. Documentation.
Security management programs, processes and procedures are to be documented.

6. Training, Drills and Guidance.
As appropriate, training, drills and guidance are to be provided for employees, contractors, service providers, value chain partners and others, to enhance awareness and capability.

7. Communications, Dialogue and Information Exchange.
Communications, dialogue and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers and government officials and agencies is to be maintained, balanced with safeguards for sensitive information.

8. Response to Security Threats.
Security threats are to be evaluated and responded to and reporting and communication of security threats is to be performed as appropriate.

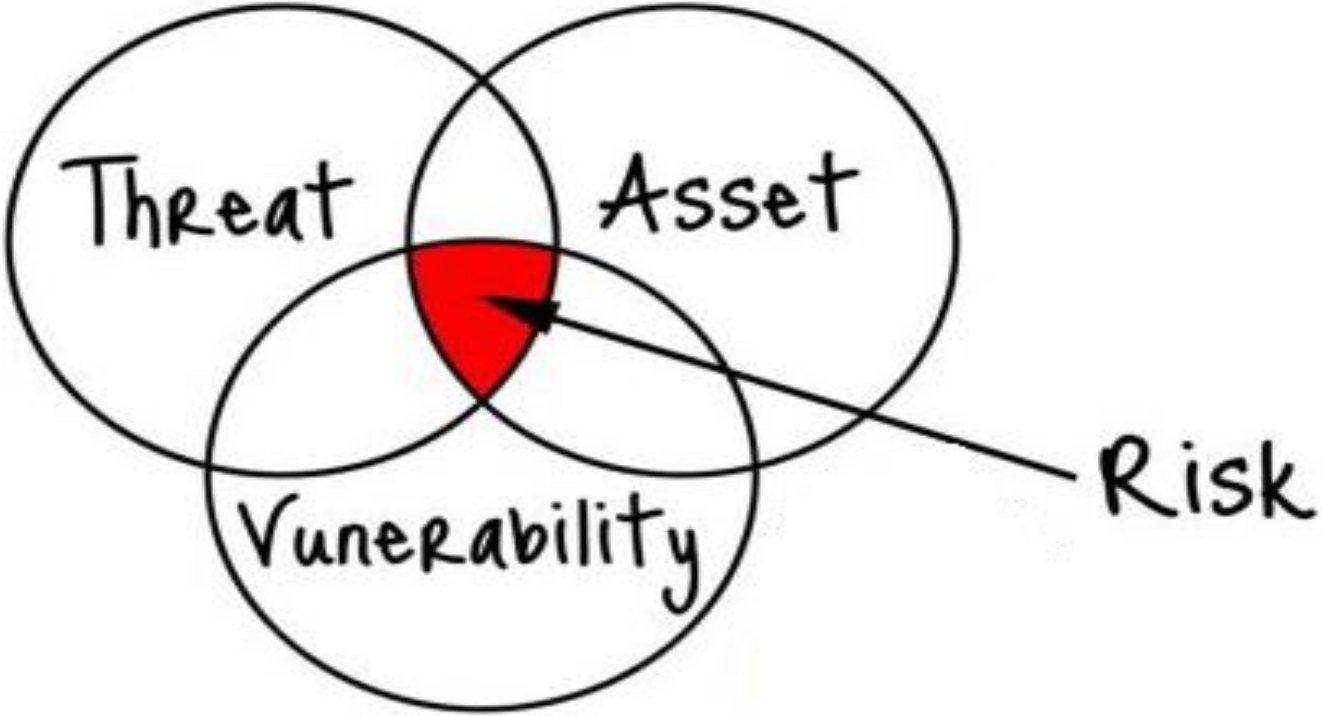
9. Response to Security Incidents.
Significant security incidents are to be evaluated, responded to, investigated, communicated as appropriate, reported to the Group, and corrective action to mitigate impact and reoccurrence implemented.

10. Audits.
Periodically, our security programs and processes and implementation of corrective actions are to be audited. This may include third-party verification where required.

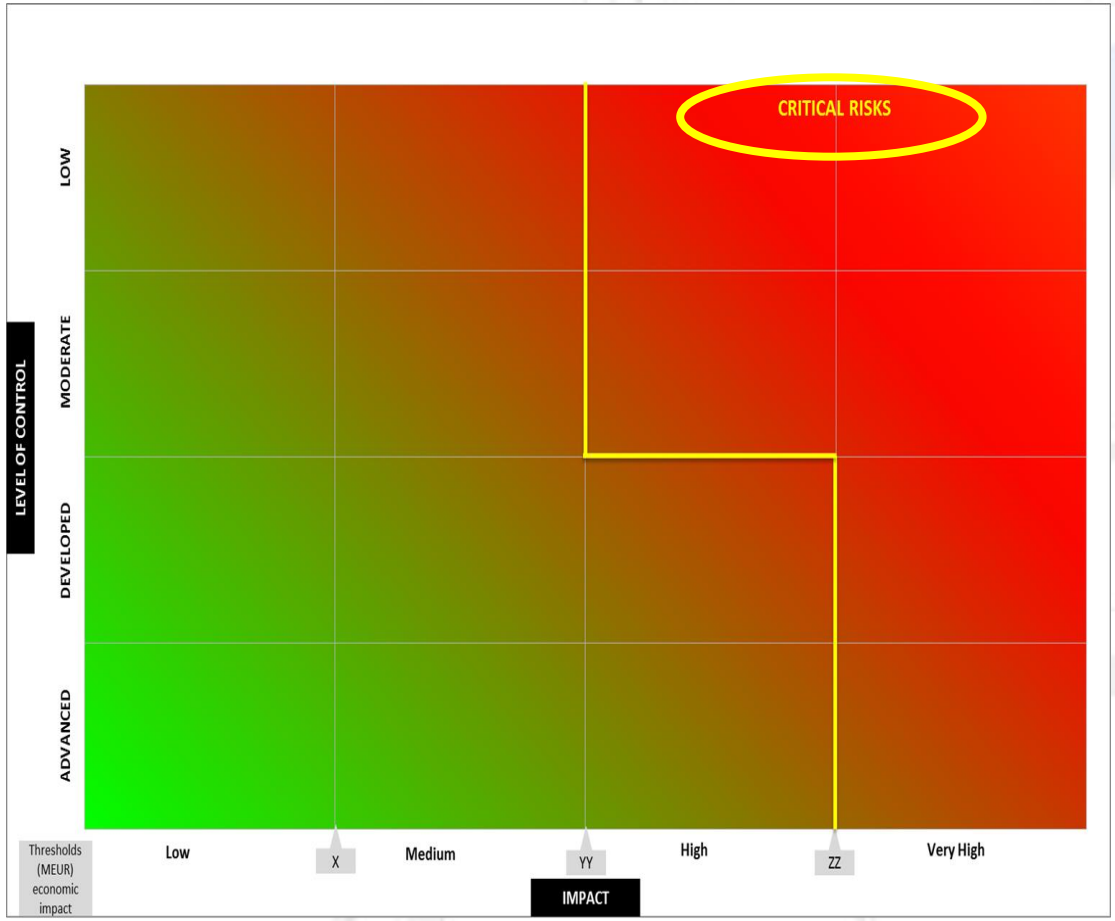
11. Management of Change.
Changes involving people, property, products, processes, information or information systems are to be evaluated for security risks, which are to be properly managed if identified.

12. Continuous Improvement.
Continuous improvement processes are to be established entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends and development and implementation of corrective actions.

SOLVAY


Threat
Asset
Vunerability
Risk

Risk Matrix

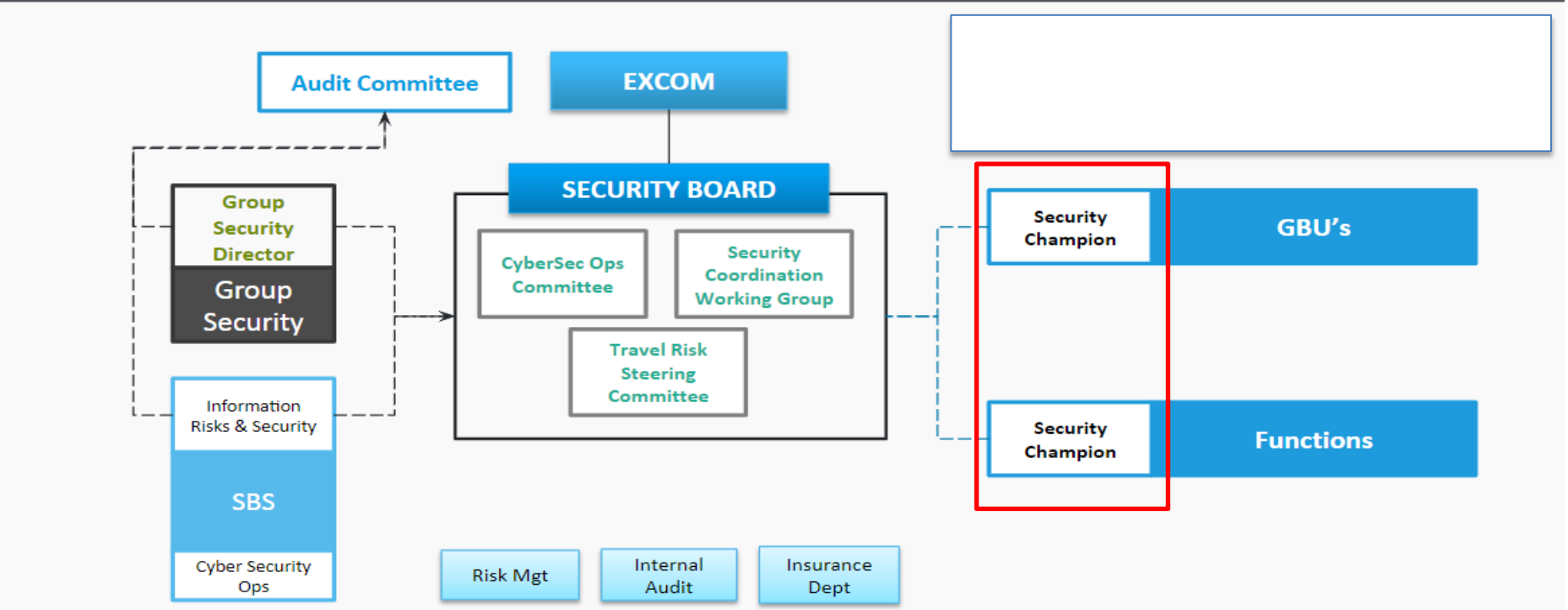


5 types of impact

- Economic
- Injury to people
- Reputation
- Environment
- Legal

L' organizzazione della Governance per la Securty

Bringing stakeholders together



CSOC – Cyber Security Operations Committee

Main purpose

- *Taking in charge the Security Board decisions and recommendations*
- *IT&OT Cyber Security program sharing before presenting to the Security Board*
- *Assuring full visibility and follow-up of the IT&OT Cyber Security program*
- *Identifying and exploiting simplification and collaboration*
- *Sharing IT&OT threat identification, vulnerability and remediation*
- *Escalation of major issues to the Security Board*

Functioning

- *6-7 CSOCs/year*
- *Composed of : Group Security, SBS-IRS, SBS-IT, digital@SBS, IND-GEC, digital@IND, Int. Audit and Risk Managers.., (+guests on demand)*

DATA CLASSIFICATION

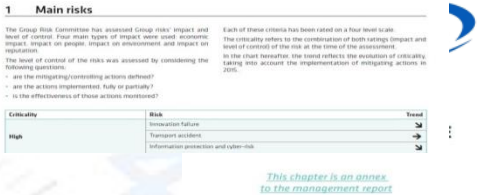
.. and Security Frameworks/Regulations implementation (NIST,GDPR,LPM/ANSSI,..), certifications (ISO9001,ISO27001,..)

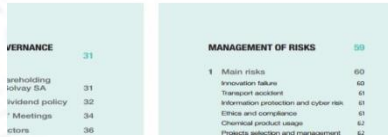
Agenda

1. Industry 4.0-background
2. La minaccia cyber per l'industria e sue attuali vulnerabilità
3. *Differenze e convergenza OT-IT*
4. La governance olistica in Solvay
5. L'approccio per la cybersecurity in Solvay
6. Il Security Profile assessment – un esempio di benchmark in OT -

L' approccio per la cyber security in Solvay

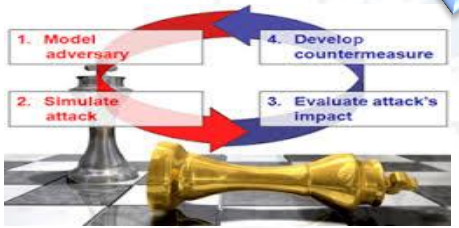
Source : PwC





Information prot

Information prot



Agenda

1. Industry 4.0-background

2. La minaccia cyber per l'industria e sue attuali vulnerabilità

3. *Differenze e convergenza OT-IT*

4. La governance olistica in Solvay

5. L'approccio per la cybersecurity in Solvay

6. Il Security Profile assessment – un esempio di benchmark in OT -

Il Security Profile assessment: - 2 possibili coordinate -

1) Security Level (rif. std IEC 62443) : è l'efficacia della nostra architettura di Sicurezza rispetto ai requisiti richiesti per il livello di minaccia da cui ci si vuole difendere :

SL1 (58 requirements)-> errore operativo inconsapevole da parte di un collaboratore distratto,
SL2 (87 requirements) -> minaccia intenzionale e criminale non sofisticata da parte di un hacker
SL3 (118 requirements)-> minaccia intenzionale criminale e sofisticata da parte di organizzazioni hactivist e terroristiche
SL4 (128 requirements)-> minaccia intenzionale da parte di organizzazioni criminali che mettono in difficoltà le infratrutture e i servizi di un intero paese fino ad immaginare una guerra Cyber

2) Maturity Level (rif. metodologia C2M2) : é l'efficacia della fase operativa-gestionale rispetto alle *best practices* di ciascuna delle 10 aree che chiede di investigare (dal Risk Management al Cyber Security Program Management) :

ML0 -> NOT Performed (assenza di practices)
ML1 -> Initiated (alcune practices documentate)
ML2-> Performed (practices documentate,shakeholders coinvolti,processi supportati,guide lines)
ML3-> Managed (governance esercitata,politiche applicate,personale con skills/resp. chiare)

Security Profile assessment [3/4]

-Il Maturity *Level (MIL0-3) secondo C2M2 :*

-Risk Management
-Asset,change and configuration management
-Identity and access management
-Threat and vulnerability management
-Situational awareness
-Information sharing and communications
-Event and incident response, continuity of operations
-Supply chain and external dependencies management
-Workforce management
-Cyber security program management

Security Profile assessment [4/4]

- esempio di un OT benchmark -

2018 - Tra i 5 Cyber Security Services leaders contattati, si riscontrano :

- ***Pochi audits realizzati in OT (sono quasi tutti in IT)***
- ***Ancor meno i case studies utili ad un benchmark OT significativo .***

Un esempio reale di un DB di un leader tra i più significativi (*) :

Comprende circa 50 audits OT w-w !

(*) Non comprende dati riconducibili al Security Profile di Solvay

La miglior difesa è grazie alle nostre persone…

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

Anie Servizi Integrati

Grazie per l'attenzione

SOLVAY
asking more from chemistry®