



La governance della cybersecurity in Solvay

Antonio Giustino
Solvay

Organizzato da



Solvay 2019 Key figures - a world leader in the chemical industry



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE





FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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.

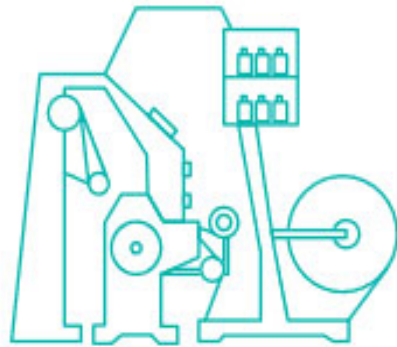
Il Security Profile
assessment
– un esempio di
benchmark in OT -



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



.....-> Industry 4.0



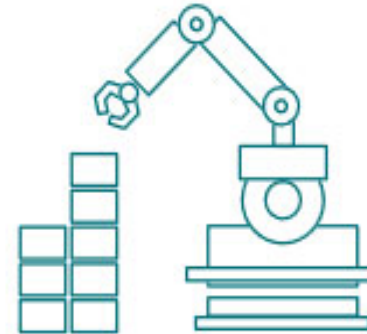
Late 18th-19th century

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
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



Le 9 componenti dell' Industry 4.0





FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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 -



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



La minaccia *cyber* per l'industria e sue attuali vulnerabilità



+ 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



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



Overview



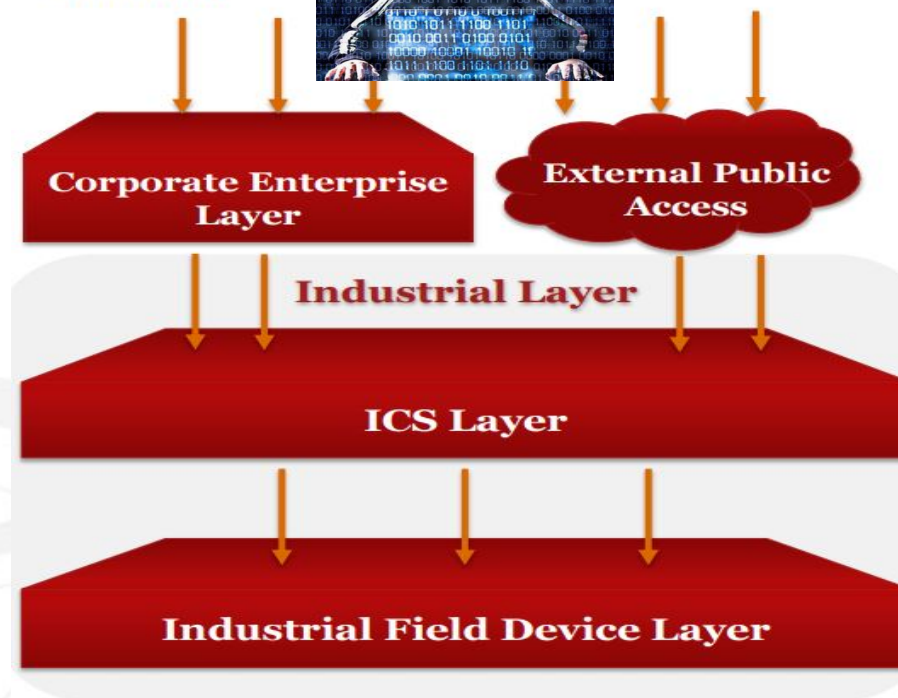
IT:
corp.network, WEB,
ERP, email ,file
servers,collaboration ...

PRINCIPALI MINACCE:

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

OT :
PLC,HMI,SIS,DCS,
SCADA ...

*Field devices
(sensori,attuatori..)*



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

Source : PWC



La minaccia *cyber* per l'industria e sue attuali vulnerabilità



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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



Equipment Damage

- *Equipment overstress*
- *Safety limits violation*

Production Damage

- *Product quality*
- *Production rate*
- *Operating costs*
- *Maintenance efforts*

Compliance Violation

- *Safety*
- *Pollution*
- *Contractual treaties*



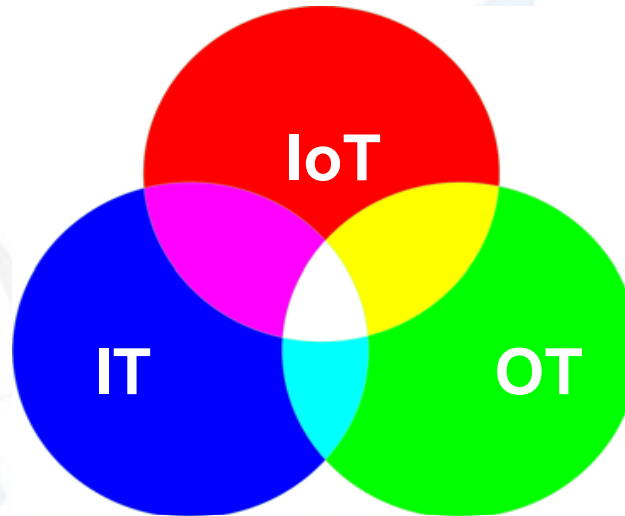
FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



La minaccia *cyber* per l'industria e sue attuali vulnerabilità



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 H1-2019/H1-2018: WHY ?

Turnover = +22%

Cyberattacks on IoT = + 300%



Fonte : F-Secure

2 recent good news from 2019 :

- ETSI released standard for IoT security (basis for IoT certification)
- EU 'Cybersecurity ACT' regulation for certification (voluntary at the moment!)

incidents are



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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 -

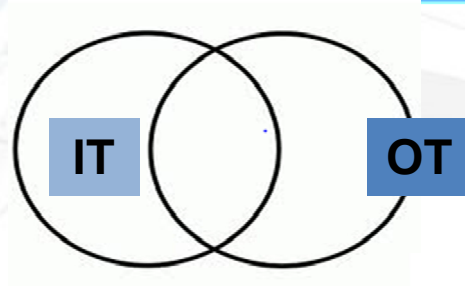
Differenti priorità rispetto alla security



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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





FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



Principali differenze operative IT vs OT



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



OT SECURITY VULNERABILITIES



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



SAFETY IS PARAMOUNT

As Safety is paramount to ICS clients, targeted polymorphic malware is a major concern in 2019-20 (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



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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



@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 ...



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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



@OT :

- evitare soluzioni innovative ignorare 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 proteggerli sistematicamente
- ...



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



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,UEBA,..)
- . Simulare scenari di crisi e relativa escalation,..



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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 -



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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.

Solvay commits us to ensure adequate protection of products, plants, transport, information and information systems against security threats: criminal, malicious and 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 recurrence 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.

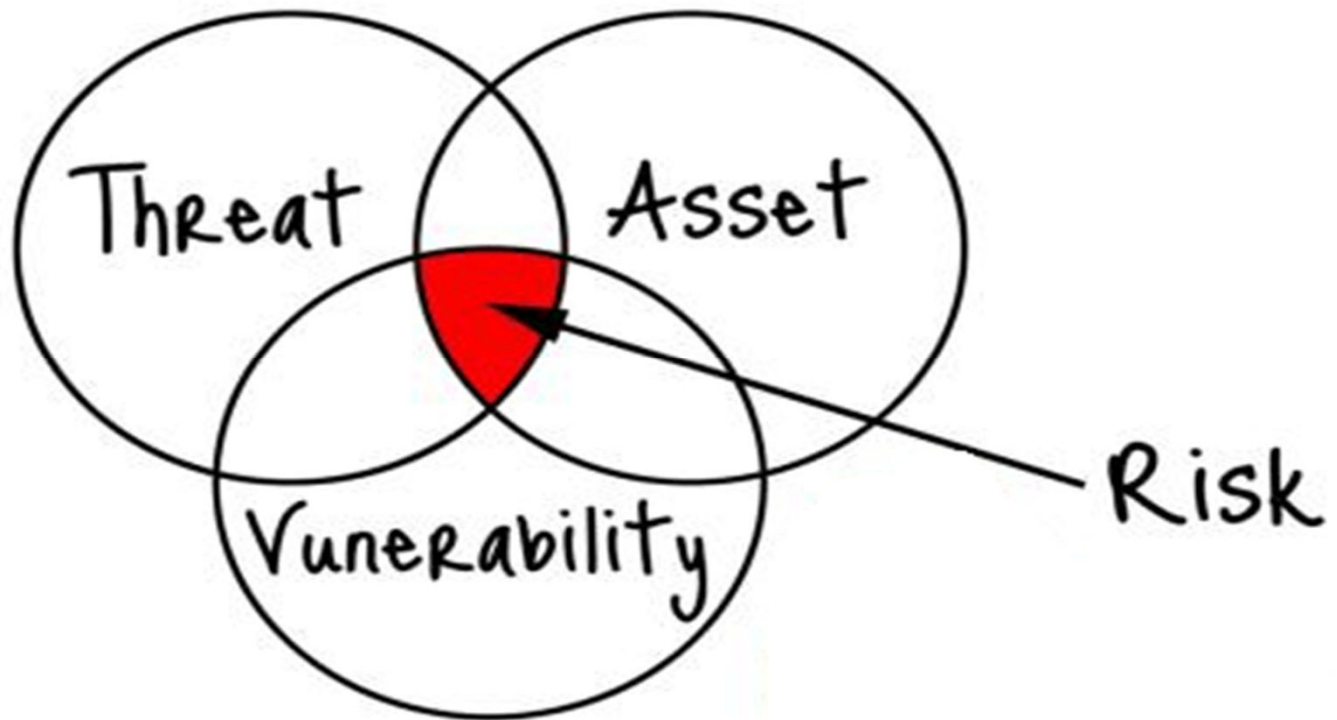
Continuous improvement processes are to be established entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends and development and implementation of corrective actions.



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



INDUSTRY

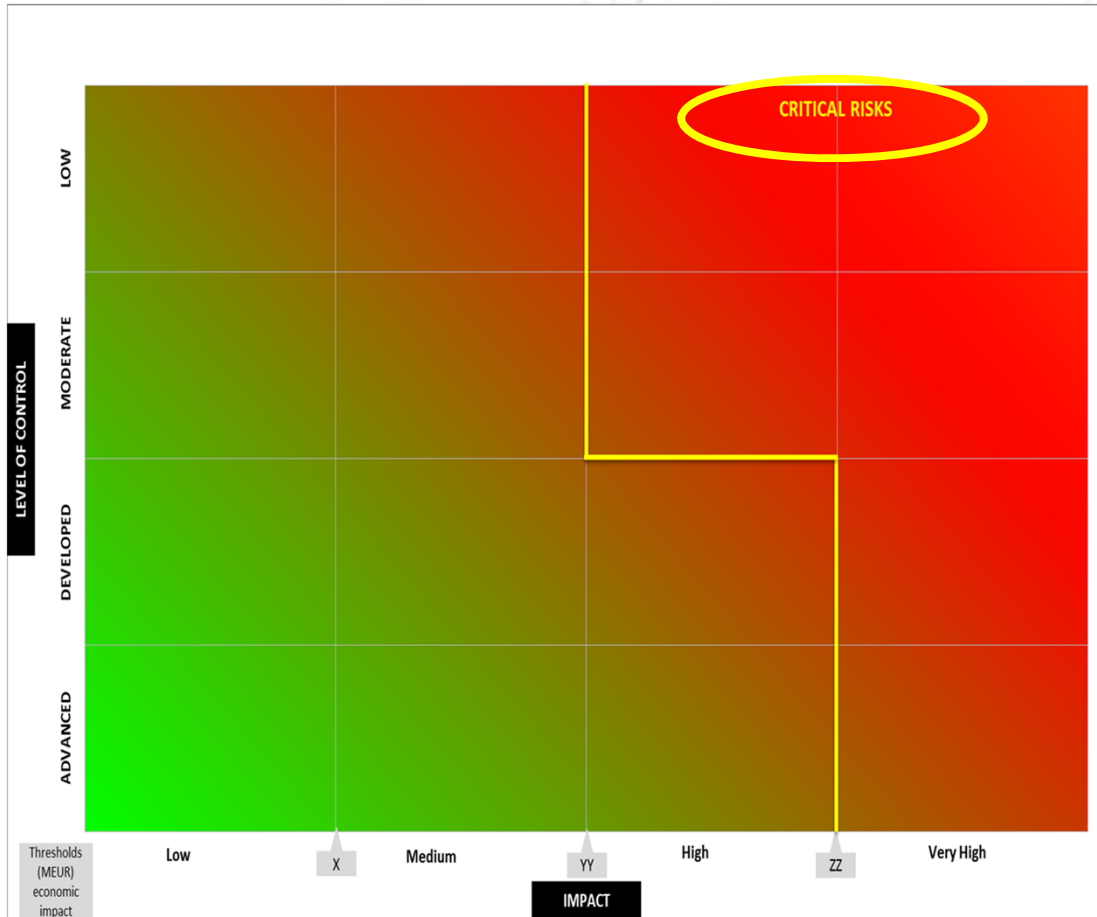




FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



Risk Matrix



5 types of impact

Economic

Injury to people

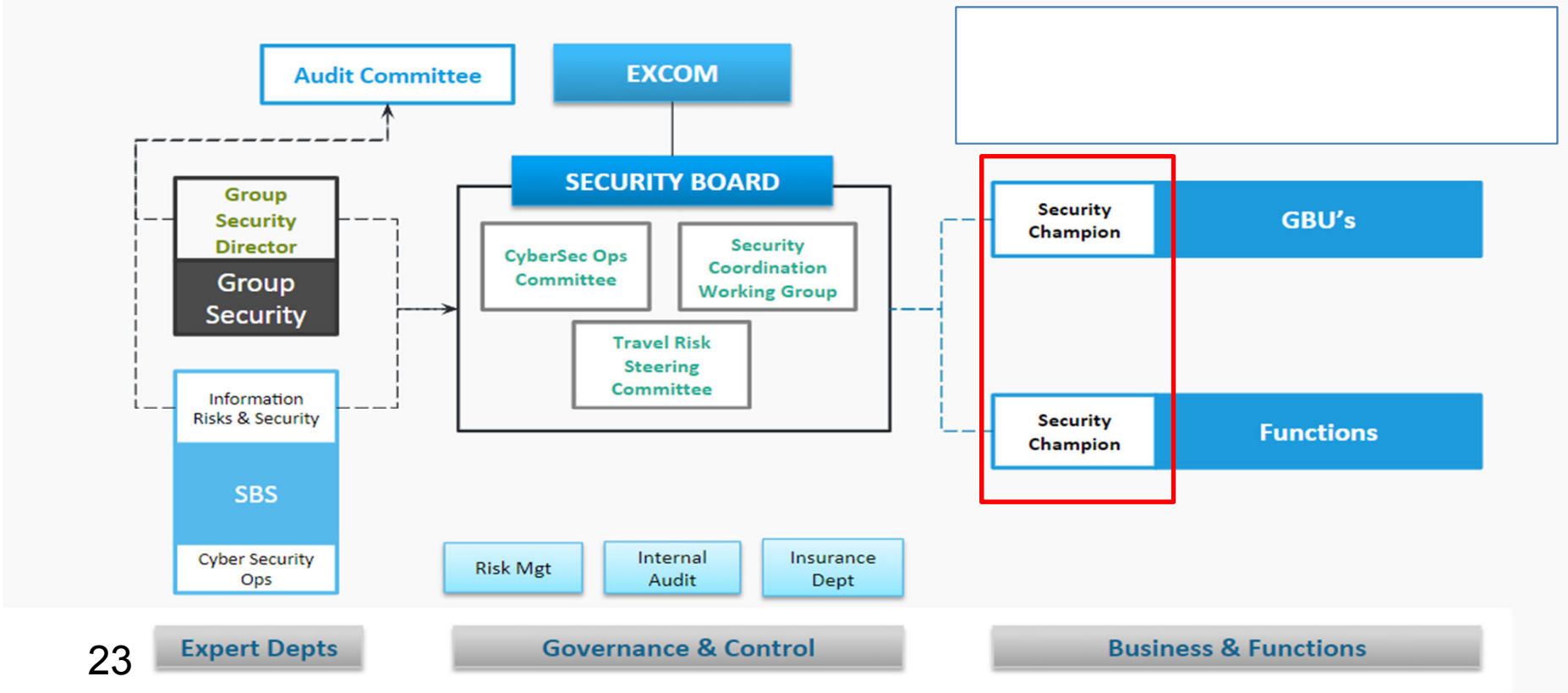
Reputation

Environment

Legal

L'organizzazione della Governance per la Security

Bringing stakeholders together





FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



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 corporate heads : Group Security, Information Risk & Security, IT , IT-Digital , Industrial Automation , Industrial-Digital, Internal Audit (+guests on demand)*



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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

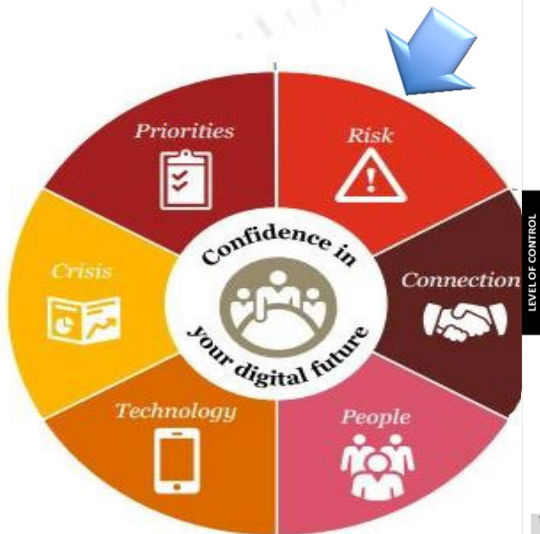
6.

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

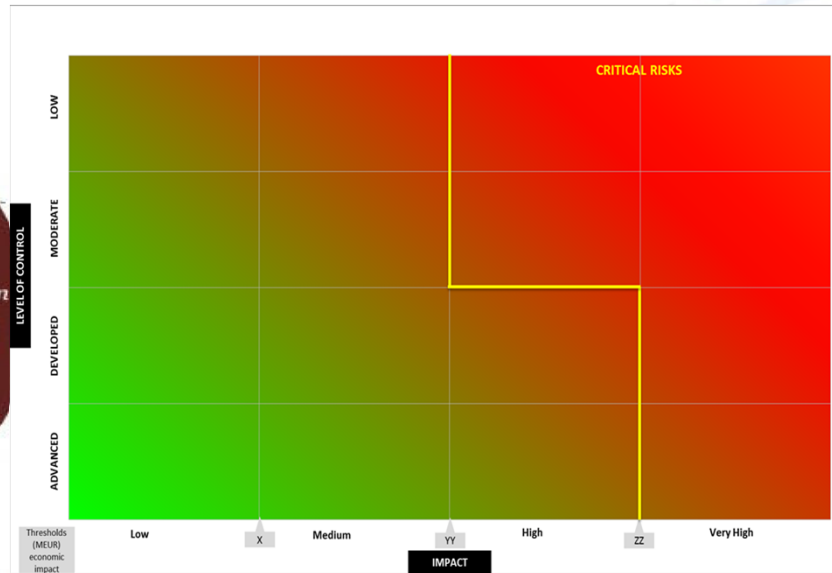
L'approccio per la cyber security in Solvay : RISK



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



Source : PwC



1
CORPORATE GOVERNANCE

This chapter is an annex to the management report.

5 types of impact

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

MANAGEMENT OF RISKS	50
1 Main risks	60
Innovation failure	61
Transport accidents	61
Information protection and cyber risk	61
Ethics and compliance	61
Chemical product usage	62
Product selection and management	62

L'approccio per la cyber security in Solvay : CONNECTION

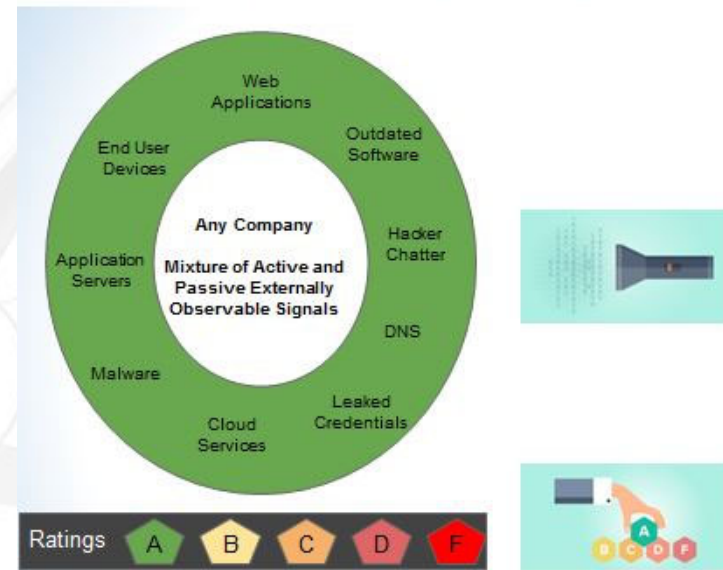


FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



Source : PwC

Cybersecurity Rating



L'approccio per la cyber security in Solvay: PEOPLE



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



Source : PwC



--- Questo messaggio è destinato all'utente Antonio-Michele Giustino ---

Buongiorno,

le ricordiamo che la formazione online training "Certificazione eSecurity" è obbligatoria per tutti i collaboratori di SOLVAY che abbiano accesso alla rete aziendale. Ha ricevuto questo messaggio perché il certificato conseguito scadrà tra 1 settimana.

Senza certificazione, il suo accesso a Internet potrebbe essere sospeso 4 settimane dopo la data di ricezione del presente messaggio. L'accesso sarà riattivato non appena avrà conseguito la certificazione.

Per accedere al programma di certificazione, è sufficiente fare clic sul link seguente: [Fare clic qui.](#)

Grazie per la partecipazione e per il contributo attivo alla sicurezza dei sistemi informativi di SOLVAY.

Cyber espionage
B. Continuity & D. Recovery
Development & integration

Privacy Regulation
ITAR
CUI (NIST)
Dual use goods (EAR)

Reputational

Provider risks
Needs definition & Maturity
Sourcing

L'approccio per la cyber security in Solvay: TECHNOLOGY



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



Source : PwC



Intelligent Detection Platform

Intelligent detection platform that continuously monitors every layer of the internet (data leak, hackers communication, sensitive code share, connected storage)



Surface Web



Deep Web & Dark Web



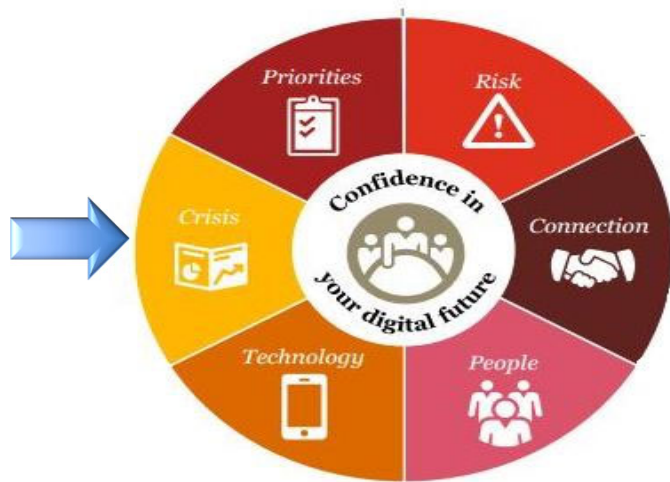
Connected Storage



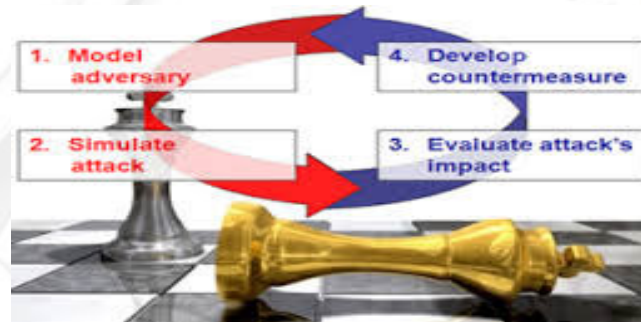
L' approccio per la cyber security in Solvay: CRISIS



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



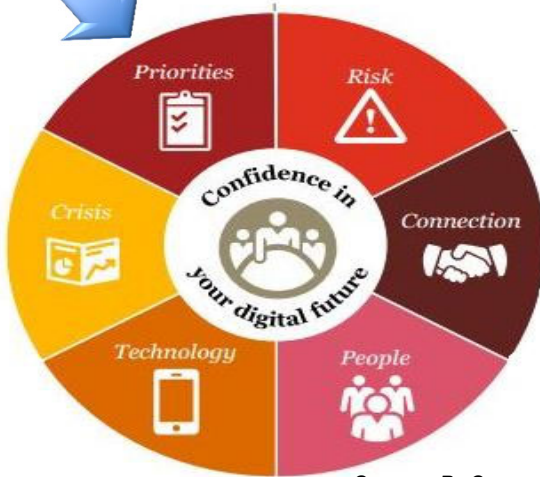
Source : PwC



L'approccio per la cyber security in Solvay: PRIORITIES



Compliance overview
Applicable Today



Source : PwC



Export Regulations	EU – Dual Use Goods Regional Regulation
	China Export National Regulation
	South-Korea Export National Regulation
DFARS Regulation	Controlled Unclassified Information National Regulation

L'approccio per la cyber security in Solvay: REPORT FINALE



1. CORPORATE GOVERNANCE Management of risks



Source : PwC

1 Main risks

The Group Risk Committee has assessed Group risks' impact and level of control. Four main types of impact were used: economic impact, impact on people, impact on environment and impact on reputation.

The level of control of the risks was assessed by considering the following questions:

- are the mitigating/controlling actions defined?
- are the actions implemented, fully or partially?
- is the effectiveness of those actions monitored?

Each of these criteria has been rated on a four level scale.

The criticality refers to the combination of both ratings (impact and level of control) of the risk at the time of the assessment.

In the chart hereafter, the trend reflects the evolution of criticality, taking into account the implementation of mitigating actions in 2015.

Criticality	Risk	Trend
High	Innovation failure	↘
	Transport accident	→
	Information protection and cyber-risk	↘

Information protection and cyber risk





FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



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 -



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



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 infrastrutture 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)



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



Security Profile assessment



-II 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**



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



Security Profile assessment - esempio di un OT benchmark -



2018/19 - Tra i 5 Cyber Security Services leaders contattati, si riscontrano ancora :

- 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 (*) :



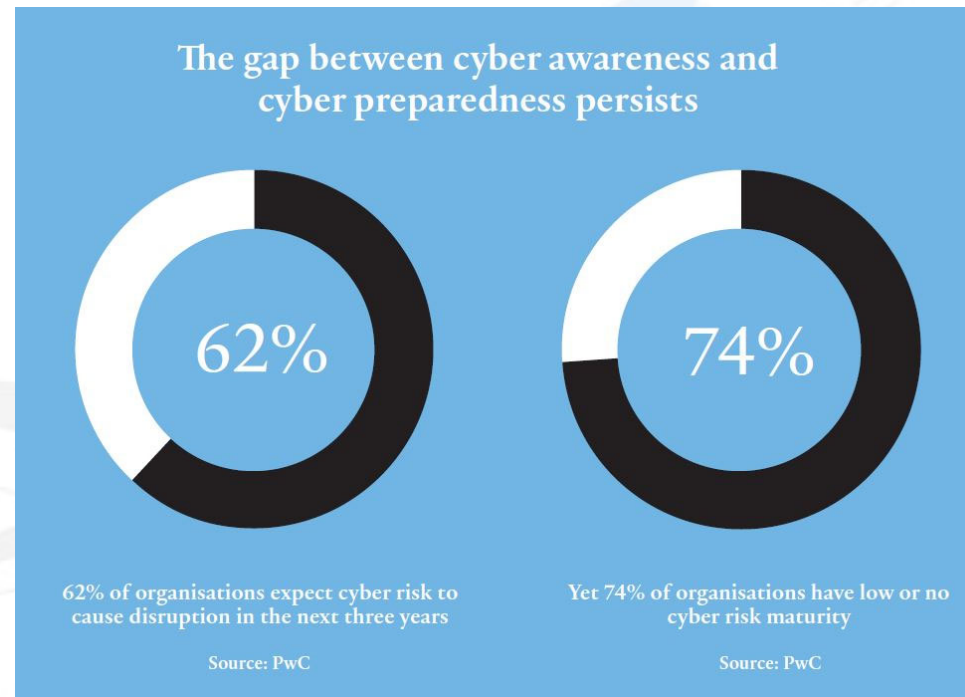
Comprende circa 50
audits OT w-w !



FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



The gap between cyber awareness and cyber preparedness (source PwC – ref. 2018)





FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



La miglior difesa è grazie alle nostre persone...





FEDERAZIONE NAZIONALE
IMPRESSE ELETTROTECNICHE
ED ELETTRONICHE



*Grazie
per l'attenzione*