Cyber Resilience in Energy ecosystems

Energy Community - Cybersecurity Coordination Group - 6th Meeting

July 5, 2022

Filipe Beato, Lead, Centre for Cybersecurity, World Economic Forum

Agenda for Today

- Why is it important?
- Reviewing the principles to drive a cyber resilience organization
- Listing the key recommendations to secure the energy ecosystem
- Defining a shared responsibility model
- Assessing third parties' cybersecurity
- Moving towards senior leadership commitment

Achieving Cyber Resilience is one of the biggest global challenges: Adopting and committing to a global collaborative approach is essential

87%	41%	13%	$4.62M	280
Senior executives plan to improve cyber resilience in their organization	Business executives believe cyber resilience is an established business priority	Cyber leaders find that cyber resilience is integrated in business strategy	Average cost of a data breach faced by organizations in light of a cyberattack	Days on average organizations take to identify and respond to a cyberattack

Source: Global Cyber Outlook 2022, World Economic Forum; Cost of a Data Breach Report 2021. 2021, IBM

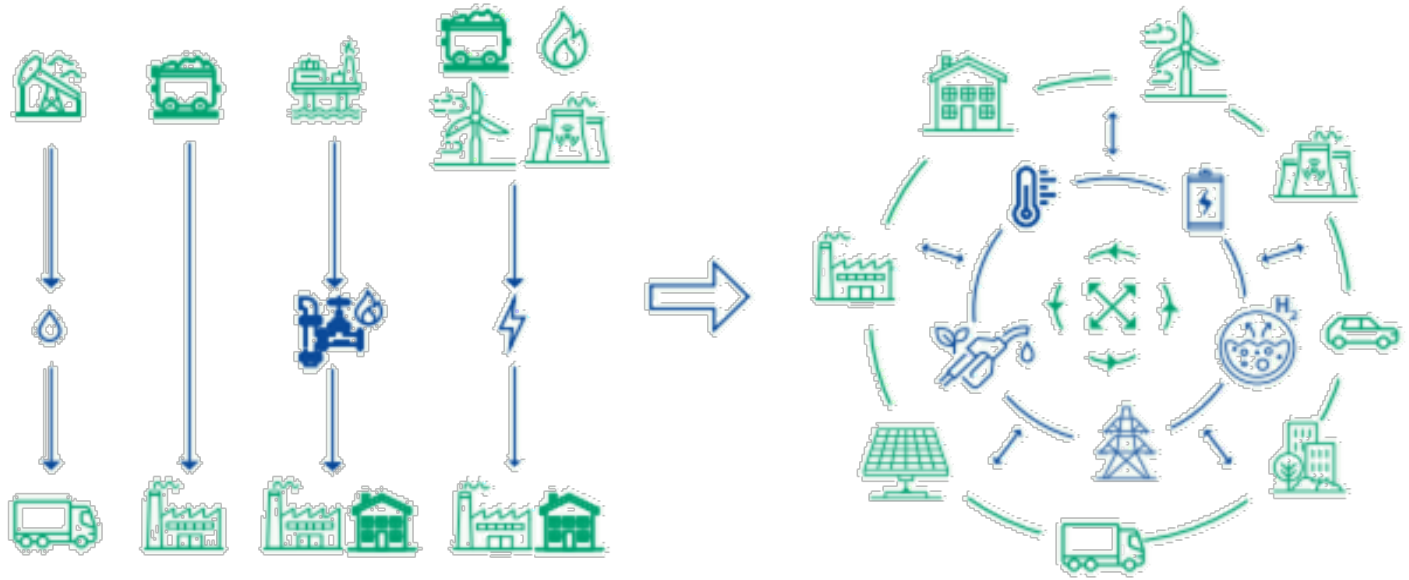
Cybersecurity in energy matters – Public, social and economic impacts are real

In 2020, Colonial pipeline attack disrupted the U.S. East-coast; with continuous attacks aiming to disrupt energy systems

The energy industry is adapting and more dependent on the full supply chain ecosystem – requires a collaborative approach

Energy system today: linear and wasteful flows of energy, in one-directional only

Future integrated energy system: multi-directional energy flows reducing wasted resources



Source: European Commission

Requires a new collaborative approach for securing the full supply chain

- Continuously evolving and changing energy industry
- Integration of new players and industries
- Change global regulatory environment
- Rapid shift and change of cyberthreat landscape

Two leading energy-related industry communities composed by cyber leaders from public-private organizations to driving collaborative action on key cyber resilience topics

Systems of Cyber Resilience: Electricity

Since **2018**, CISOs from Electricity Industry companies around the world have joined our dialogues on enhancing the resilience of critical electricity infrastructure, focusing on organizational culture, policy and supply chain. Taking into account the differential characteristics of the electricity ecosystem: real-time supply, cascading effects and legacy equipment.

Cyber Resilience in Oil and Gas

Since **2020**, CISOs from diverse organizations from the Oil and Gas ecosystem across 20 different geographies, joined to strengthen the cyber resilience across the industry. Driving priority topics on organization culture and strategy and supply chain security following the digitalization and innovation growth of the industry complex ecosystem of assets and changing business models.

Driving organizational change from the top leadership.

Six principles were developed collaboratively by experts on cyber risk in order to integrate and update the leading guidance for directors

Source: Principles for Board Governance of Cyber Risk, World Economic Forum in partnership with NACD and Internet Security Alliance

holistic approach to third-party risk governance

Planning

Plan and select the third party following internal requirements and nature of the service

Assessment and evaluation

Assess the adequacy of your third parties' control environment and recommend remediation activities for improvement

Contract and commissioning

Set up the purchase and contracting methods for procurement with SLAs and KPIs

Operation and monitoring

Perform ongoing monitoring during operation by setting monitoring requirements, timelines, updates and consequence management

Offloading

Finalize the exit relationship strategy and transition plans

Securing the energy critical infrastructure is a **complex** task that requires a **consistent** and **harmonized approach** between all ecosystem parties

Organizations vs. Policy-makers

3 key recommendations to policy-makers to improve the energy critical infrastructure out of 15 presented to the NIS 2.0 directive after SolarWinds:

Ensure a **consistent and harmonized approach** across the EU Member states and the ecosystem

Agree a **common**, minimum global baseline standard for large and smaller enterprises

Focus on incentivizing and rewarding good cybersecurity practices and behaviors

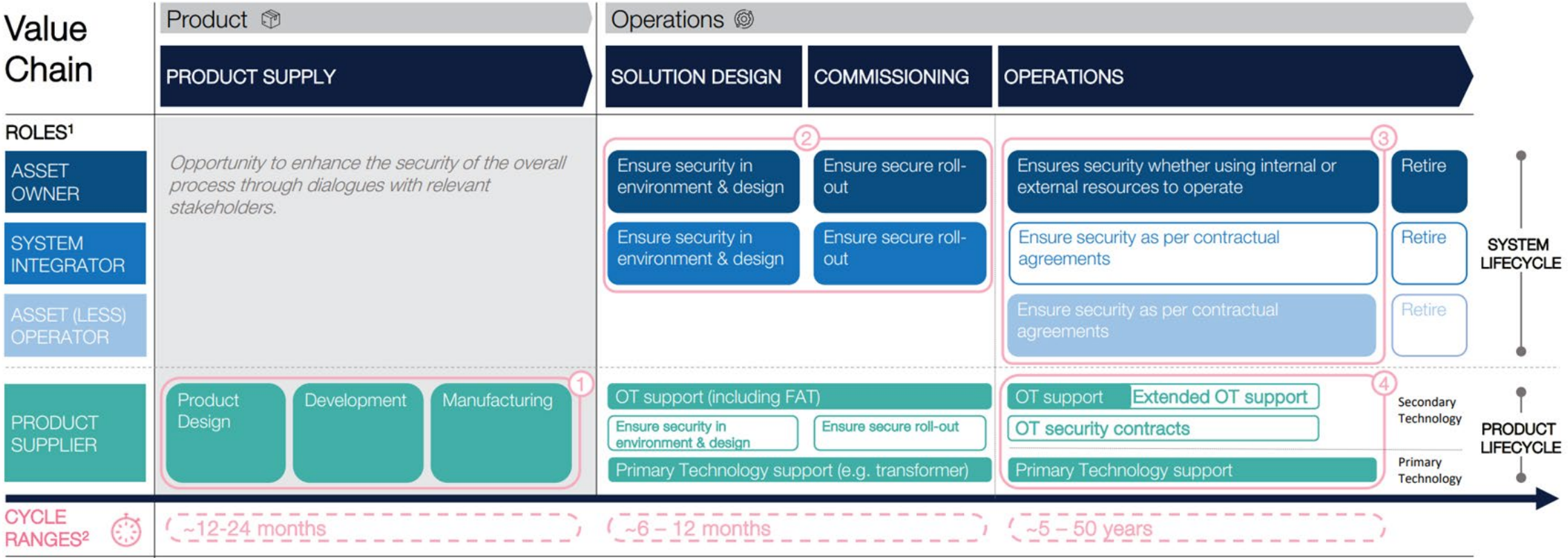
Source: Advancing Supply Chain Security in Oil and Gas: An Industry Analysis; European Commission's Cybersecurity Package Commentary in light of recent sophisticated supply chain attacks

10 key actions for organizations in establishing a common cybersecurity baseline

1. Govern third parties' risk by establishing roles and responsibilities
2. Develop the cyber literacy and education of employees handling third parties
3. Establish access controls and management of critical assets
4. Implement change and configuration management
5. Require secure-by-design and by-default systems, services and interfaces
6. Maintain response mechanisms by ensuring incident management, BCM and DRP
7. Protect critical information while aligning with relevant regulations and guidelines
8. Secure operational and physical environments by using leading safety practices
9. Implement a secure development lifecycle of products, systems and tools
10. Provide support for vulnerability management and patching

Source: Advancing Supply Chain Security in Oil and Gas: An Industry Analysis

Protecting the energy industry supply and value chains go beyond securing individual products or systems – it requires a shared responsibility to be integrated into a secure system and operated in a secure context



Source: Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain

No silver bullet to evaluate third-parties across the supply chain, with the combination of multiple assessment types is advised depending on the scalability and coverage required

	Scoring ratings	Shared assessments	Internal assessments	Industry certifications
	Cybersecurity ratings are a data-driven, objective, and dynamic measurement demonstrating the cybersecurity posture level of organizations	Third party risk programs providing organizations a detailed report on the cybersecurity maturity of third-parties (people, process and procedures)	Internal assessments are based on organization's specific cybersecurity requirements following the criticality of the service provided by third parties	Cybersecurity industry certifications provide a form of attestation on the level of security controls of organizations based on external audit exercises
Scalability	High to rapid	High but dependent on the eco-system	Low	Low
Scope	Partial	Variable	Variable	Variable (depending on certification)
Frequency	Continuous	On demand	Event driven	Annual
Methodology	Scan of external facing assets	Proprietary security assessment	Proprietary security assessment and organization-based accreditation	Audit, Proprietary security assessment
Intrusiveness	Low, public data from internet/market	High, needs NDA	Variable, may need NDA	High, needs NDA
Supplier cost/effort	None	Vendor (also) pays but sponsoring is possible	Variable	Moderate to High
Consumer cost/effort	Moderate	High	Moderate to High	None for organization

Scalability → Coverage of assessments

Source: Advancing Supply Chain Security in Oil and Gas: An Industry Analysis

How do we plan to continue drive collective action for addressing industry and systemic global challenges?

- Ensure public commitment at highest level
- Foster lessons sharing and thought leadership
- Develop new approaches, solutions and best practices

Cyber Resilience Pledge

Strengthen cyber resilience across industry ecosystems

WORLD ECONOMIC FORUM

Cyber Resilience Pledge aims to signify global commitment to strengthen cyber resilience across industry ecosystems

Moving cybersecurity from a business cost to a business benefit

Purpose

Foster collaborative and collective action to strengthen cyber resilience globally

Approach

Leverage multi-stakeholder communities of cyber leaders to take an ecosystem-wide approach endorsed by CEOs

Outcome

Create a vibrant industry-community dedicated to cyber resilience bounded by a public-facing common brand

Cyber Resilience Pledge championed by 20+ CEOs from the Cyber Resilience in Oil and Gas industry – to be scaled to other industries and systemic global challenges for a public commitment and action...

Global CEOs announce Cyber Resilience Pledge at Davos

POLICY

Global oil and gas compa... pledge for cyber resilience

BY INES KAGUBARE - 05/25/22 1:12 PM ET

SECURITY May 26, 2022

Global oil and gas firms pledge to take action towards cyber resilience

Eighteen companies have taken a Cyber Resilience Pledge with the aim to ...itment towards strengthening cyber resilience across ...

Global CEOs Commit To Collective Action On Cyber Resilience

May 25, 2022 Eurasia Review 0 Comments

OIL AND GAS

WEF: Global CEOs commit to collective action on cyber resilience in oil and gas industry

The pledge promotes a shift towards a resilience-by-design culture, ecosystem-wide, cyber-resilience plans and greater collaboration between players

Oil and gas companies take cyber resilience pledge

18 energy corporations have agreed to cooperate on dedicated solution to strengthen cybersecurity across the industry

Scale learnings to other industries

Address industry-specific challenges collaboratively

Commit publicly to drive actions on systemic global challenges

Thank you!

Filipe Beato, Lead, Centre for Cybersecurity