RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: STR-T08

The Journey of Cybersecurity in Kuwait's Oil and Gas Industry

Dr. Reem F. Al-Shammari

Information Security Team Leader "CISO"
Kuwait Oil Company
LinkedIn: Dr.Reem AlShammari
Twitter: @Q8Thunders

About Me

Team Leader Information Security “CISO”, Kuwait Oil Company;

Ranked # 1 at IFSEC Global Top Influencers in Security & Fire 2019 “CyberSecurity Category”

Linkedin: Dr.Reem AlShammari

Twitter: @Q8Thunnders

Dr. Reem Al-Shammari, Information Security Team Leader at Kuwait Oil Company, Kuwait. She is recognized as a “Wild Card” who continues to ‘push the envelope’ to get to the most optimum outcome on an initiative or a project. She has played a huge role in changing the maturity of the Kuwait’s Oil and Gas sector cyber security and also contributed in maturing country’s national cybersecurity. Contributes greatly into empowering Women in Cyber Security specifically and into the Cybersecurity Community around the globe as a whole through various initiatives and programs.

Government:
- Chairperson, Kuwait Oil Sector’s “K-Sector” Cyber Security Committee.
- Technical lead in GCC Cyber security Committee.

Women Initiatives:
-Cofounder & Board member- Women in CyberSecurity Middle East (WiCSME) Group
- Kuwait Representative in UK-Gulf Women in Cyber Fellowship Program

Academia:
- Phd in Business.
- Graduate from **Harvard Business School**, General Management Program for Executive Education, Nov. 2019.

Fora & Awards:
- Keynote Speaker.
- International, Regional, & national Awards (Regional Leadership Award – EWF, Arab CISO,MESA)

Kuwait Oil Company
إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Agenda

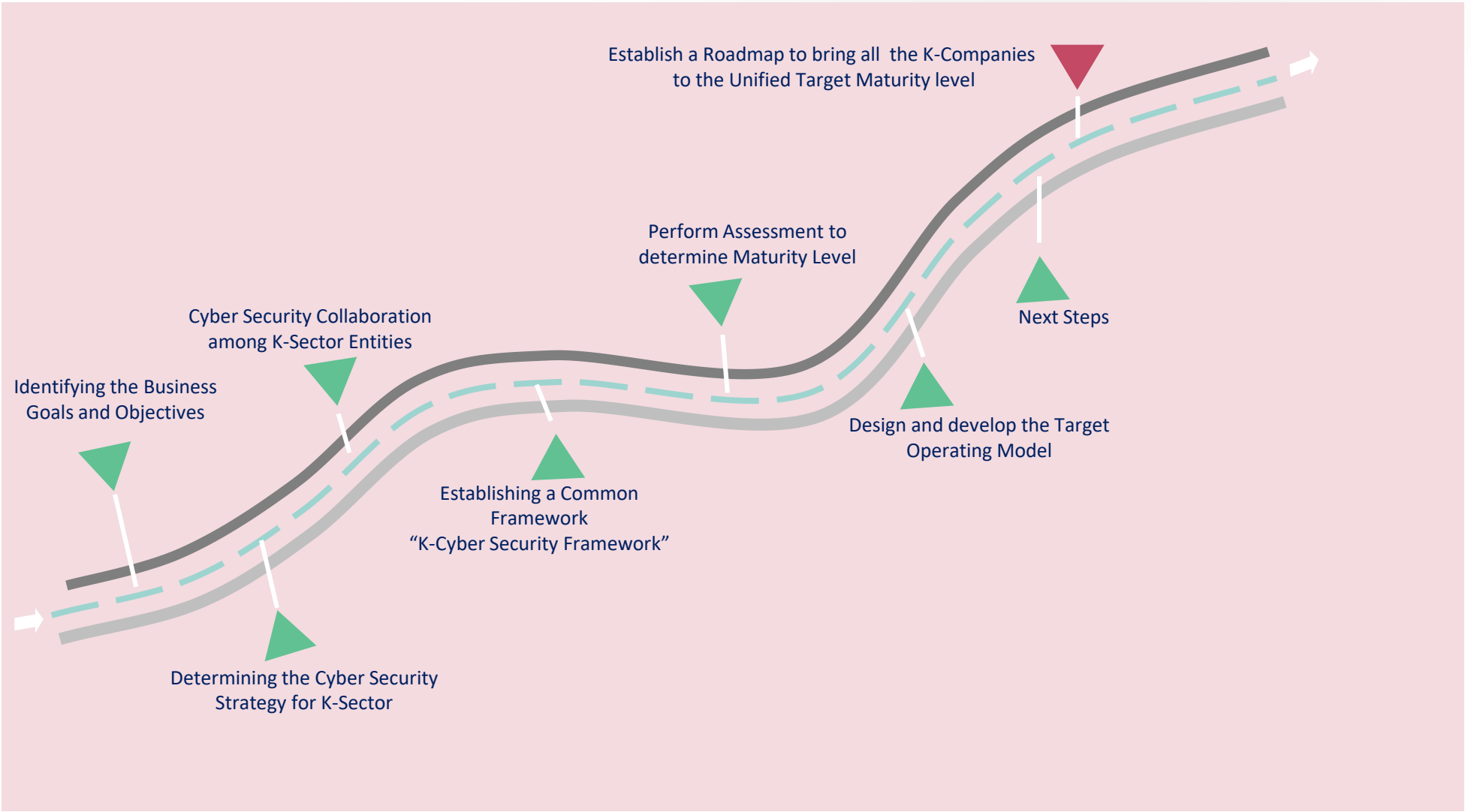
1. The Cyber Security Journey in Kuwait's Oil &Gas Sector
2. The Cyber Security Collaboration within the K-Sector
3. K-Cyber Security Framework
4. K-Cyber Security Maturity Assessment
5. Alignment with National CyberSecurity Strategy
6. The Way Forward - Information Security Roadmap
7. Strategic Outcomes
8. The Takeaways

شركة نفط الكويت
Kuwait Oil Company
إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

RSAConference2020

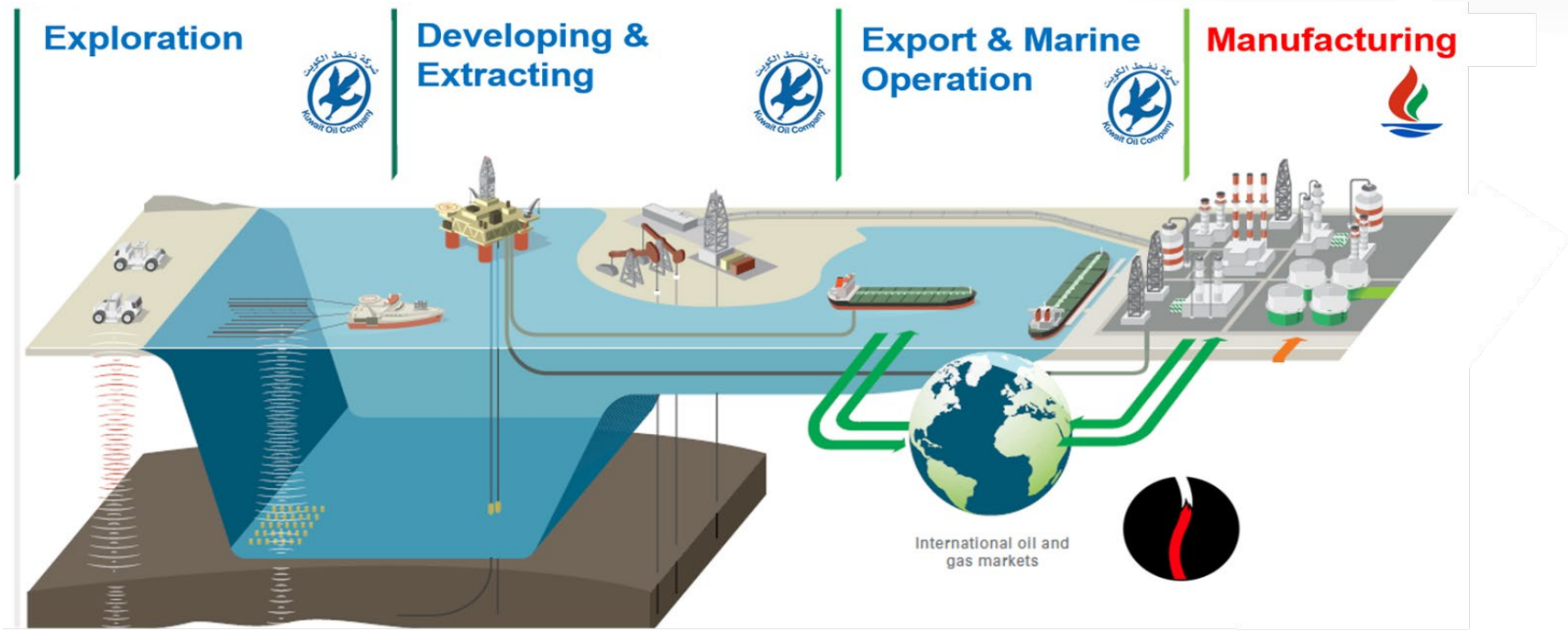
Cyber Security Journey in Kuwait's Oil &Gas Sector

The Cyber Security Journey in Kuwait's O&G Sector



The Cyber Security Journey in Kuwait's O&G Sector

Impacts of Cyber Security on our Core O&G Operations



Attackers can interfere and cause severe Impacts and interruptions to business operations and Strategic Objectives.

Technology comes with Price.

O&G Industry Percentage (10%) of annual total cost of cyber crime

≈ *$44 Billion*

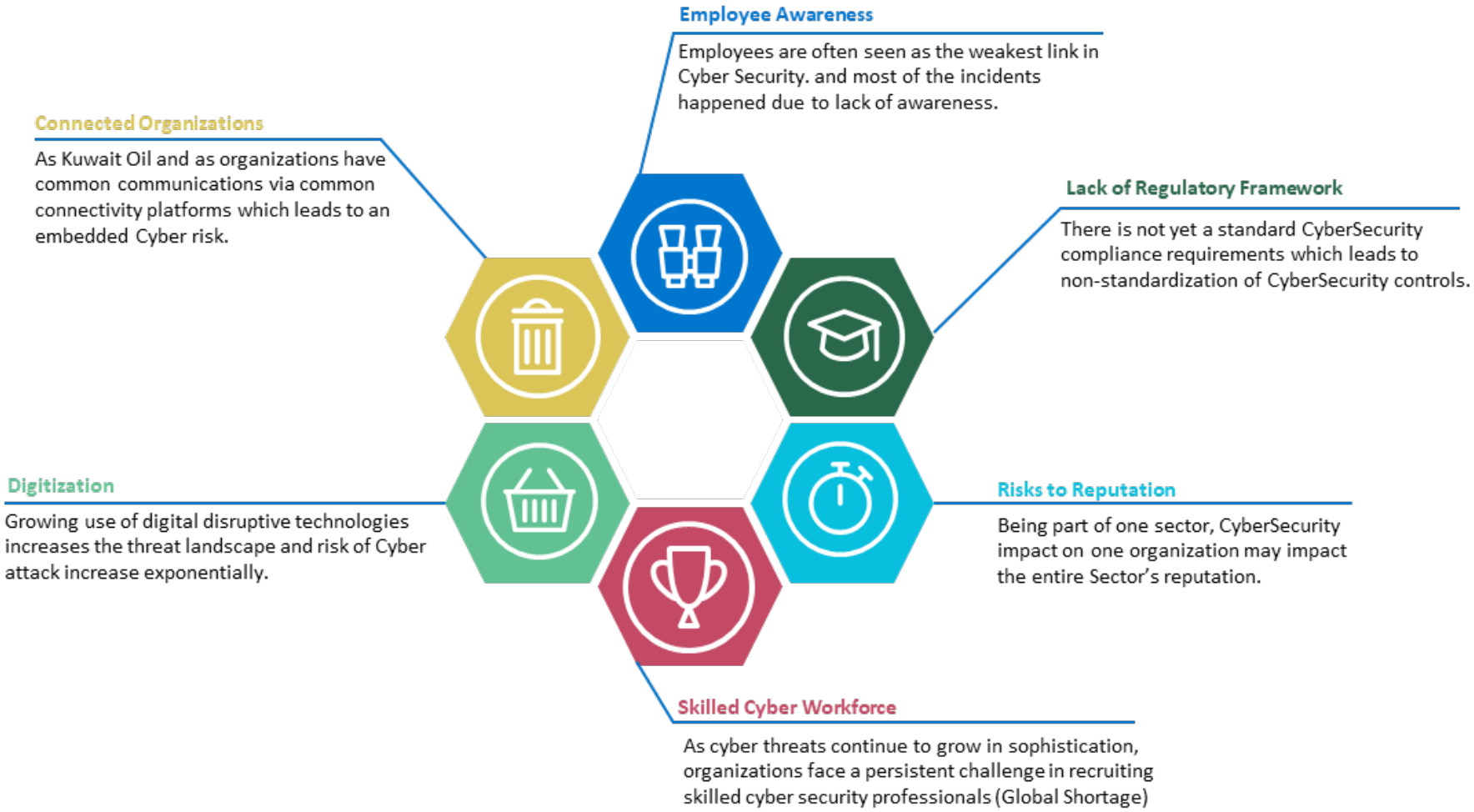
* Statistics provide by Symantec's Internet Security Report 2015 & Ponemon Institute - The Impact of Cybercrime on Business Report 2013

Kuwait Oil Company
إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

The Cyber Security Journey in Kuwait's O&G Sector

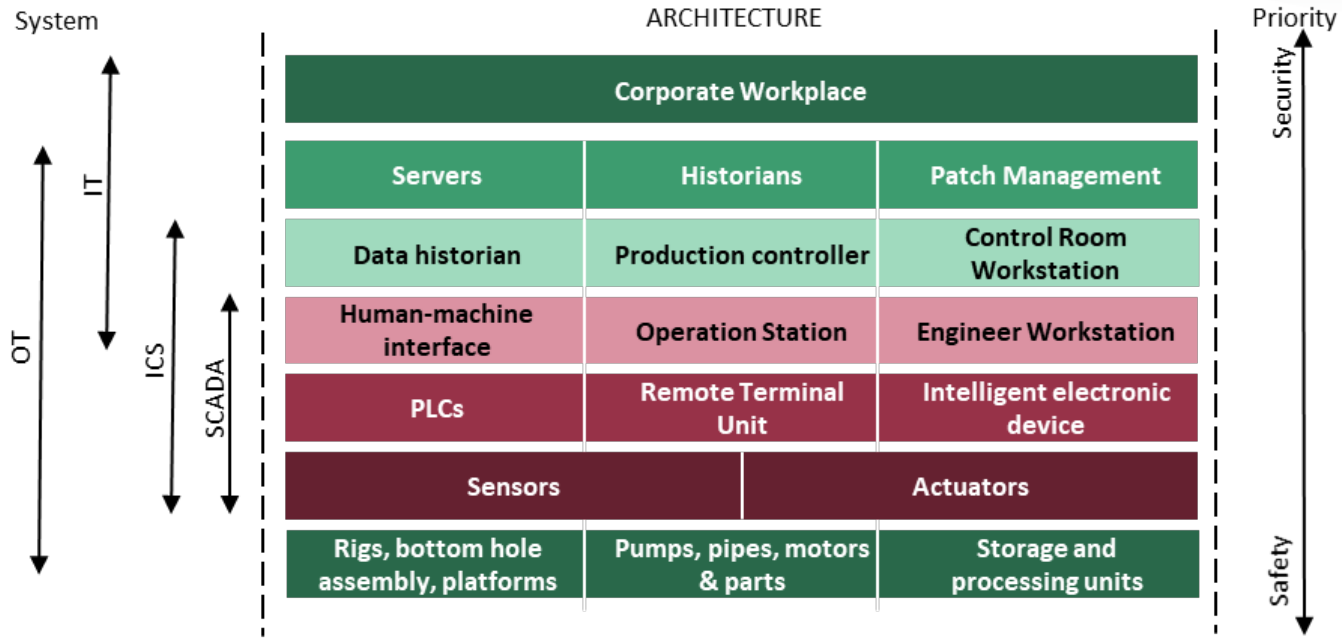
Common Concerns across the K-Sector

K - Sector (Group of companies under umbrella of Kuwait Petroleum Corporation KPC) represents Kuwait's oil and gas companies



The Cyber Security Journey in Kuwait's O&G Sector

ICS/OT Environment Related Concerns



RSAConference2020

The Cyber Security Collaboration within The K-Sector

Cyber Security Collaboration within the K-Sector

Collaboration's objectives was to address the below main challenges:

1 **Absence of a common Cyber Security Strategy**
Cyber Security activities did not branch out from the Cyber Security Strategy that would be tied to the business strategy.

2 **Lack of Budget**
The allocation of individual Cyber Security budget for each company in the K-Sector made establishing cyber capabilities an expensive task.

3 **Cascading attack**
An attack in one K- Company could possibly compromise another.

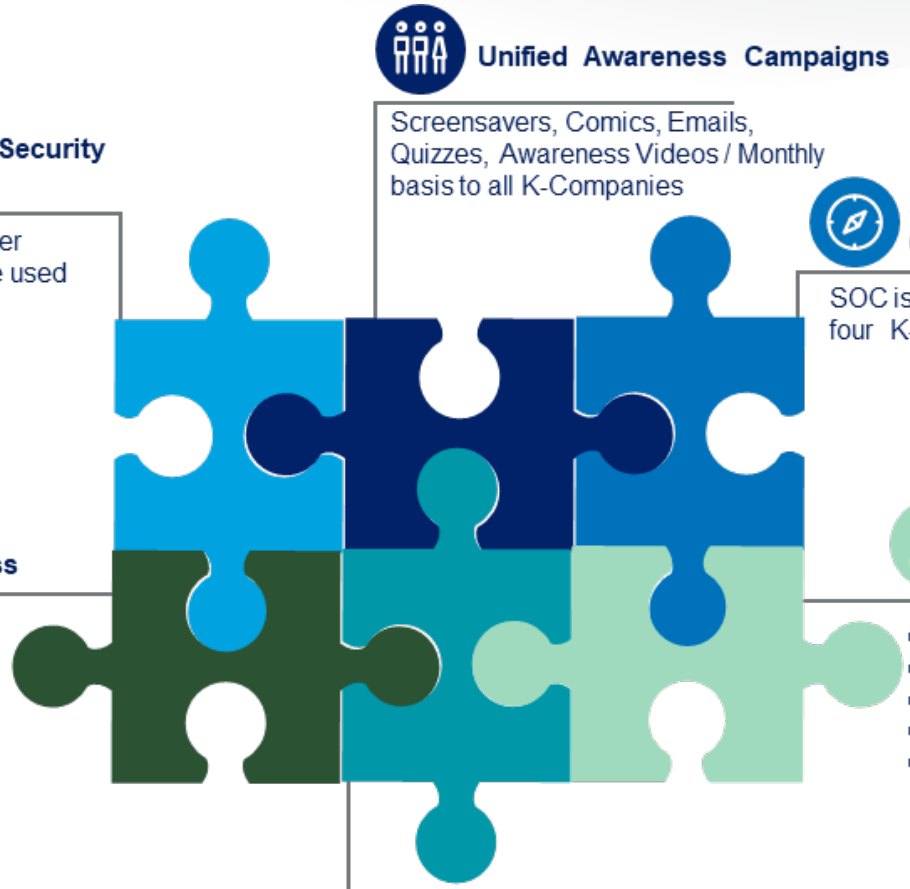
To lead the K-Companies Cyber Security Agenda through collaborative approach:

- Raises the CyberSecurity Maturity Level.
- Enhances vigilance (information sharing & intelligence)
- Leveraging all available capabilities/resources.

Kuwait Oil Company
إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Cyber Security Collaboration within the K-Sector

K-Cyber Security Achievements



Unified Awareness Campaigns

Screensavers, Comics, Emails, Quizzes, Awareness Videos / Monthly basis to all K-Companies

Unified K-Cyber Security Framework

Developing a Unified Cyber Security Framework to be used for K-Companies.

Security Operation Center (Hybrid)

SOC is established Serving four K-Companies (24/7/365)

Cyber Security Program Progress

Maturity assessment, asset classification, Compliance to leading practices, Operating Models & Roadmaps, and current initiative mapping is initiated for K- Companies.

Multiple Cyber Security Initiatives

- K-Cyber Security SMAIP
- Active Threat Intelligence Sharing
- Compromise Assessments
- K-Cyber Insurance Study
- Technologies/Solutions Information Security Risk Assessments

Compliance

K-Companies overall compliance level to international information Security standards has increased due the multiple Cyber Security initiatives.

RSAConference2020

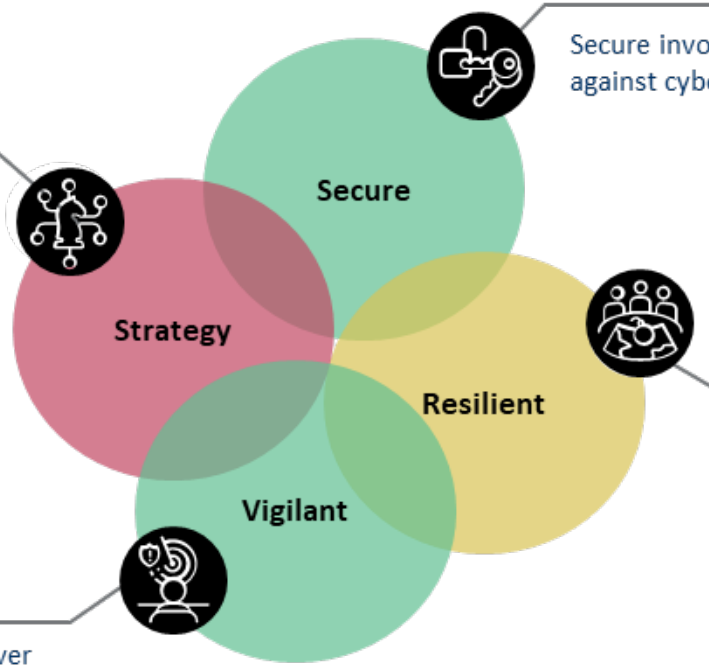
K-Cyber Security Framework

K-Cyber Security Framework

Development of a Common Framework

34

Cyber Security Capabilities



Secure involves establishing proactive protection against cyber attacks before their occur

Strategy involves ensuring that the organization has a clear direction to maintain and enhance the organization's cyber security capabilities.

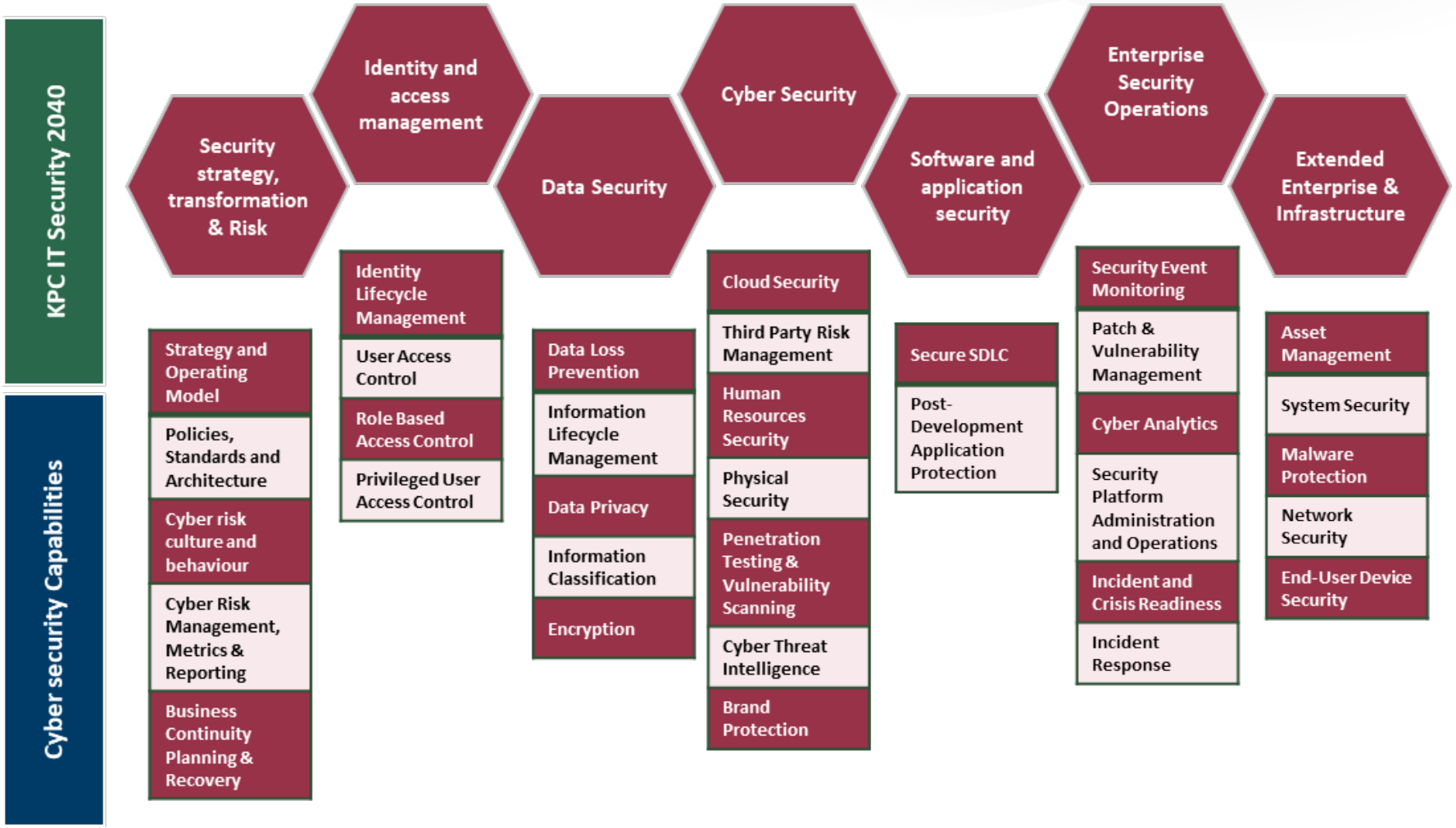
Resilient involve the ability to respond to and recover from cyber attacks after their occur in order to minimize any adverse impact to the organization.

Vigilant involves the ability to discover internal and external threats by leveraging threat intelligence.

Kuwait Oil Company
إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

K-Cyber Security Framework

Mapping with K-Sector's Cyber Security Strategy 2040



*K-CSF is based on controls from different international standards and leading practices (NIST / ISO / CIS / SANS)

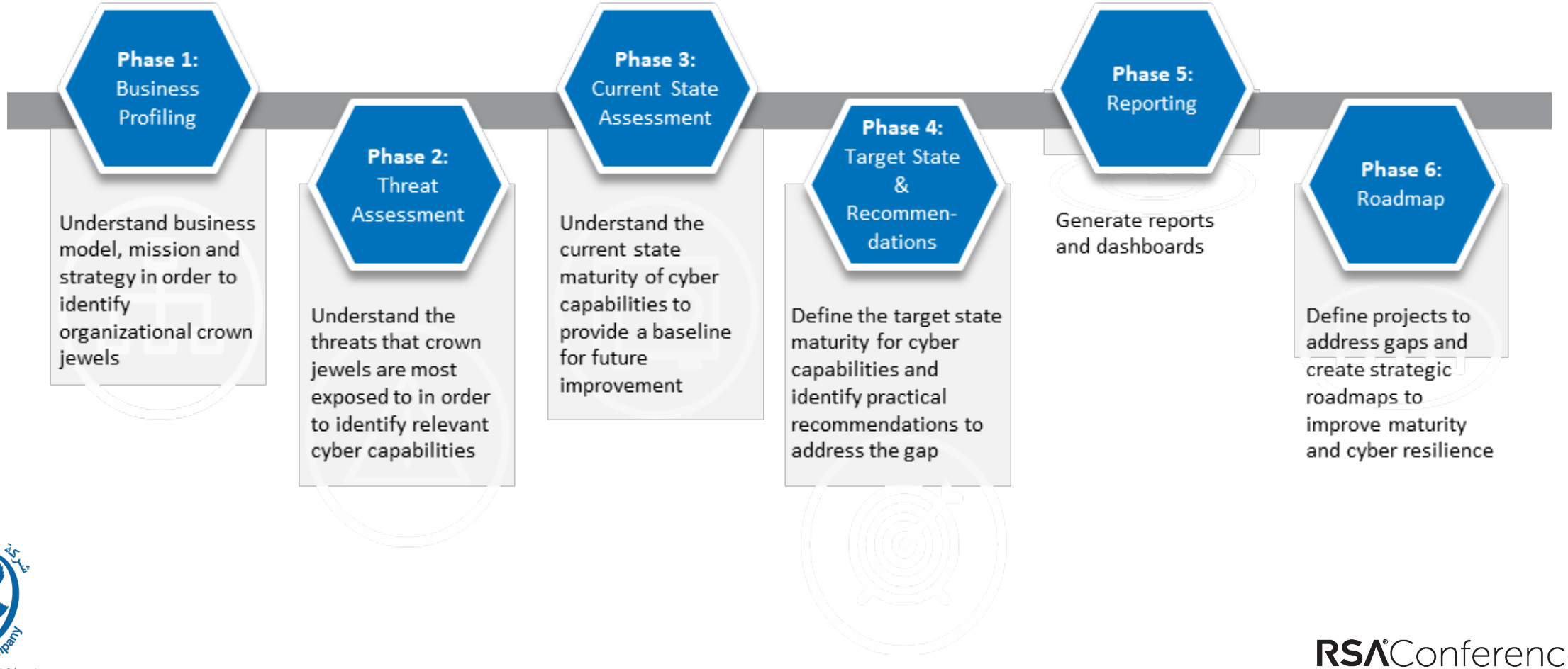
RSAConference2020

K-Cyber Security Maturity Assessment

K-Cyber Security Maturity Assessment

Methodology & Approach

The CSF assessment Methodology consisted of a **six stage process** encompassing K-companies **Business**, **Threats** and **Capabilities**.



K-Cyber Security Maturity Assessment

Scale of Efforts "Number Talks"

The CSF assessment Methodology consisted of a **six stage process** encompassing K-companies **Business**, **Threats** and **Capabilities**.

Perform Cyber Security Maturity Assessment

Interviews conducted

150+

150+ Interviews were conducted across all organizations

Questions Surveyed

2000+

2000+ Questions were surveyed in each K-Company

Rounds of review

≥ 2

Minimum two (2) Rounds of review was done with each K-Company

Analysing and Reporting the results

400+

400+ hours were spent for each K-Company for analyzing and reporting the results

Time spent by K-company personnel

50+

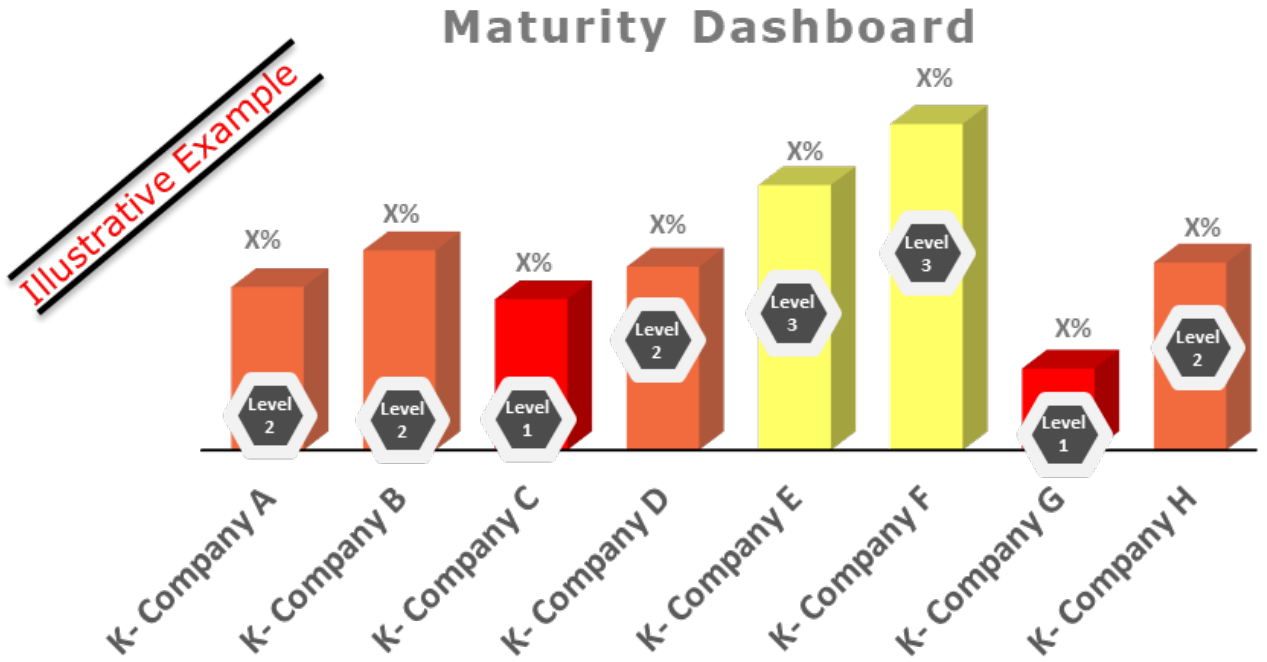
50+ hours were spent by each K-Company personnel during the assessment

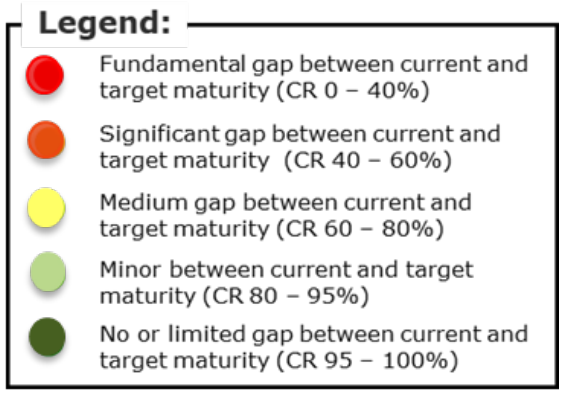
شركة نفط الكويت
Kuwait Oil Company
إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

K-Cyber Security Maturity Assessment

Cyber Resilience Examples– Maturity Dashboards

Capabilities were assessed in terms of their Cyber Resilience % (CR%). Cyber resilience refers to the extent to which the organization is secure against its most important threats.





** Above is sample results only from the Cyber Security Assessment

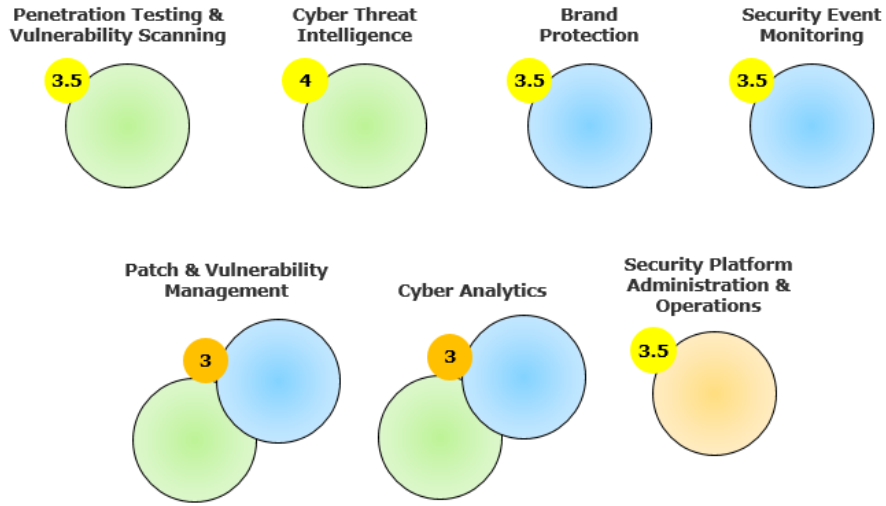
K-Cyber Security Maturity Assessment

Cyber Resilience Examples – Vigilant Dashboards

Capabilities were assessed in terms of their Cyber Resilience % (CR%). Cyber resilience refers to the extent to which the organization is secure against its most important threats.

Vigilant

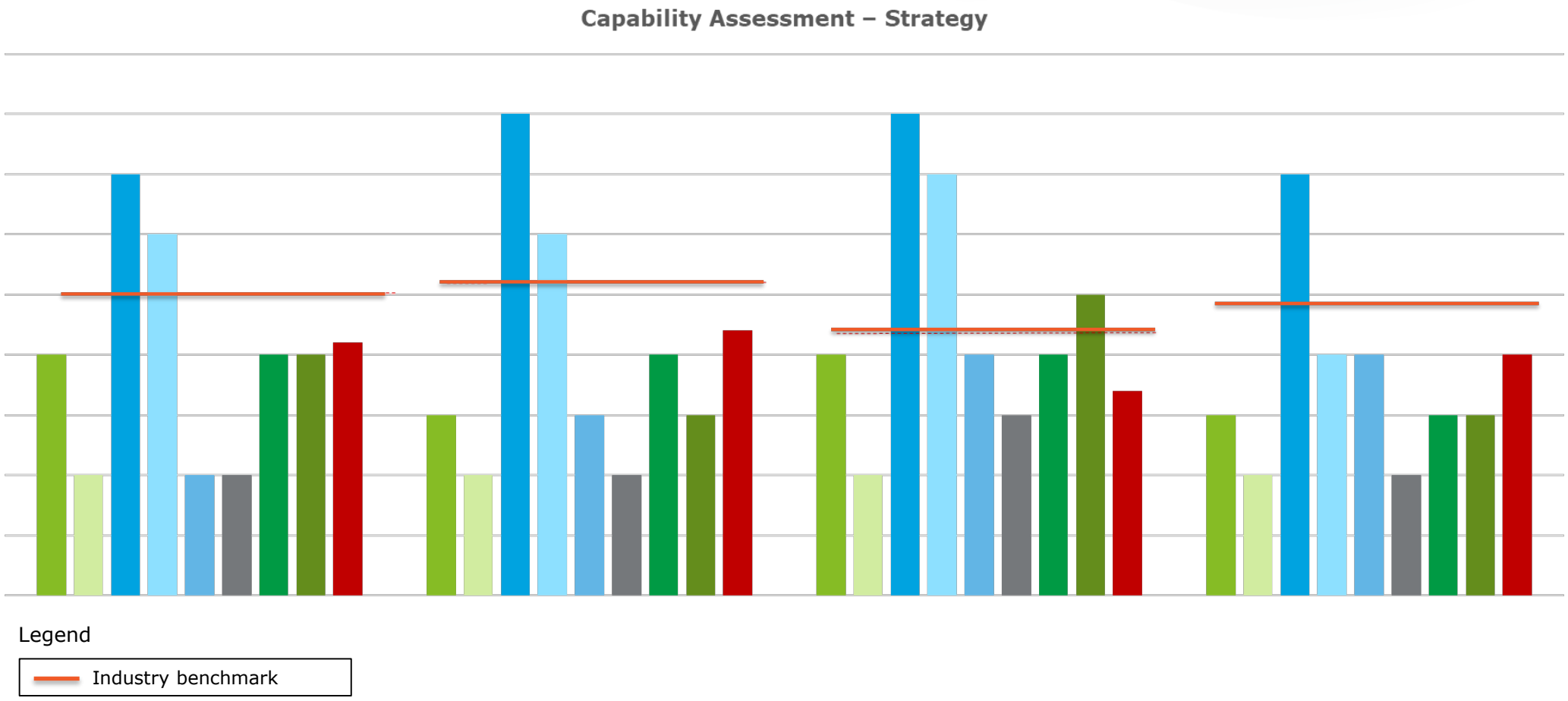
Highest Maturity



- Leveraging from Companies with High Maturity Score
- Deploying solutions and techniques with proven success factor
- Cost Reduction

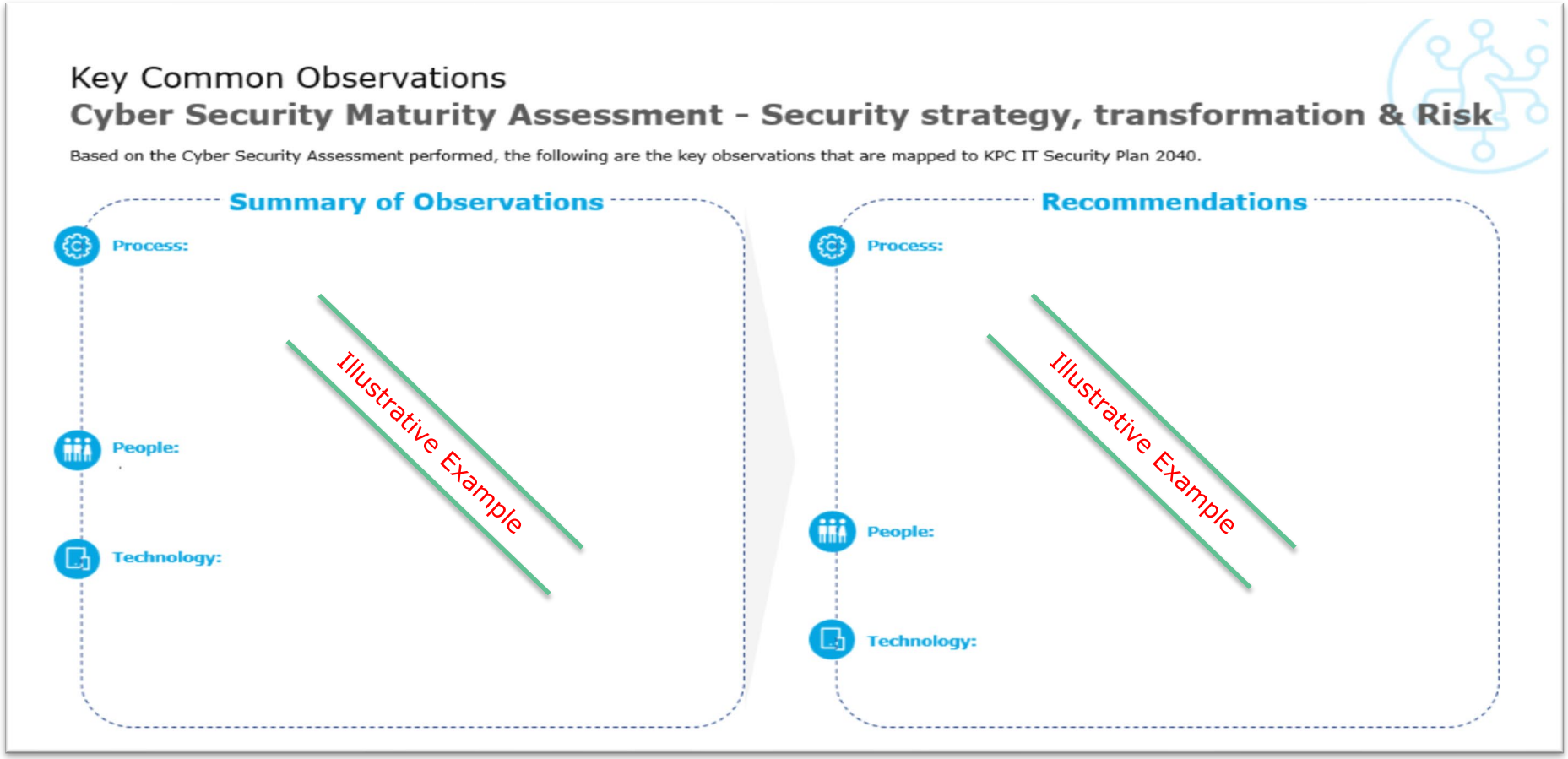
K-Cyber Security Maturity Assessment

Cyber Resilience Examples – Strategy Dashboards



K-Cyber Security Maturity Assessment

Common Observations & Recommendations



RSAConference2020

Alignment with National Cyber Security Strategy

Alignment with National CyberSecurity Strategy

K-Sector initiatives and cooperation to aling with National Strategical Objectives

1 Promote a culture of Cyber Security that supports safe and proper usage for the Cyber Space

Through K-Cyber Security collaboration, K-Sector Wide Cyber Security Awareness Campaigns has been established (Ex. Active sharing of awareness messages, Cyber Events and Forums, Cyber simulations exercises, online trainings,..etc).

2 Safeguard and continuously maintain the security of national assets, including critical infrastructure, national data, communication technologies and the Internet within the State of Kuwait

The O&G K-Sector contributes highly to the country's GDP and is considered as National Critical Infrastructure "NCI" that impacts the national economy. Through K-Cyber Security collaboration internally within the sector and nationally with other NCI entities, the K-sector is supporting raising the maturity, intelligence sharing & incident response to protect national interests.

3 Promote the cooperation, coordination and information exchange among local and international bodies in the field of cyber security

Regional Level : Collaboration of GCC O&G Sector Cyber Security Teams/Groups

National Level: Communication with CITRA & other NCI on Cyber Related Matters

RSAConference2020

The Way Forward – Information Security Roadmap

The Way Forward - Information Security Roadmap

5 Dimensions shaping the K-Companies Information Security Capabilities Roadmap

People

This will include support during recruitment of resources, knowledge transfer & training, and handover of services to new hires of the team.

Business strategy and alignment

The roadmap ensures the alignment of Information Security with K-Sector's business objectives through embedding Information Security culture within business processes

K-Cyber Security Framework

K-Cyber Security Framework integrates other 4 dimensions into the overall architecture

Processes

The end-to-end Information Security processes required to support and manage the Information Security function.

Technology

Roadmap identifies the technology initiatives required to support the achievement of target maturity of the Information Security capabilities

RSAConference2020

The Strategic Outcome

Strategic Outcomes

1

Define the minimum Baseline
Facilitates minimum baseline to be adopted by the whole sector to implement minimum information security controls to an acceptable CyberSecurity posture.

2

Sharing Knowledge & Best Practices
Facilitates understanding of the threat landscape in the sector leveraging from lessons learnt and promotes effective security practices.

3

Adopting a Common Strategy to Increase Maturity
Enabled the K-Sector to adopt a common unified strategy that provided clarity & focus to the K-Sector's information security Journey.

4

Incident Preparedness and Recovery
Bring synergies to different organizations which enable them to effectively share threat intelligence, respond and recover more efficiently from cyber security incidents as a collective response.

RSAConference2020

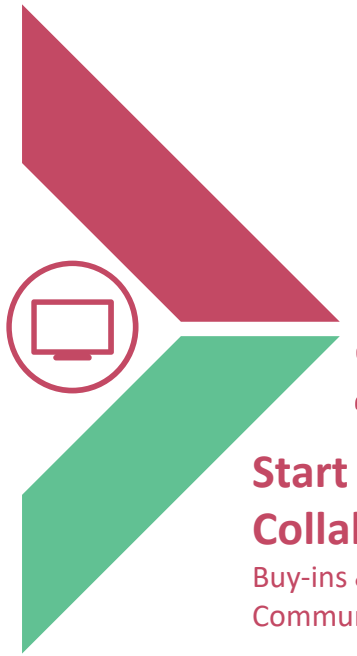
The Takeaways

Apply What You Have Learned Today

1

Define Minimum Baseline

Set a minimum baseline (in alignment with organization's strategic objectives).



2

Start Collaborating

Buy-ins & Communications.

3

Focus on Crowne Jewels

Prioritize always. Work on stages.

RSAConference2020

Thank You