

Improving Cyber Security Resilience Through Cyber Awareness

Kuwait Cyber Security Education and Research Conference

Mohammad H. Al-Sarraf

Team Leader Information Security (CISO)

www.kockw.com



إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Agenda

1 Why Cyber Security Culture is Important?

2 Examples of People Actions Leading to Cyber Security Incidents

3 Benefits of Enhancing Cyber Security Awareness

4 Methods to Improve Cyber Security Awareness

5 The Need of Awareness Program Measurement

6 Key Takeaways

Why Cyber Security Culture is Important?

www.kockw.com



إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Why Cyber Security Culture is Important?

Factors Integrated into Resilient Cyber Security Program

A resilient Cyber Security program that is secured against potential cyber security threats is centered on the intersection of people, processes and technology as shown below.

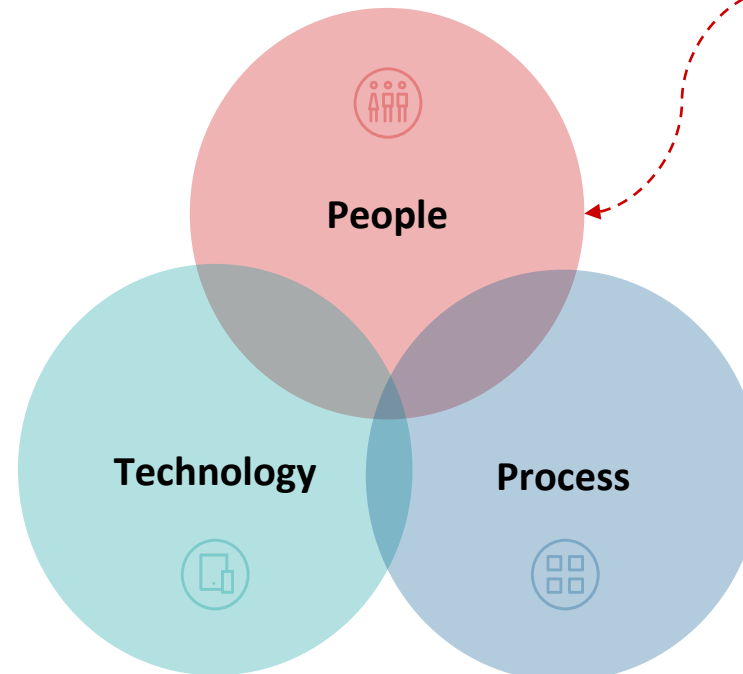
People

The “people” component of cyber security ensures that employees are adequately trained and informed about essential cyber security matters. Additionally, the “people” component is centered on ensuring that employees are supportive of the intended cyber security objectives.

Effective cyber security awareness efforts are important to ensure a resilient Cyber Security Program

Technology

The “technology” component of cyber security ensures that employees are equipped with the appropriate technologies and tools that are needed to fulfill the intended cyber security objectives.



Process

The “process” component of cyber security ensures that policies, procedures and processes are designed in a way that integrates the existing technologies

Why Cyber Security Culture is Important?

Business Impacts of a Cyber Security Culture

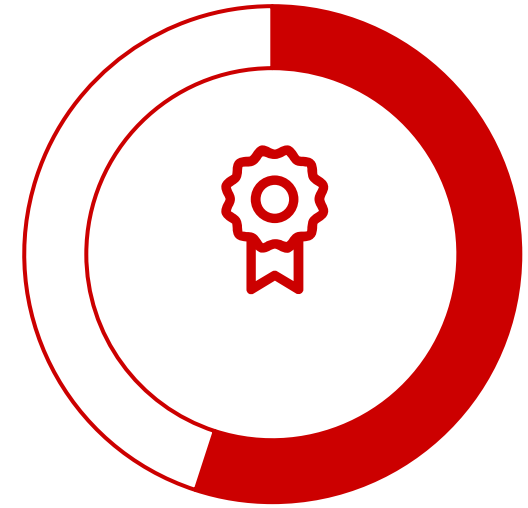
According to a ISACA cyber security culture study the top three benefits realized from successful cybersecurity culture include:



66% reduction in
cyber attacks



65% increase in
customer trust



55%
improvement in
brand image

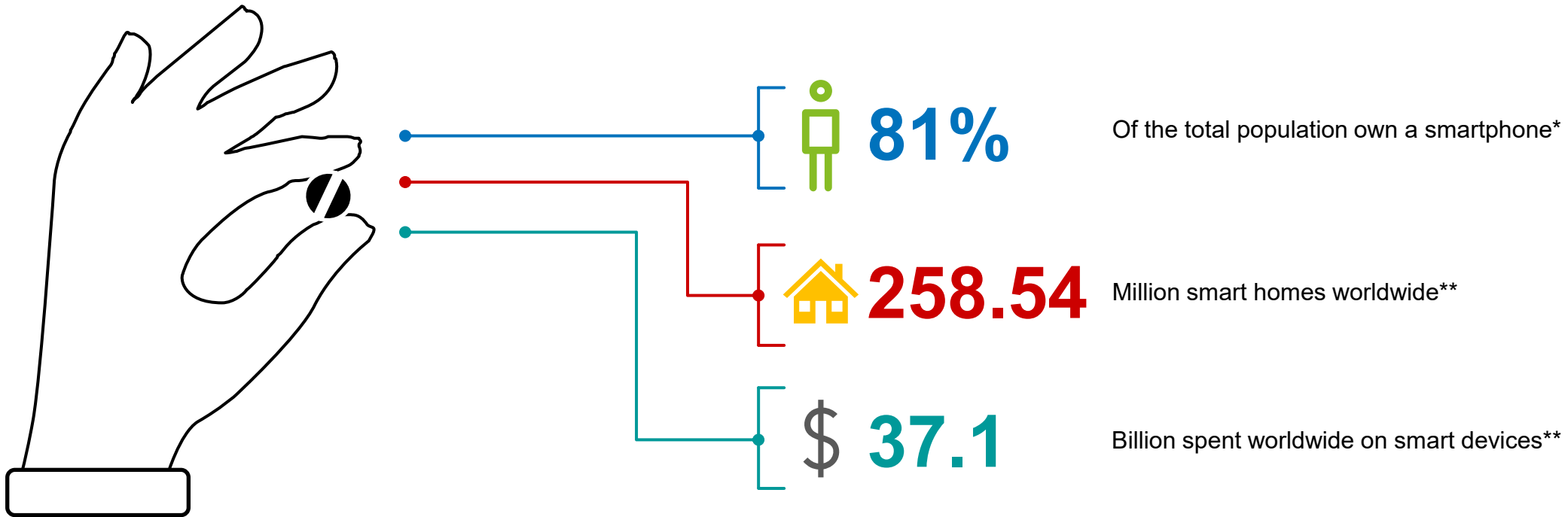
Source -

[THE BUSINESS IMPACTS OF A cyber security CULTURE](#)

Why Cyber Security Culture is Important?

The Increased Use of Smart Devices

People's acceptance and adoption of smart devices are steadily increasing.



Source -

*[HOW MANY SMARTPHONES ARE IN THE WORLD?](#)

**[Statista](#)

Why Cyber Security Culture is Important?

Cyber Security Threats in our Daily Lives

The increased use and adoption of smart devices also increases the Cyber Security Threats in our daily lives.



General cyber security Threats

General cyber security Threats

- Social engineering
- Privacy threats
- Exploitable vulnerabilities
- Loss/theft/damage of devices
- Hack/compromise of user accounts



Downloadable Threats

Downloadable cyber security Threats

- Spyware
- Malware
- Ransomware

Why Cyber Security Culture is Important?

Impact of Cyber Security Attacks on Organizations

Cyber Security attacks impose reputational, financial, operational and cultural impacts that an organization would need to endure.



Reputational

Loss of customer's trust and deterioration of brand image

Financial

Costs incurred as a result of fines, compensations and loss of business opportunities



Operational

Costs incurred as a result of the Disruption to business-critical operations

HSE / Environmental

Potential health consequences/injuries/Pollution

Examples of People Actions Leading to Cyber Security Incidents

www.kockw.com

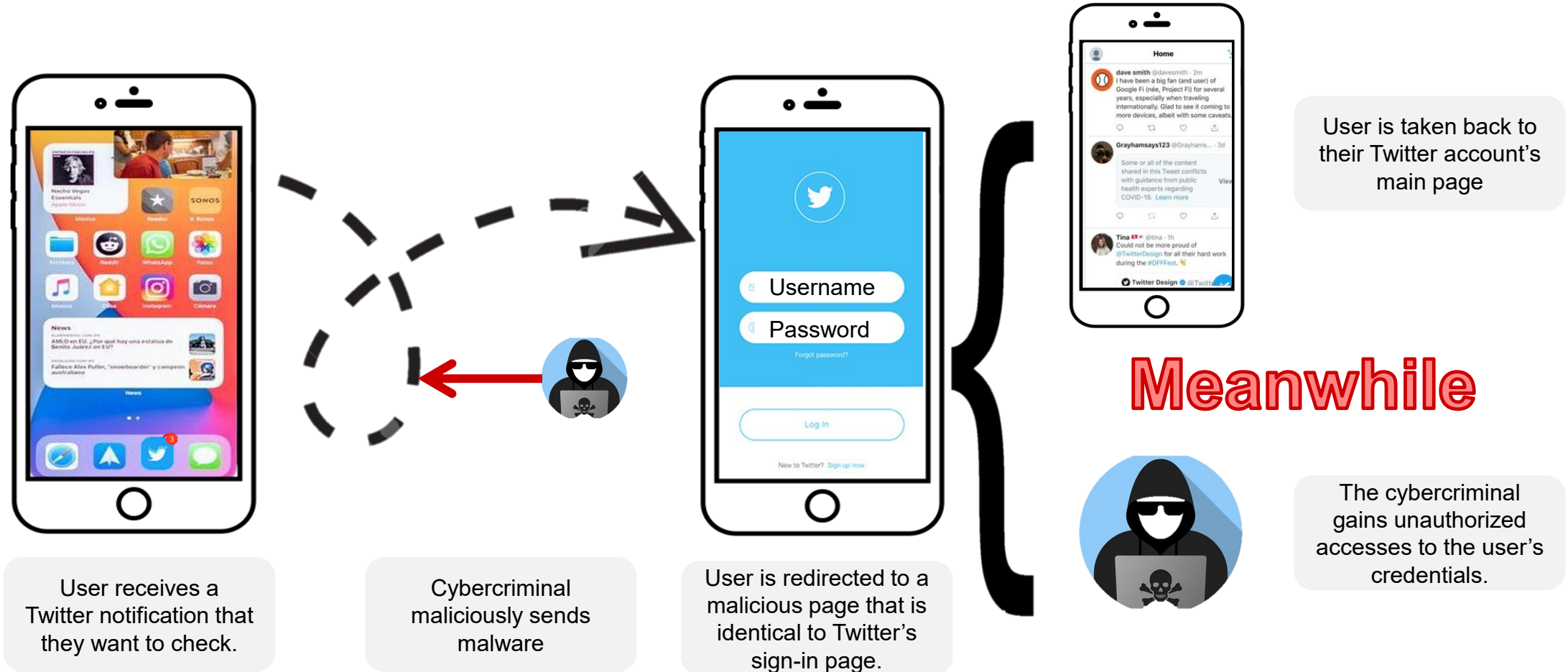


إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Examples of People Actions Leading to Cyber Security Incidents

Potential Cyber Security Incidents when using Technologies on a Daily Basis

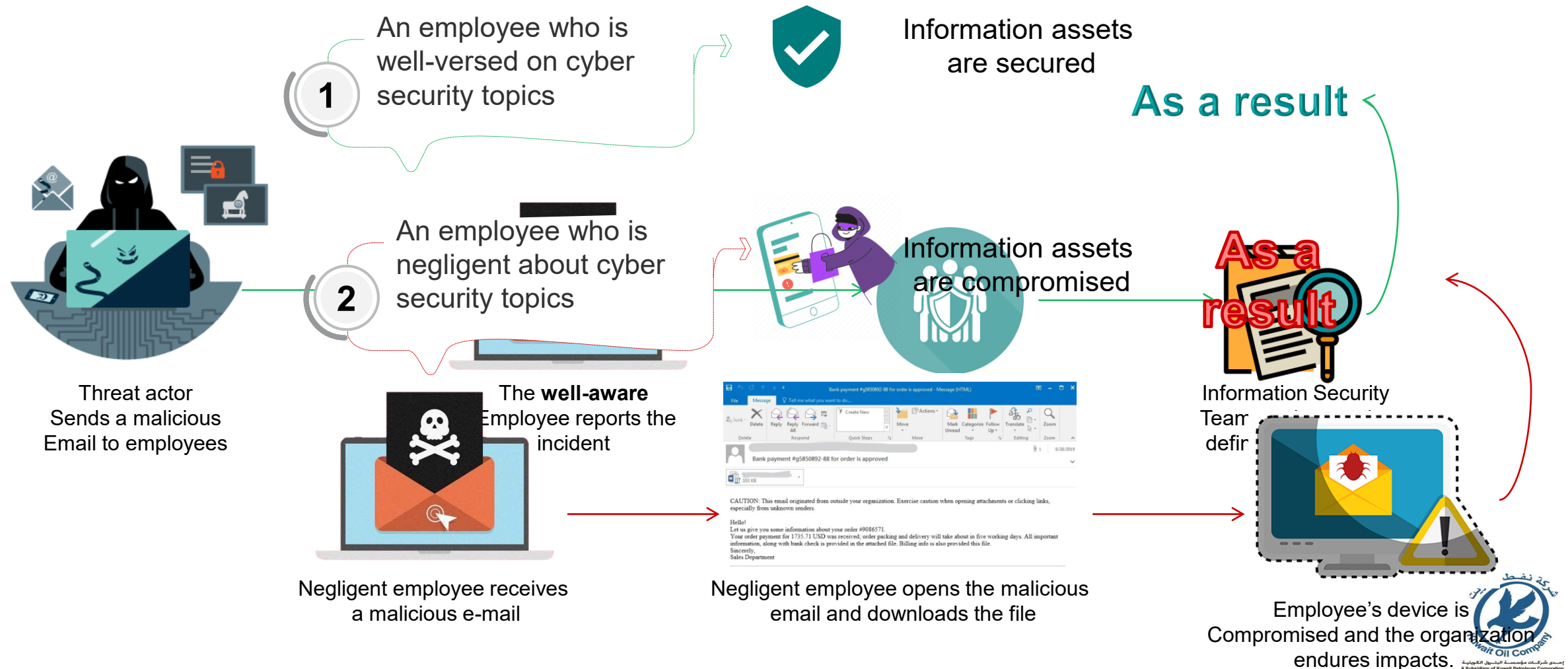
Cyber Security incidents could occur on any day without the user's knowledge as they are using their devices.



Examples of People Actions Leading to Cyber Security Incidents

Organizational Asset Usage

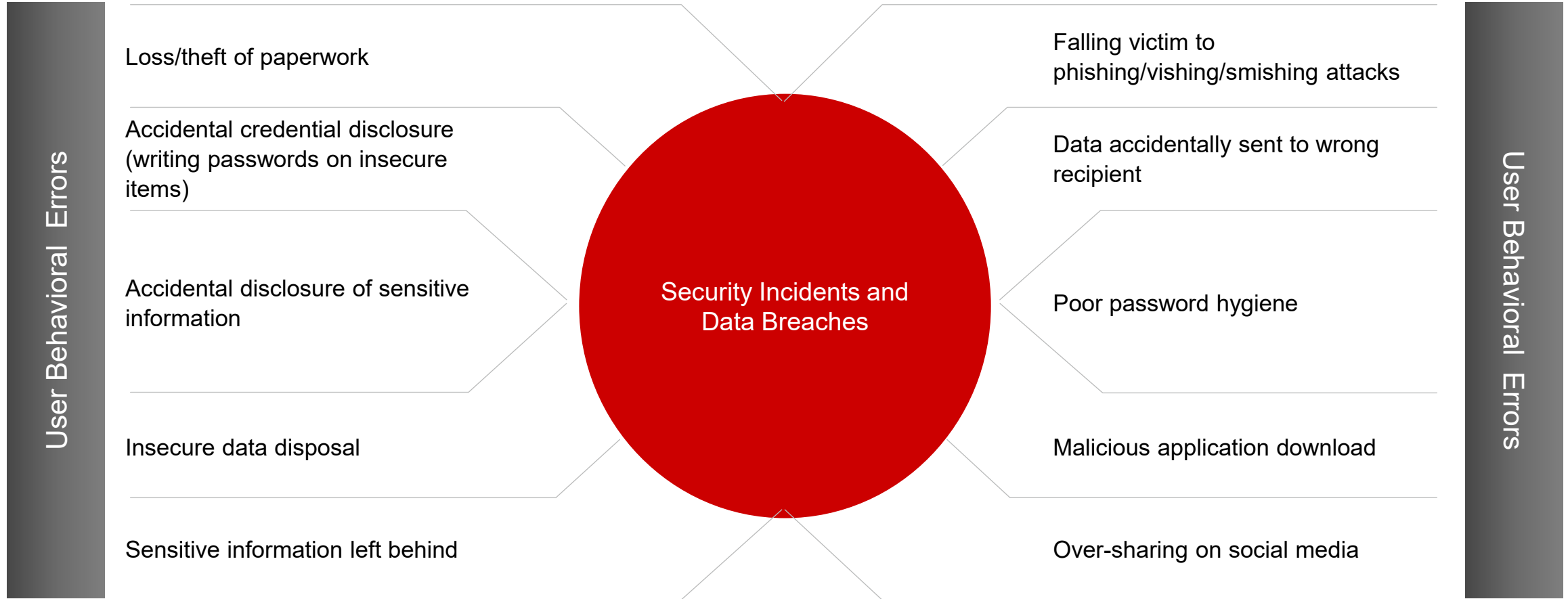
The security of an organization's assets are directly associated with employees' awareness of cyber security matters.



Examples of People Actions Leading to Cyber Security Incidents

Cyber Security as a Field that is Centered on Human Behavior

Users may unintentionally contribute to the success of a cyber security attack as a result of some of their behaviors.



Benefits of Enhancing Cyber Security Awareness

www.kockw.com

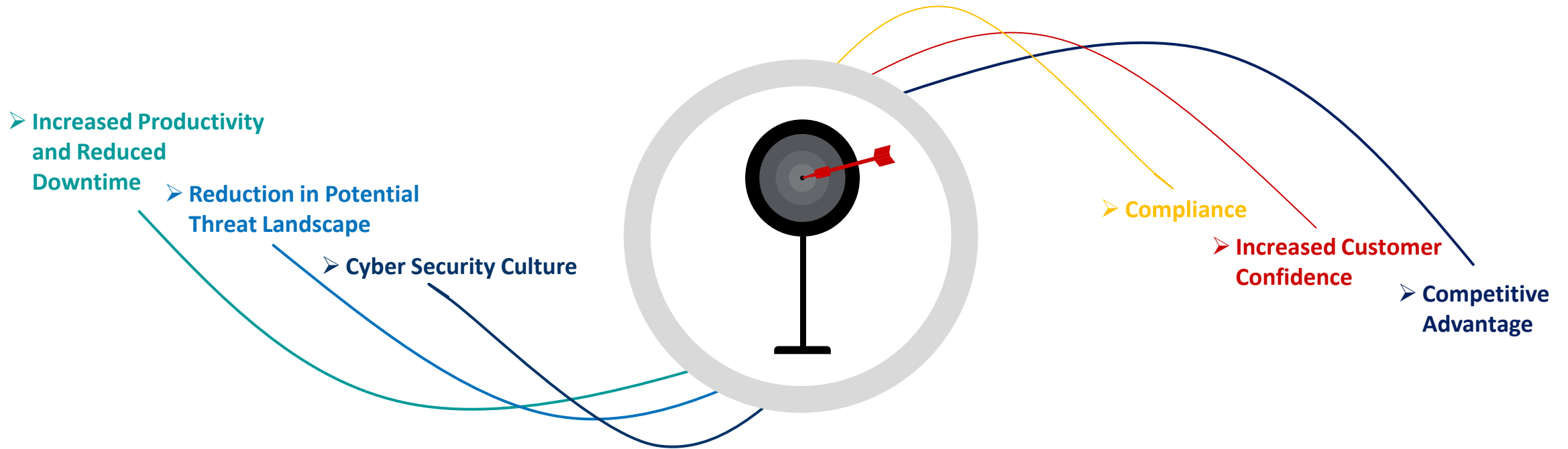


إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Benefits of Enhancing Cyber Security Awareness

Why should an Organization Focus on Enhancing Employee Awareness

Organizations would enjoy the following benefits once they ensure that their employees are adequately informed of cyber security topics.



Methods to Improve Cyber Security Awareness

www.kockw.com



إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Methods to Improve Cyber Security Awareness

The Goal of a Cyber Security Culture

There are multiple factors that are entailed into the establishment of an effective cyber security culture



Understanding/Comprehension

The ability to understand and comprehend cyber security concepts so that they could be shared with others.



Awareness/Knowledge

Employees can implement the key takeaways of the awareness sessions provided to them.



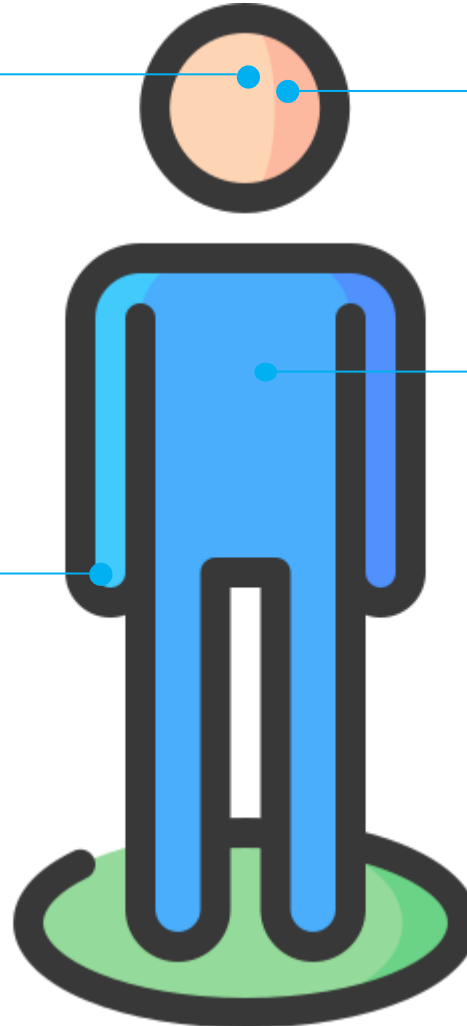
Actions

Employees behave in a way that does not expose themselves or their organization to cyber security threats.



Commitment

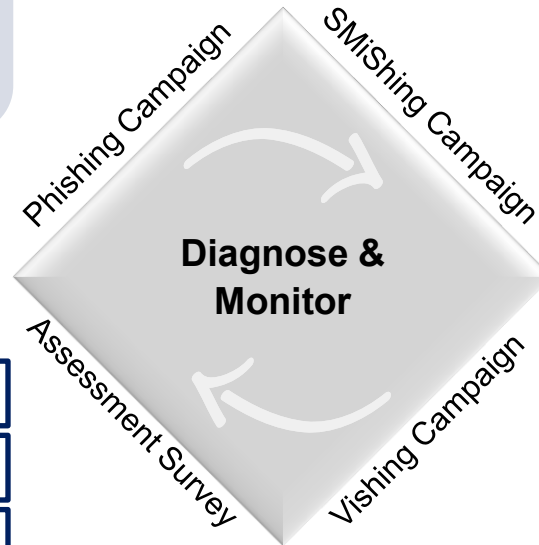
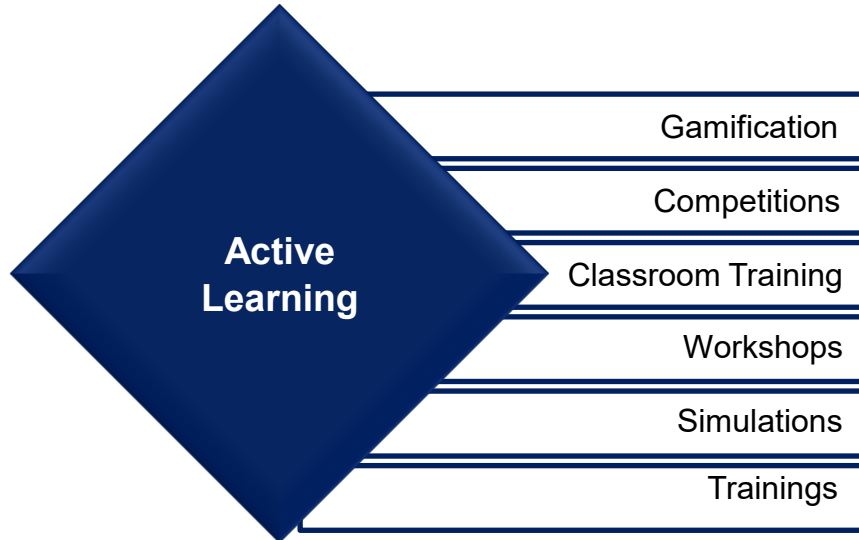
Employees value the importance of cyber security and support the organization in achieving its cyber security goals.



Methods to Improve Cyber Security Awareness

Classifying Methods used to Enhance Cyber Security Awareness

Focuses on engaging the employees to ensure that they are learning the required skills



Focuses on delivering the information to the employees and expects them to internalize it.

Methods to Improve Cyber Security Awareness

Traditional Awareness Methods – Passive Learning

Awareness Messages

- Postmasters
- Screen Savers
- Portal Banners
- SMS/WhatsApp/E-mail Messages
- Guidelines

GCC O&G Cyber Awareness Campaign

September
October
November

احذر من فيروس الفدية
Beware of Ransomware Threat

1 DO NOT click links or download attachments in suspicious emails.

Information Security Postmaster

توعية أمن المعلومات: حماية المعلومات السرية لشركة نفط الكويت

شركة نفط الكويت
أخبار أمن المعلومات

تقاس مدى قوة أمن المعلومات بقدر قوة أضعف
كن أنت الحلقة الأضعف!

حماية المعلومات السرية لشركة نفط الكويت
أنا ملتزم بحماية
أبرز سياسات أمن المعلومات في شركة نفط الكويت

Beware!!
of falling into the trap of Cyber Criminals who are utilizing Global fears from the Global Pandemic "Corona Virus" to steal your critical information.

Coronavirus-based Malware & Phishing Lures

Cyber Criminals are using coronavirus-based Cyber attack campaigns and phishing traps.

Where it infects victims with malware to steal their Critical information & Credentials.

Malware may steal browsing history, ID/passwords and may allow remote access to infected devices.

Data Protection

Useful tips to be Cyber Safe...

- Beware** of COVID-19 related malicious attachment or hyperlink.
- Use only trusted sources** for information about COVID-19 such as moh.gov.kw/ ; corona.e.gov.kw/; who.int/.
- Do not** respond to emails with your **personal** or **financial** information.
- Be Cautious** when **downloading** and **running** files from the Internet.

المكان

٢ لا ننسى تسجيل الخروج
احرص على تسجيل الخروج من الخوادم والواقع والشبكات والنظم (بما في ذلك البريد الإلكتروني) عند الانتهاء

بعد مرور عدة أيام...

استخدام كلمات مرور سهلة التخمين تسهل الوصول إلى أنظمتك و

KOC Information Security Team
Corporate Information Technology Group

K Cyber Security Committee

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

Methods to Improve Cyber Security Awareness

Traditional Awareness Methods – Active Learning

Awareness Activities

- Trainings Sessions
- Events & Forums
- Behavioral Activities
(Phishing/Vishing/Smishing/
Walkthrough Exercises)

Learning (e-learning/classrooms) topics that could be covered to

#	Scenario	Vishing Activity Script
1	Technical Conference	<p>Cyber Criminal: Hello this is Khaled from HR, am I speaking to Abc?</p> <p>Victim: Yes this is Abc speaking</p> <p>Cyber Criminal: As you might have heard, the 27th technical conference of the gas processes association GCC chapter is going to be held on the 12th -14th of August 2020 in Al Jumerah Hotel.</p> <p>Victim: Yes I've heard about it.</p> <p>Cyber Criminal: KOC employees will be receiving 60% discount during those days. We wanted to see if you would like for us to book you a room in the hotel during the conference duration.</p> <p>Victim: Yes of course.</p> <p>Cyber Criminal: Okay great, can you please send me a copy of your passport and working ID on this email: Khaledabck@gmail.com</p> <p>Victim: yes sure</p> <p>Cyber Criminal: Okay one second let me check.</p> <p>*Checks to see if the email is sent*</p>


Methods to Improve Cyber Security Awareness

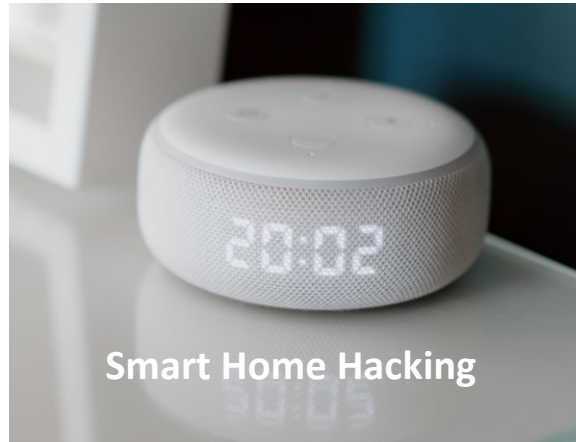
The Modern Approach to Cyber Security Awareness

Modern approaches to cyber security awareness focus on active learning.




Virtual Reality

 A Virtual Reality (VR) experience where participants find themselves in an 360° virtual office and must identify potential security breaches which are located around the office and try to prevent incidents from occurring.




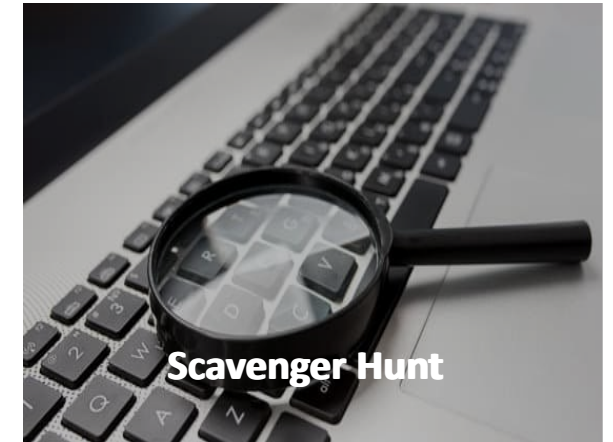
Smart Home Hacking

 A live demonstration where participants will realize the extent to which home devices are vulnerable, and how these vulnerabilities can be exploited. The activity demonstrates household IoT devices being hacked.




Cyber Escape Room

 Each team will attempt to escape the room by solving challenges. The players will have to prevent a cybersecurity attack from occurring by determining all the mistakes made by an employee.



Scavenger Hunt

 Participants find hidden clues and read awareness messages along the way. When missions are completed, they gain points and can view their scores in comparison to others based on the public score board.

The Need of Awareness Program Measurement

www.kockw.com



إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

The Need of Awareness Program Measurement

Why is Measurement Important?

Effective measurement is important for ensuring effectiveness of Cyber Security Program

The Ultimate Goal : A Resilient Cyber Security Posture

Establishes a baseline for current cyber security posture.

Allows the identification of existing gaps in the organization's cyber security topics.

Enables organizations to develop personalized and tailored awareness plans.

Quantifies progress and enables organizations to improve their cyber security awareness program.

Benefits of Measurement

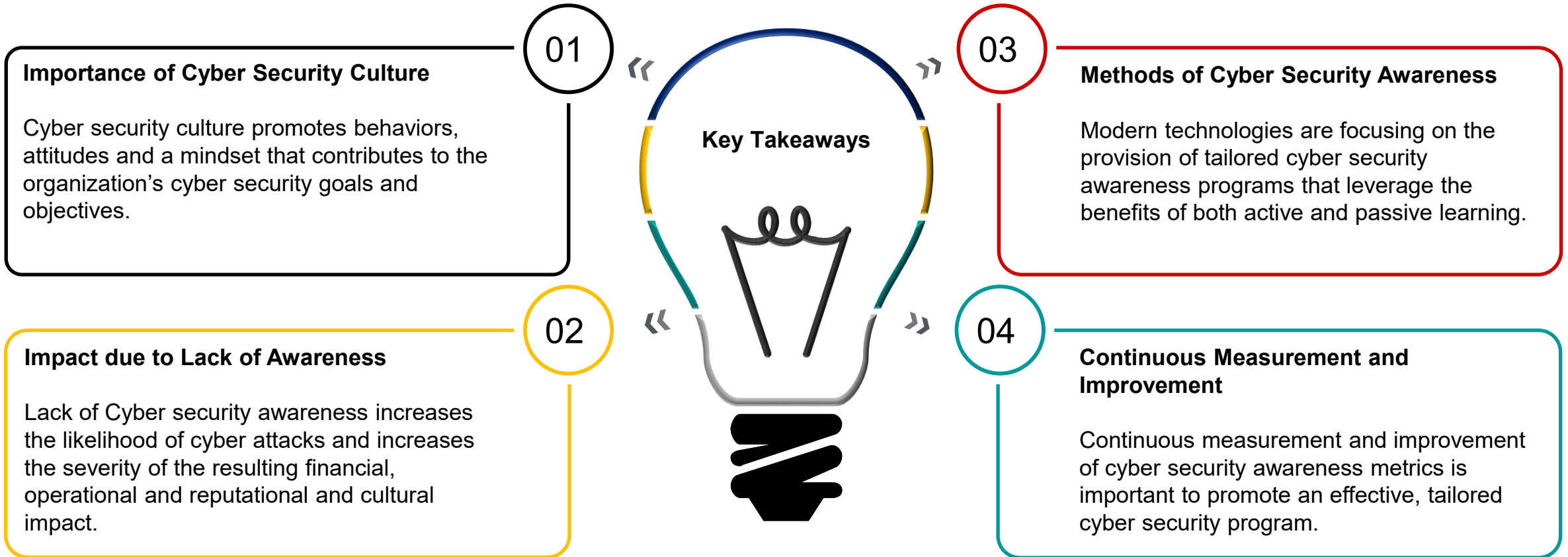
Key Takeaways

www.kockw.com



إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation

Key Takeaways



Thank You

www.kockw.com



إحدى شركات مؤسسة البترول الكويتية
A Subsidiary of Kuwait Petroleum Corporation