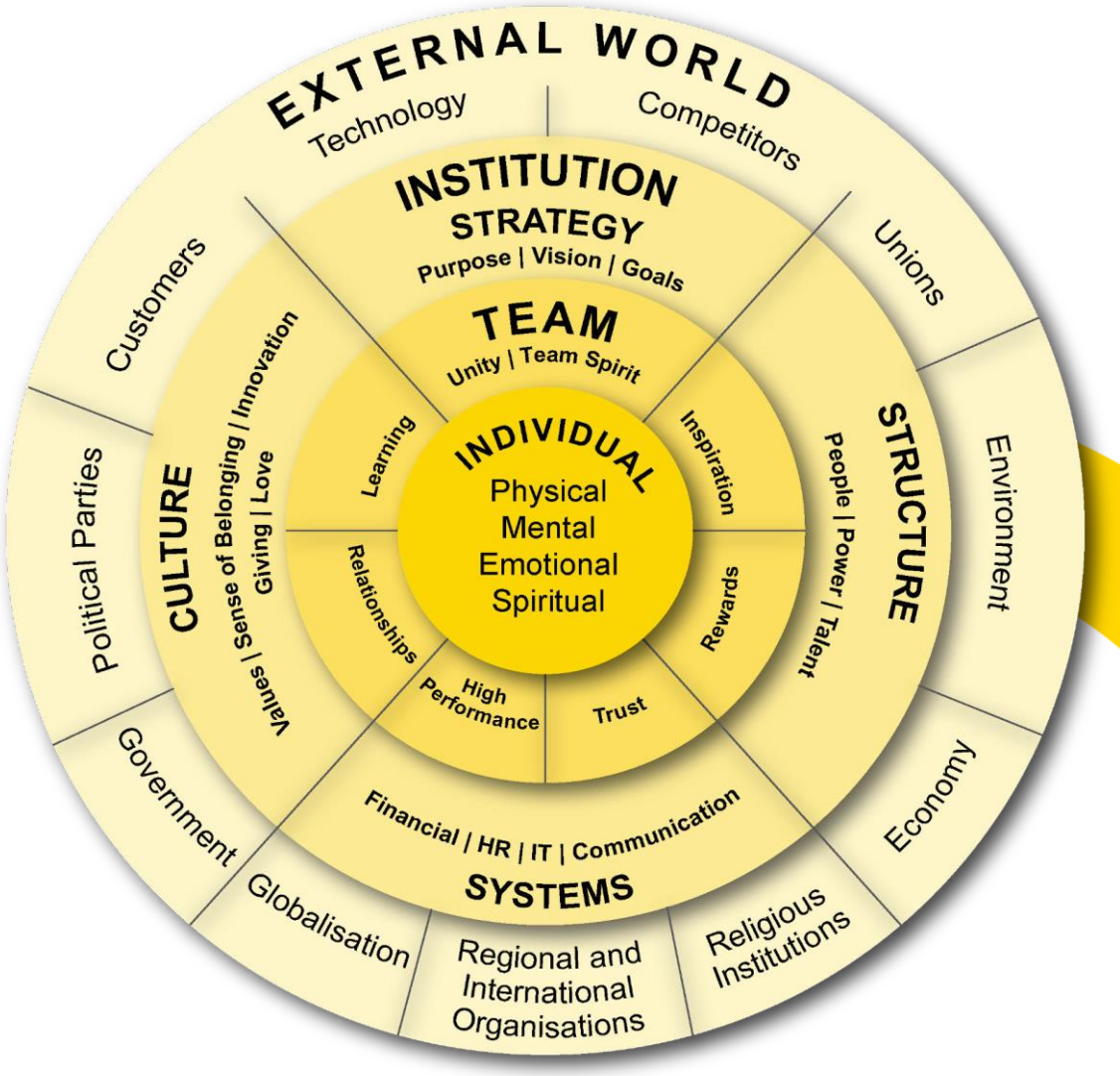
CYBER SECURITY FUNDAMENTALS

DATE: 28.02.2025 & 01.03.2025

DIGITAL REGENESYS
Awakening Potential

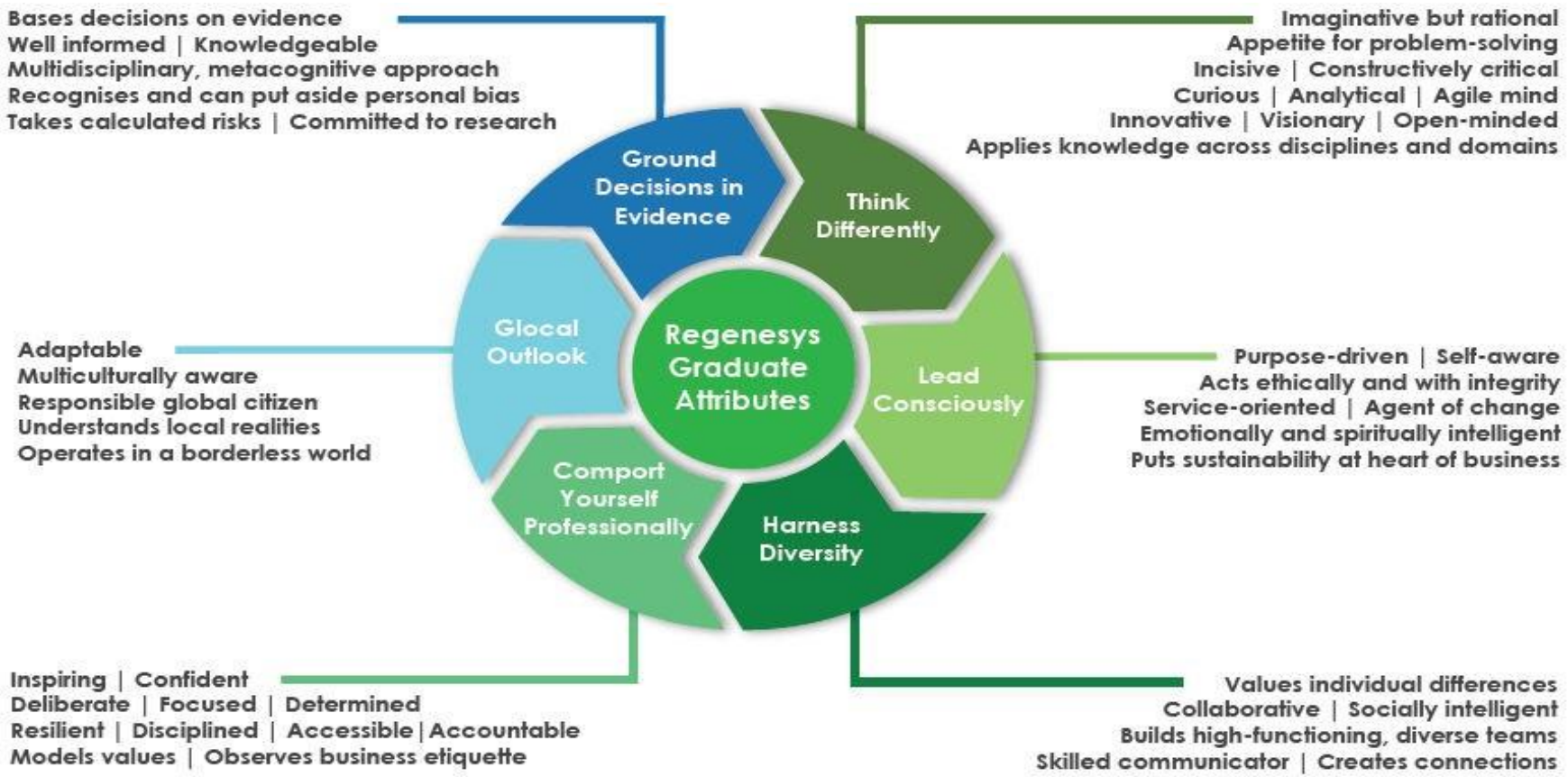
REGENESYS' INTEGRATED LEADERSHIP AND MANAGEMENT MODEL:

- **Holistic** focus on the individual (SQ, EQ, IQ, and PQ)
- **Interrelationships** are dynamic between individual, team, institution and the external environment (systemic)
- **Strategy** affects individual, team, organisational, and environmental performance
- **Delivery** requires alignment of strategy, structure, systems and culture



DIGITAL REGENESYS
Awakening Potential

REGENESYS GRADUATE ATTRIBUTES:



DIGITAL REGENESYS
Awakening Potential

KNOW YOUR FACILITATOR:

Dr. Saquib Ahmad Khan

- Dr. Saquib Ahmad Khan is a highly respected professional in the cybersecurity field.
- He holds a Ph.D. in Computer Science and possesses multiple cybersecurity certifications, establishing him as an esteemed expert in cybersecurity.
- Dr. Khan is a prolific author, with numerous research papers and articles to his credit, focused on advancing the field of cybersecurity.
- He is a frequent speaker at prominent industry conferences and events, where he imparts his knowledge and insights to fellow professionals.
- Dr. Khan also possesses a strong foundation in marketing, management, information technology, and various applications, bolstered by multiple degrees.

DIGITAL REGENESYS
Awakening Potential

GROUND RULES:

- Be open-minded
- When speaking, use “I think”, “I feel”, etc.
- (you are a very important aspect of this learning)
- Listen carefully
- One conversation at a time
- Respect the opinions of others
  - Give constructive feedback
  - Build on the ideas of others rather than destroying them
- Take some risks and share new ideas

HAVE FUN AND ENJOY THE EXPERIENCE !

DIGITAL REGENESYS
Awakening Potential

MODULE 04

DIGITAL REGENESYS
Awakening Potential

Cybersecurity Fundamentals: Protecting Digital Assets and Ensuring Business Continuity

- Developing an Incident Management and Response System
- Digital Forensics Business
- Continuity and Disaster Recovery
- Wi-fi Network Security
- Web Security

On completing this module, you should be able to:

- Learners will acquire a comprehensive understanding of incident response phases and their interconnections, contributing to effective incident handling and response planning.
- Learners will develop the skills to create, implement, and tailor incident response plans to real-world scenarios and organizational needs, considering roles, responsibilities, communication, and resource allocation.
- Learners will gain the ability to form, structure, and coordinate incident management teams, ensuring well-orchestrated responses through defined roles, responsibilities, and collaboration.
- Learners will gain foundational knowledge in digital forensics, covering core elements, ethical considerations, and maintaining digital evidence integrity.
- Learners will become proficient in digital forensics processes, including evidence collection, preservation, analysis, and reporting.
- Learners will understand the different disciplines within digital forensics and acquire specialized skills in their chosen area, such as computer or mobile device forensics.

On completing this module, you should be able to:

- Learners will learn the role of digital forensics in legal investigations and court proceedings, ensuring evidence validity and protection of rights.
- Learners will gain skills in assessing risks and impacts for effective business continuity and disaster recovery, aligning these plans with organizational strategic objectives.
- Learners will become aware of the vulnerabilities and threats associated with Wi-Fi networks, enabling them to identify potential security risks and understand the strengths and weaknesses of various Wi-Fi security protocols.
- Learners will learn best practices for securing Wi-Fi networks, ensuring the confidentiality, integrity, and availability of data, and selecting the most suitable security measures for specific network requirements.

PHASES OF AN INCIDENT RESPONSE PLAN:

- Phase 1: Prepare
- Phase 2: Identify
- Phase 3: Contain
- Phase 4: Eradicate
- Phase 5: Recover
- Phase 6: Review

DIGITAL REGENESYS
Awakening Potential

TIPS TO BUILD A CYBER INCIDENT RESPONSE PLAN:

STEP 1: ESTABLISH AN IR TEAM

STEP 2: CONDUCT THREAT ANALYSIS

STEP 3: OUTLINE QUICK RESPONSE GUIDELINES

STEP 4: DEVELOP PROCEDURES FOR EXTERNAL COMMUNICATION

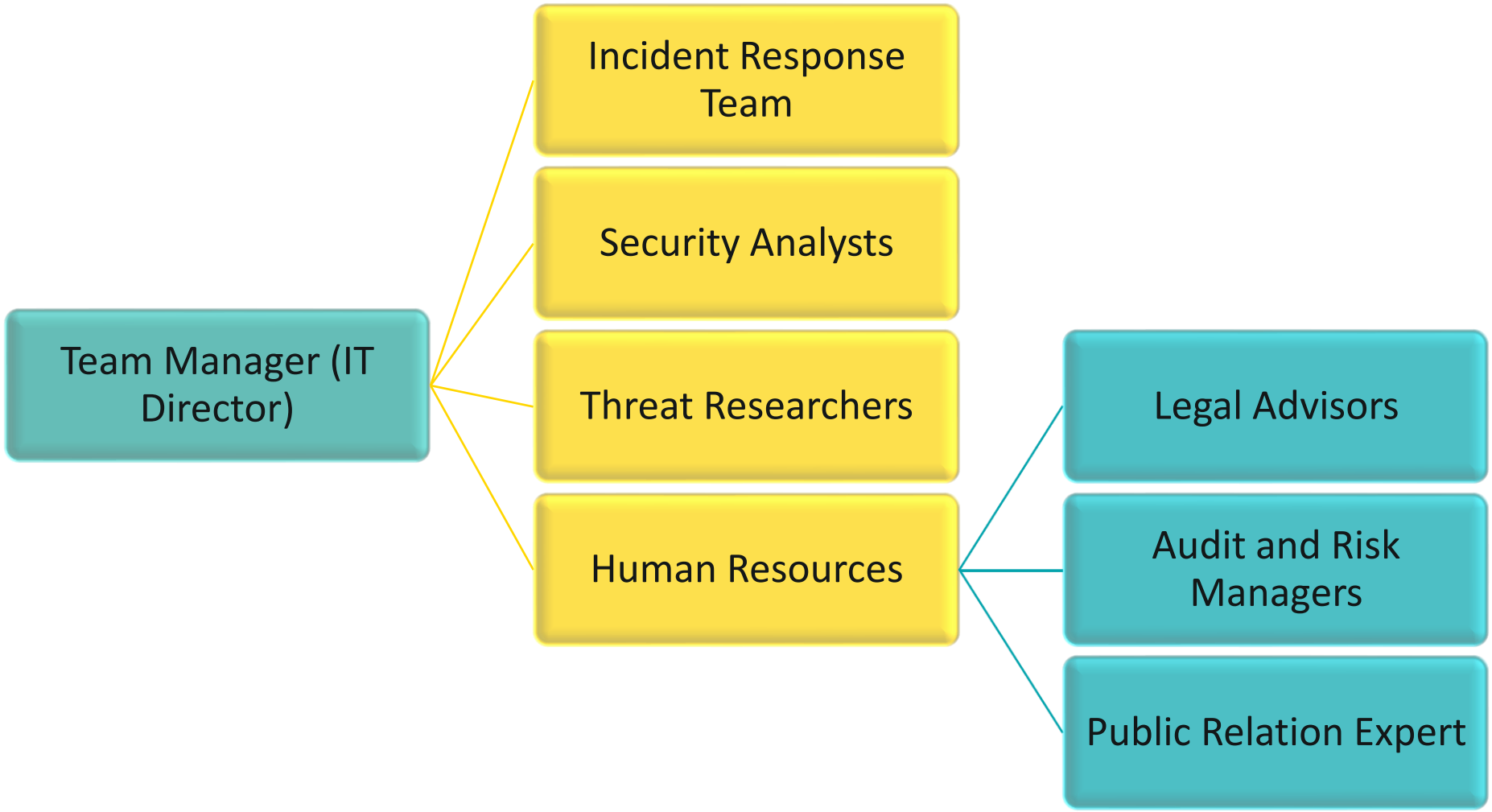
STEP 5: TRAIN EMPLOYEES

STEP 6: TEST IR PLAN

STEP 7: LEARN

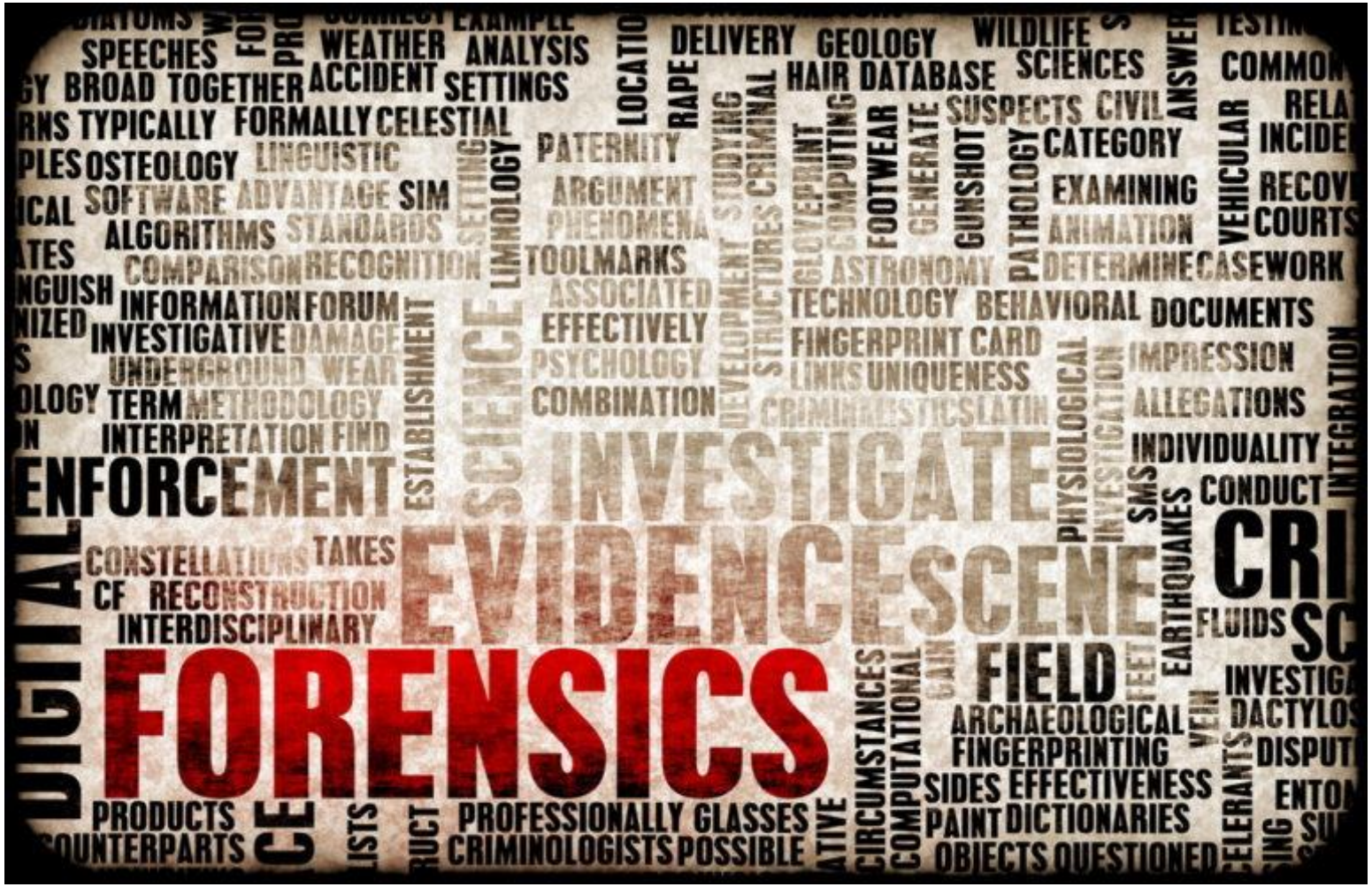
DIGITAL REGENESYS
Awakening Potential

INCIDENT MANAGEMENT PLAN TEAM:



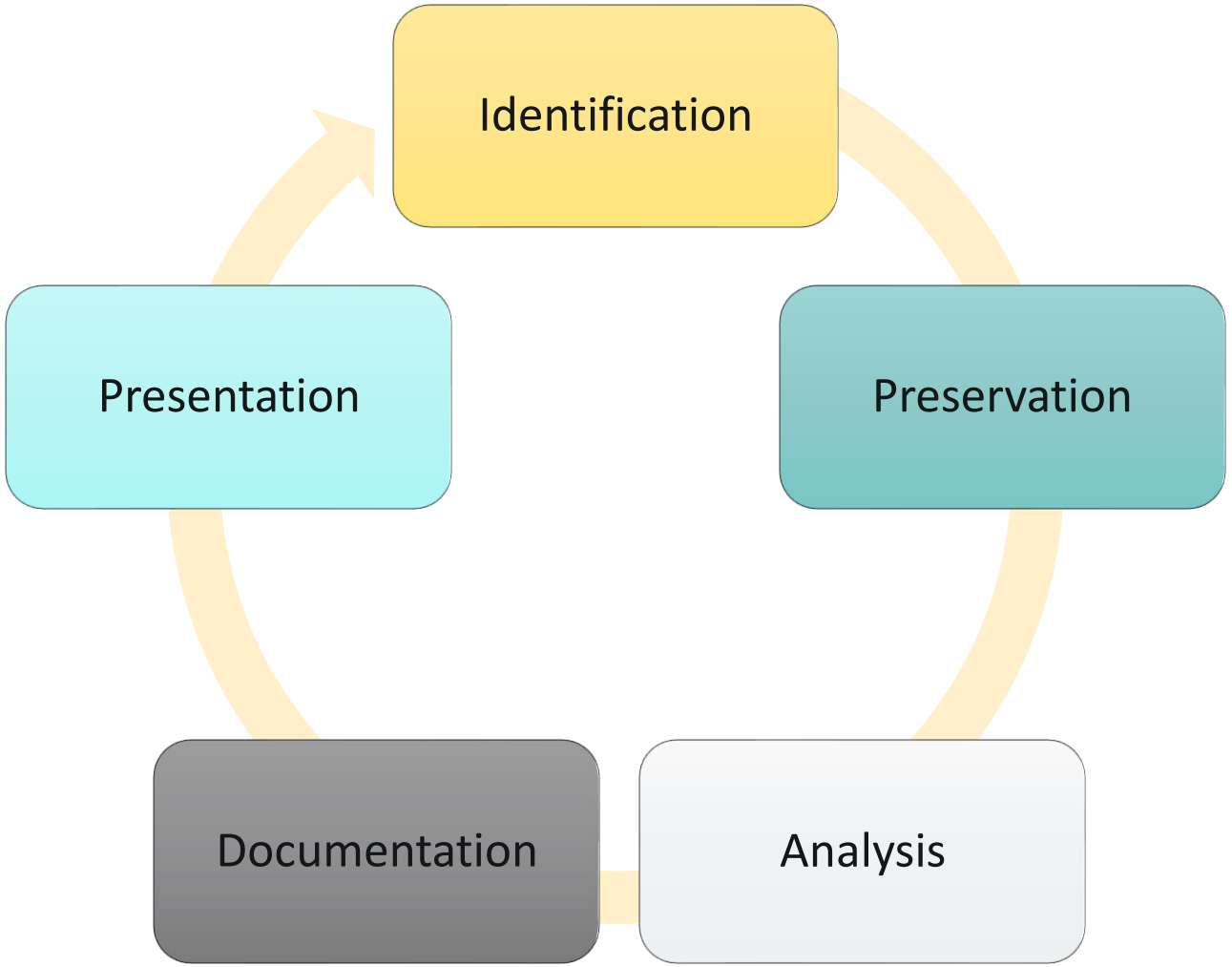
DIGITAL REGENESYS
Awakening Potential

DIGITAL FORENSICS:



DIGITAL REGENESYS
Awakening Potential

DIGITAL FORENSICS PROCESS:



DIGITAL REGENESYS
Awakening Potential

TYPES OF DIGITAL FORENSICS:

- Disk Forensics
- Network Forensics
- Wireless Forensics
- Database Forensics
- Malware Forensics
- Email Forensics
- Memory and Mobile Forensics

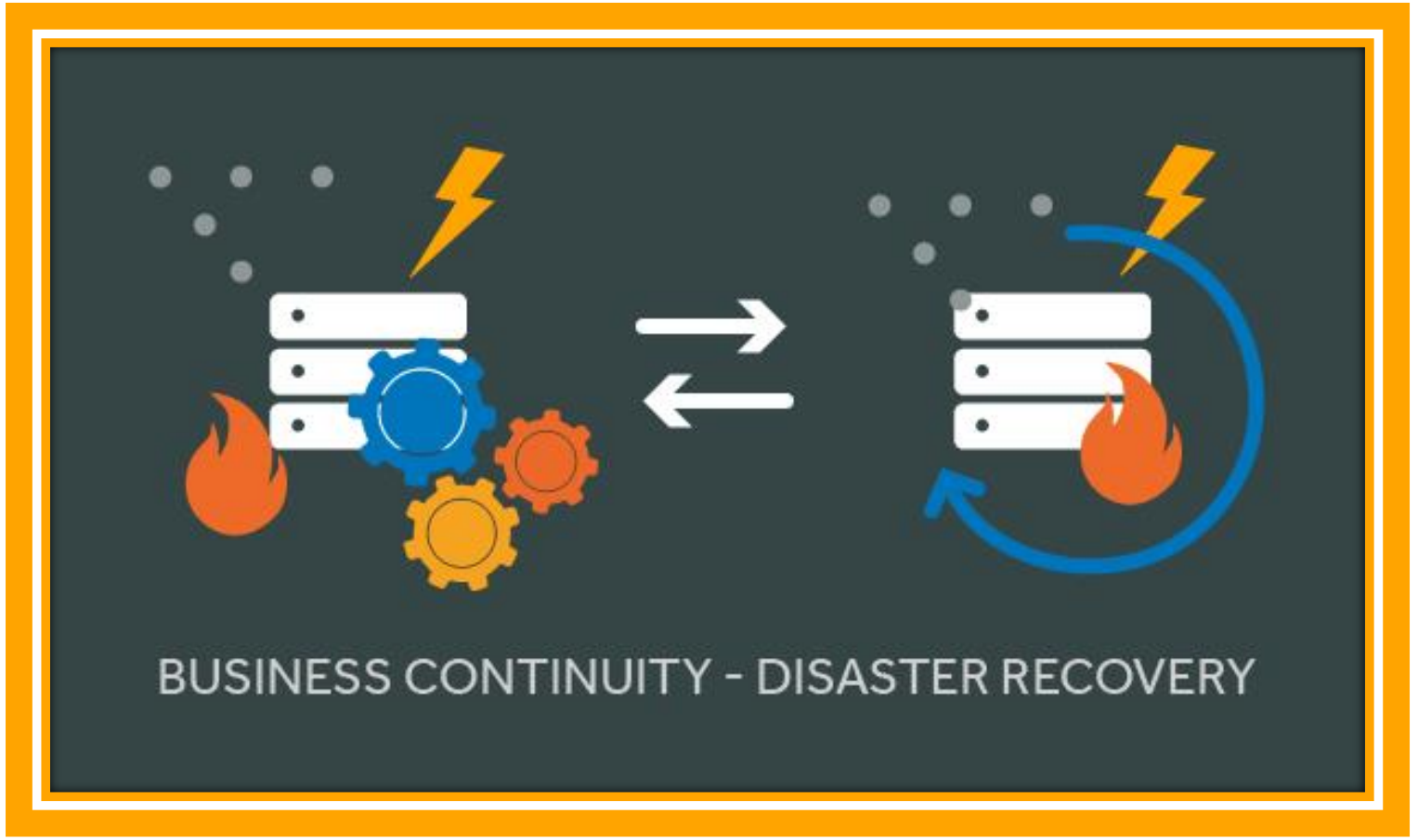
DIGITAL REGENESYS
Awakening Potential

THE QUESTION IS….

Why is
Digital Forensics
Important ?

DIGITAL REGENESYS
Awakening Potential

CONTINUITY AND DISASTER RECOVERY:



(Source: Tech, K. (2022, September 9). *What is the difference between Disaster Recovery Plan & Business Continuity Plan?* King Tech Repair. https://www.kingtechrepair.com/blog/what-is-the-difference-between-disaster-recovery-plan-business-continuity-plan/)

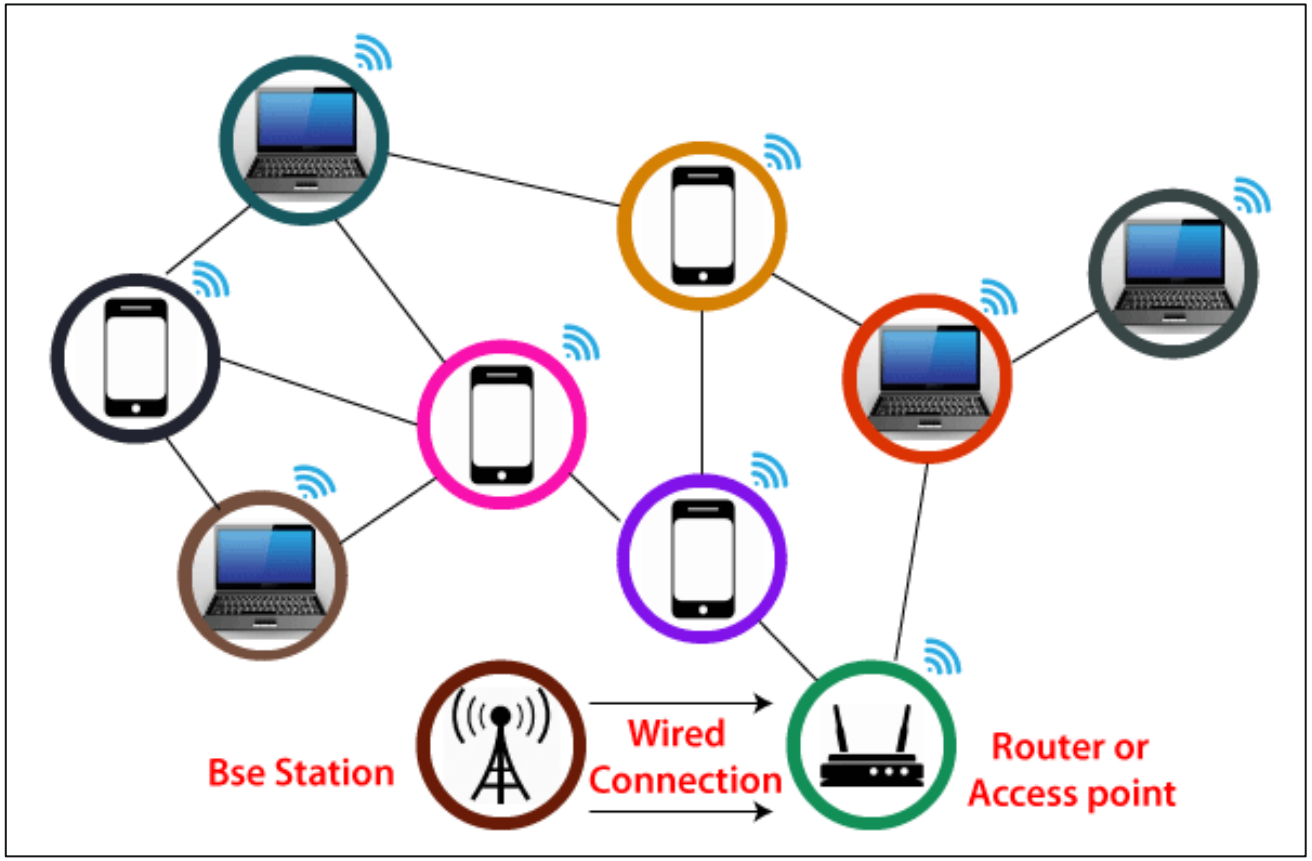
DIGITAL REGENESYS
Awakening Potential

GOALS OF BCDR:

- Assess the state of business
- Find weaknesses and provide solutions
- Review and test the plan
- Identify location for data storage
- Know the disaster recovery teams

DIGITAL REGENESYS
Awakening Potential

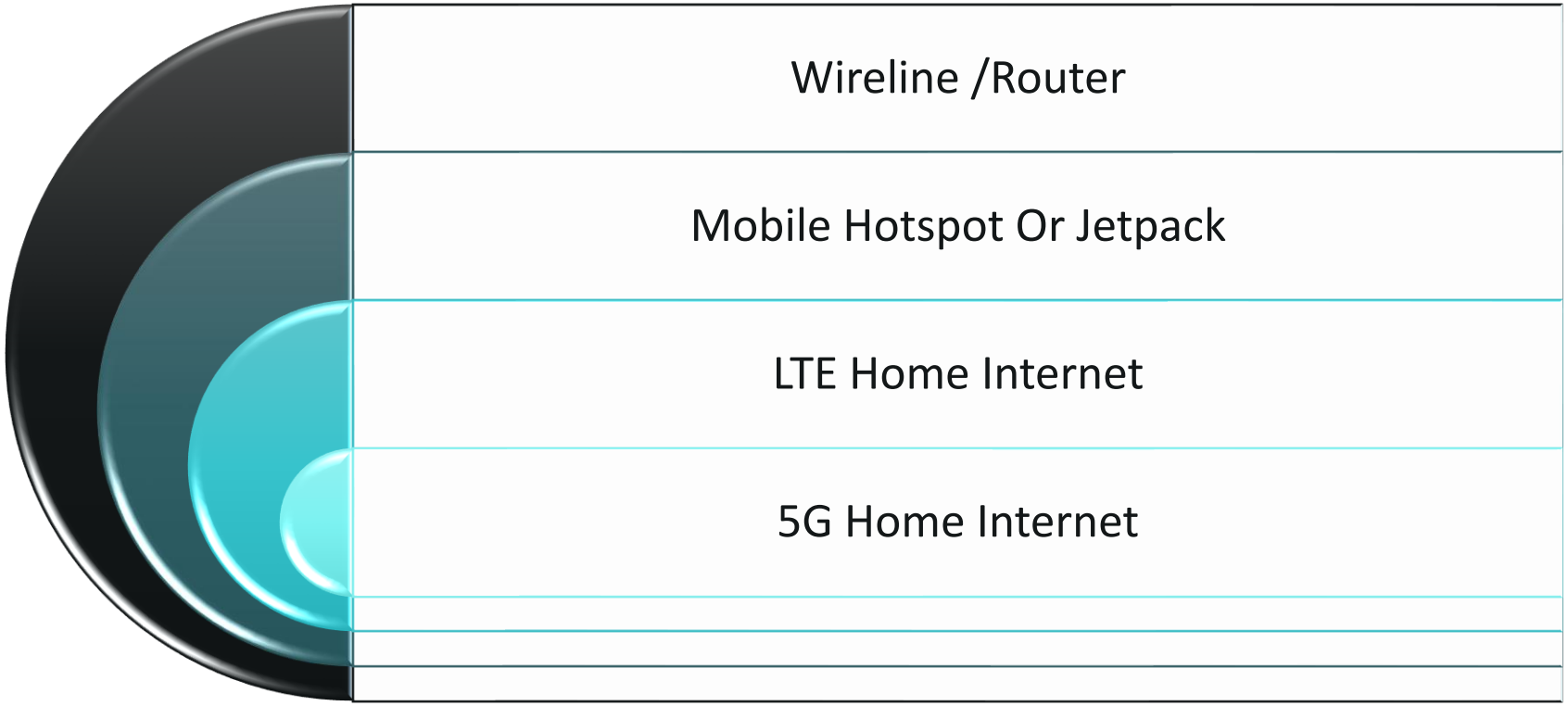
WI-FI NETWORK SECURITY:



(Source: *WIFI - Wireless Fidelity - Javatpoint*. (n.d.). Www.javatpoint.com. https://www.javatpoint.com/wifi-wireless-fidelity)

DIGITAL REGENESYS
Awakening Potential

TYPES OF WI-FI NETWORK SECURITY:



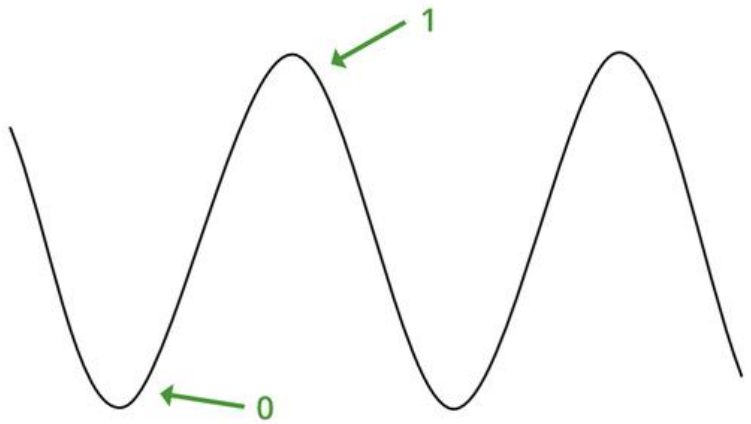
DIGITAL REGENESYS
Awakening Potential

THE QUESTION IS….

HOW TO GET

WI-FI

AT HOME ?



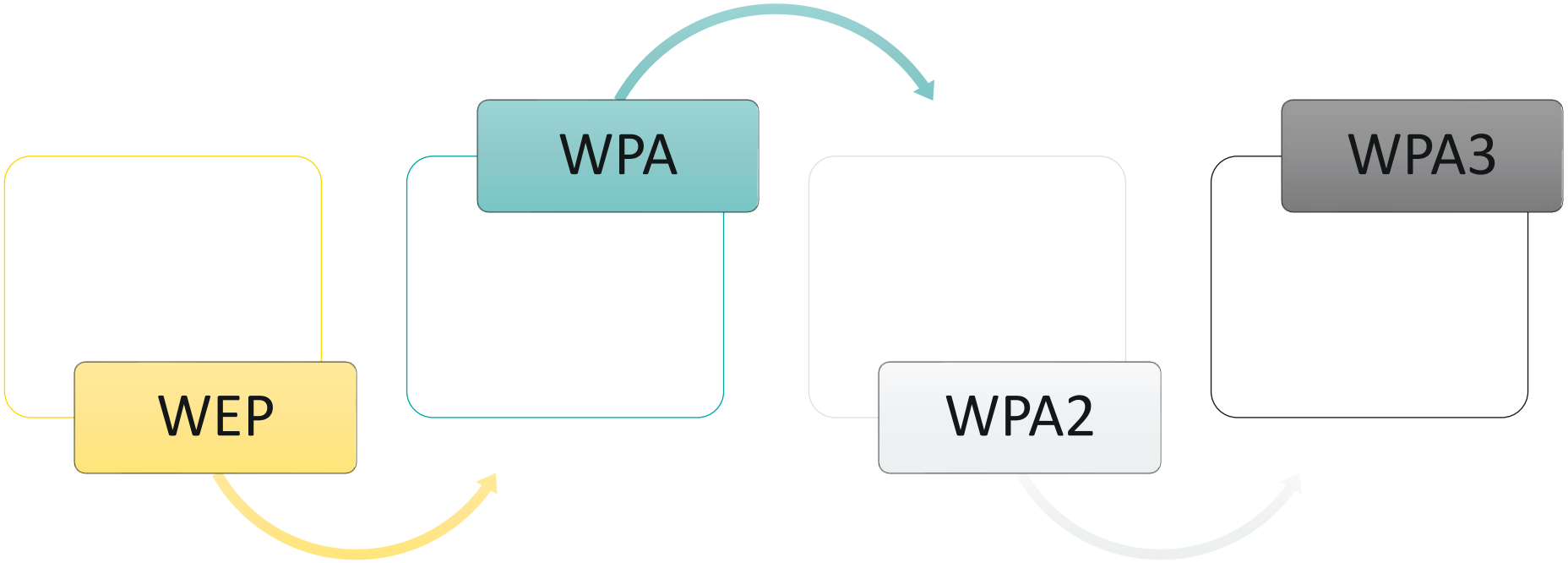
DIGITAL REGENESYS
Awakening Potential

PROTECTING WI-FI NETWORK:

- Media Access Control (MAC) addresses
- Encryption
- Virtual private networks (VPNs)
- Security software

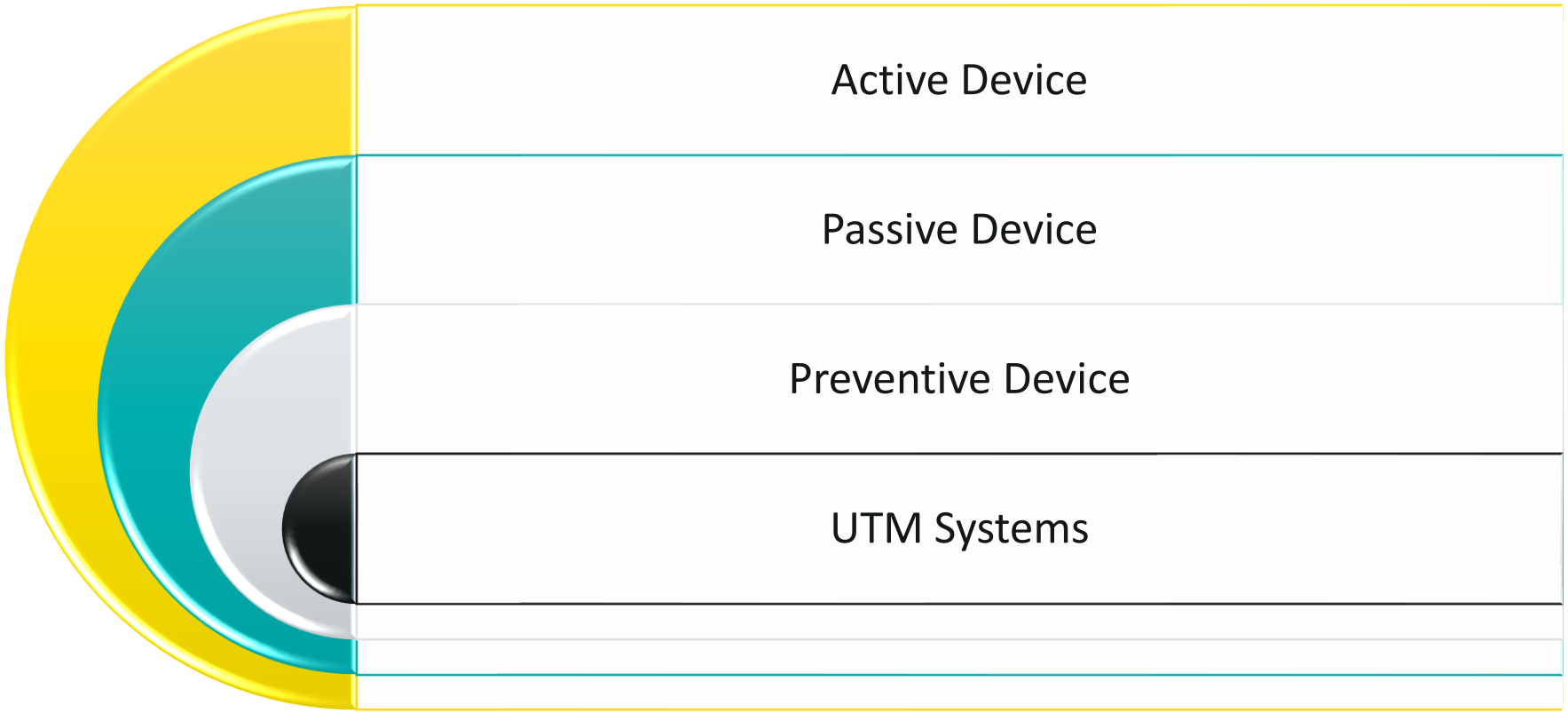
DIGITAL REGENESYS
Awakening Potential

WI-FI SECURITY PROTOCOLS:



DIGITAL REGENESYS
Awakening Potential

NETWORK SECURITY DEVICES:



DIGITAL REGENESYS
Awakening Potential

SECURITY ISSUES FOR WI-FI USERS :

- Unsecured Wi-Fi Networks
- Weak Encryption Standards
- Man-in-the-Middle (MitM) Attacks
- Evil Twin Attacks
- Malware Distribution
- Inadequate Network Segmentation
- Wi-Fi Password Cracking

DIGITAL REGENESYS
Awakening Potential

RESEARCH ASSIGNMENT….

Apple Cyber Attack

(September 2022)

Attack on PayPal

(January 2023)

DIGITAL REGENESYS
Awakening Potential

PRINCIPLES OF WEB SECURITY:

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accountability
- Non repudiation

DIGITAL REGENESYS
Awakening Potential

WHAT DOES WEB SECURITY PROTECT AGAINST?

- Ransomware
- General Malware
- Phishing
- SQL injection
- Denial of service (DoS)
- Cross-site scripting (XSS)

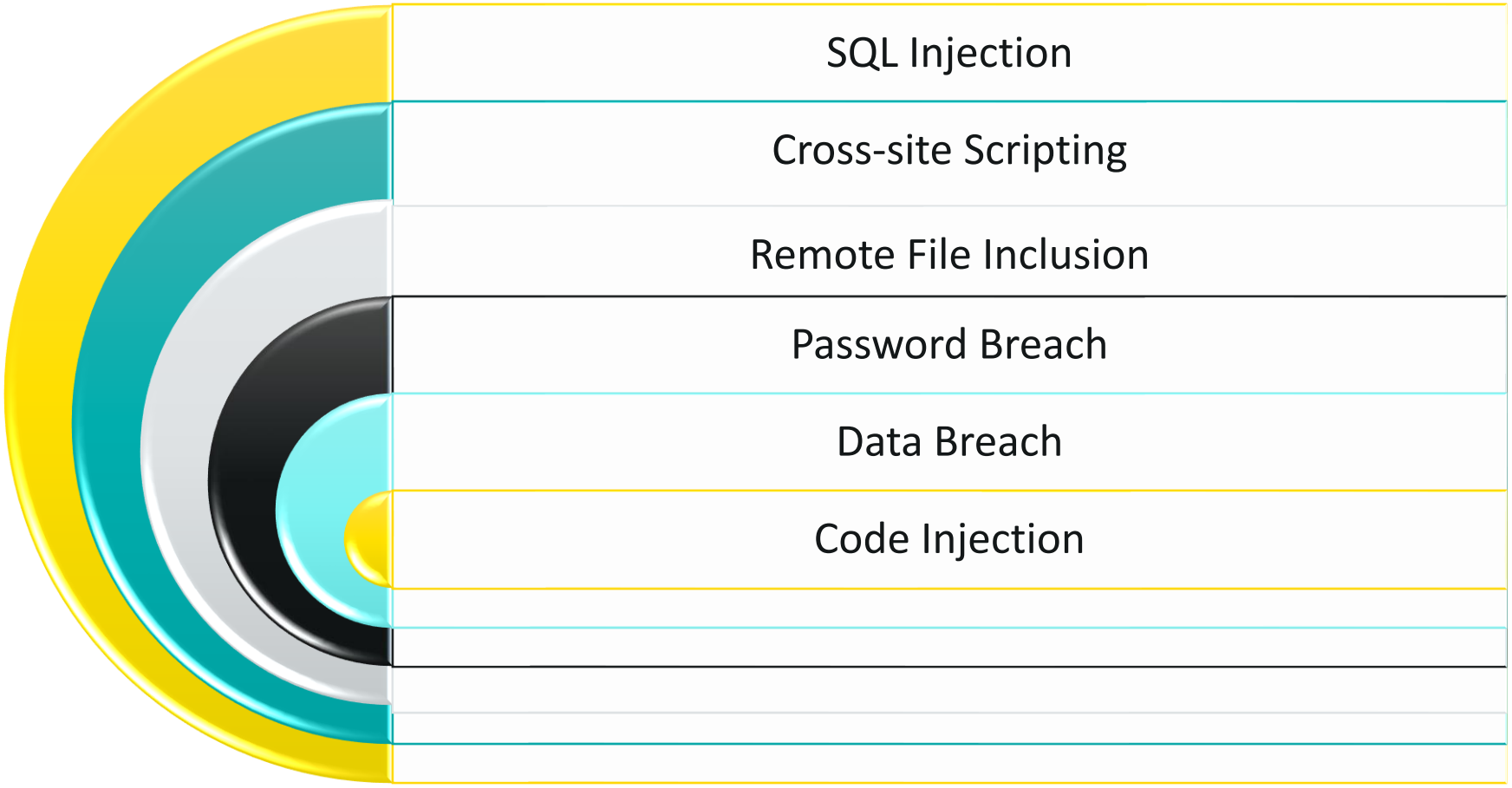
DIGITAL REGENESYS
Awakening Potential

TECHNOLOGIES FOR WEB SECURITY:

- Web Application Firewalls (WAFs)
- Security or Vulnerability Scanners
- Password-cracking Tools
- Fuzzing Tools
- Black Box Testing Tools
- White Box Testing Tools

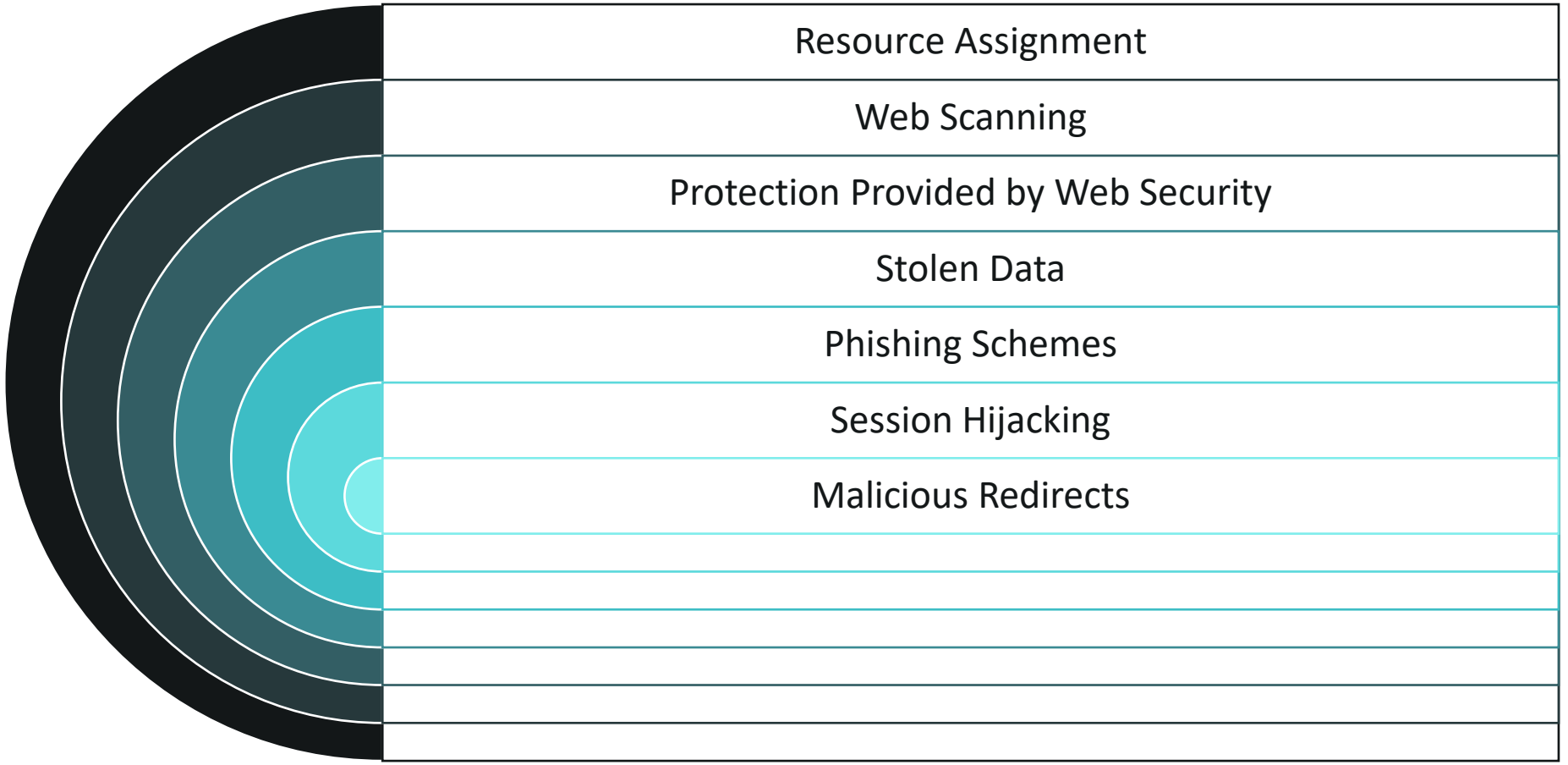
DIGITAL REGENESYS
Awakening Potential

THREATS TO WEB SECURITY:



DIGITAL REGENESYS
Awakening Potential

DEFENSE STRATEGIES FOR DEVELOPER FOR WEB SECURITY:



DIGITAL REGENESYS
Awakening Potential

THANK YOU

DIGITAL REGENESYS
Awakening Potential