CYBER SECURITY FUNDAMENTALS

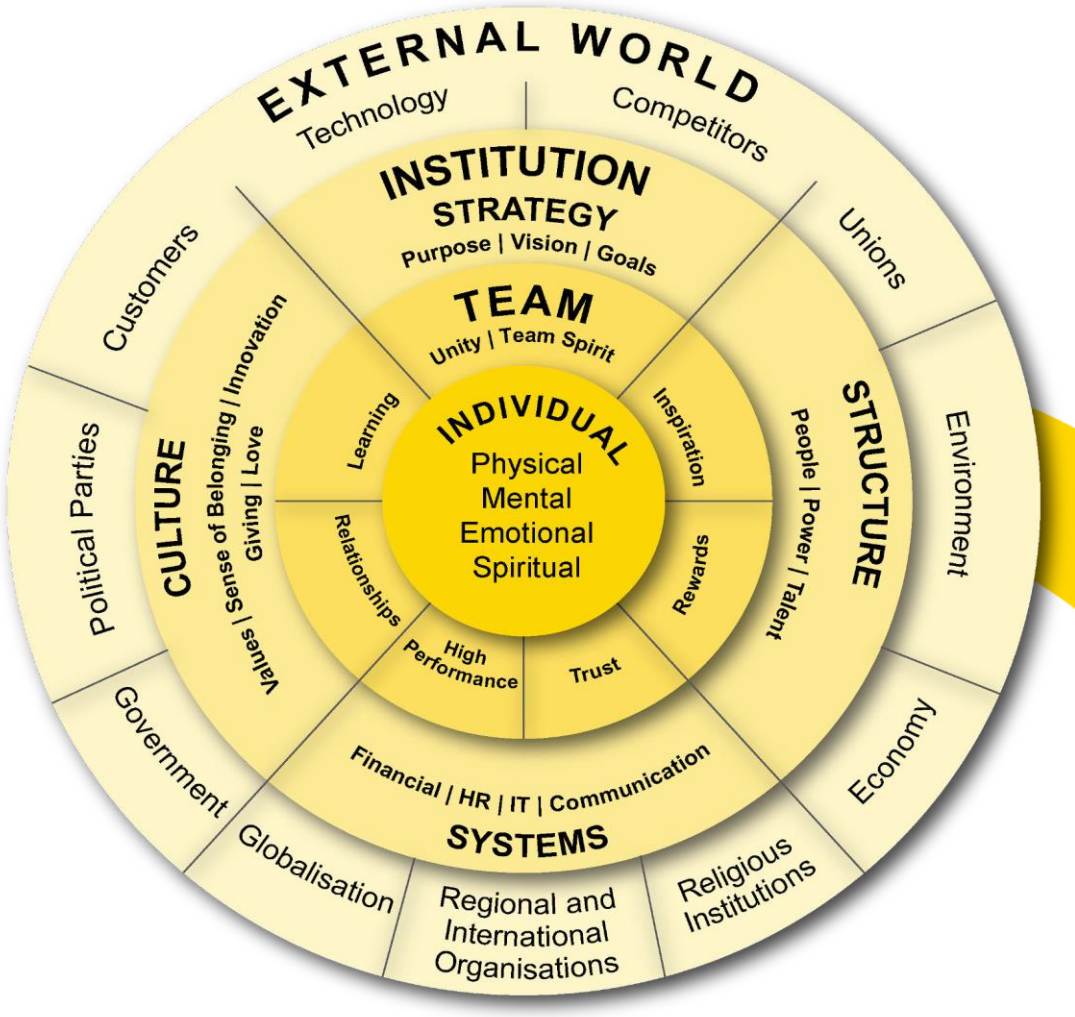
- Dr. Saquib Ahmad Khan

Date: 07.01.2025 & 08.02.2025

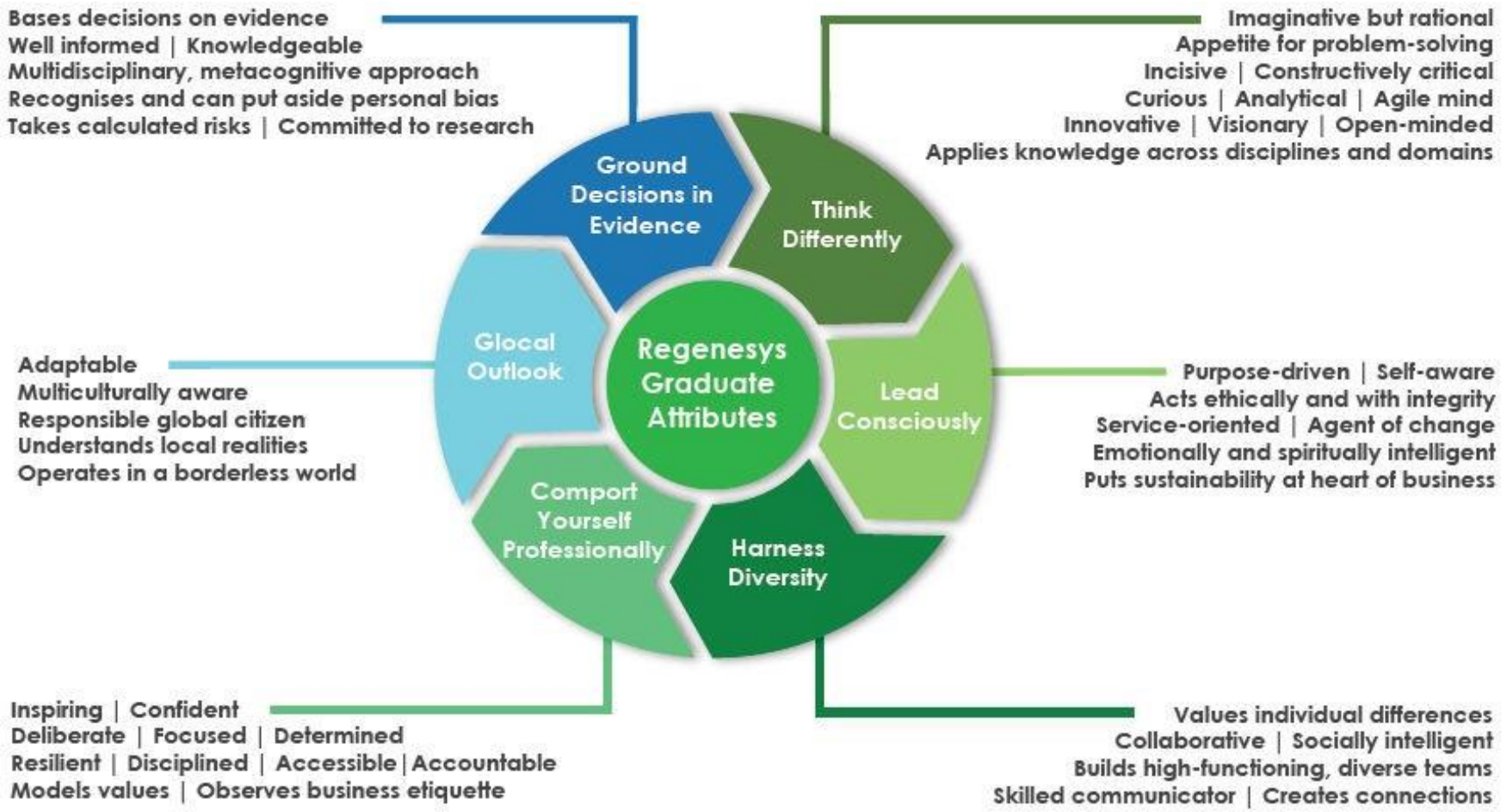
DIGITAL REGENESYS
Awakening Potential

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



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.

GROUND RULES:

- Participate actively
- Be open-minded
- Listen carefully
- One conversation at a time
  - Keep Cameras off for better bandwidth
  - Mute yourself when you're not talking
- 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
- When speaking, use "I think", "I feel", etc.
  (you are a very important aspect of this learning)

HAVE FUN AND ENJOY THE EXPERIENCE !

DIGITAL REGENESYS
Awakening Potential

MODULE 01

DIGITAL REGENESYS
Awakening Potential

Module 01- Comprehensive Cybersecurity Primer: Concepts, Practices, and Strategies

- Fundamentals of cyber security threat actors, attacks, and mitigation
- Cyber Security Fundamentals
- Security Policies and Procedures
- Cyber Security mitigation methods
- CIA Triad

On completing this module, you should be able to:

- List different kinds of cybersecurity protections and understand why they are important today.
- Explain what cyber threats are, sort them into different types, and identify who is behind them.
- Identify various types of cybersecurity protections and understand their importance in today's world.
- Define cyber threats, categorize them, and Identify actors involved in cyber threats..
- Examine the importance and functions of cybersecurity policies, and categorize them into different types.
- Use effective strategies and security measures to prevent cyber-attacks and protect your mobile device.
- Describe the CIA Triad principles, explain their importance with real-life examples, and demonstrate how to apply them in practical situations.

CYBER SECURITY:

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cyber security.

Cyber Security

Cyber refers to the technology that includes systems, networks, programs, and data.

Security is concerned with the protection of systems, networks, applications, and information.

DIGITAL REGENESYS
Awakening Potential

CYBER SECURITY TYPES:

Network Security

Application Security

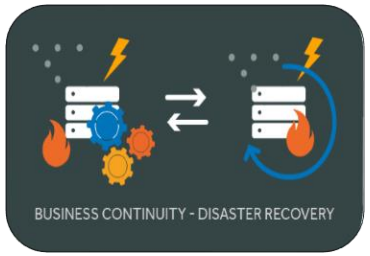
Information / Data Security

Identity Management

Operational Security

Mobile Security

Cloud Security



Disaster Recovery and Business Continuity

End-User Education

DIGITAL REGENESYS
Awakening Potential

THE QUESTION IS....

Why is Cyber Security important?

DIGITAL REGENESYS
Awakening Potential

CYBER SECURITY THREAT:

A cyber security threat is a **malicious** and **deliberate attack** by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

A Cyber Threat or a Cyber Security Threat is a malicious act performed by hackers to intentionally steal data or other assets, misuse them, or simply cause disruption in digital life in general.

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

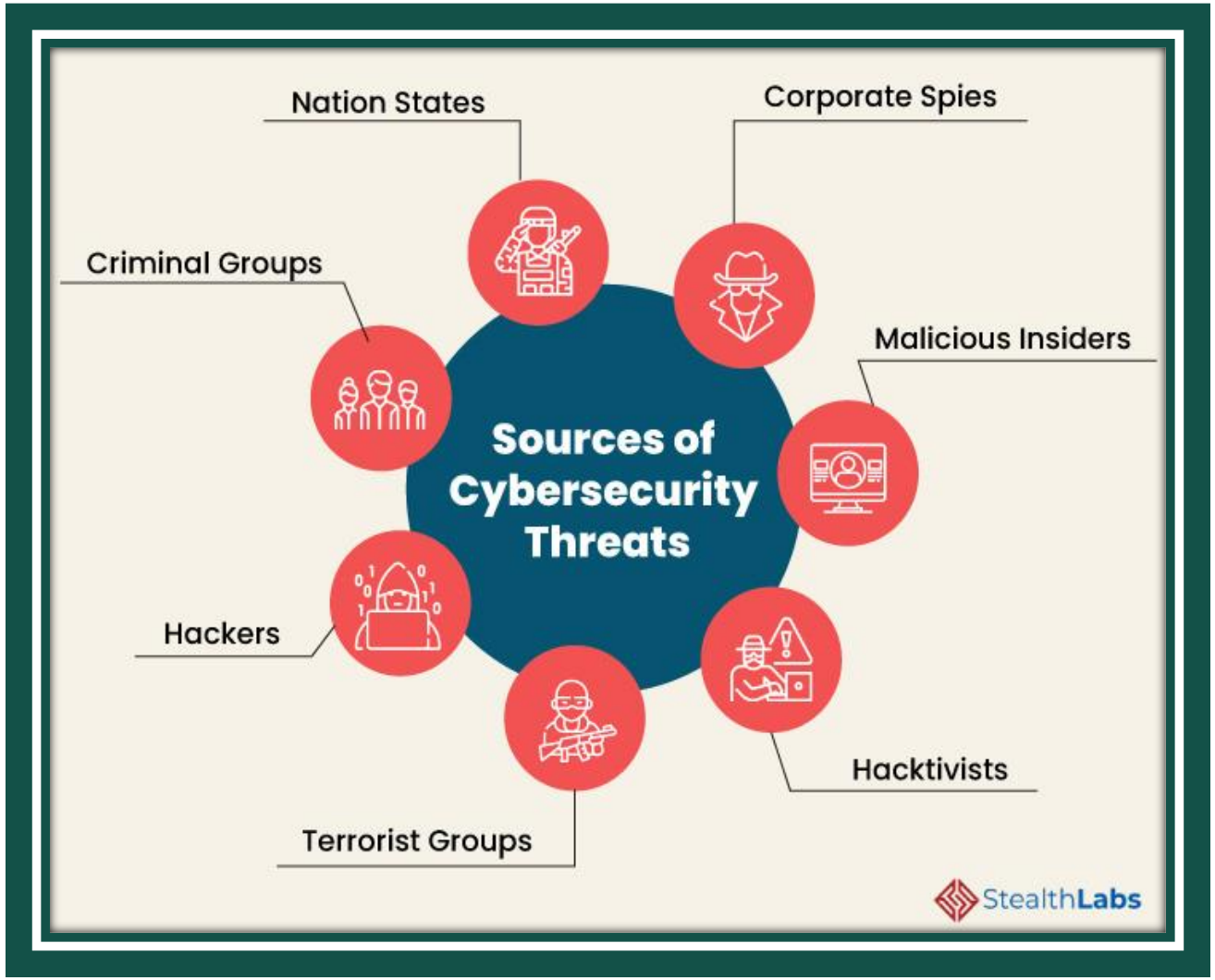
DIGITAL REGENESYS
Awakening Potential

TYPES OF CYBER SECURITY THREAT:

- Malware
- Phishing
- Social Engineering
- MitM Attacks
- DoS and DDoS Attacks
- Zero-Day Exploits
- SQL Injection
- Cross-Site Scripting (XSS)
- Ransomware
- Insider Threats

DIGITAL REGENESYS
Awakening Potential

CYBER SECURITY THREAT ACTORS:



(Source: https://www.stealthlabs.com)

DIGITAL REGENESYS
Awakening Potential

CYBER SECURITY POLICIES:

Policies are divided in two categories –

User Policies

IT Policies

- General Policies
- Server Policies
- Firewall Access and Configuration Policies
- Backup Policies
- VPN Policies

DIGITAL REGENESYS
Awakening Potential

TIPS FOR MITIGATING CYBER ATTACKS:

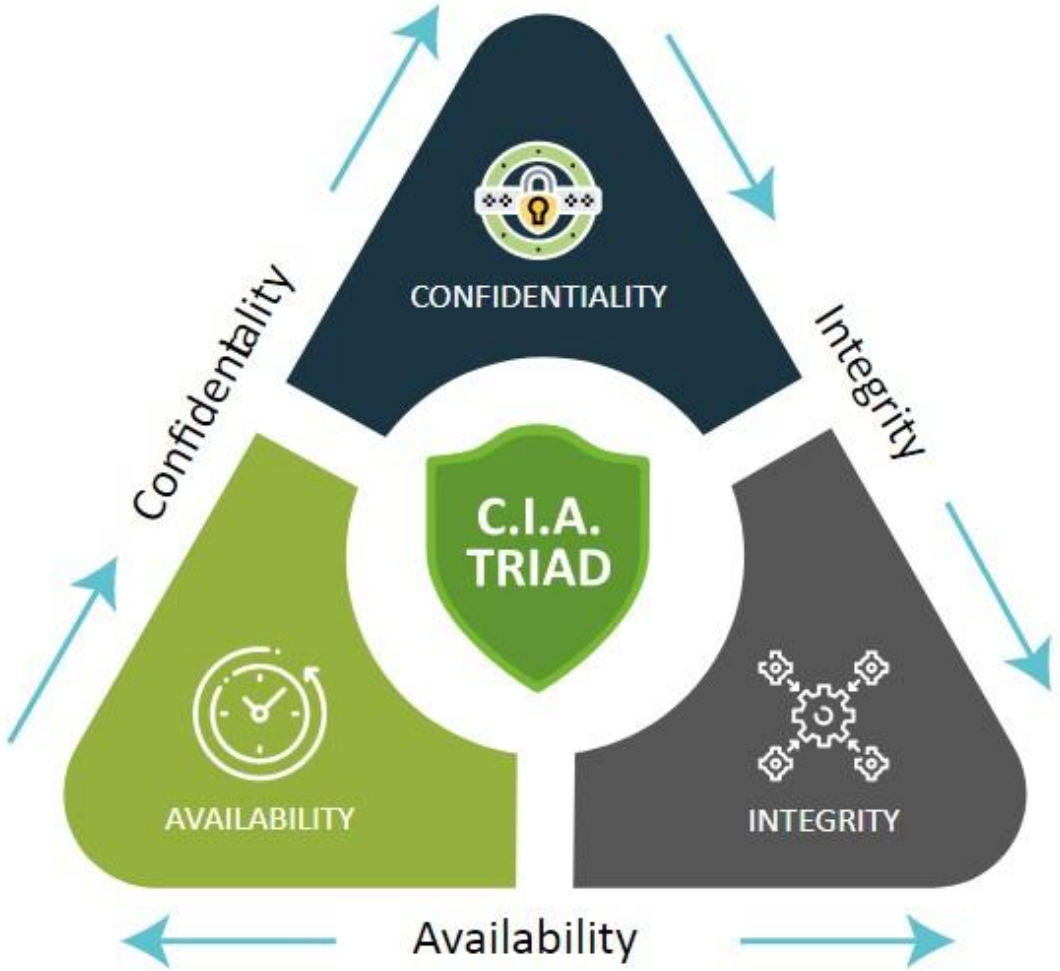
Update and upgrade software	Limit and control account access	Enforce signed software execution policies	Formalize a disaster recovery plan
Actively manage systems and configurations	Hunt for network intrusions	Leverage hardware security features	Segregate networks using application-aware defense
Consider using threat reputation services	Leverage multifactor authentication	Monitor third-party security posture	Assume insider threats exist

DIGITAL REGENESYS
Awakening Potential

SECURING YOUR MOBILE DEVICE:

1. Use strong passwords/biometrics
2. Ensure public or free Wi-Fi is protected
3. Utilize a VPN
4. Encrypt your device
5. Install an Antivirus application
6. Update to the latest software
7. Be discerning

DIGITAL REGENESYS
Awakening Potential



(Source: Team, C. (2022, July 26). Website Security: SSL Certificate, Web Secrity, Hosting & Backup. Website Security Store. https://websitesecuritystore.com)

DIGITAL REGENESYS
Awakening Potential

THE QUESTION IS....

Why is CIA TRIAD so important?

RESEARCH ASSIGNMENT....

The Facebook and Cambridge Analytica Scandal.

DIGITAL REGENESYS
Awakening Potential

WHY SHOULD YOU USE THE CIA TRIAD?

The CIA triad offers a simple yet comprehensive checklist to evaluate your cyber security measures and tools. An effective security system provides all three components – confidentiality, integrity and availability. An information security system that doesn't encompass all three aspects of the CIA triad is insufficient.

The CIA triad is also helpful after an attack to find out what went wrong and what, if anything, worked well. For instance, availability may be compromised after a ransomware attack, but the systems might still maintain other important information. Such data can be used for addressing weak points and replacing them with more effective measures and policies.

THE QUESTION IS....

How To Apply The CIA Triad Principles?

DIGITAL REGENESYS
Awakening Potential

THANK YOU