RAWASI
SYSTEMS

Why Organisations need Cybersecurity framework

RAWASI SYSTEMS

Cybersecurity Framework

- Organisations will continue to have unique risks, different threats, different vulnerabilities and different tolerances
- Organisations can determine activities that are important to critical services delivery ad can priorities investments to maximise the impact of budget spent
- The cyber security framework is aimed at reducing and better managing cybersecurity risks

We are committed to your Business development!

What is a Cybersecurity Framework

RAWASI SYSTEMS

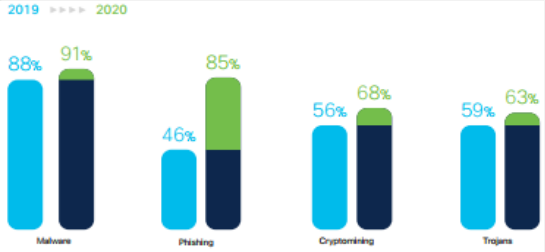
Cybersecurity Framework

- The Cybersecurity Framework in not a one-size-fits-all approach to manage cybersecurity risk for critical infrastructure.
- Cybersecurity Framework is a guidance on how both internal and external stakeholders of organizations can manage and reduce cybersecurity risk. It lists organization specific and customizable activities associated with managing cybersecurity risk and it is based on existing standards, guidelines, and practices.

"Adapted form NIST Cybersecurity Framework"

We are committed to your Business sustainability!

Cyberthreat Landscape



Cyberthreat increase 2019 - 2020

- The cyber threat landscape is constantly evolving. The COVID-19 pandemic is having a direct impact on the increasing cyber risk level.
- The rising threat of cyber incidents can pose financial and reputational damage.
- Cyberattacks make headline news and continue to exercise the minds of cybersecurity professionals around the world. Ransomware attacks, Denial of service attacks, man-in-the-middle attacks, phishing and malware have become common parlance in a world battling with the challenge.

We are committed to your Business enablement!

National Cyber security Authority of Kingdom of Saudi Arabia (NCA)

RAWASI SYSTEMS

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

National Cybersecurity Authority KSA

NCA introduced the Essential Cybersecurity Controls (ECC – 1: 2018) and developed the controls by reviewing legal and regulatory requirements, global cybersecurity best practices, analyzing cybersecurity incidents and attacks on government establishments

The Essential Cybersecurity Controls (ECC) consists of:

- 5 Cybersecurity Main Domains.
- 29 Cybersecurity Sub-Domains.
- 114 Cybersecurity Controls.

We are committed to your Business enablement!

Rawasi Systems portfolio in Cybersecurity space

RAWASI SYSTEMS

Rawasi Systems

At Rawasi Systems we assist and help our customers to recoginise how their priorities align and achieve Cybersecurity objectives. We provide Cybersecurity audits, consultation, Cybersecurity frameworks and policies, Cybersecurity technology design and implementation in order to quickly address compliance requirements

We are committed to your Business enablement!

Basic and Foundational controls

RAWASI SYSTEMS

Basic Controls

- Inventory and control of hardware assets
- Inventory and control of software assets
- Continuous Vulnerability Management
- Controlled use of administrative privileges
- Secure configurations of hardware and Software
- Maintenance, Monitoring and Analysis of Audit Logs

Foundational Controls

- Email and Web browser protection
- Malware defences
- Limitation and control of network ports, protocols and services
- Data recovery capabilities
- Secure configuration for network devices
- Boundary defences
- Data protections
- Controlled access based on the need to know
- Wireless access control
- Account monitoring and control

We are committed to your Business enablement!

Organisational controls

RAWASI SYSTEMS

Organisational Controls

- Implement a security awareness and training programme
- Application software security
- Incident response and management
- Internal and external penetration testing

We are committed to your Business enablement!

Contact Info

RAWASI SYSTEMS

Visit our website:

www.rawasisystems.com

Contact us at:

contact_us@rawasisystems.com

Office Address

2855 Imam Saud Bin Abdulaziz Bin Mohammed Rd, Al Mugharrazat District, Riyadh 12483