



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER



10 Areas to Improve Cybersecurity Readiness



#CyberWiser
www.ncsc.gov.bh

For more info
Scan here!





Protection of data is a continuous cycle

Data at creation, in transit and stored is vulnerable to unauthorized access, modification, deletion or another types of threats such as ransomware. Apply protection measures and assurances needed to prevent data loss/breach and maintaining the "CIA Triad".



Implement/Configure Security Monitoring & Logging

To understand how your systems are being used you need to have security monitoring and logging. This is one of the proactive steps to identify potential indicators of compromise at an early stage and investigate them effectively.



Invest in Cybersecurity Readiness (IR & Management)

It is crucial to have the ability to identify, prevent and respond to cyber threats as part of your cybersecurity policy. Plan in advance and in accordance with the Baseline Cyber Security Controls to have an Incident Response plan in place and the cooperation needed with vendors and responsible national entities.



Identity and access management

Ensure greater control of user access and keep track of employee activity to protect your data and devices. Consider also what systems are authorized to access data and make changes within other systems.



Supply Chain Security

Understand the risk in supply chain and transform risk to your advantage by maintaining a close working relationship with vendors and suppliers through frequent visits and communications to exchange best development and procurement practices.



Vulnerability Management

Keep your infrastructure safe from known exploitations and ensure it stays compliant with any regulatory/standards requirement.. It is important to prioritize dealing with vulnerabilities that are of high criticality (CVSS score) and is equally important to identify critical systems and which vulnerabilities could impact your organization.



Asset Management

Identify and on a Real Time basis, keep track of what systems and data your organization owns and the potential security risks or gaps that affect each one, and the role they serve in the business.



Engagement and Training

It starts with building a positive cybersecurity risk culture in your organization, as "Cybersecurity" being everyone's responsibility. Empower and equip your people with skills and knowledge through Awareness and effective training.



Secure Architecture & Configuration

Employ a defense-in-depth approach to incorporate secure zones and configurations for all the systems and devices in your organization; another concept to consider in this approach is security by design which will help proactively protect Cyber Threats.



Cyber Security Risk Management

All successful cyber security programs implement risk-based approach tailored to specific organizational needs and operational vulnerabilities.