CISO GUIDE TO CYBER RESILIENCE ROADMAP

1 Multi-Factor Authentication

- **Basic**
  - Every User
  - 14+ character Passphrase
  - Unique Passwords
  - Context Awareness
  - Password Manager
- **Medium**
  - Contect Awareness
- **Advanced**
  - Device Authentication

2 Security Policies

- **Basic**
  - Review annually & update
- **Medium**
  - Annual sign off of key policies by employees

Due Diligence

- Ensure following policies

3 Security and Risk Management

- **Basic**
  - Align with budget
  - Risk Assessment
  - Risk Register
- **Medium**
  - Management Coordination
  - Report risks up
  - Define most Critical Assets
- **Advanced**
  - KPIs
  - Monitor

4 Secure Your Endpoints

- **Basic**
  - Anti-virus
  - VPN
  - Test home firewall
  - Secure browser
- **Medium**
  - Email Scanner
  - Application firewall
  - Disk Encryption
- **Advanced**
  - EDR

5 Data Safeguarding

- **Basic**
  - Offline Backups
  - Testing Your Backups
  - Availability in the Cloud
- **Medium**
  - Backup as a Service
  - Business Continuity
  - Disaster Recovery

6 Security Awareness

- **Basic**
  - Annual Training for every user
- **Medium**
  - Security Awareness is Tracked

7 Vulnerability Management

- **Basic**
  - CISA's KEV
  - CVSS Metrics:
    - Attack Vector
    - Attack Complexity
    - Privileges Required
    - CVE Score
- **Medium**
  - SAST/DAST/IAST/SCA
  - Pen Test
- **Advanced**
  - Fuzzing

8 Asset Inventory

- **Basic**
  - Asset Inventory
  - Change Management
  - Mobile Device Management
  - Know your network
- **Advanced**
  - Change Management Board

9 Data Protection

- **Basic**
  - Encrypt data when stored
  - Encrypt data in transit
- **Medium**
  - Impact Level of PII
  - Third-Party Risk Management
- **Advanced**
  - Data Discovery of PII
  - Data Loss Prtoection (DLP)

10 Endpoints to Next Level

- **Basic**
  - EDR
  - X.509 certificates
  - DNS Protection
- **Moderate**
  - MDR
- **Advanced**
  - XDR
  - CSPM
  - CNAPP
  - Zero Trust

11 Secure Configuration Baseline

- **Basic**
  - CIS IG1
- **Moderate**
  - CIS IG2
- **Advanced**
  - CIS IG2
  - CIS IG3 for Critical Assets
  - STIGS
  - Monitoring

12 Classify Data & Assets

- **Basic**
  - IDS/IPS
- **Advanced**
  - CIEM
  - SIEM

13 Artificial Intelligence

- **Basic**
  - AI Policy
  - Pull system under business RMF and cyber program
- **Moderate**
  - Document system
  - Human Oversight
  - Secure AI Framework
- **Responsible AI**
  - NIST AI RMF
  - BIAS

TrustedCISO

WWW.TRUSTEDCISO.COM