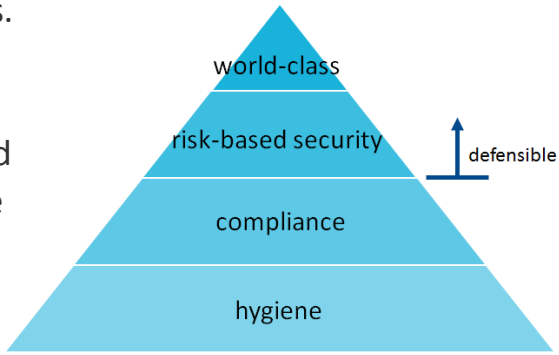
Defensible Security for Public Sector Organizations

Cybersecurity has never been as imperative as it is today. Most organizations have failed to invest at a rate that has sustained previously achieved capability levels. Others have never reached a level of security maturity adequate to mitigate risks to an acceptable level. Organizations must target a level at or above risk-based security. It is critical to ensure hygiene and compliance level controls are in effect. Public sector organizations have a responsibility to apply appropriate safeguards and maintain a defensible level of security.

Defensible security is at or above hygiene + compliance:



The following are pre-requisites to success for security:

- ❑ Ensure the importance of cybersecurity is recognized by executives
- ❑ Information Security roles and responsibilities are identified and assigned
- ❑ Identify critical systems and data as the crown jewels of the organization
- ❑ Organization's risk appetite is known and a risk register is reviewed quarterly
- ❑ Risk assessments are conducted for new systems and material changes to existing ones
- ❑ Conduct security assessments regularly against an established security standard

Organizations must have documented, followed, reviewed, updated, and tested:

- ❑ Asset Management & Disposal
- ❑ Change Management
- ❑ Incident Management
- ❑ Business Continuity Plan (BCP)
- ❑ Disaster Recovery Plan (DRP)
- ❑ Backup & Retention
- ❑ Logging & Monitoring
- ❑ Physical Security & Visible Identification
- ❑ Security Incident Response
- ❑ Information Security Policy
- ❑ Information Security Program
- ❑ Information Security Classification
- ❑ Criminal Record Checks
- ❑ Security Awareness Program & Course
- ❑ Vendor Security Requirements

The following practices must be in effect:

- ❑ Access Control
- ❑ Defence in Depth for Endpoints and Networks
- ❑ Security Governance
- ❑ Vulnerability Management & Patching

Pre-requisites for success

- **Ensure the importance of cybersecurity is recognized by executives** (H)
  - review security threat landscape and request executive support
  - this can be accomplished with a 30-60 minute presentation, conversation, or briefing note with 5-10 hours of preparation time

- **Information Security roles and responsibilities are identified and assigned** (H)
  - document the roles, approve them, and communicate who is responsible and who is accountable for security
  - ensure employee, contractor, and vendor responsibilities are covered as ultimately security is everyone's responsibility

- **Identify critical systems and data as the crown jewels of the organization** (W)
  - build, review, and update a list of key systems and data and the controls in place to protect them
  - if controls are inadequate then review for opportunities to improve
  - ensure availability requirements are documented and met

- **Organization's risk appetite is known and a risk register is reviewed quarterly** (hygiene, W)
  - assess organization's risk appetite (may simply ask, review actions, or both)
  - populate, publish, review, and update risk register quarterly
  - compare residual risk with risk appetite and augment as necessary

- **Risk assessments are conducted for new systems and material changes to existing ones** (hygiene, W)
  - process documented and followed with signoff on risk assessments

- **Conduct security assessments regularly against an established security standard** (W)
  - identify an appropriate security standard and determine whether self-assessment or third-party (for independence)
  - conduct review, identify gaps, build plan to remediate, execute

Durations are based on an average-sized organization and intended as a guide. Whether an organization must invest more or less time will depend on scope , volume, and maturity.

H *hours* W *week(s)* M *month* ! *hazard* *hygiene*

Defensible Security – Definitions (1/3)

- **Access Control** ⚠ M
  - policy is documented, followed, reviewed, and updated regularly
  - address onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges, inactivity timeouts
  - employees/contractors/vendors should be provided only with the access they are authorized to use
  - conflicting duties and areas of responsibility must be identified and segregated to reduce incidents of fraud and other abuse (separation of duties)
  - multi-factor authentication is required for access to sensitive data from untrusted networks
  - system accounts unable to use multi-factor must leverage strong authentication (eg. password aging, length/complexity, history)

- **Asset Management & Disposal** W
  - policy is documented, followed, reviewed, and updated regularly
  - includes both hardware and software and other critical business assets
  - inventory must include name of system, location, purpose, owner, and criticality
  - assets are added to inventory on commission and removed on decommission
  - disposal requirements are based on the sensitivity of the information

- **Backup & Retention** W
  - policy is documented, followed, reviewed, updated, and tested regularly
  - regular backups are taken and tested regularly in accordance with backup policy
  - frequency and completeness should be based on the value of the information (eg. 6 months for high value information)

- **Business Continuity Plan (BCP)** M
  - plan is documented, followed, reviewed, updated, and tested regularly

- **Change Management** M
  - policy is documented, followed, reviewed, updated, and tested regularly
  - changes to production environments must be reviewed and approved

- **Criminal Record Checks** H
  - employees must complete a satisfactory criminal record check regularly and are required to proactively disclose offences

Defensible Security – Definitions (2/3)

- **Defence in Depth for Endpoints and Networks** M
  - endpoints include servers, desktops, laptops, tablets, mobile devices
  - networks include wired and wireless and require secure perimeter, network segmentation, and known ingress/egress points
  - controls must exist to prevent, detect, and respond to security incidents
  - technologies must include firewall, intrusion prevention, web content filtering, email content filtering, and anti-virus at a minimum
  - systems must be hardened (eg. default passwords and shared accounts may not be used, unnecessary services are disabled, insecure protocols disabled)
  - additional controls may be required to mitigate risk to your organization

- **Disaster Recovery Plan (DRP)** M
  - plan is documented, followed, reviewed, updated, and tested regularly

- **Incident Management** M
  - policy is documented, followed, reviewed, updated, and tested regularly

- **Information Security Classification** M
  - classification is documented, approved, communicated, and followed
  - employees must understand not all data is created equal, some data is more sensitive than others and should benefit from greater controls
  - employees should possess only the sensitive information they need, handle it carefully, and label it as appropriate
  - sensitive information must be encrypted in-transit and at rest
  - prohibit production data in test environments unless security controls are equivalent to production or better

- **Information Security Policy** M
  - policy is documented, approved, followed, reviewed, and updated regularly
  - policy should be standards-based in order to evolve over time
  - include Appropriate Use so employees know what they may and may not do

- **Information Security Program** M
  - program is documented, approved, executed, reviewed, and updated regularly
  - align with organization's mission, vision, and goals
  - provides clear direction on security strategy

- **Logging & Monitoring** M
  - collect system logs to determine who did what when, retain according to retention policy, correlate and monitor to identify and act on suspicious activity

Defensible Security – Definitions (3/3)

- **Physical Security & Visible Identification** M
  - policy is documented, followed, reviewed, updated, and tested regularly
  - facilities must benefit from adequate controls (eg. alarms, fences, locks, lighting, access control systems, cameras, guards)
  - staff and visitors must wear visible identification (including a picture) and challenge those who do not

- **Security Awareness Program and Course** M
  - program is documented, followed, reviewed, and updated regularly
  - includes annual information security course for employees
  - educate users on common threats and impacts to business such as not sharing credentials, not clicking on suspicious links and attachments, reporting security incidents, maintaining clean desk, locking inactive systems, concealing valuables

- **Security Governance** M
  - security review to be performed on each business case prior to allocation of capital and implementation of systems (security by design) with business signoff
  - applications, programming interfaces developed according to industry standards

- **Security Incident Response** M
  - plan is documented, followed, reviewed, updated, and tested regularly
  - dedicated, virtual, or on-retainer team to lead response activities
  - identify roles and responsibilities in advance (eg. communications)
  - address preparation, identification, containment, eradication, recovery, and lessons learned and ensure chain of custody, impartiality, and follow evidence

- **Vendor Security Requirements** M
  - vendor requirements are documented, followed, reviewed, and updated regularly
  - requires vendors to meet or exceed organizations' security policy
  - vendors are required to demonstrate evidence of compliance
  - supply chain security risks are identified, mitigated, and reviewed regularly

- **Vulnerability Management & Patching** M
  - policy is documented, approved, followed, reviewed, and updated regularly
  - scans to be performed prior to and following production launch
  - systems must be patched regularly to ensure current OS and application levels
  - vulnerability assessments are regularly conducted as part of a program and vulnerabilities must be rated according to criticality
  - high and critical vulnerabilities must be remediated through patching, decommission, or compensating controls