Defensible Security

For Public Sector

Ken Prosser Director, Cybersecurity Intelligence and Investigations

Information Security Branch

BRITISH COLUMBIA

OCIO

Office of the Chief Information Officer

Defensible Security

1. Introduction
2. DefSec Triage
3. Control Objectives
4. Next Steps

Data Breach Statistics

EVERY DAY

5,146,763

Records

EVERY HOUR

214,448

Records

EVERY MINUTE

3,574

Records

EVERY SECOND

60

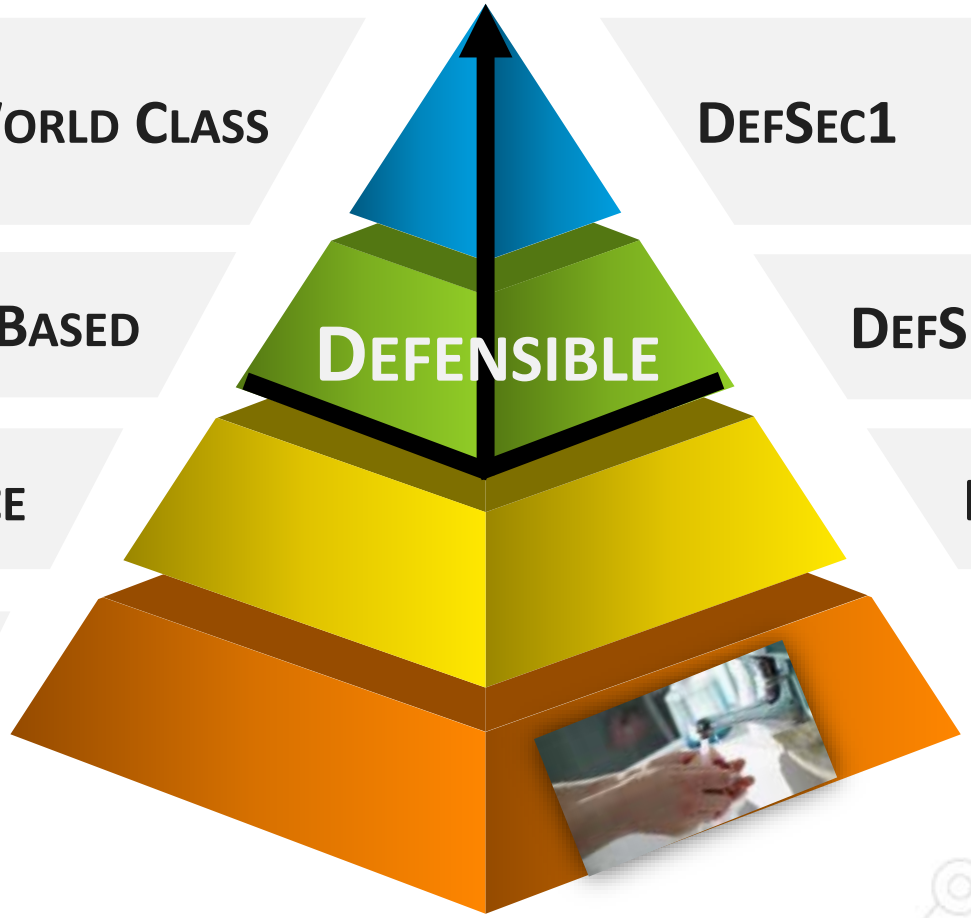
Records

Source: http://breachlevelindex.com/

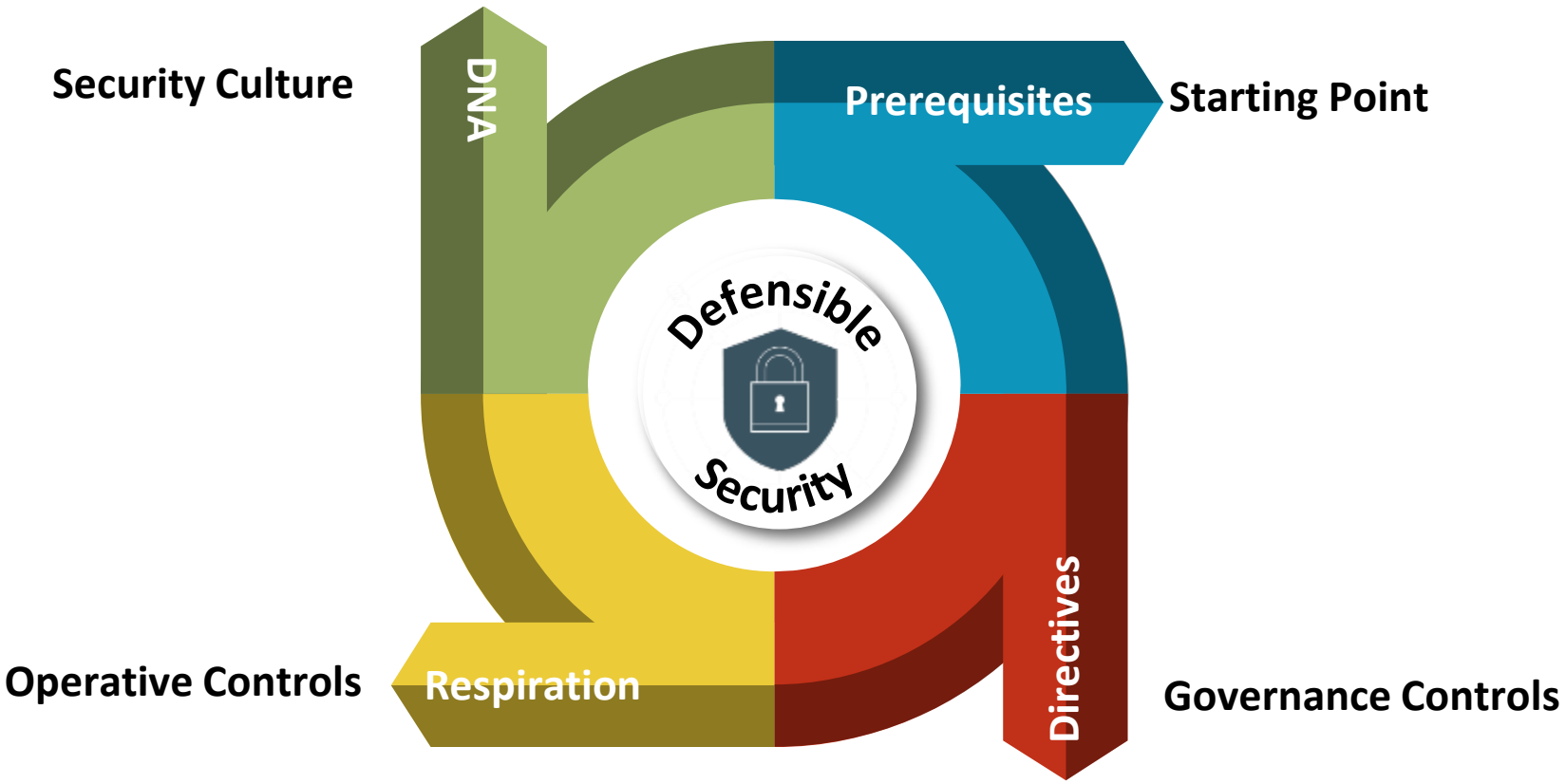
What is Defensible Security?

An initiative
to raise the level
of information security
across the public sector

DefSec for Public Sector Organizations



DefSec Triage



DefSec -Security Prerequisites

Executive Support
Roles & Responsibilities
Crown Jewels
Risk Appetite & Register
Risk Assessment
Security Assessment

DefSec –Security Directives

Asset Management & Disposal
Change Management
Incident Management
Business Continuity Plan (BCP)
Disaster Recovery Plan (DRP)
Security Incident Response
Information Security Policy

DefSec –Security Respiratory Controls

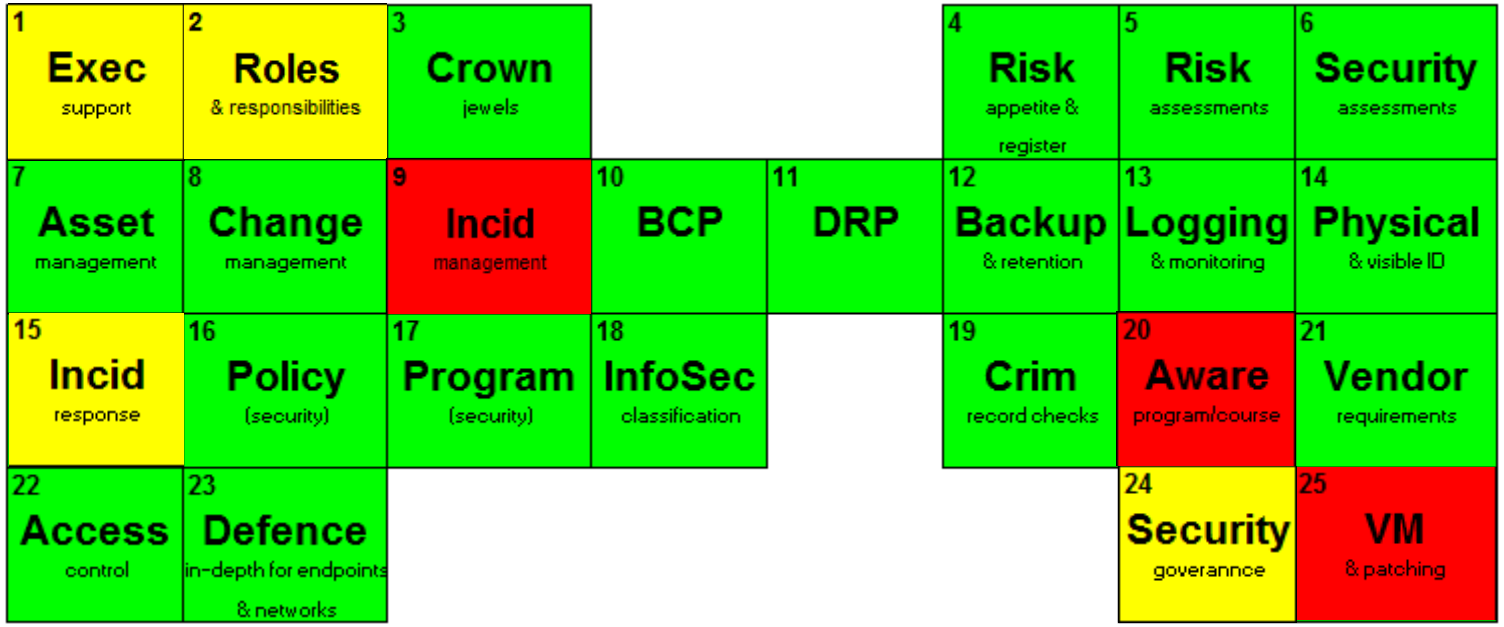
Backup & Retention
Logging & Monitoring
Physical Security & Visible ID
Background Checks
Vendor Security Requirements
Access Control
“DiD” for Endpoints & Networks
Vulnerability Management

DefSec Security Embedding (DNA) Controls

Information Security Program
Information Security Classification
Security Awareness
Security Governance

Sample Assessment Exercise

You can use this simple dashboard to perform assessments on any system, project or incident to determine what your organizations gaps are.



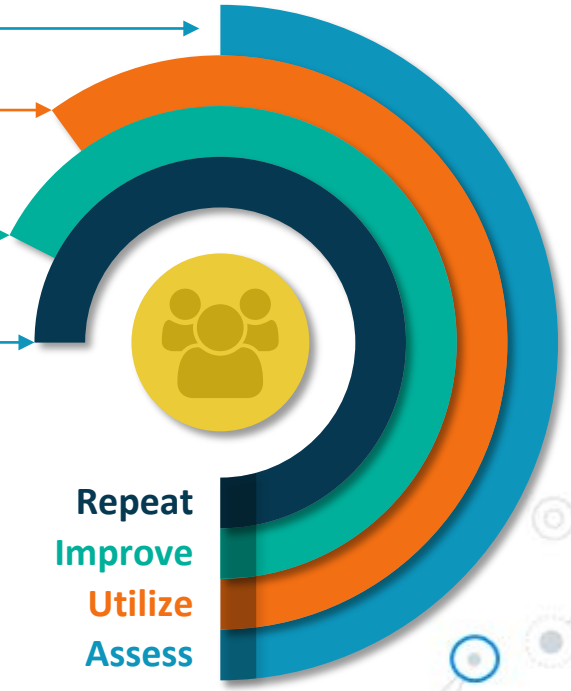
What are the next steps?

Assess: Organization

Utilize: DefSec Resources

Improve: Security Posture

Repeat: Continuous Improvement



Security is everyone's responsibility:
Let's collaborate in improving the security posture across the public sector.

Thank You!

For more information visit: gov.bc.ca/defensible-security

BRITISH COLUMBIA

OCIO

Office of the Chief Information Officer