

Building Cybersecurity Immunity in eHealth Ecosystem

Eric Wong

Senior System Manager, Hospital Authority

The evolutionary journey of eHRSS



Key Achievement

5.6 Million Citizens; Over 5000 Professionals ; 2600HCPs; 2.9 Billion Shared Record

Core Business Objective

Join & share Consent

HCPs Portal

Data Standard & Terminology

HCPs Data use support

eHealth App

Radiology Image sharing

Chinese Medication Support

Enhanced Security and Privacy

COVID
-19

Hong Kong's e-Health Ecosystem

Public-Private Partnership Programmes



eHR Sharing



E-Health Programme



Primary Care

Vaccine Pass



Collaborative Care



New public-private partnership model

Public / Private Health Care Providers

What is Cybersecurity Immunity

Human Immunity vs Cybersecurity Immunity

先天免疫

Innate Immunity

- Non-specific
- Fast respond
- First line of defense

Known Threats

- Access Control / 2FA
- Anti-virus
- Firewall
- Intrusion detection / protection

後天性免疫

Acquired Immunity

- Specific
- Slower respond
- Learn > adapt > remember > develop
- Secondary or tertiary defense

Unknown Threats

- Zero-day
- Threat analytic / intelligence
- Abnormally detection / intervention

增強免疫

Boosting Immunity

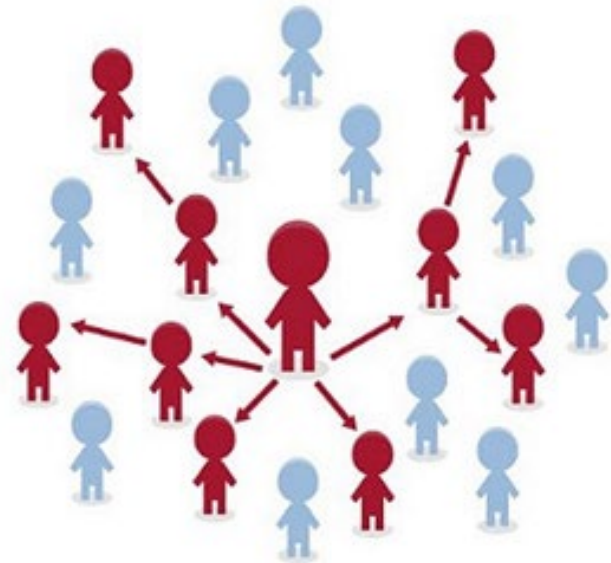
- Personal hygiene
- Healthy diet and exercise
- Vaccination

Boosting Immunity

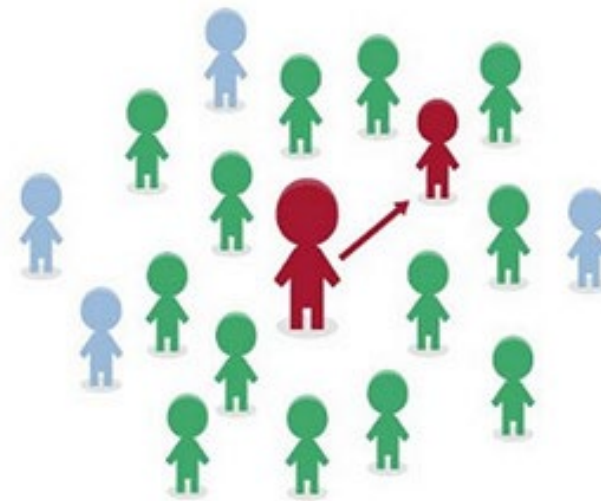
- Cyber hygiene
- Updated preventive measures
- Regular review / risk assessment

預防勝於治療

Why do we need Cyber Immunity ?



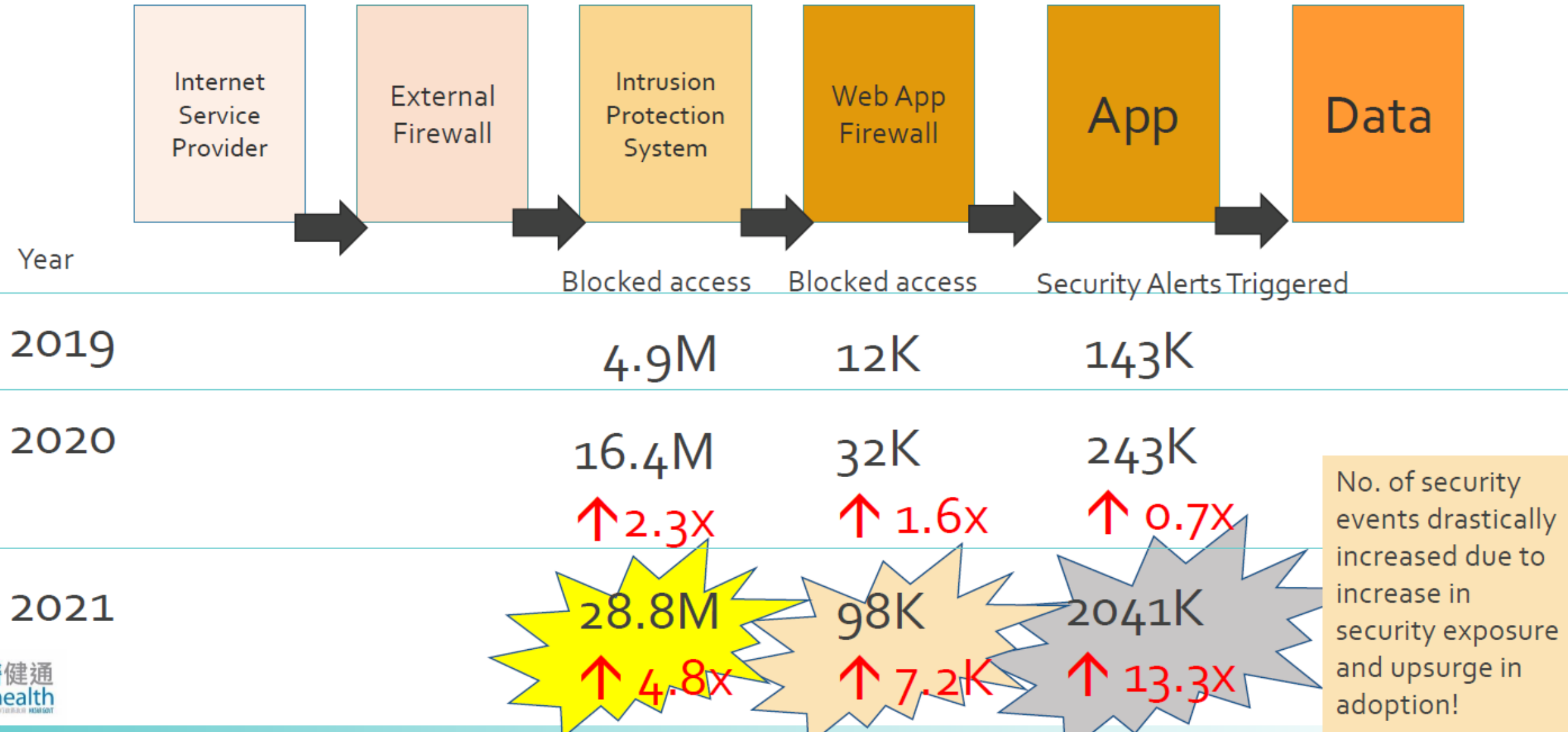
No herd immunity



Herd immunity achieved

● Susceptible ● Infected ● Immune → Disease transmission

Security Events in eHRSS



Taxonomy of Cyber Security

Cyber Security threats

- Social Engineering
- Third-Party Exposure
- Configuration Mistakes
- Poor Cyber Hygiene
- Cloud Vulnerabilities
- Mobile Device Vulnerabilities
- Internet of Things
- Ransomware

Objectives of Security



Elements of Cybersecurity

- Application security
- Information security
- Disaster Recovery Planning
- Network Security
- End-user Security
- Operational Security

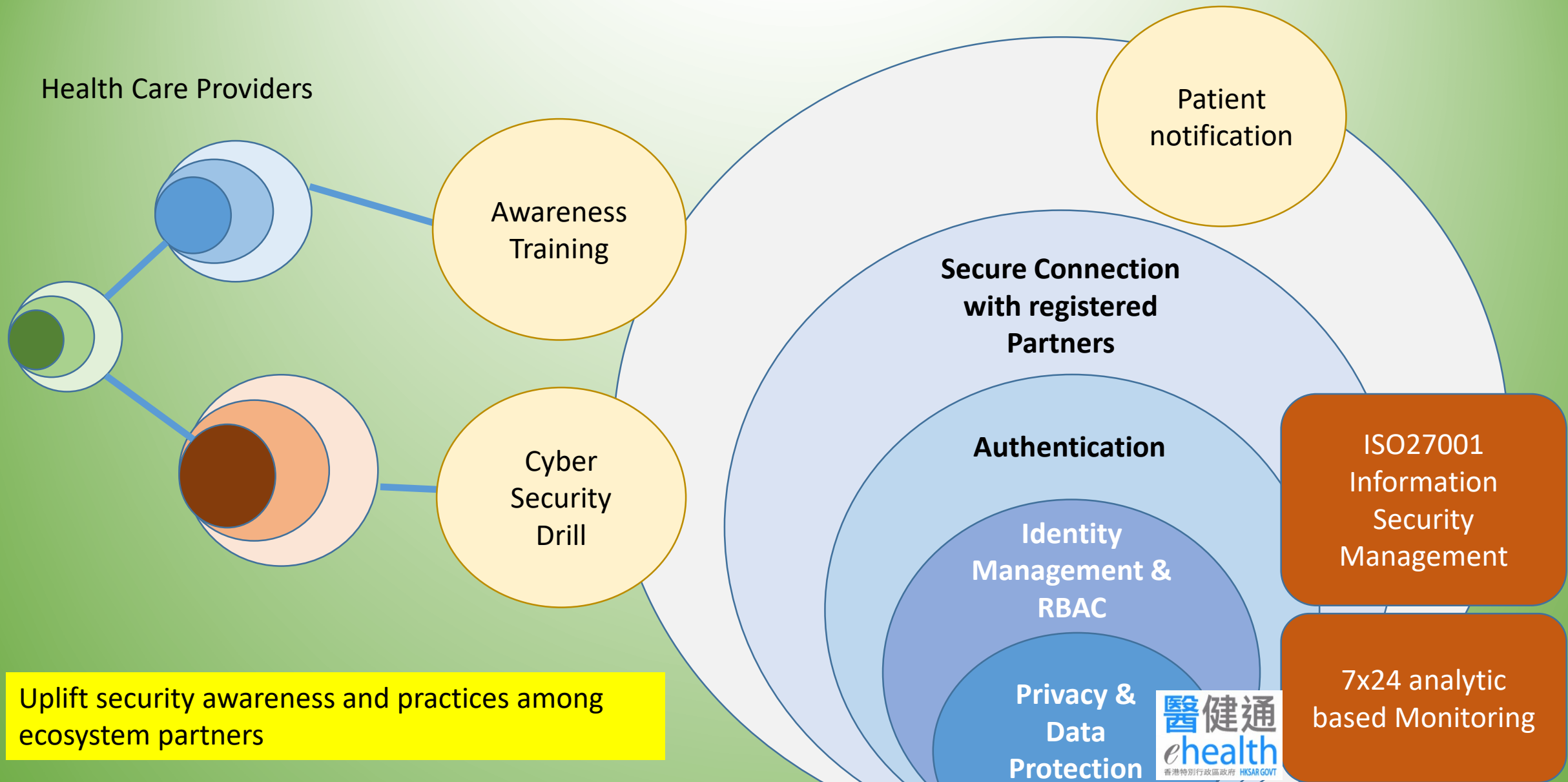
Types of Cybersecurity

- Network Security
- Cloud Security
- Endpoint Security
- Mobile Security
- IoT Security
- Application Security
- Zero Trust

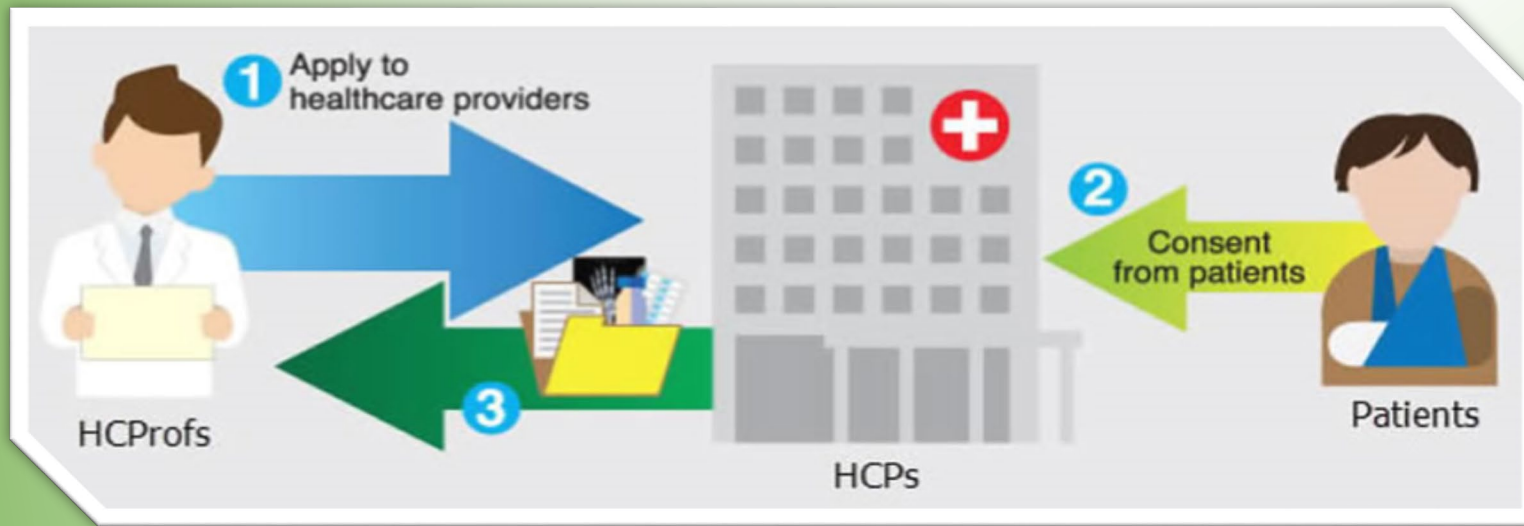
Aspects of security

- Physical security
- Digital security
- Operational security
- Administrative security

How do we enhance Cybersecurity Immunity ?



Sharing Consent



Explicit Consent
given by participants



Indefinite sharing consent

Consent will remain valid until revoked or updated by the patient, or the patient's registration is withdrawn or cancelled



One-year sharing consent

Consent will expire after one year or lapse if revoked or updated by the patient, or the patient's registration is withdrawn or cancelled

Role Based Access Control

Professional Registration and verification



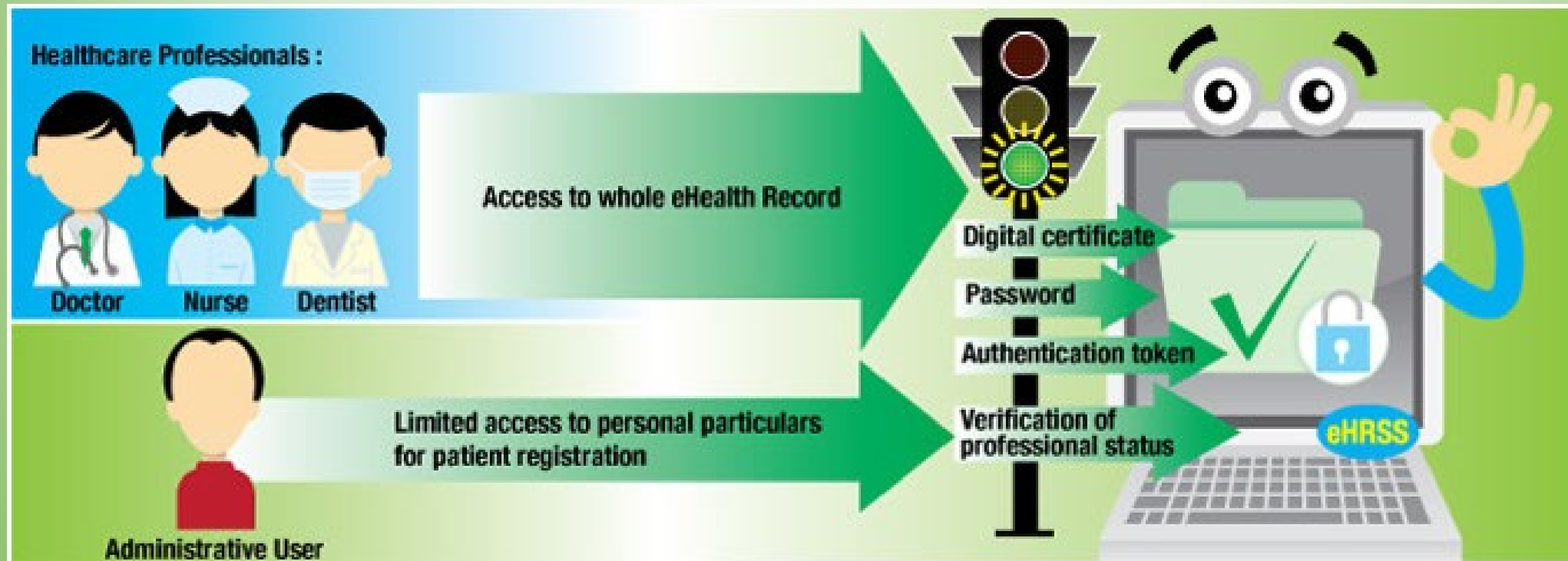
Role Based Access Control



Fine grained control to different record type

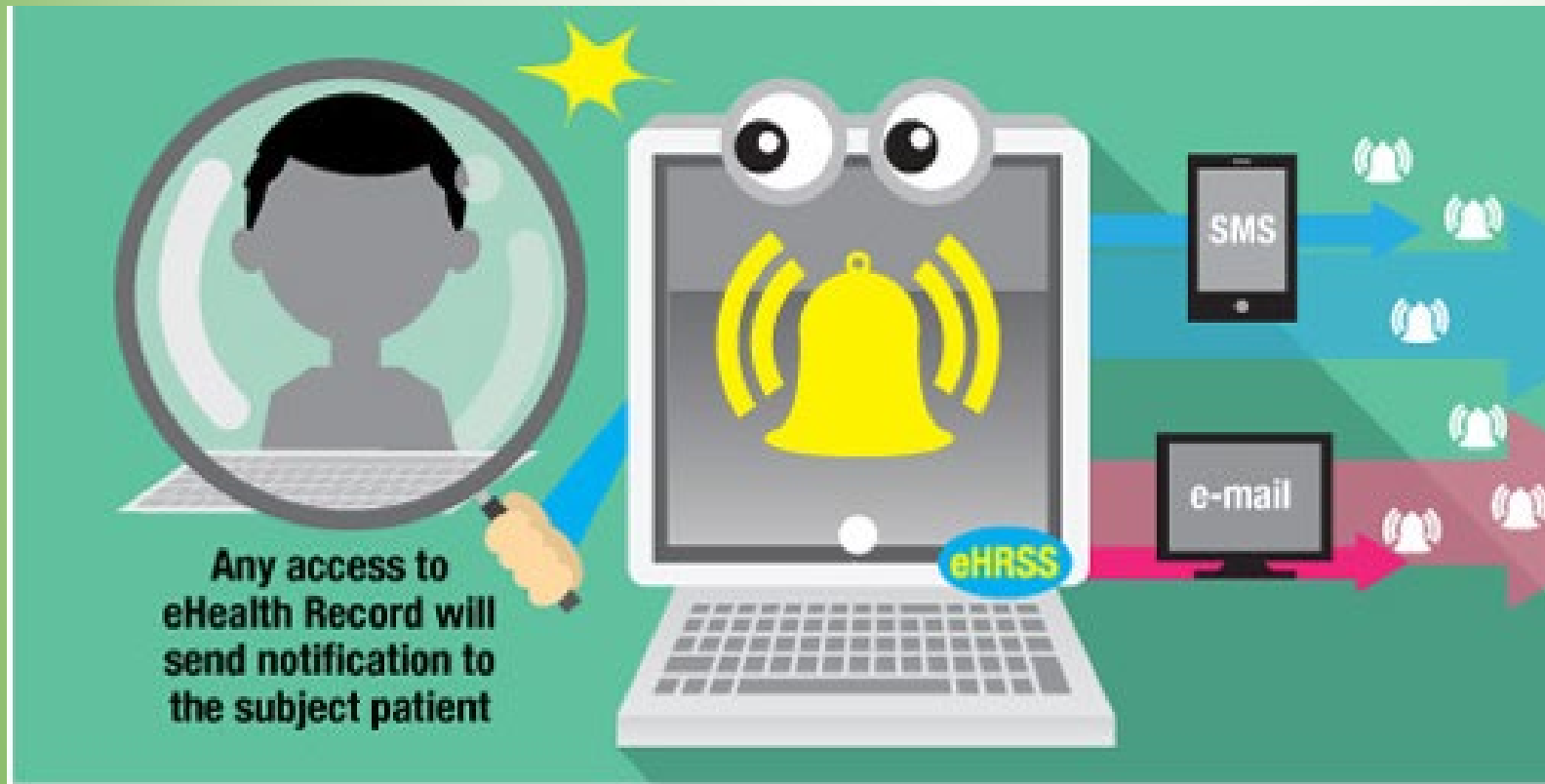
	Demographic Data	Encounters/ Appointments	Allergies & Adverse Drug Reactions	Medication	CM-Medication	Laboratory Reports	Radiology Reports	Other Investigation Reports	Clinical Note and Summary	CM-Clinical Note and Summary	Diagnosis	CM-Diagnosis	Procedures	CM-Procedure	Immunization Records	Healthcare Referrals	Birth Records
Doctor/Nurse/Dentist					NA					NA		NA		NA			
Pharmacist					NA					NA		NA		NA			
Part I Optometrist					NA					NA		NA		NA			
Physiotherapist					NA					NA		NA		NA			
Occupational therapist					NA					NA		NA		NA			
Lab Technologist					NA				NA	NA	NA	NA		NA			
Radiographer					NA				NA	NA	NA	NA		NA			
Chinese Medicine Practitioners				NA		NA	NA	NA	NA		NA					NA	NA

Secured Connection and Authentication

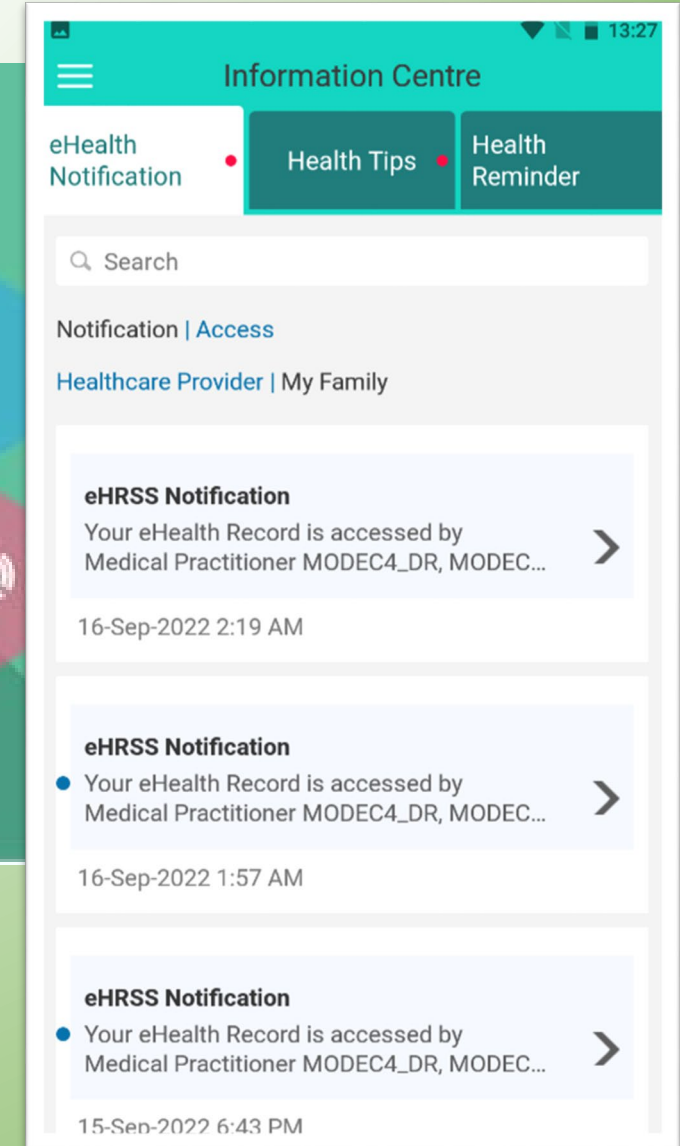


1. Registered HCP
2. Secure Connection Software → ELSA replacement to be introduced soon
3. 2FA Authentication (SMS, Im Smart and more..)

Audit log, abnormality detection and notification



1. Full access Log of user activities
2. 7x24 Security Operation Center, threat analytic
3. Patient notification via SMS, eMail and eHealth App (at a glance view of all access history)



The Weakest Link in Cybersecurity Immunity...



Social Engineering bypass all technologies including firewalls.

- Kevin Mitnick



"Amateurs hack systems;
professionals hack people."

— Bruce Schneier

The weakest link in any chain of security is not the security itself, but the person operating it !

How do I know if Im Healthy ?



How to gauge
Security Risk
Exposure and take
appropriate
actions ?

What is ISO 27001

An Information Security Management System (ISMS) is a management system that helps to ensure

security risks are properly managed by

appropriate risk treatment options and security controls

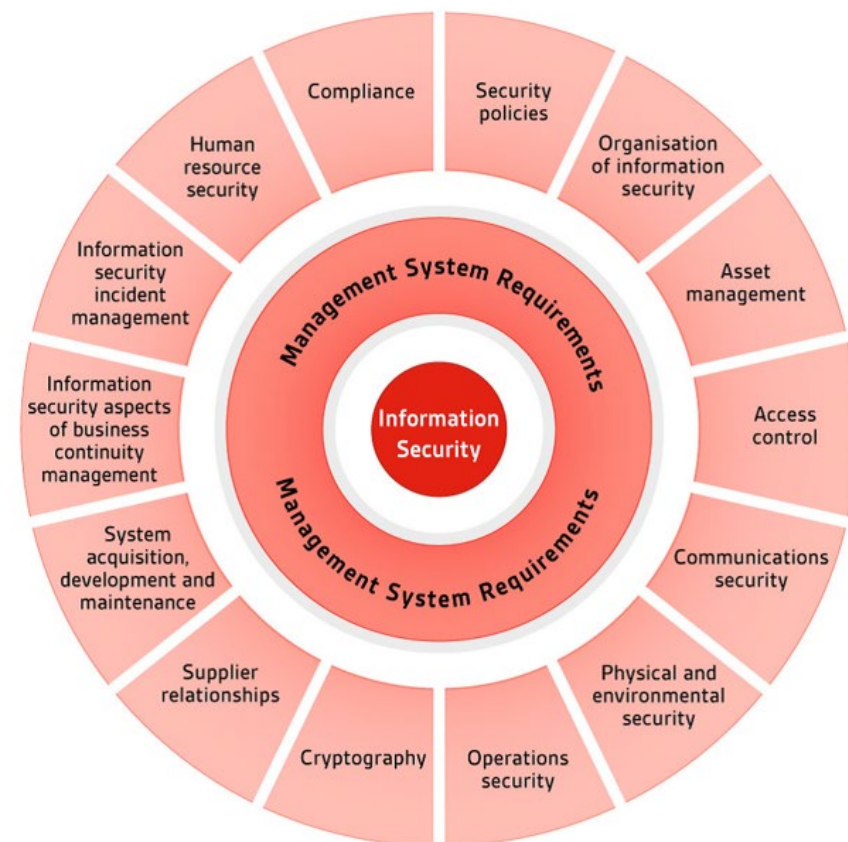


What is ISO 27001

14 Control Areas

35 Control Objectives

114 Security Controls



Why ISO27001 ?



Increasing risk
of security
attacks

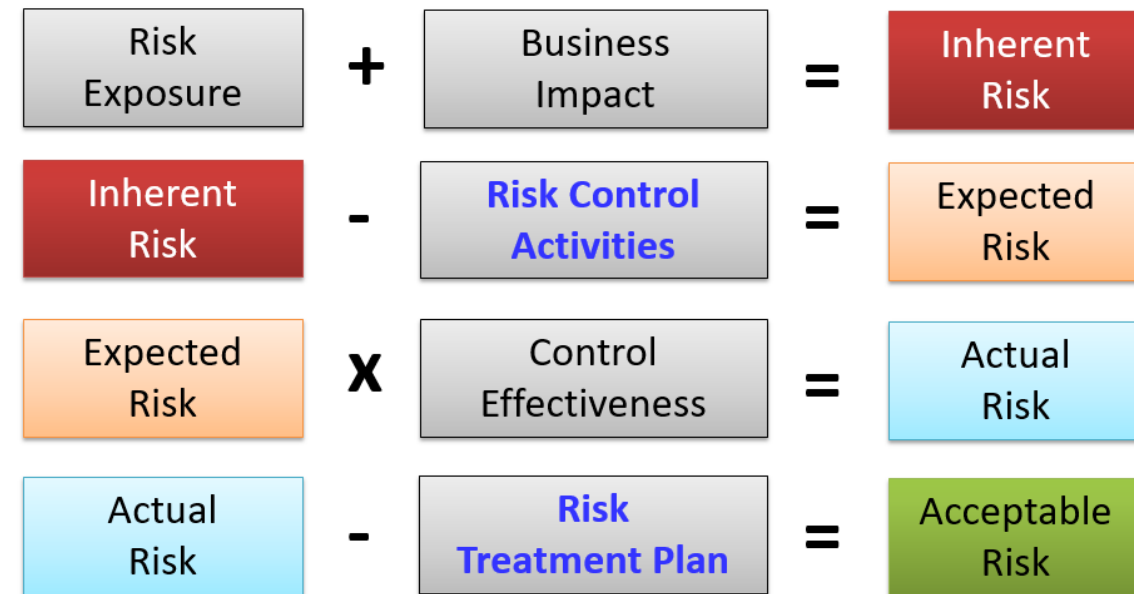


Commitment to
information
security & earn
public trust



Gauge against
industry
standards to
improve
capabilities

Risk assessment & treatment



Cyber Security Drill

Cyber-attack is
not IF but
WHEN ?

Prepare for your
immunity respond !

- **HHB**
 - **eHRO**
 - **eHRSS ISIRT**
 - **HHB ISIRT and DITSO**
- **HA**
 - **eHRSS Support Team**
 - **eHR Registration Office**
 - **IT Call Centre**
- **HKPF**
 - **CSTCB**
- **OGCIO**
 - **GIRO**
- **Participating HCP**

Annual Drill Exercise

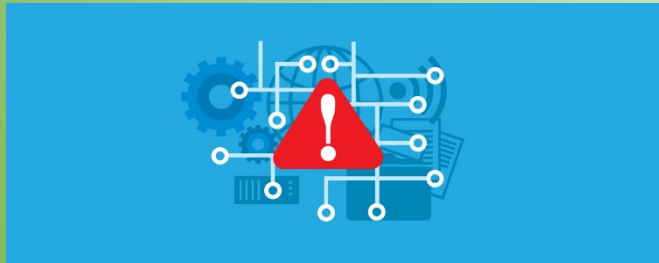
Year	Drill Scenario
2018 Nov	Remote Desktop Attack
2019 Nov	Ransomware Attack
2020 Nov	COVID-19 Themed Phishing (Phishing email + zero-day malware)
2021 Nov	Ransomware of Application Servers
2022 Nov	Malware Attack & Phishing Email

Cyber Security Tips



Immunize your computer asset

- Anti-virus
- Regularly update your software
- Backup and secure your backup



Incident Respond

- Training
- Well-defined procedure
- Seek advice from appropriate org



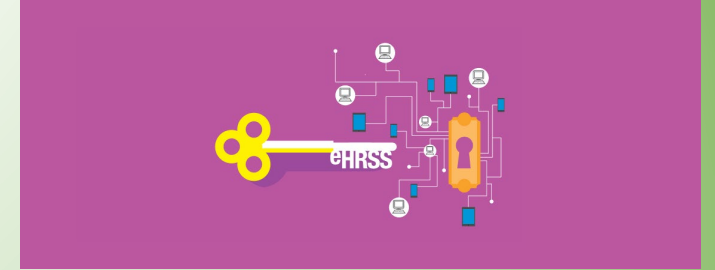
Protect against ransomware

- Beware of suspicious email / links
- Backup! Backup! Backup!



Password

- Enable multi-factors
- Avoid reuse
- Strong password – the longer the better



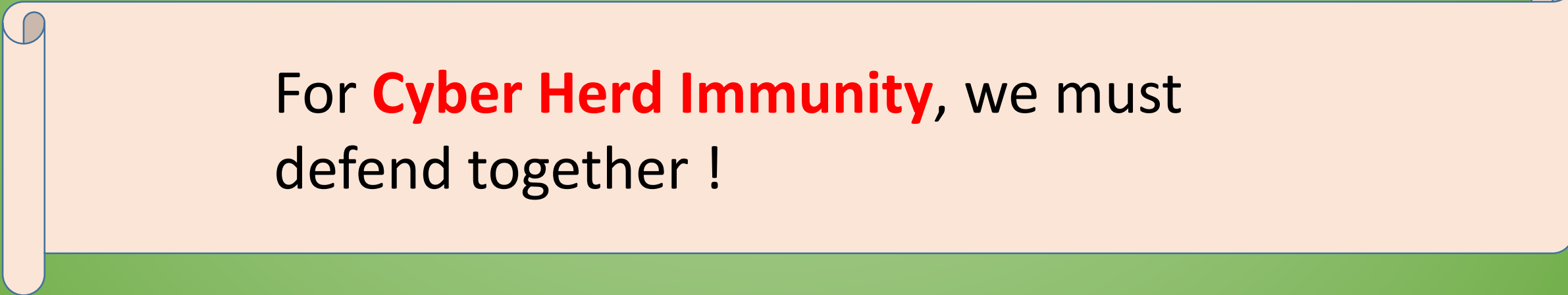
Take care of your gadgets

- Avoid taking photos of sensitive info
- Double check before you share anything online !
- Enable encryption
- Strong password & multi-factor authentication

Cybersecurity is
a **Shared
Responsibility**



Cybersecurity is
a **Team Sport**



For **Cyber Herd Immunity**, we must
defend together !