Enhance eHealth+ Cybersecurity Defense - A Joint Effort Approach

協同努力提升eHealth+網路安全防禦

Eric Wong
HAIT
2024-10-21

Development of eHealth

醫健通
eHealth
香港特別行政區政府 HKSARGOVT

2009 - 2022

Stages 1 & 2 Development

- eHRSS Ordinance (2015)
- eHR sharing platform (2016)
- eHealth App (2021)

2024

eHealth Today

- Over **6 million** registrants
- Over **3.4 million** eHealth App downloads
- Over **220 000** records accessed per month

2024 - 2028

eHealth+

- Comprehensive healthcare information infrastructure for data sharing, service support and care journey management

Future Development Trends

Smart Healthcare

Primary Healthcare

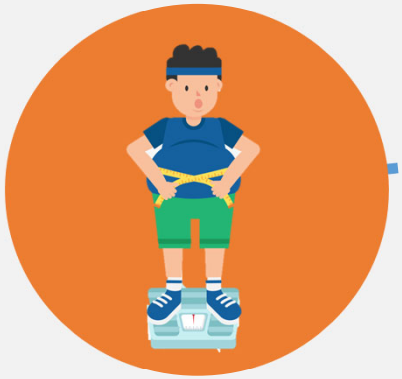
Cross-boundary Healthcare

Health Innovation

Vision and Mission of eHealth+

Care Coordination

Cross-sector Collaboration



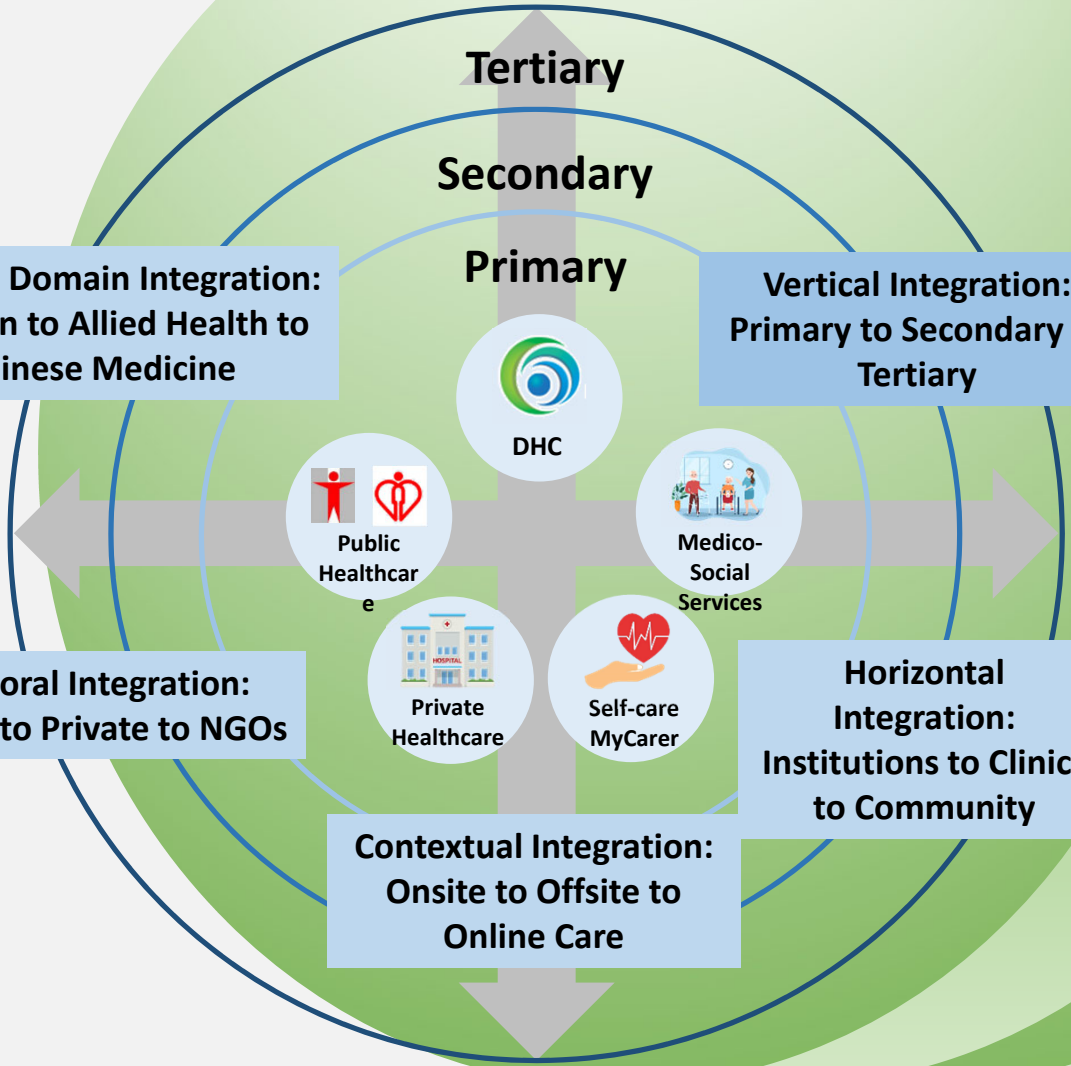
Health Surveillance

Active Health Management

Care Coordination & Cross-Sector Collaboration

eHealth App as a "Digital Front-Door" for empowerment & self-healthcare

Integrate records of all subsidised health programmes and all public or subsidised healthcare services



Medical Domain Integration: Western to Allied Health to Chinese Medicine

Vertical Integration: Primary to Secondary to Tertiary

eMedication & telehealth to enable new service capabilities

eHealth as central data hub for medical research, trials, innovations and healthcare policy formulation

Sectoral Integration: Public to Private to NGOs

Horizontal Integration: Institutions to Clinics to Community

Contextual Integration: Onsite to Offsite to Online Care

AI / BI / ML / Big data / Cloud / IoT Data analytics

Support cross boundary healthcare services

eHealth participation

Healthcare providers coverage

All public hospitals and clinics, **13** private hospitals and over **2,900** private healthcare organisations at **5,400** service locations

Over **54,000** healthcare professionals

Population coverage

6.2M (82%)

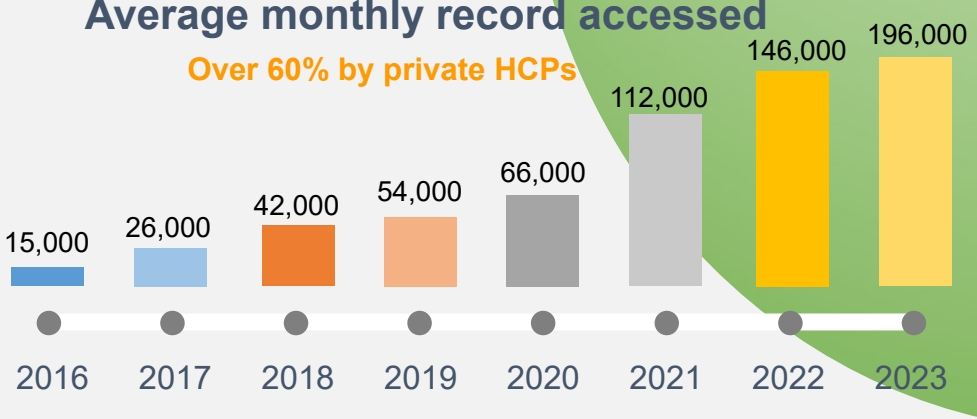
eHealth App

Over **3.2M** downloads

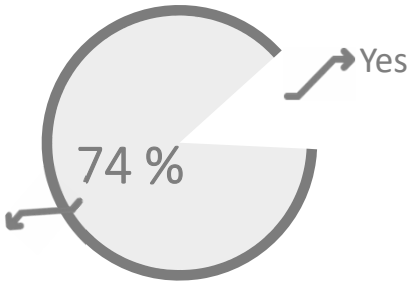
800,000 average monthly access **(1.6M in 2022)**

Average monthly record accessed

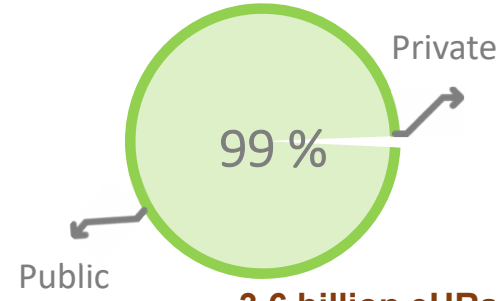
Over 60% by private HCPs



Sharing consent to private HCPs



Data sharing by HCPs



3.6 billion eHRs

Cybersecurity challenges in the age of digital healthcare

Landscape

Highly Digitize & Digitalized

Increased Connectivity

Increased complexity

External Threats

Easy & lucrative cybercrime model. Supply-chain dependency

Internal Threats

Ignorance / Negligence

Lack proper controls / contingency

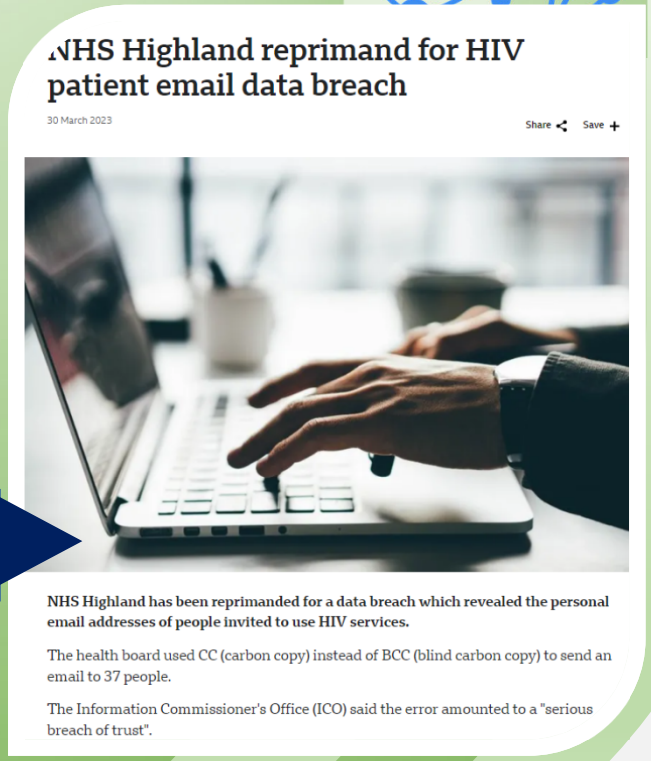
Higher risk exposure

Case Study - Insider / external Threats

Lesson learned

- NO role based access
- Lack protection for sensitive targets

Privilege Abuse



Lesson Learned

- Awareness gap
- Lack proper procedure for sensitive data handling

Un-intentional Leakage

Case Study - Insider / external Threats

Privilege Abuse

…uance Ex-Employee Indicted for Breach Affecting 1 Million

DOJ Says Vendor's Terminated Worker Unlawfully Accessed Geisinger Patient Info

Marianne Kolbasuk McGee (HealthInfoSec) · June 26, 2024

Share Tweet Share Credit Eligible Get Permission

Geisinger

NUANCE

Lesson Learned

- Weak account termination procedure
- Lack monitoring
- Poor vendor management

Lesson Learned

- Everything is breakable!
- Need contingency and backup systems

Unexpected disruption

CrowdStrike outage hits US hospitals

The cybersecurity firm released what was meant to be a routine software update, but now health systems, including CommonSpirit Health and Cleveland Clinic, are locked out of Windows systems.

Published July 19, 2024

By Susanna Vogel
Staff Reporter

Case Study – External Threats


ODYSSEY
cybersecurity

WHY ODYSSEY OUR APPROACH SOLUTION
RESOURCES WHO W

Ransomware attacks targeting Healthcare Organizations on the Rise

Threat Level Description

Threat Level: High – An attack is highly likely. Additional and sustainable protective measures reflecting the broad nature of the threat combined with specific busines geographical vulnerabilities and judgments on acceptable risk.

Description

We have observed a rise in ransomware attacks targeting hospitals, Health Care in Insurance organizations in Middle East and US.

These attacks could result not only in money extortion, but also in Critical Data exp leakages of patients' files (profile, medical history, social number), financial and le

We have identified that two ransomware families are commonly used by the

Ransomware attack on the rise

Lesson Learned

- Cyber attack does not require sophisticated skills and anyone can initiate attacks easily.

Cyber Attack Price List –

- **Phishing Kit from Dark Web: USD $5 -100**
- **Email Spoofing Tools : $10-50**
- **Infrastructure cost : $200-500**

Potential Return –
- 10X !

Case Study – External Threats

Lesson Learned

- Hong Kong SMEs are considered easy targets!

Use CIA Triad to safeguard information security

Objectives of Security

機密性

可用性　　完整性

3 key principles are essential for protecting information from cyber attacks -

Confidentiality - the ability to keep information secret from unauthorized individuals.

Integrity - the ability to ensure that information is accurate and complete..

Availability - the ability to ensure that information is accessible to authorized individuals when needed.

Elevating Security Standard in eHealth ECO systems through participation & sharing

- **Security by Design**
- **Privacy by default**
- **Zero Trust**
- **Role-based access**
- **End-to-end protection**
- **Continuous monitoring**
- **Business Continuity**

Framework to enhance Cybersecurity protection in eHealth ECO System

Governance, compliance Funding, management responsibilities

Regular assessment to identify threats and prioritize mitigation measures

Implement controls and continuous monitoring. Regularly review effectiveness

Develop risk respond playbook. Ensure actionable BCP/backup & recovery plan. Conduct regular drills & external assessments

People are always "the weakest link" in cyber security. Regular training is a must.

Be vigilant about supply chain risk

Know your risk through assessment – Security Risk Assessment

Risk Assessment Process

Risk assessment & treatment

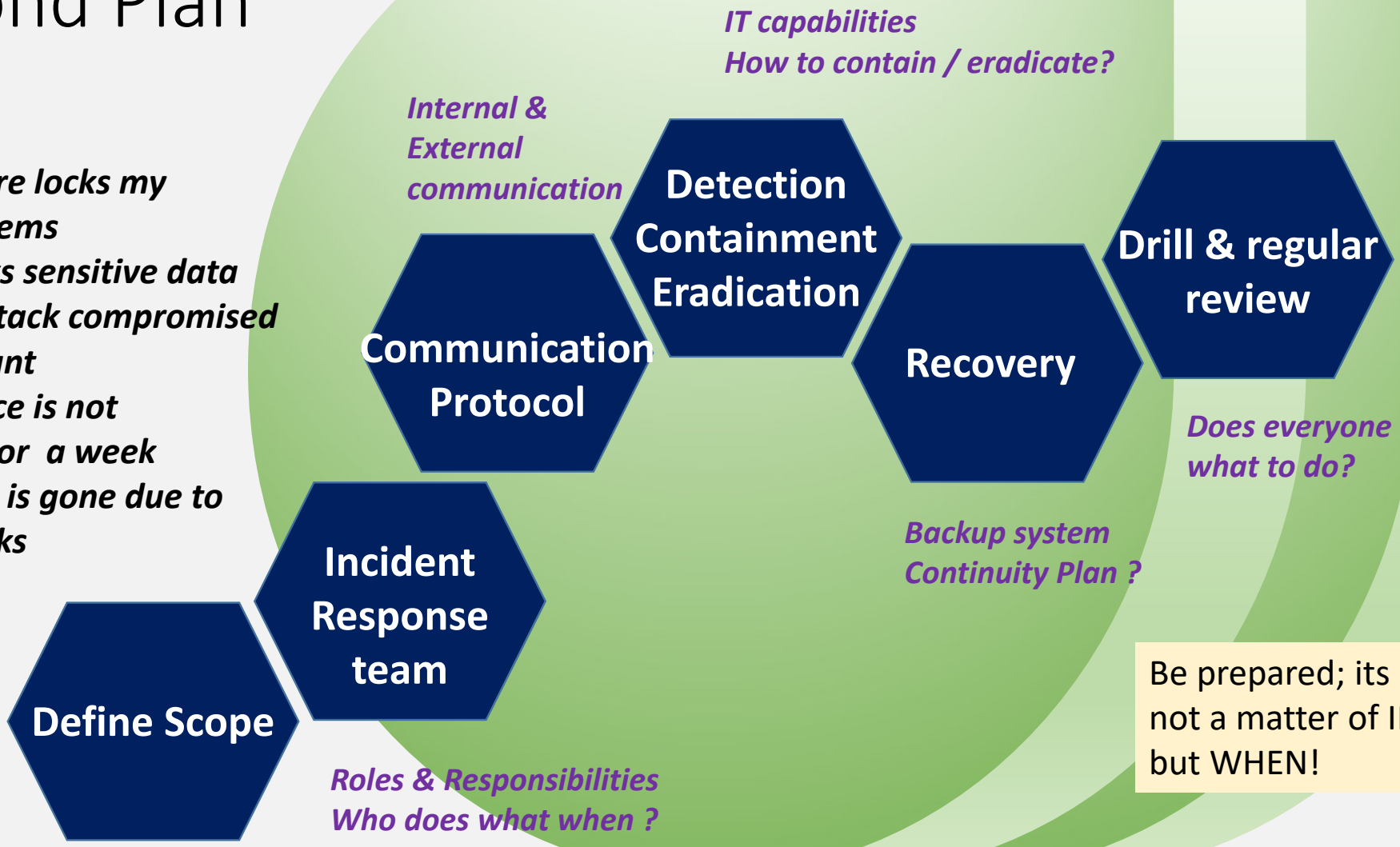
Risk Exposure	+	Business Impact	=	Inherent Risk
Inherent Risk	-	Risk Control Activities	=	Expected Risk
Expected Risk	x	Control Effectiveness	=	Actual Risk
Actual Risk	-	Risk Treatment Plan	=	Acceptable Risk

Reference : ISO27001

Formulate your “What-if” Cyber Security Risk Respond Plan

What If

- ***Ransomware locks my clinical systems***
- ***Insider leaks sensitive data***
- ***Phishing attack compromised CFO’s account***
- ***Cloud service is not accessible for a week***
- ***All my data is gone due to cyber attacks***
- ***..***



Be prepared; its not a matter of IF, but WHEN!

Cyber-security Tips

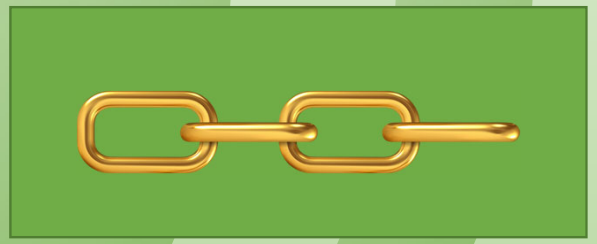
Immunize your computer asset
- Anti-virus
- Backup

Protect against ransomware
- Update your software
- Beware of suspicious email / links

Beware of emerging risk
- Understand your risk exposure
- Proper control & protection

Incident Respond
- Awareness Training &
- Well-defined procedure

Password
- Enable multi-factors password
- Don't share



Beware of supply chain attack
- Due diligence on suppliers
- Access Control
- Respond plan

https://www.ehealth.gov.hk/en/healthcare-provider-and-professional/resources/cyber-security/index.html

Key takeaways

Beware of both insider and external threats

Cost of cyber attack is low & cybercriminals seek easy targets !

Be prepared, its not a matter of IF, but WHEN

THANK YOU

Cybersecurity is a never-ending battle.

Its not about winning but NOT loosing.

Stand together against cybercriminals