



Keeping EHR Safe

ERIC WONG

Senior System Manager

2019-09-13



Quest Diagnostics Says Up to 12 Million Patients May Have Had Financial, Medical, Personal Information Breached

It includes credit card numbers and bank account information, according to a filing

Published Jun 3, 2019 at 8:49 AM | Updated at 7:38 PM EDT on Jun 4, 2019

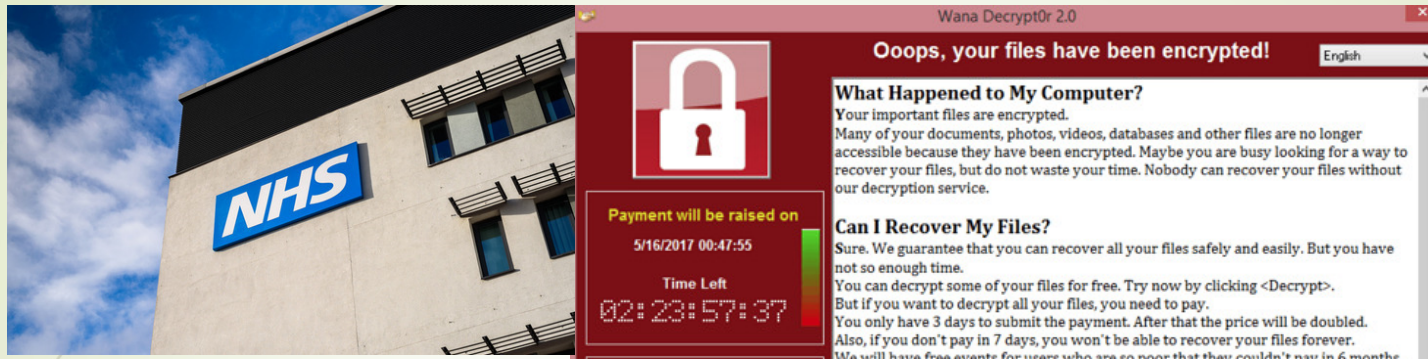
Summary

- In June 2019, 12M patients records including Credit Cards, Personal data and medical information was stolen
- The breach was a result of malicious activity on a third-party collections vendor named American Medical Collection Agency (AMCA)
- At the time of hacking, AMCA payment site **did not enforce encryption** and also used wrong certificate when manually switch to secure connection
- The breach lasted 8 months from August 1, 2018 until March 30, 2019
- Multiple lawsuits filed for Quest and AMCA. AMCA has filed bankruptcy protection

SingHealth Cyberattack July 2018

Summary

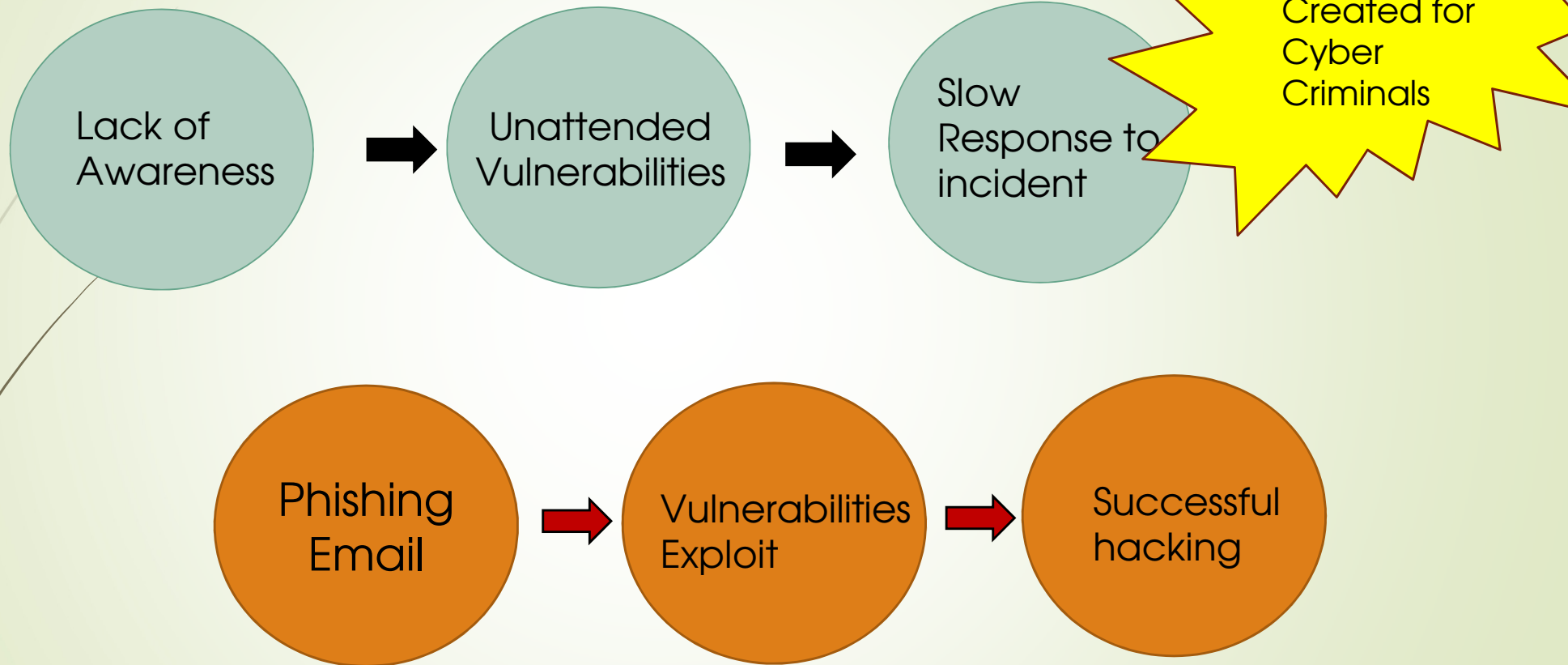
- In July 2018, 1.5M Patient and medical records including Prime Minister was hacked
- Initial attacks day back to 2017 when a workstation was compromised by **phishing email**.
- Attacks gained privileged access through servers that **had not been patched for 14 months**
- Senior manager **reluctant to report** suspicious activities to avoid pressure from top and also not sure about his role in reporting security incident



Summary

- The WannaCry cyber attack began on the morning of Friday 12 May 2017, affected 4.7% of all NHS computers running **Windows XP or unpatched Windows 7**
- The attack targeted known Windows vulnerabilities but the patch had been made available 2 months before the attacks
- Cancelled 19,000 appointments and cost £92m to clean-up
- As of today, NHS admitted there are still over 2300 workstations running 17 years old Windows XP, 2 years after WannaCry attack

Similarity of these incidents



Takeaways



Cyberworld is full of dangers and traps

Inaction / inattentive to vulnerabilities = open invitation to hackers

Be cyber resilience!

The Hacking Economy

71% of Ransomware Attacks Targeted Small Businesses in 2018

Ransomware attacks hit healthcare the hardest last year, with small to medium sized businesses targeted most by hackers due to fewer security resources than their larger counterparts.



Patient medical records sell for \$1K on dark web

Mackenzie Garrity - Wednesday, February 20th, 2019 [Print](#) | [Email](#)

[SHARE](#) [Tweet](#) [Share 21](#)

Healthcare data protection company Protenus revealed there were 222 hacking incidents in 2018, up nearly 25 percent from 2017. Of these data breaches, more than 11 million patient records were affected, *CBS News* reports.

Often these patient records can be found on the dark web or black market. Sellers offering patient records promote they have gained access to the medical information through hacking a hospital or payer database.

One seller offered children's health records from a pediatrician. Another dark web post advertised for an entire Georgia hospital database, filled with 397,000 patient records.

Patient records can sell for up to \$1,000 due to the amount of information found in the documents, including date of birth, credit card information, Social Security number, address and email. Social Security numbers can be purchased for as little as \$1, and credit card information sells for up to \$110, according to *CBS News*.

Of the patients who have their medical records compromised, many are left grappling with the effects years later.

Social Security Number : US\$1
Identity Proof : US\$ 30
Credit Card # : US\$ 110
Online Banking : US\$160
Medical Records : US\$ 1000

Attacks on healthcare are expected to increase by

400%

in 2020



The cost of cyber crime is expected to exceed

\$6 Trillion

Annually by 2021



SURFACE WEB

Bing

Google

4%

Wikipedia

DEEP WEB

(not accessible to Surface Web crawlers)

Medical Records

Legal Documents

Scientific Reports

Subscription Information

Competitor Websites

Academic Information

Multilingual Databases

Financial Records

Government Resources

Organisation-specific Repositories

90%

DARK WEB

(only accessible through certain browsers such as TOR. Deep web technologies has zero involvement with the Dark Web)

TOR Encrypted sites

Drug Trafficking

Private Communications

Political Protests

Illegal Information

6%

A hand holding a stack of cash, with the text overlaid. The background is a teal gradient. The hand is dark, and the cash is a lighter shade of teal. The text is white and bold.

Cybercrime black markets: Dark web services and their prices

A closer look at cybercrime as a service on the dark web

Ransomware-as-a-Service

The screenshot displays the Ranion ransomware website, which is hosted on a .onion domain. The page features a header with the Ranion logo and the text "RANION - Better & Cheapest FUD". Below the header, there are links for "BUY - FAQ - REVIEW". The main content area includes a disclaimer: "DISCLAIMER: Our Products are, Don't use them for illegal activities. Y Our Products/Services are sold". A table titled "PACKAGES COMPARISON" lists various features and their availability across four subscription packages: Package #3, Package #2, Package #1, and Package #ELITE. The features include Subscription, Darknet C&C Dashboard, Features (Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer), Offline Encryption, Support, Real-Time Client Manager, Dropper, Clone, FUD+Obfuscator, Unkillable Process, FUD Stub #, and Price.

RANION - Better & Cheapest FUD

[BUY](#) - [FAQ](#) - [REVIEW](#)

*We provide an already configured and ready to use ransomware.
We are the only that provide a FREE Anonymizer.
We also provide additional FREE Customization.*

DISCLAIMER: Our Products are,
Don't use them for illegal activities. Y
Our Products/Services are sold

PACKAGES COMPARISON

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	12
Price	120 USD	490 USD	900 USD	1900 USD

Image 2: Subscription plans offered by cybercriminals for Ranion ransomware

Selling Access to Servers

UAS - Ultimate Anonymity Services

Country: Colombia State: Select State City: Select City ZIP: Select ZIP

ISP: Select ISP OS: Select OS Resell: Yes

Direct IP: No Admin Rights: No No PayPal: No No Poker: No

Port: 80: No Port: 25: No

Search Reset

Total found: 250

Items per page: 50



IP	Country	State	City	ZIP	OS	RAM	Dwn.	UpL.	Direct IP	Admin Rights	Added	Price, \$
181.51.*.*	CO	Atlantico	Barranquilla	-	Windows Server 2008	--	7.82 Mbit/s	5.47 Mbit/s			24.10.2018	10.00
190.29.*.*	CO	Antioquia	Medellin	-	Windows 7 Professional	--	10.65 Mbit/s	7.45 Mbit/s			5.10.2018	10.00
190.67.*.*	CO	Distrito Capital de Bogota	Bogota	-	Windows Server 2008 R2 Standard	--	5.98 Mbit/s	4.19 Mbit/s	✓		25.10.2018	10.00
200.24.*.*	CO	Caldas	Manizales	-	Windows Server 2012 Standard	--	8.36 Mbit/s	5.85 Mbit/s			5.10.2018	9.00

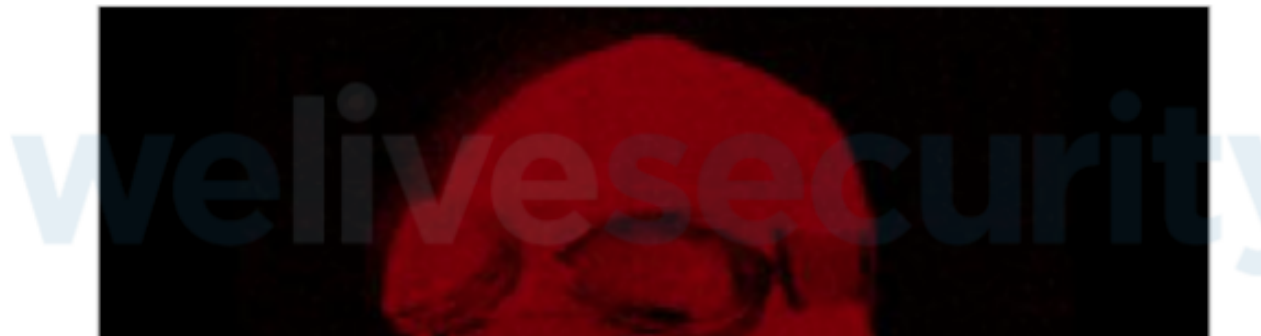
You don't want your computers listed in the market place



DDoS-as-a-Service

3 hours ddos botnet attack (~ 200k requests / sec)

Vendor  (760) (4.97★) 
Price ฿0.00911 (\$57.772)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow No





Takeaways

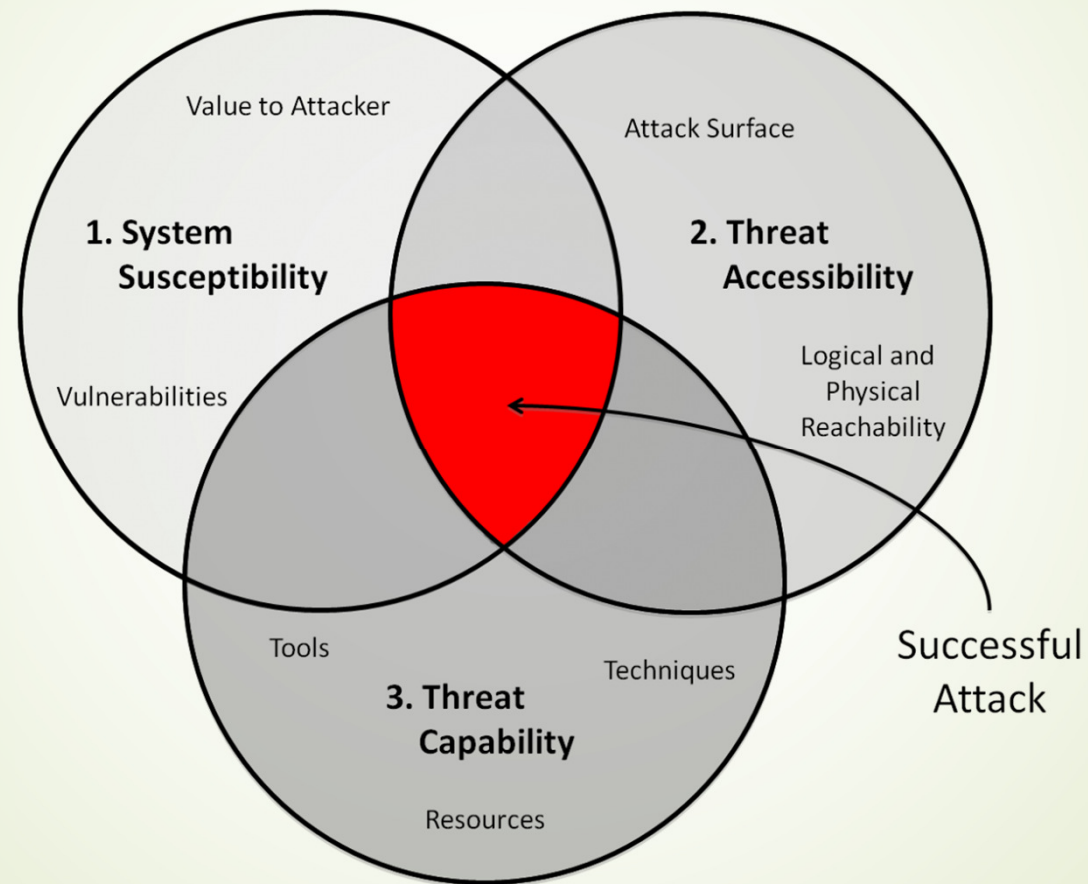


Cybercrime has become a commodity

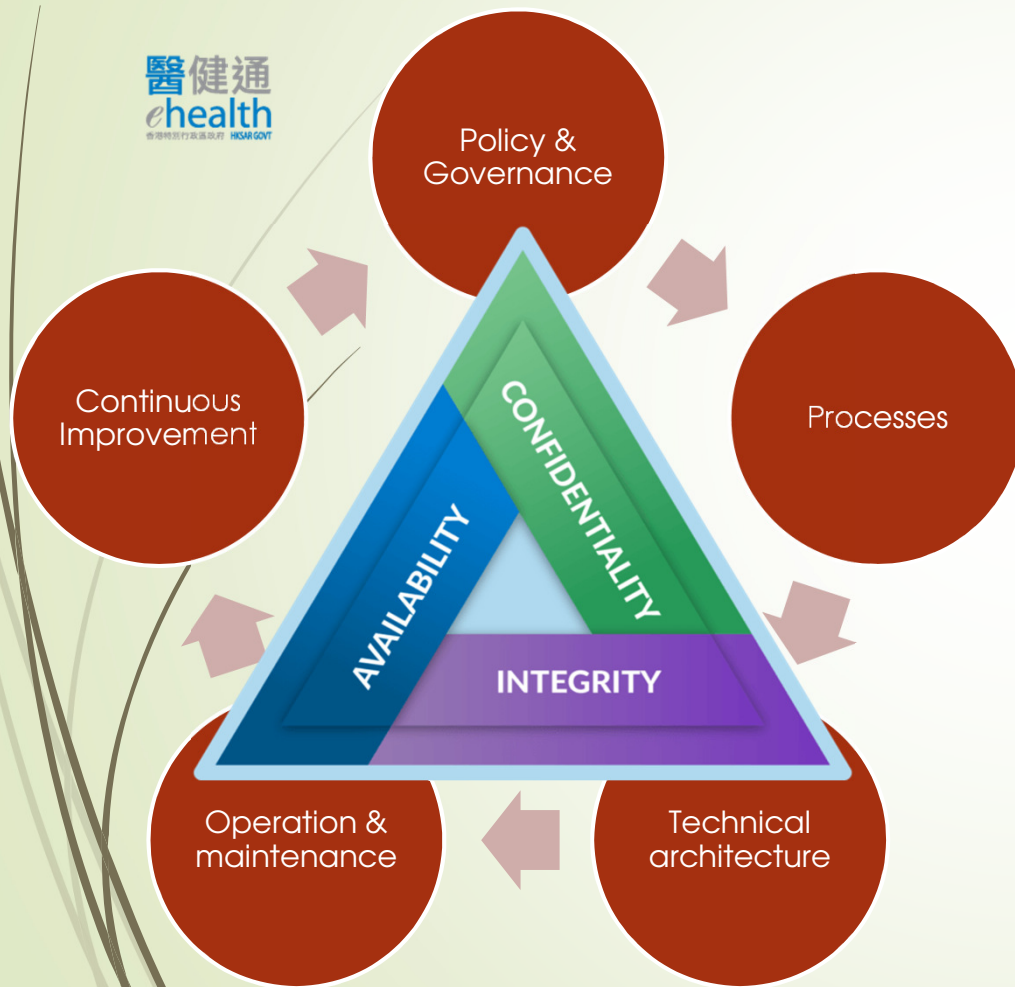
Healthcare data theft is lucrative and easy

Be cyber resilience!

Cyber security is an end-less Tug-of-War



Key Objectives of eHR Security



➤ Confidentiality

- Ensuring that information is accessible only to those authorised to have access
- Compliance with eHR Ordinance & PDPO

➤ Integrity

- Safeguarding the accuracy and completeness of information and processing methods

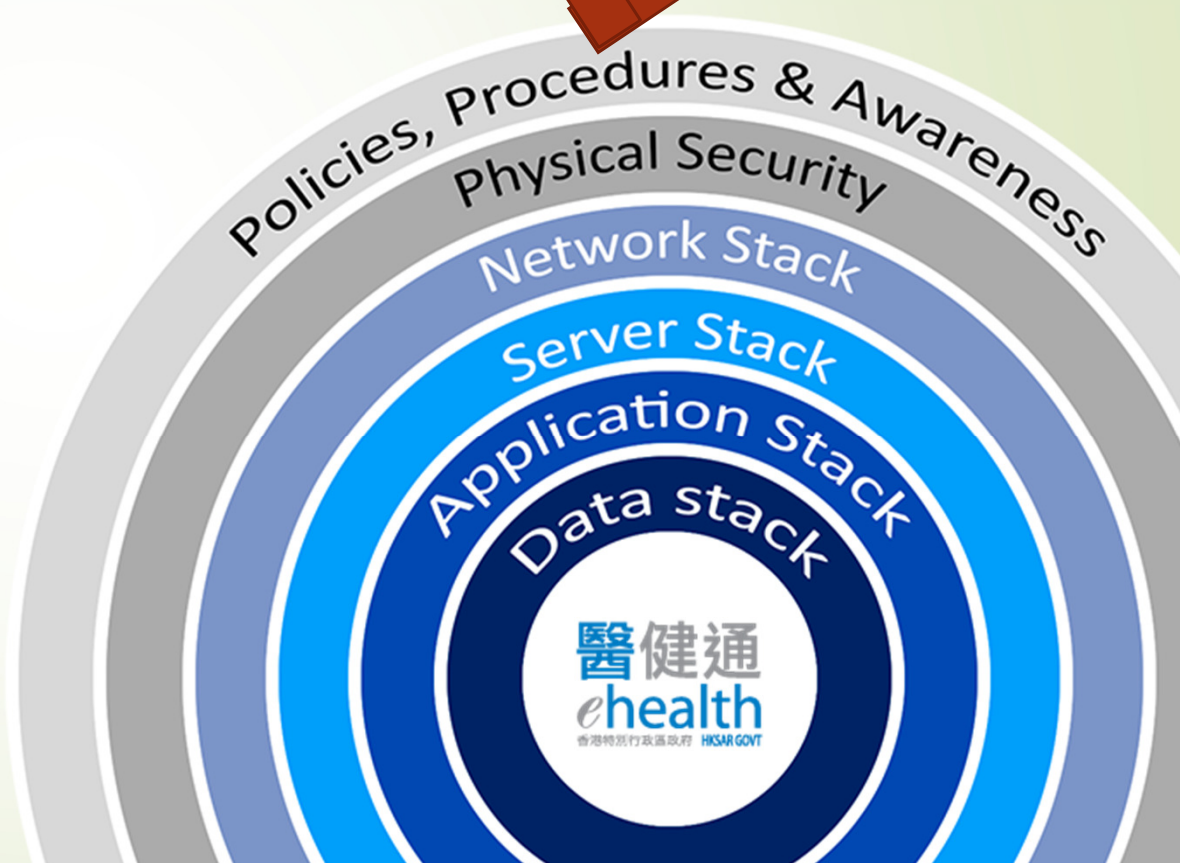
➤ Availability

- Ensuring that authorised users have access to information and associated assets when required
- Ensuring the overall system reliability

Security by Design

- Defence In Depth
- Minimize attack surface
- External is insecure
- Business Continuity
- Monitoring & Audit

Fortify and
defend against
known threats



Strong Access Control and Traceability

- Least Privilege Access
- Separation of duties
- Privacy by default
- Fully audit on all control
- Notification to patients



On going monitoring & threat detection



Service Level
Reports



Security
Dashboards



System
Recommendations



Interface
Monitor



Security
Alerts

- The operation of eHRSS is ISO 27001 certified
- But no system is invincible !
- Exercise of due diligent, regular review etc. is critical for discovery of unknown threats, eg. Zero day vulnerability
- Regular drills & awareness training turn discipline to habit



Modernized & automated Security Practice

Pave way to a new era....

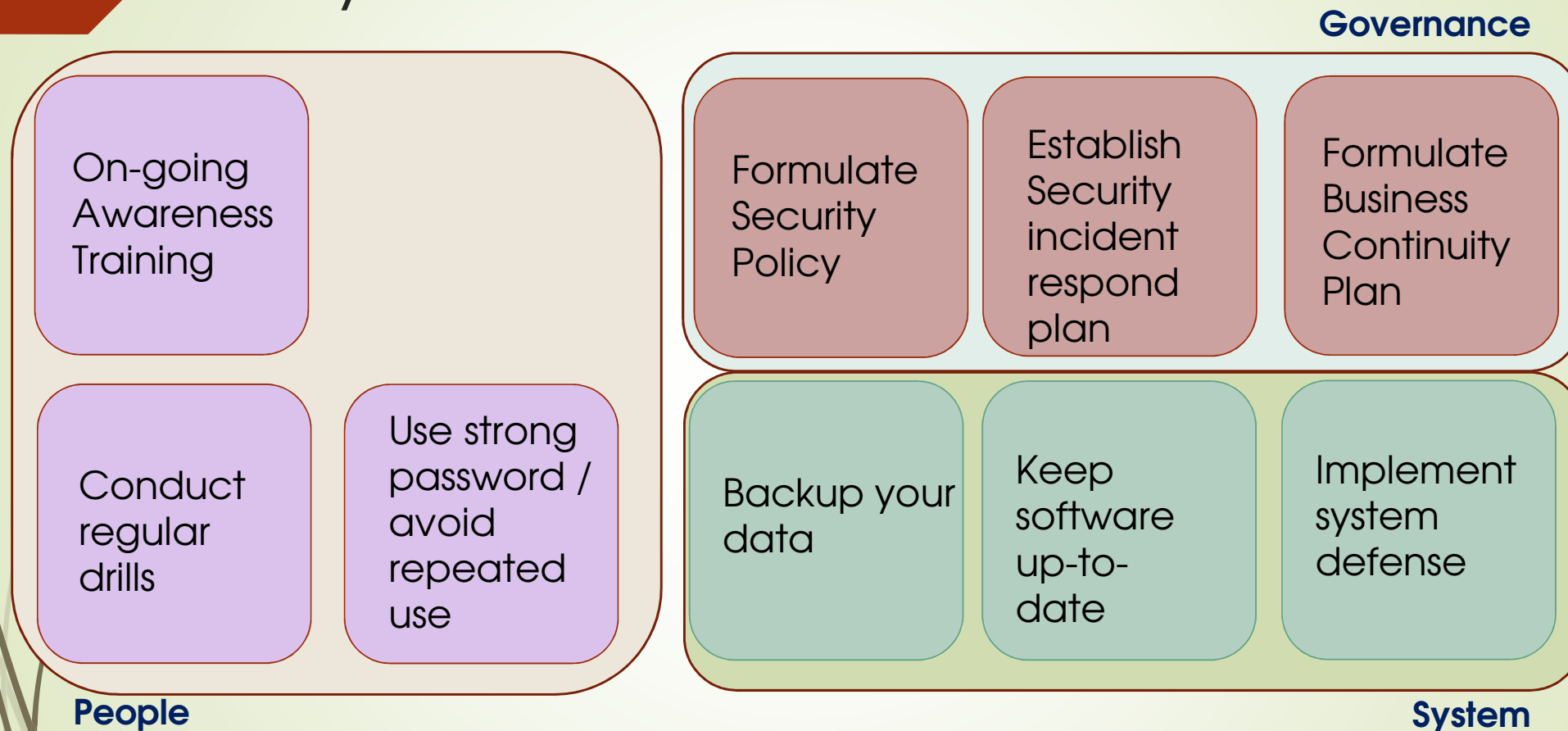


Vulnerability Alerts
Guidance &

Attack Protection &
Threat Intelligence



Be Cyber Resilience



Be prepared for hack!

Key takeaways

A graphic featuring a background of blue and black binary code (0s and 1s). A large, stylized red padlock is positioned on the left side, partially overlapping the text boxes. The text is presented in two stacked dark blue rectangular boxes with white, bold, sans-serif font.

CYBERSECURITY

**EVERYONE MUST
SHARE THE
RESPONSIBILITY**

- Maintain cyber hygiene
- eHR is a ecosystem and keeping eHR Safe is everyone's responsibility
- Be cyber resilience!



THANK YOU