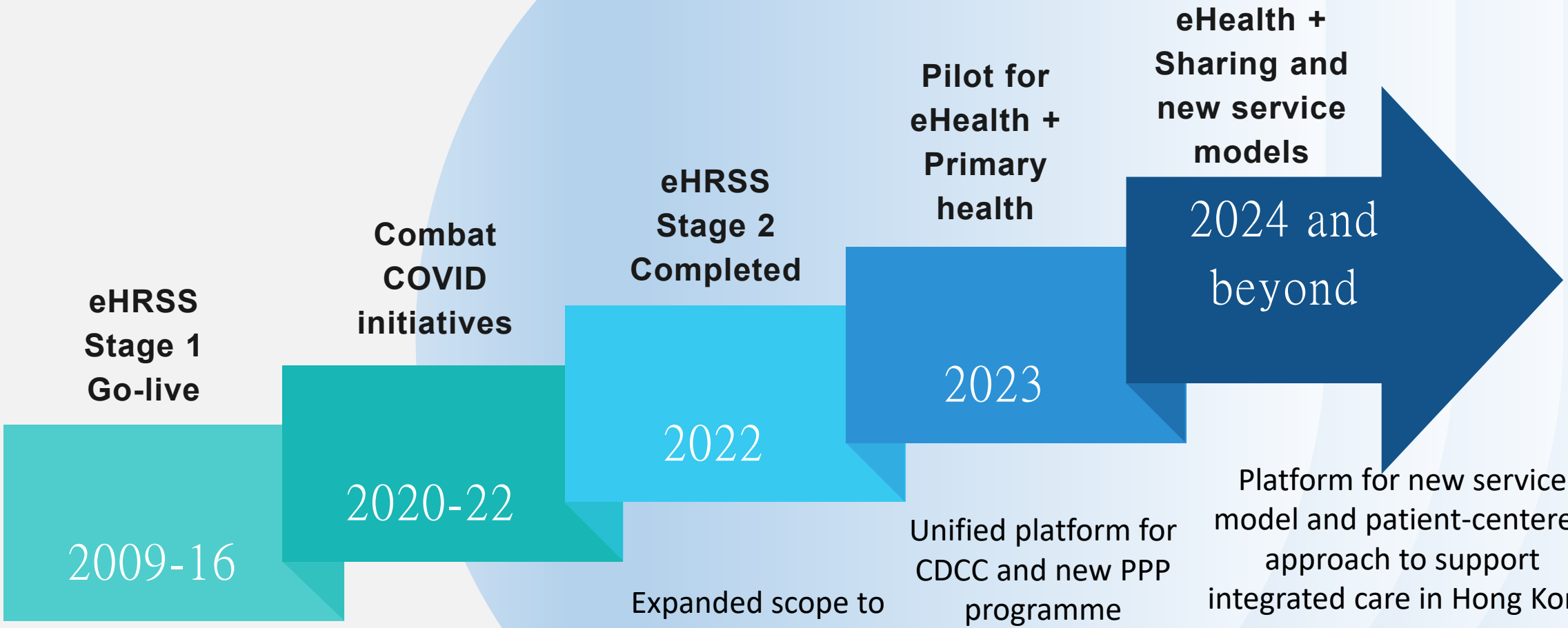
Building a Secure and Connected Healthcare ECO System in Hong Kong – the Journey from eHRSS to eHealth+ and beyond

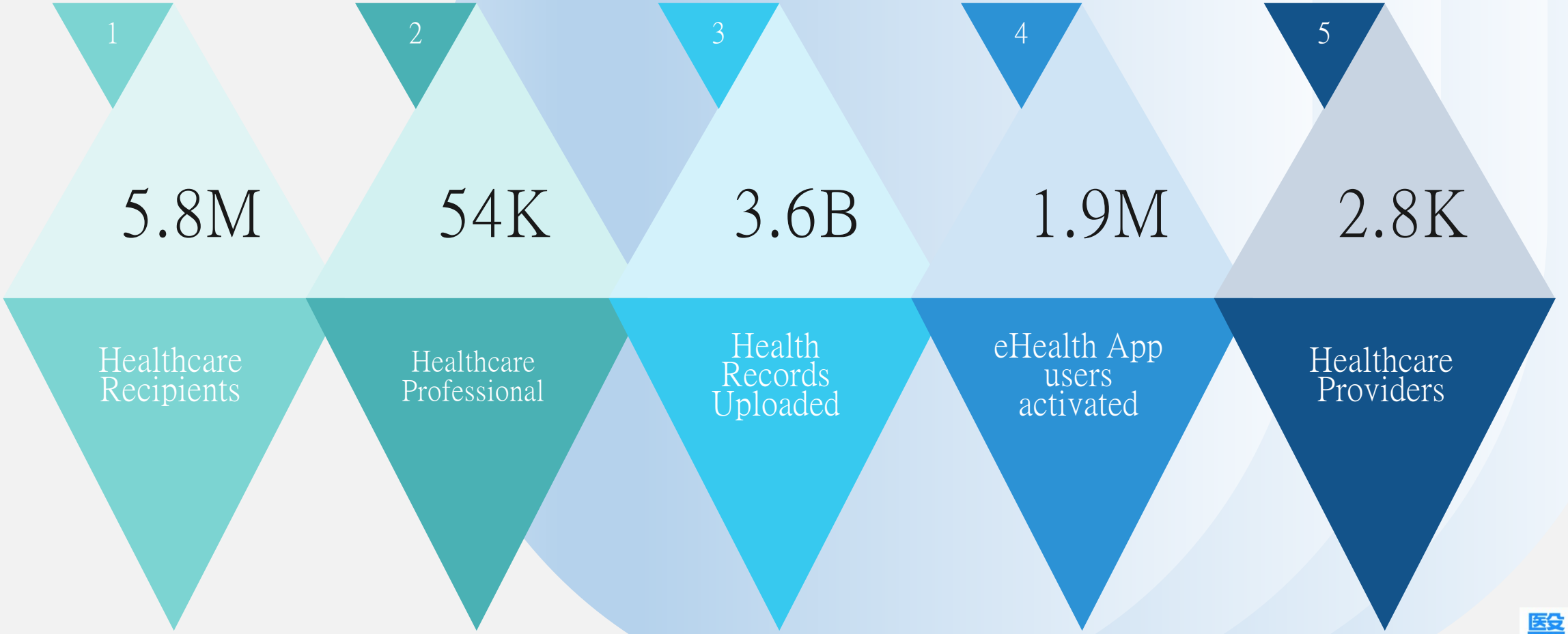
在香港建立安全及聯繫的醫療保健生態系統 - 從 eHRSS 到 eHealth+ 及未來的旅程

Eric Wong
HAIT
2023-10-03

From eHRSS to eHealth +



eHRSS Participations



From eHRSS to eHealth + and beyond

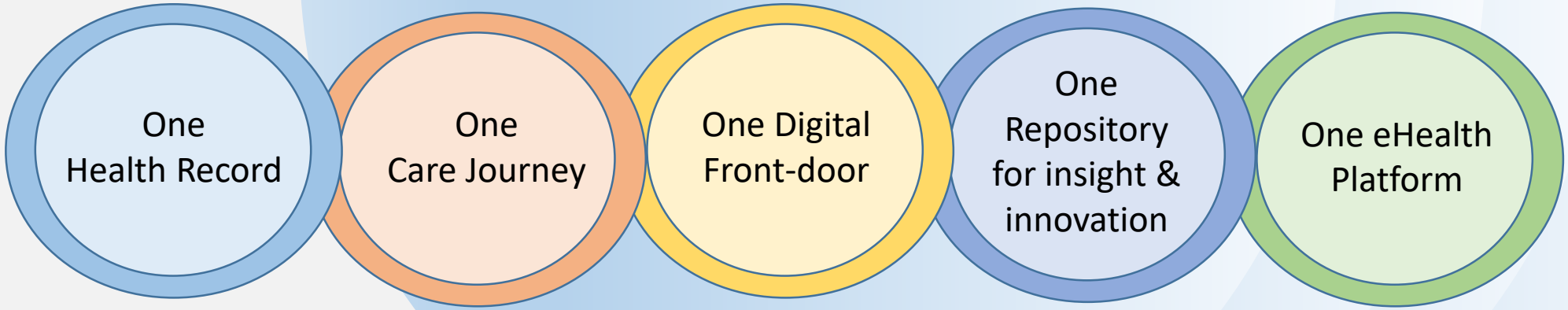
Vision

To be a comprehensive and integrated health information infrastructure that ultimately support the provision of safe, efficient, and quality healthcare with better health outcomes for Hong Kong citizens

Mission

To be an enabler for enhancing care coordination, active health management, cross-sector collaboration and health surveillance, bring about a seamless and personalized care experience for each individual

Goals



One Health Record	One Care Journey	One Digital Front-door	One Repository for insight & innovation	One eHealth Platform
Encourage data contribution build life-long eHR Profile	Continuity of care, coordination and referral. GBA collaboration	Individual access, self-health management	Eco-system development, innovative services	Modern digital health platform for all eHealth services

Integrated Eco-system Supported by eHealth+

eHealth App as a "Digital-Front-Door" for empowerment

Extend PPP / DHC/ CDCC / SP/ Primary Care service and sharing scope

Medical Domain integration
Western to Allied Health to Chinese Medicine

Vertical integration
Primary to Secondary to Tertiary

Tertiary

Secondary

Primary

DHC / CDCC

Public / DH services

Medico-Social Services

Private healthcare

Self-Care MyCarer

Telehealth enable new service capabilities

eHealth as central data hub* for research and analytics
Data Linkage with HCPs, Insurance and B&D

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

Cross border data access and download

*Transactional, Financial, Health Information and Time Relation

Real-time Threat map

Cyber attacks, an increasingly imminent and ongoing threat, continues to shape the landscape of global security and necessitates our constant vigilance for the sake of preserving the integrity of our digital infrastructure.

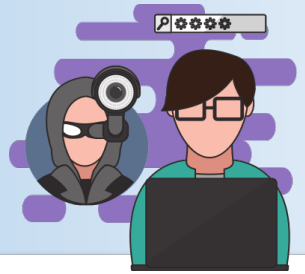
There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.

MAP | Kaspersky Cyberthreat real-time map

Live Cyber Threat Map | Check Point

Live Cyber Attack Threat Map | Radware

Healthcare industry is a lucrative market to cyber attack



CommonSpirit Health Confirms System Outages Caused by Ransomware Attack

Posted By Steve Alder on Oct 13, 2022

On October 3, 2022, CommonSpirit Health experienced a data security incident that forced it to take systems offline, including its electronic medical record (EHR) and other critical IT systems. These steps were taken to protect systems from damage, contain the breach, and prevent unauthorized access to sensitive data. CommonSpirit Health issued a statement on October 4, 2022, that provided a brief explanation of the incident, stating there was an IT issue that was being investigated that had resulted in system outages at some of its hospitals and care facilities. CommonSpirit Health is one of the nation's largest health systems and is the second-largest non-profit health system in the United States, consisting of around 1,500 clinics and hospitals in 21 states. CommonSpirit Health was formed by the merger of CHI Health and Dignity Health in 2019.

Community First Medical Center Suffers 216K-Record Data Breach

Posted By Steve Alder on Sep 28, 2023

Community First Medical Center in Chicago, IL, has started notifying 216,047 patients about a cyberattack that saw an unauthorized third party gain access to its computer systems on July 12, 2023. According to the September 26, 2023, breach notifications, a forensic investigation was launched that determined on July 28, 2023, that the third party had accessed files that contained patients' protected health information.

The types of information compromised in the incident varied from individual to individual and may have included full names, telephone numbers, email addresses, Social Security numbers, medical record numbers, and Medicare numbers. Community First Medical Center said it is unaware of actual or attempted misuse of patient information; however, as a precaution, individuals who had their Social Security numbers exposed have been offered complimentary credit monitoring services. Community First Medical Center said many precautions had been taken prior to the cyberattack to secure patient data and that it will evaluate and modify its security practices to prevent further security breaches.

CareSource Facing Multiple Class Action Lawsuits Over MOVEit Data Breach

Posted By Steve Alder on Sep 27, 2023

The Dayton, OH-based Medicaid and Medicare plan provider, CareSource, is facing multiple class action lawsuits over a recent cyberattack and data breach. The Clop threat group exploited a zero-day vulnerability in the MOVEit Transfer file transfer solution and obtained the protected health information of 3,180,537 individuals, including names, addresses, date of birth, Social Security Numbers, health plan information, medications, and other health information.

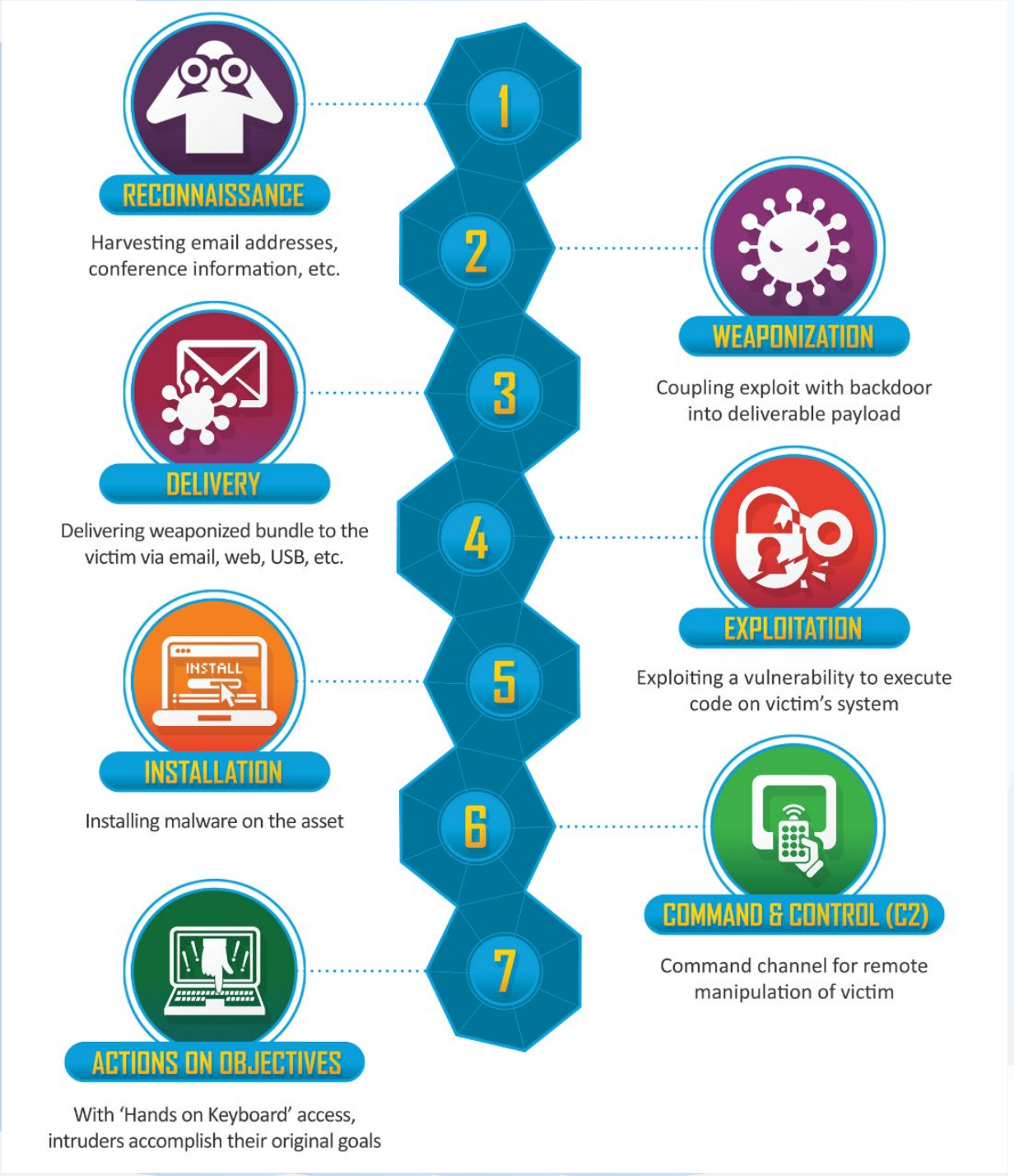
- High value records (USD500-1000 per records)
- Larger attack surfaces (legacy system, multiple entry points)
- Double extortion
- Relatively less protected

Source THE HIPAA JOURNAL

醫健通 ehealth 香港特別行政區政府 HKSAR GOVT

How attackers gain access to your systems

- **The Cyber Kill Chain (CKC) is a seven-stage model of a cyber attack, developed by Lockheed Martin in 2011.**
- **A popular way for cyber criminals to launch attacks**
- **Cyber criminals leverage AI to develop even more sophisticated attacks**



Use CIA Triad to safeguard information security

Cyber Security threats

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

Objectives of Security

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

Confidentiality - the ability to keep information secret from unauthorized individuals. This can be achieved through encryption, access control, and other security measures.

Integrity - the ability to ensure that information is accurate and complete. This can be achieved through checksums, digital signatures, and other security measures.

Availability - the ability to ensure that information is accessible to authorized individuals when needed. This can be achieved through redundancy, disaster recovery, and other security measures.

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

Supply-chain attacks – medical devices, IoT and commercial systems

The Risk of Log4j Vulnerabilities to Healthcare Organizations

Log4j vulnerabilities present a significant risk to the healthcare industry. In January 2022, the Office of Information Security at the Department of Health and Human Services released a threat brief about the Log4j vulnerabilities in the healthcare sector. It noted that while no healthcare company has yet reported a major compromise, the industry remains "highly vulnerable."

One reason for the heightened risk is that healthcare institutions typically have a large variety of devices and back-end systems, some of which can be more than a decade old. This complexity and volume of endpoints can make it challenging to find and identify vulnerabilities, says McKee.

"It could be a pump, a patient monitor or a back-end system like Epic," he explains. "The challenge is understanding where they are vulnerable, where they are using it and how it affects their network."

In 2021, the Kaseya ransomware attack targeted a software vendor that provides software to healthcare organizations. The Kaseya ransomware attack encrypted data on the software vendor's systems, which made it difficult or impossible for healthcare organizations to access their software.

Prevention & Protection

- Conduct due diligence on suppliers to assess their security posture.
- Implement security controls to protect against supply chain attacks, such as multi-factor authentication and data encryption.
- Have ***incident response plan*** in place to respond to supply chain attacks.

Risks of cloud services

Microsoft worker accidentally exposes 38TB of sensitive data in GitHub blunder

Included secrets, private keys, passwords, 30,000+ internal Teams messages

Jessica Lyons Hardcastle — Mon 18 Sep 2023 // 18:03 UTC

A Microsoft employee accidentally exposed 38 terabytes of private data while publishing a bucket of open-source AI training data on GitHub, according to Wiz security researchers who spotted the leaky account and reported it to the Windows giant.

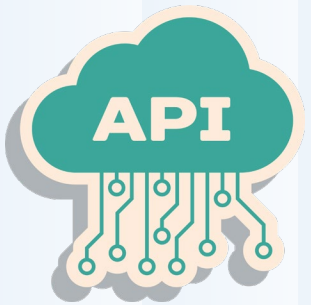
Redmond, in a Monday write-up, downplayed the blunder, saying it was merely "sharing the learnings" to help customers avoid making similar mistakes. This is despite Wiz claiming the leaky data bucket had private keys, passwords, and over 30,000 internal Microsoft Teams messages, as well as backup data from two employees' workstations.

Prevention & Protection

- Zero-trust (including Vendor)
- Protect remote access
- Continuous scanning & monitoring
- Timely respond to abnormally

- Have ***incident response plan*** in place to respond to supply chain attacks.

Increasing connectivity increases security exposure



79% Of Healthcare Organizations Experienced an API Security Incident in the Past 12 Months

Posted By Steve Alder on Sep 29, 2023

78% of healthcare organizations experienced an Application Programming Interface (API) security incident in the past 12 months, up 9% from 2022, according to a new survey from Noname Security.

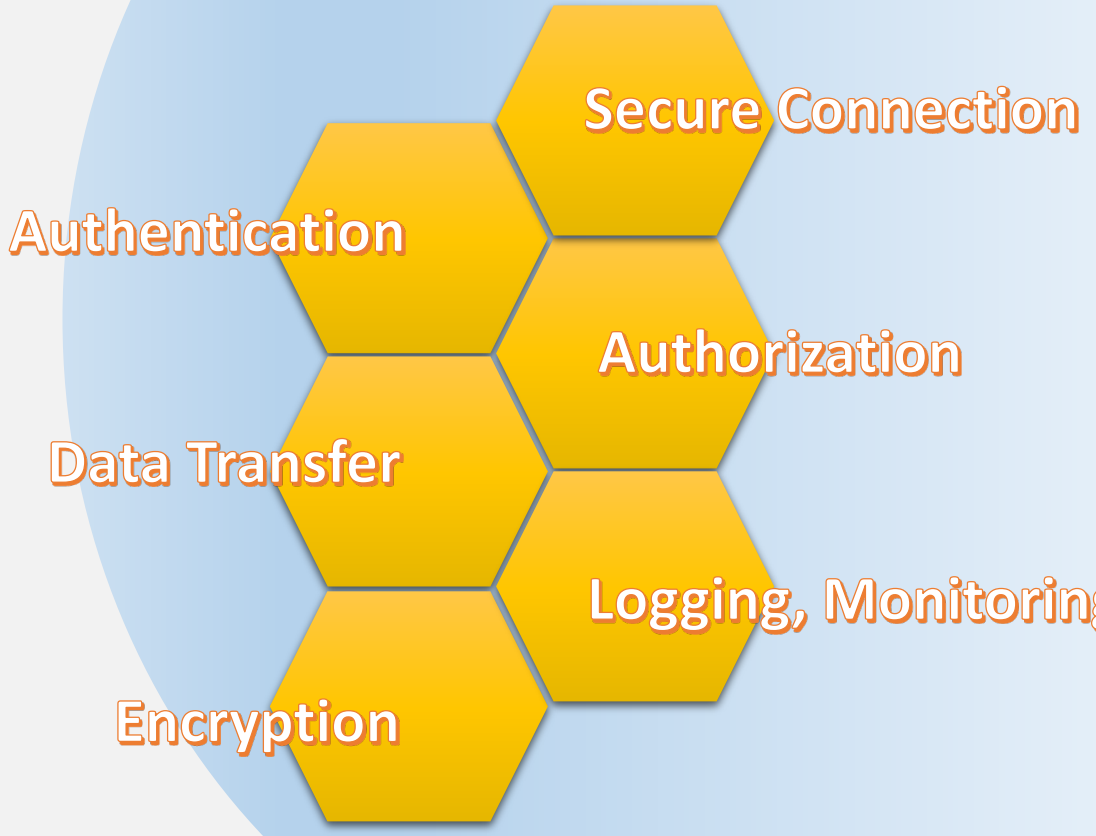
APIs continue to pose significant risks to organizations and security incidents are increasing, especially in industries that store large volumes of personally identifiable information such as healthcare, eCommerce, and financial services, which saw the biggest increases in attacks. Healthcare experienced the biggest increase in API security incidents out of the 6 industries represented in the study and is the second most likely industry to experience an API security incident, behind financial services.

Source: https://www.hipaajournal.com/79-of-healthcare-organizations-experienced-an-api-security-incident-in-the-past-12-months/

How IT system ensure secure exchange of sensitive systems

- Established encrypted channel for secure data transmission
- Use digital certificate to verity identity

- Verify individual identity with user/name password
- Multi-factor authentication



- What records can be accessed
- Consent given by participant
- Need-to-know basis

- Conformance to data standard
- Transfer of data using agreed protocol
- Acknowledgement of receipt of data

- Use strong encryption to protect data-at-rest

- Trail of access & event – forensic evidence
- Troubleshooting
- Monitoring of abnormally
- Compliance
- Policy violation

ChatGPT Opportunities and Risks

Opportunities
- Patient Summary
- Clinical Decision Support
- Medical translation – coding
- Virtual Assistance
- Provide relevant clinical guidelines
- Remote patient monitoring

Risks
- Privacy and safety
- Current model has limited medical knowledge
- Misinformation & hallucinations
- Liability

Need Policies for use of ChatGPT at Work

1. Never input sensitive information / patient details
2. Verify source of information
3. Know its limitation
4. Be wary of copyrighted material
5. Take full responsibility of generated works

Cyber-security Tips

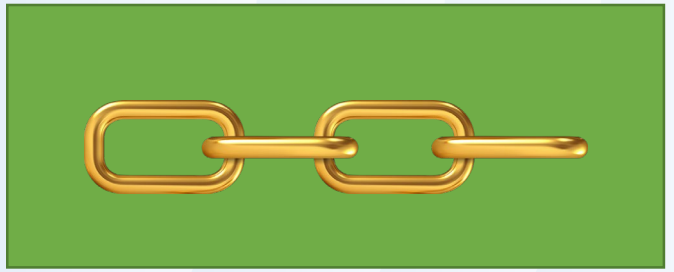
Immunize your computer asset
- Anti-virus
- Backup

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

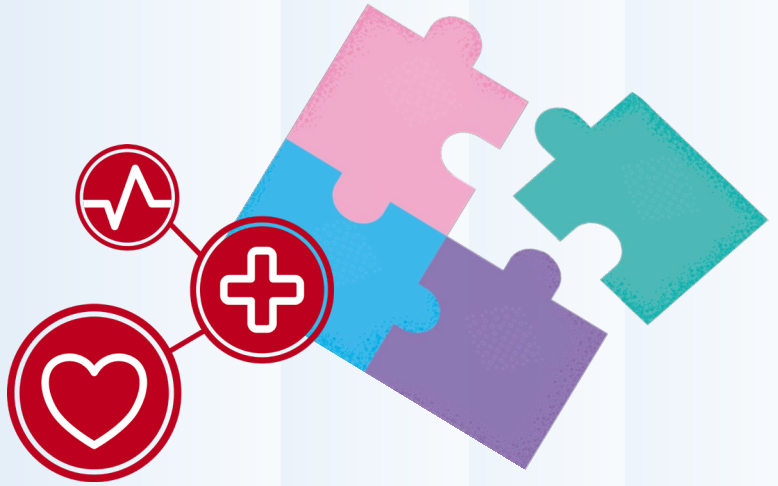
Password
- Enable multi-factors password
- Don't share



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

Thank You



In our connected eco-system, Cyber Defense is Everyone's Duty !

[網絡安全資訊站-香港|主頁 (cybersecurity.hk)]

[資訊安全網: 網絡安全意識 (infosec.gov.hk)]

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

醫健通 ehealth 香港特別行政區政府 HKSAR GOVT