Defending against the Emerging Cybersecurity Threats and Risk in Healthcare Sector
應對醫療保健業新興的網絡安全威脅和風險

Fuller Yu

Chief Information Security Officer (CISO), Hospital Authority
Co-Chair of Cyber Security Work Stream, Global Digital Health Partnership
Ex-Co Member of Cybersecurity Specialist Group, HK Computer Society

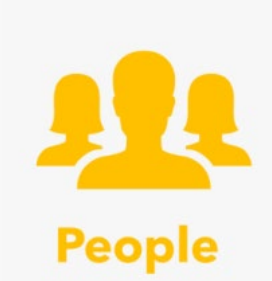
October 2023


The Cyber Landscape in 2023

2023 Predictions on Cyber Landscape Made in Oct 2022

- Ransomware as a service will continue to increase
- Changing ransomware models will lead to changing targets
- Dwell time will continue to decrease
- Supply chain attacks will increase as adversaries compromise partner and supplier ecosystems
- Ransomware will be used as a wiper to destroy data in the increasing geopolitical tensions

Cybersecurity Threats and Challenges in Healthcare Sector

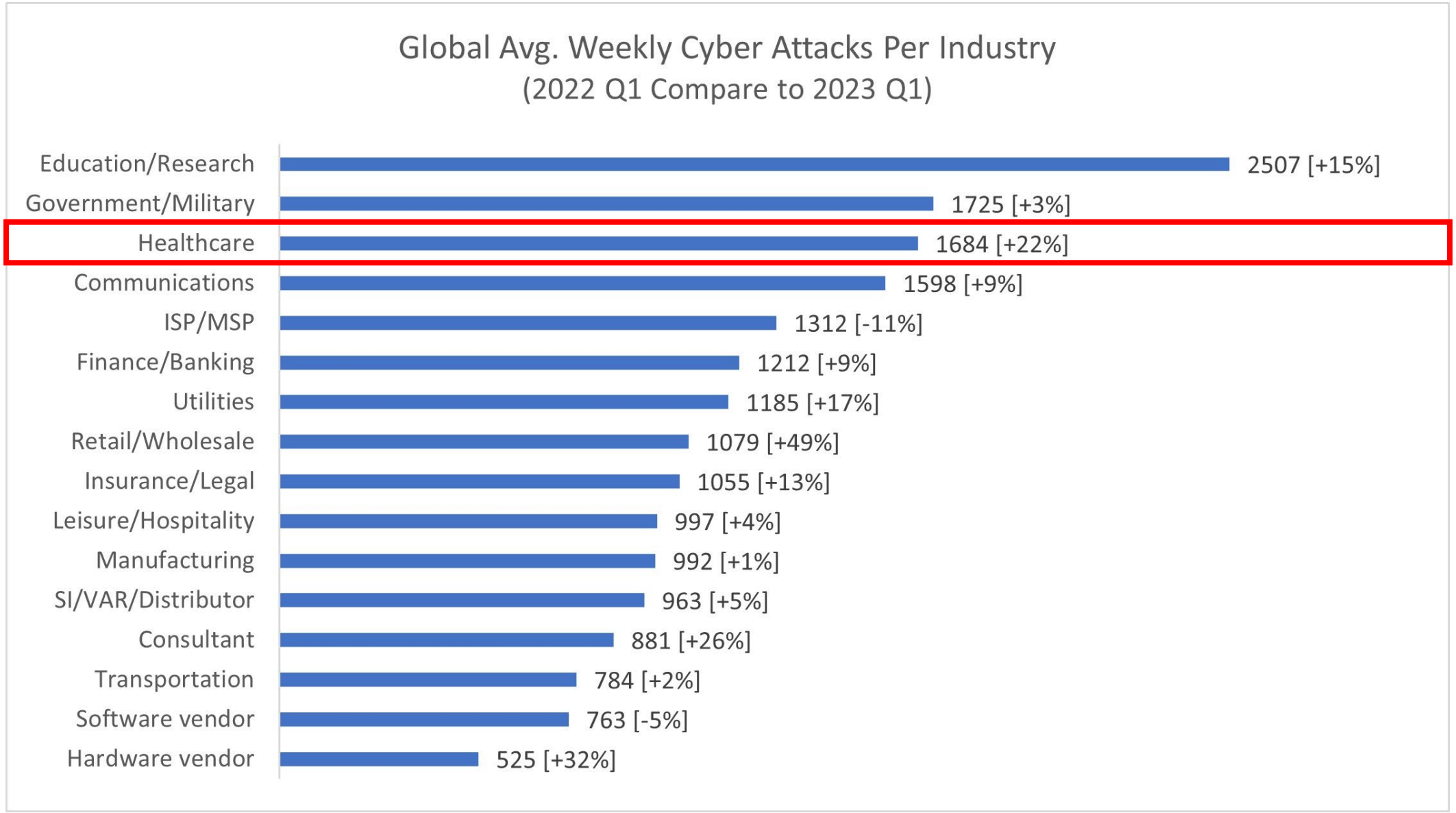


- Low level of cyber literacy among healthcare workers
- Shortage of cybersecurity talents to secure healthcare systems
- High demands on anytime anywhere access to clinical data

- High value of medical data to support business targeted by cyber criminals
- Increased attack surfaces from extended data exchanges
- Inconsistent security control processes and practices

- Clinical systems became mission critical and subject to ransomware attacks
- Inadequate controls on medical devices and legacy systems
- New Risks of emerging technologies (e.g. AI, 5G and IoT)

Healthcare Sector is the Top Target of Cyber Attack Globally in 2023



Source: Check Point Research 2023 Cyber Attack Trend

Ransomware is Prevailing Cyber Threat for Healthcare

- Ransomware attacks are increasing, caused both operational and patient safety impacts
- Healthcare is most likely to pay the ransom compared to other sectors
- Highest loss for 13th consecutive years among all industries at USD$11 Million per incident

BW BUSINESSWORLD

September 10, 2023

Ad served by G

Ad options | Send feedback

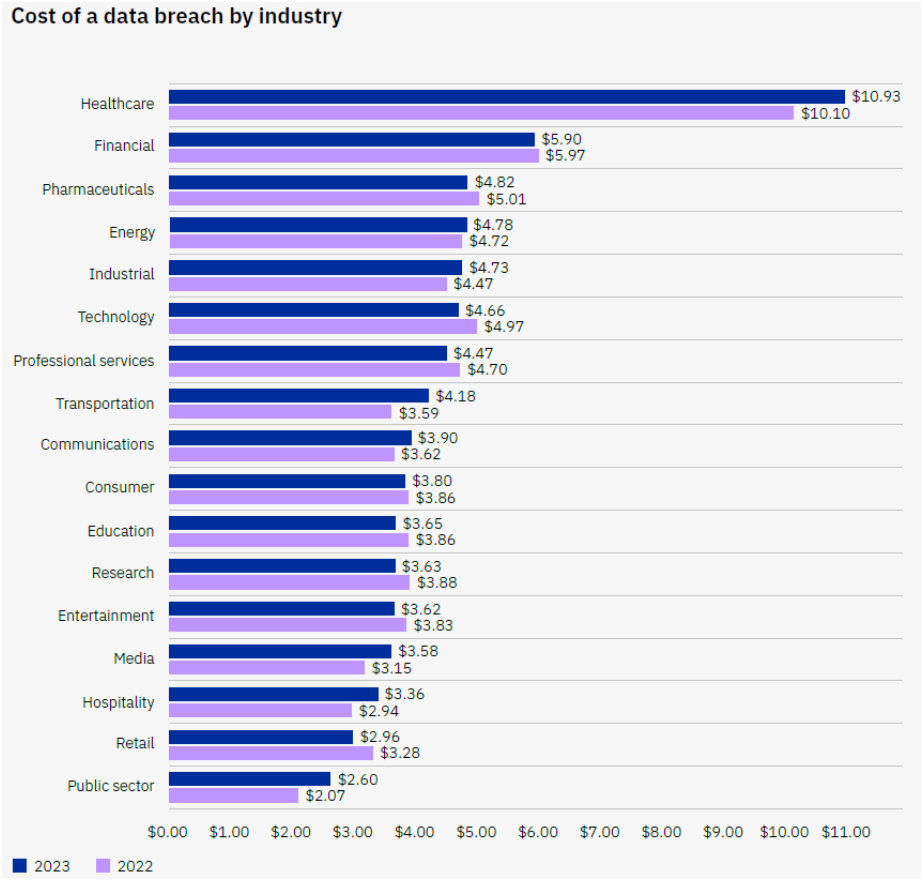
News | Columns | Interviews | BW Communities | Events | BW TV | Subscribe to Print

Healthcare Firms Are 73% Likely To Pay Ransom In A Cyber Attack: Report

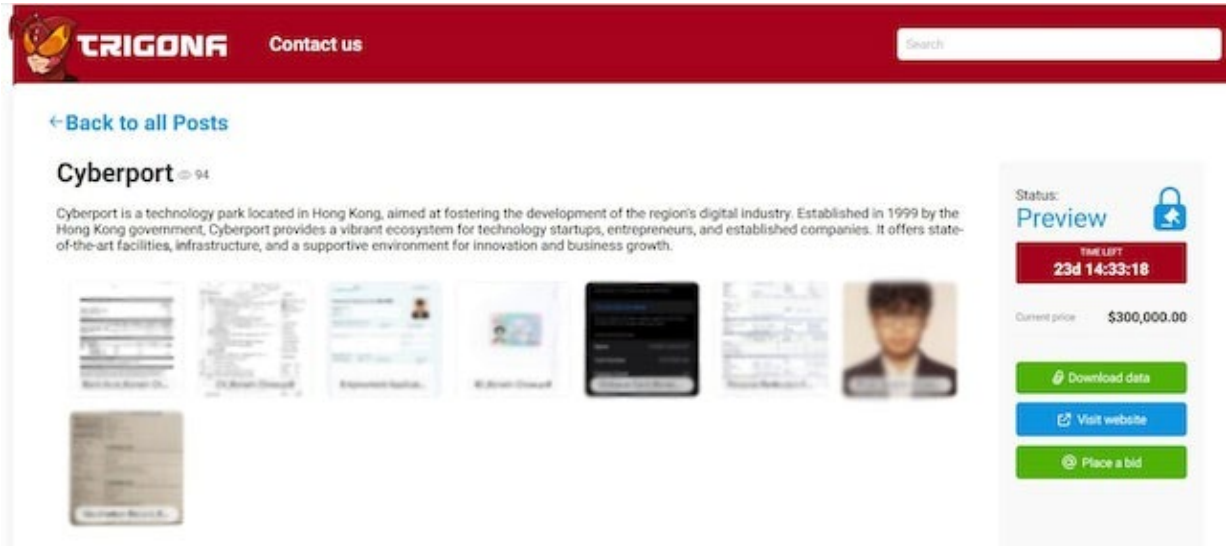
Follow

Arete, a cyber risk management company, focuses on the healthcare sector and explores the most prolific ransomware families, ransom demand and payment trends, and the most impactful controls and mitigation tactics

Source: Business World Report



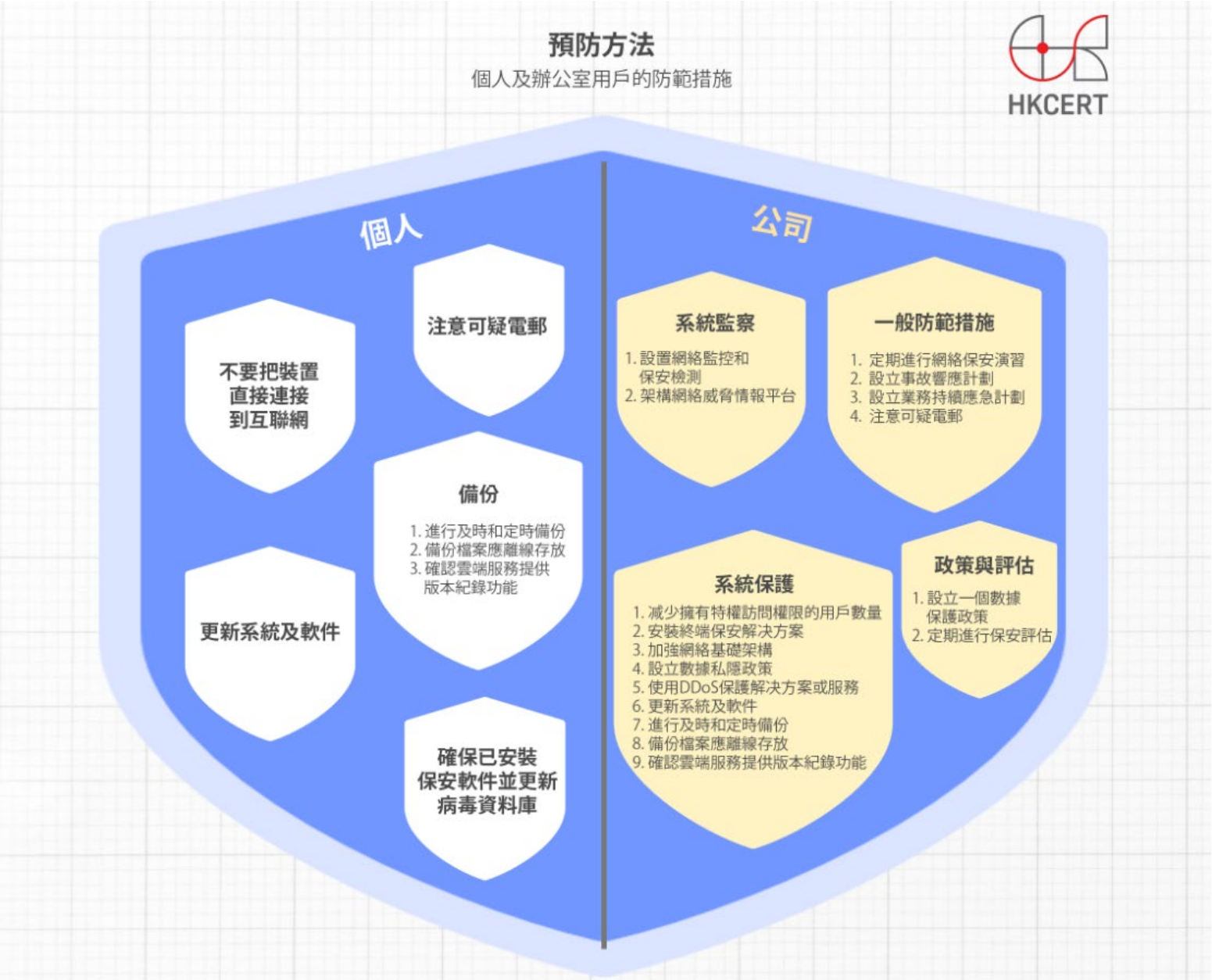
Source: IBM Cost of a Data Breach Report 2023



數碼港昨日(6日)公布發現一宗網絡安全事件，涉及未經授權的第三方入侵數碼港部分的電腦系統。


ARE
YOU
READY?

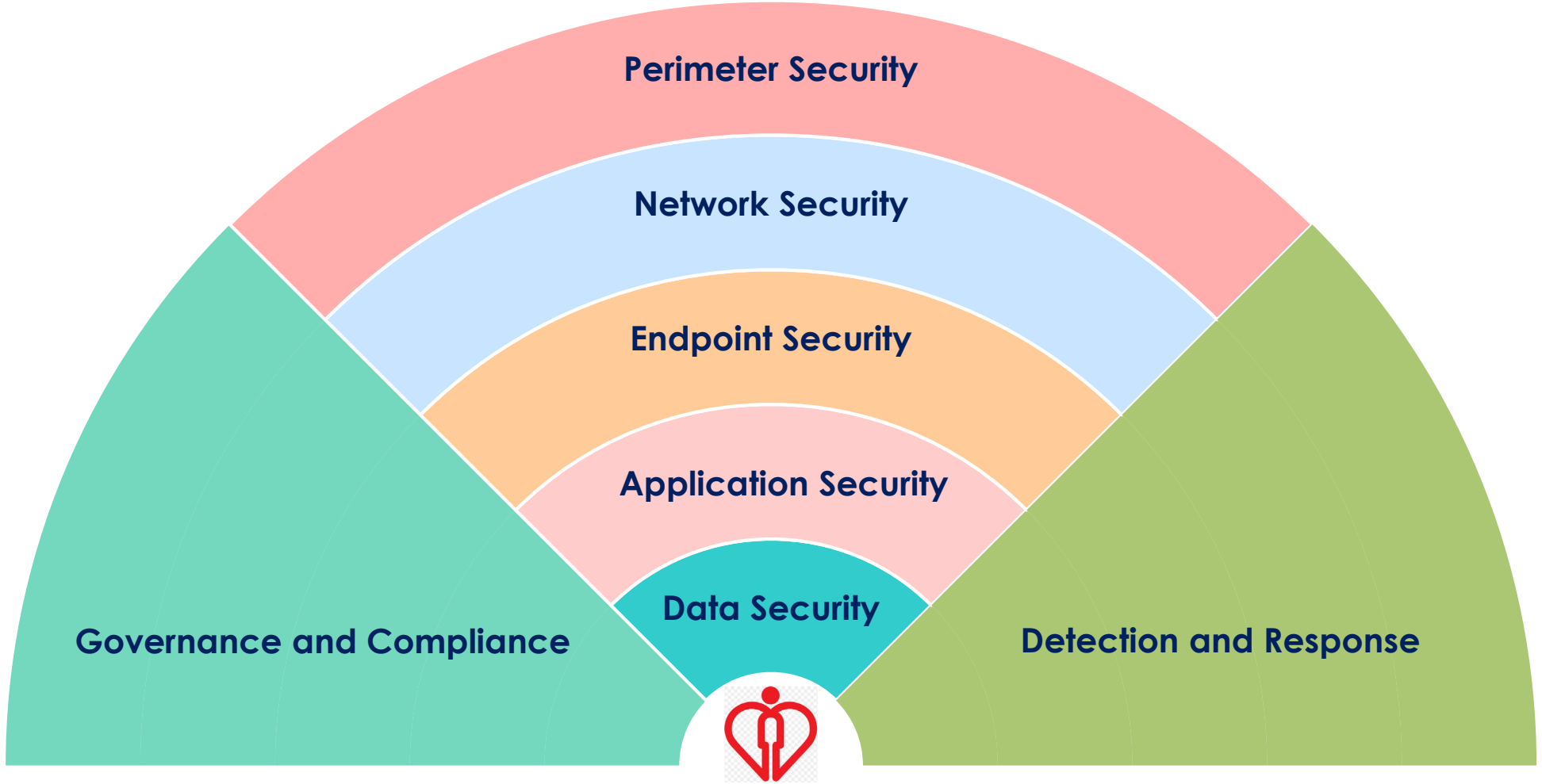
Get the Basic Right to Avoid Being Low Hanging Fruit



Source: HKCert.org

Defense-in-depth Approach

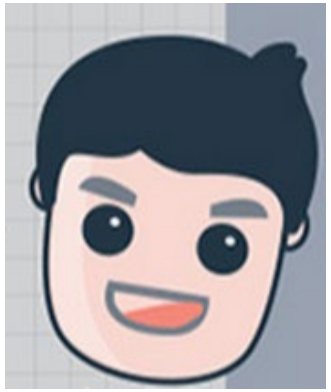
- Defend information asset against cyber attacks with multiple layers of security controls
- Provide redundancy in the event one layer of security controls failed or was exploited

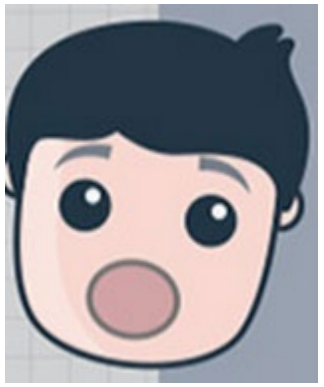


90% of all Cyber Attacks Begin with a Phishing Email

Tips to spot Phishing Email 網路釣魚 全攻略

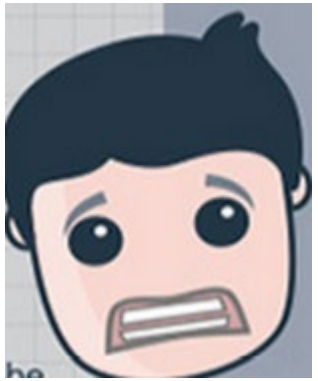
Greed
邊有咁大隻
蛤蜊隨街跳





Urgency
十萬火急
幫緊你

Curiosity
開心些牙



Fear
怯 你就輸成世

Practice Makes Perfect!

Mock Phishing Exercise 網路釣魚郵件模擬演習

Objective

- Part of overall Cybersecurity Awareness Programme
- Provide a safe and real-life setting for users to experience phishing email
- Create staff awareness on risk of phishing email and best practices

Summary of the Exercise

- Target for staff who have Internet email address
- Leverage a professional phishing campaign platform for the exercise
- Ran for few days for each hospital or healthcare services provider
- Need supports and coordination efforts from management and IT dept

Reminder Sent to Staff Before the Exercise

Email

Tue 9/8/2022 10:14 am

HO IT&HI Information Security Office

提防網絡釣魚電郵 Be Aware Of Phishing Emails

To ⊞ Staff - Hospital Authority

Dear Colleagues,

HAChat

Example – “Free Staycation Package”

“Phished” staff would receive instant cyber tips on phishing email

Staff Welfare <staffwelfare@hasw.org>

[員工快閃優惠] 免費Staycation 套票 [Special Offers] Free Staycation Package

To Yorky WONG, HOIT&HI SA(ISO1)1

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

各位同事：

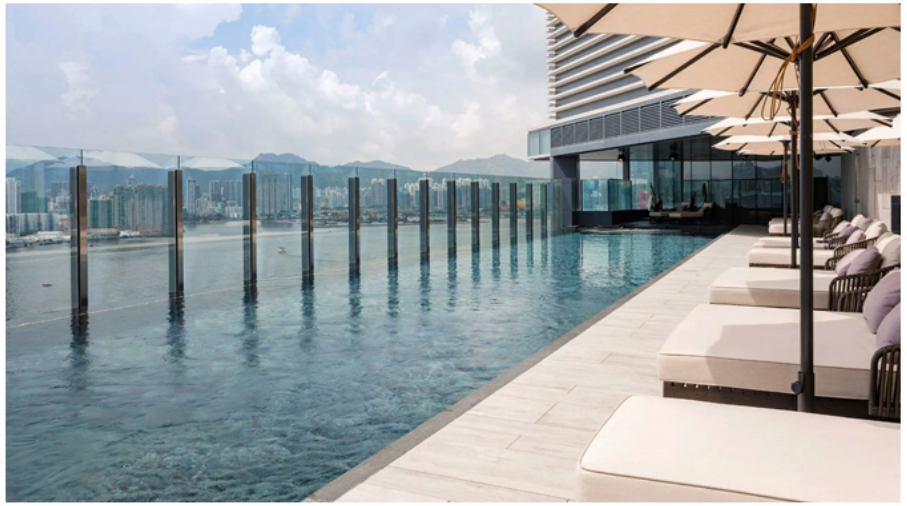
中秋節臨近，我們現與香港瑰麗酒店(Rosewood Hotel) 及香港迪士尼樂園酒店 (Hong Kong Disneyland Hotels)合作推出Staycation憂惠，向首三百位成功登紀的同事提供價值港幣4 ,000元的憂惠套票！

請立刻按此連結 登紀！

Dear Colleague,

Mid-Fall Festival are coming! We now offering FREE Staycation package worth HKD$4,000 (Rosewood Hotel or Hong Kong Disneyland Hotels) for firstly 300 successful register staff.

Now click here to registering!



Regards,
Staff Welfare

Clicked link

這是一個網絡釣魚練習，你剛才點擊了網絡釣魚電郵的連結。
This is a mock phishing exercise. You just clicked the link in a phishing email.

請留意這個釣魚電郵的例子，及時刻謹記：
Please pay attention to the following example of phishing email, and be reminded that:

1. 點擊連結前要三思
   Think twice before you click. Only click the expected emails.
2. 有懷疑時不要提供任何個人資料
   Do not provide any personal information if in doubt
3. 利用Outlook內的 “Report Phishing Email” 功能來報告任何可疑電郵
   Report any suspicious email by clicking “Report Phishing Email” button in Outlook

釣魚電郵的5個特徵
5 Signs of a Phishing Email

Phishing Email with Red Flags

外部發件人使用不明確的部門名稱，偽裝為內部電子郵件
External sender pretending internal email with ambiguous department name

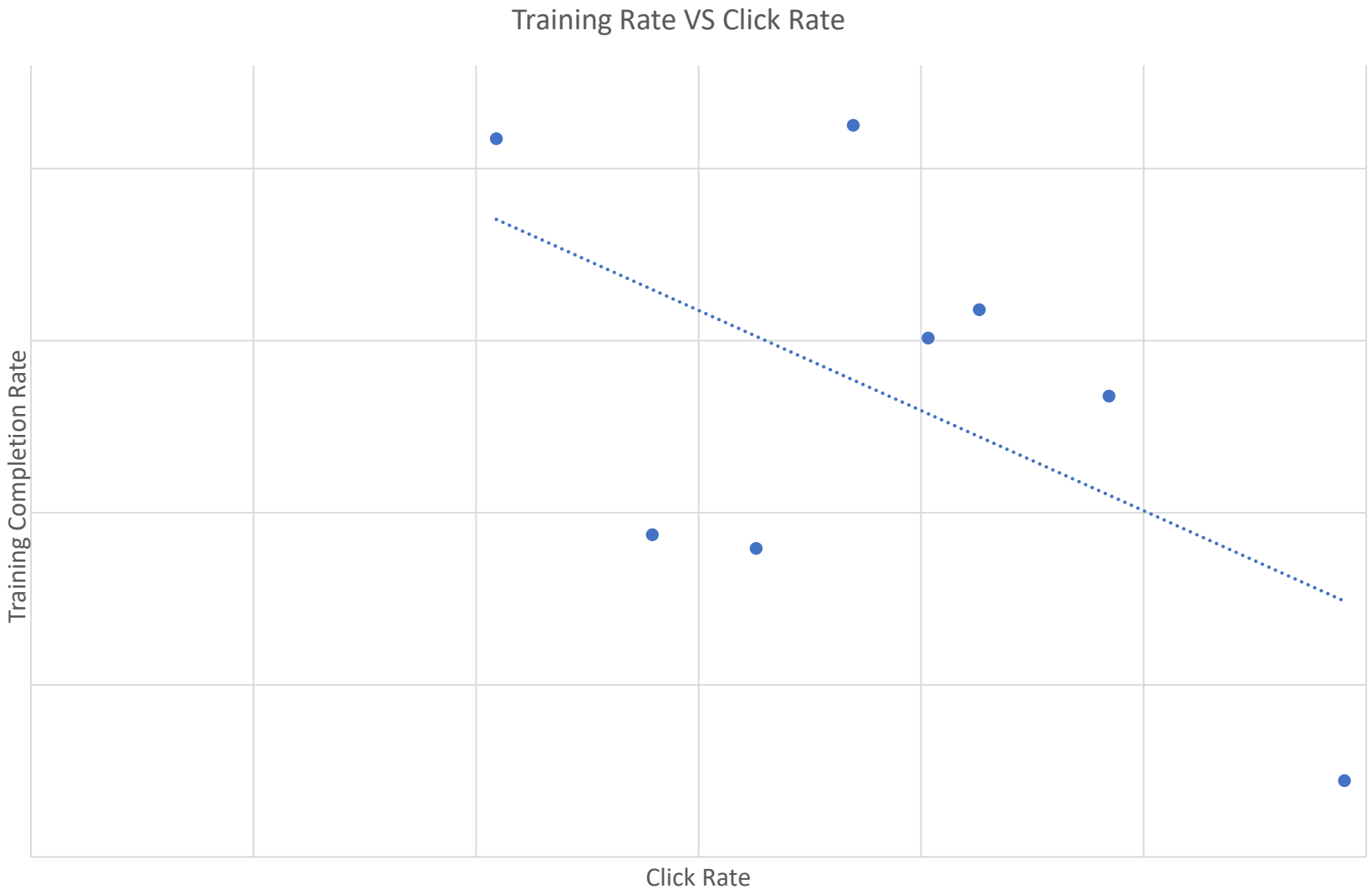
明顯的錯別字/語法錯誤
Obvious typos/ grammatical errors

內容過於吸引 (貪念)
Too good to be true offer (Greed)

緊急請求
Call for urgent action (Urgency)

引誘點擊連結(好奇心)
Lure to click the link (Curiosity)

Trained Users are Less Likely be the Victim



More Resilient with Continuous Mock Phishing Exercises

Collaboration with Your Trusted Partners

Health Bureau
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

香港警務處
網絡安全及科技罪案調查科
Hong Kong Police Force
Cyber Security and Technology Crime Bureau

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

醫院管理局
HOSPITAL
AUTHORITY

醫健通
ehealth
香港特別行政區政府 HKSAR GOVT

Thank you!