A CYBERWAR THAT YOU DON'T KNOW ABOUT

David vs Goliath: The Struggle for Cyber Security in Healthcare

Pascal Tse

St. Teresa's Hospital & St. Paul's Hospital

3 October 2023

Agenda

- ***<u>Existing landscape</u>***
  - Cyber attack like cancer
  - Healthcare attacks and success case
- Challenges and difficulties
  - People: Phishing, User & IT staff
  - Technology: Vendor, Upgrades, New tech
  - Resources: Ever growing needs, Money
- Road ahead
  - Back to basic
  - Management awareness
  - External engagement & sharing

Key messages

- Caner = Cyber attack
- Young lady = New developed system
- Old lady = Well developed system
- Married lady = Have install basic protection


STAY VIGILANT
MY FRIENDS

ALJAZEERA News Ukraine war World Cup Economy Opinion Video

Economy | Cybercrime

Cyberattack on top Indian hospital highlights security risk

The attack on AIIMS crippled operations as patients couldn't register for appointments, doctors couldn't access medical records.

The hospital normally treats thousands of patients a day and those queues got longer as appointments were not possible [File: Altaf Qadri/AP Photo]

7 Dec 2022

The leading hospital in India's capital limped back to normalcy on Wednesday after a cyberattack crippled its operations for nearly two weeks.

https://www.aljazeera.com/economy/2022/12/7/cyberattack-on-top-indian-hospital-highlights-security-risk

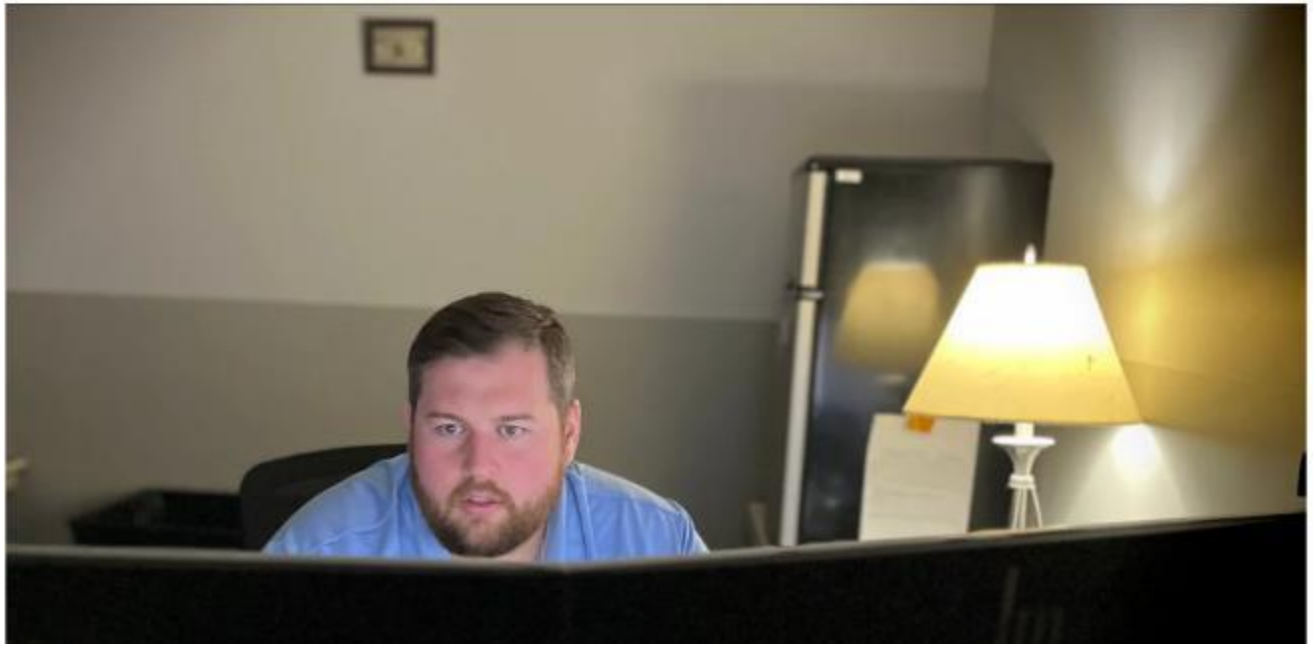
HEALTH REPORTING IN THE STATES

Cyberattacks on health care are increasing. Inside one hospital's fight to recover

May 8, 2023 · 5:00 AM ET

FROM SIDE EFFECTS PUBLIC MEDIA

By Farah Yousry



https://www.npr.org/sections/health-shots/2023/05/08/1172569347/cyberattacks-on-health-care-are-increasing-inside-one-hospitals-fight-to-recover

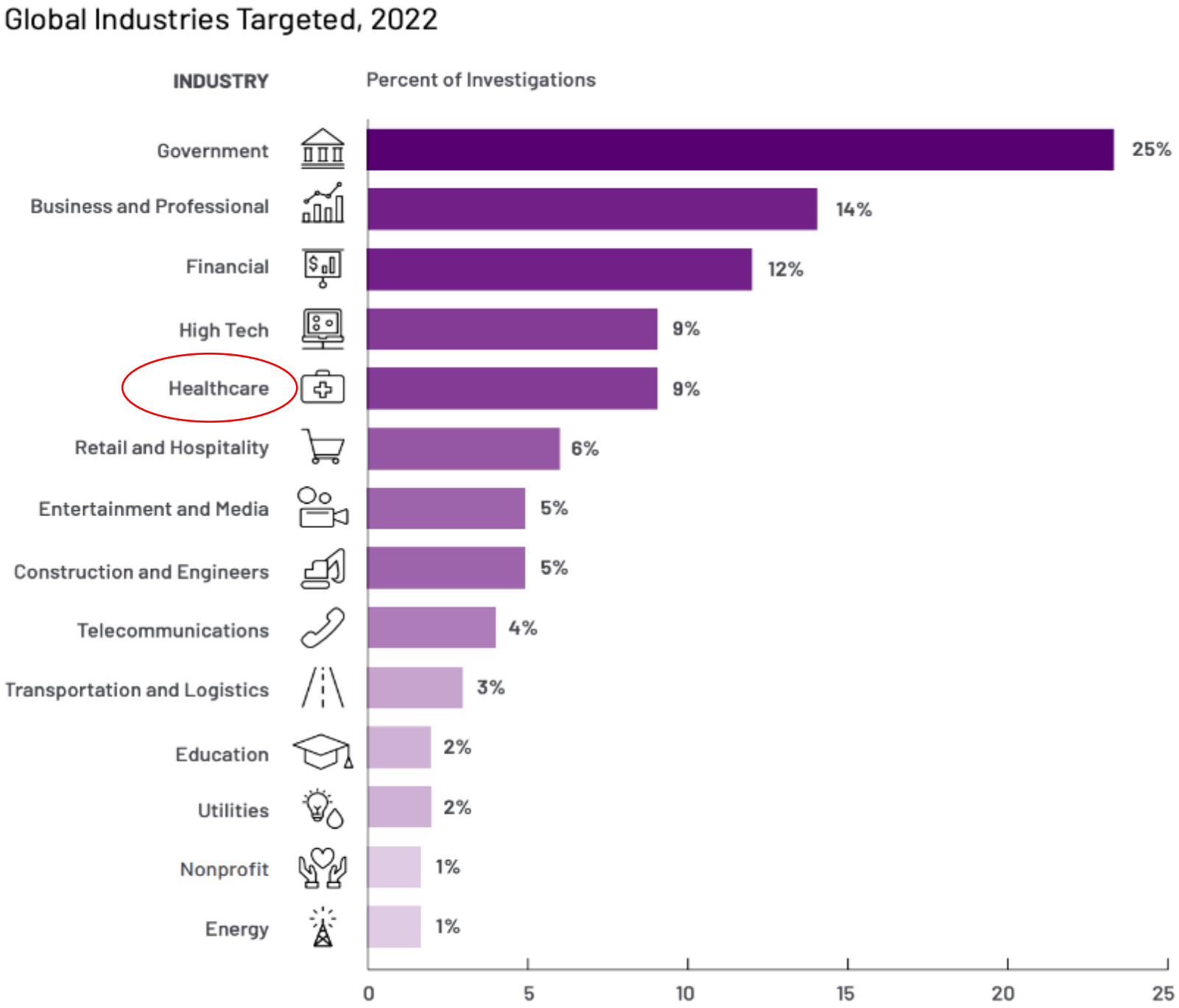
https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

Top 5 Biggest Data Breaches in Healthcare Ranked by Impact

Name	Date	Impact	How	What	Lessons Learned
Tricare Data Breach	Sep 2011	5 million	Stolen encrypted backup tapes	• Social Security No • Name • Address • Phone # • Health data etc.	Encryption method aligned with federal standard
Community Health Systems Data Breach	April-June 2014	4.5 million	Software vulnerability	• Names • Birth dates • Social Security numbers • Phone numbers • Addresses	Patch vulnerabilities
UCLA Health Data Breach	July 2015	4.5 million	Wasn't aware of attack which was more than 6 months	• Names • Dates of birth • Social security numbers • Medicaid • Health plan identification numbers • Some medical data	Investigation whenever suspicious activity

Top 5 Biggest Data Breaches in Healthcare Ranked by Impact

Name	Date	Impact	How	What	Lessons Learned
Advocate Health Care Data Breach	August 2013	4.03 million	Stolen PC with unencrypted medical information	• Demographics • Credit card numbers with expiration dates • Clinical information • Health insurance information	Encrypt data at rest
Medical Informatics Engineering Data Breach	July 2015	3.9 million	Compromised username and password and undetected for 19 days.	• Demographics • Usernames, hashed passwords, security questions and answers • Clinical information	Dark web monitoring solution



Industry Targeting

1) Government
2) Business & Professional
3) Financial
4) High tech and
5) Healthcare industries

are favoured by adversaries.

These industries remain attractive targets for both financially and espionage motivated actors.

source: https://mandiant.widen.net/s/dlzgn6w26n/m-trends-2023

Health data US$350
VS
Credit card US$1

HAS 協力Link

醫院管理局 HOSPITAL AUTHORITY

A A A 繁 EN

01 2020

Fighting a zero-day attack

The evening of 2 September 2019 had been peaceful and uneventful at the Hospital

FROM THE EDITOR

- Lesson learnt from cyber war victory
- Editorial Board
- Editorial Team

Fighting a zero-day attack

The evening of 2 September 2019 had been peaceful and uneventful at the Hospital Authority (HA)Information Technology Operation Centre in Kowloon Bay when an alert on the computer-monitoring dashboard suddenly lit up and jolted employees into urgent action. A network server was running with abnormal high utilisation rose from 10% to 70% for unknown reasons. What followed was a fortnight-long battle to defend the authority's systems against hackers who tried to break into the HA network with terrifying stealth in an apparent attempt to steal the data of millions of patients.

Malicious attack detected

Server utilisation is the system loading rate measuring the amount of computational work performed. When an incident of any kind is detected, IT team experts handled the IT glitch and restarted the server promptly, so that the server returns to normal. In this case, the IT team discovered hackers had tried to penetrate the HA network in a sophisticated 'zero-day attack' that accessed systems without leaving a trace, indicating a particularly ominous threat to patient data. The incident was reported to the Office of the Government Chief Information Officer and the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force.

"The zero-day attack deployed a new malware tailored to HA's IT system," explains Chief Information Security Officer **Fuller Yu**, whose team quickly concluded the attack was the work of an advanced hacking team, making it challenging for the IT team to clean up malware that had not yet been publicly disclosed and patched. "We were at a disadvantage – it was

FROM THE EDITOR
- Lesson learnt from cyber war victory
- Editorial Board
- Editorial Team

COVER STORY
- Fighting a zero-day attack
- Masterstroke to combat cyber attack
- Fight cyber criminals
- Understand HA network from 10 numbers

HELEN HA
- Let's get ready on race day
- New blood donation vehicle is hitting the road!

PEOPLE
- A love affair with the sky
- Is it a UFO? The delights of cross-country flying

WHAT'S NEW
- New Chairman steers a course towards common goals
- Getting to know Henry Fan
- Better patient care through dementia-friendly ward
- Myths about dementia
- Take complaints and feedback as health check

Agenda

- Existing landscape
  - Cyber attack like cancer
  - Healthcare attacks and success case
- ***Challenges and difficulties***
  - People: Phishing, User & IT staff
  - Technology: Vendor, Upgrades, New tech
  - Resources: Ever growing needs, Money
- Road ahead
  - Back to basic
  - Management awareness
  - External engagement & sharing

Cyber Security war in Healthcare is like David vs Goliath

Infected is so easy

To err is human

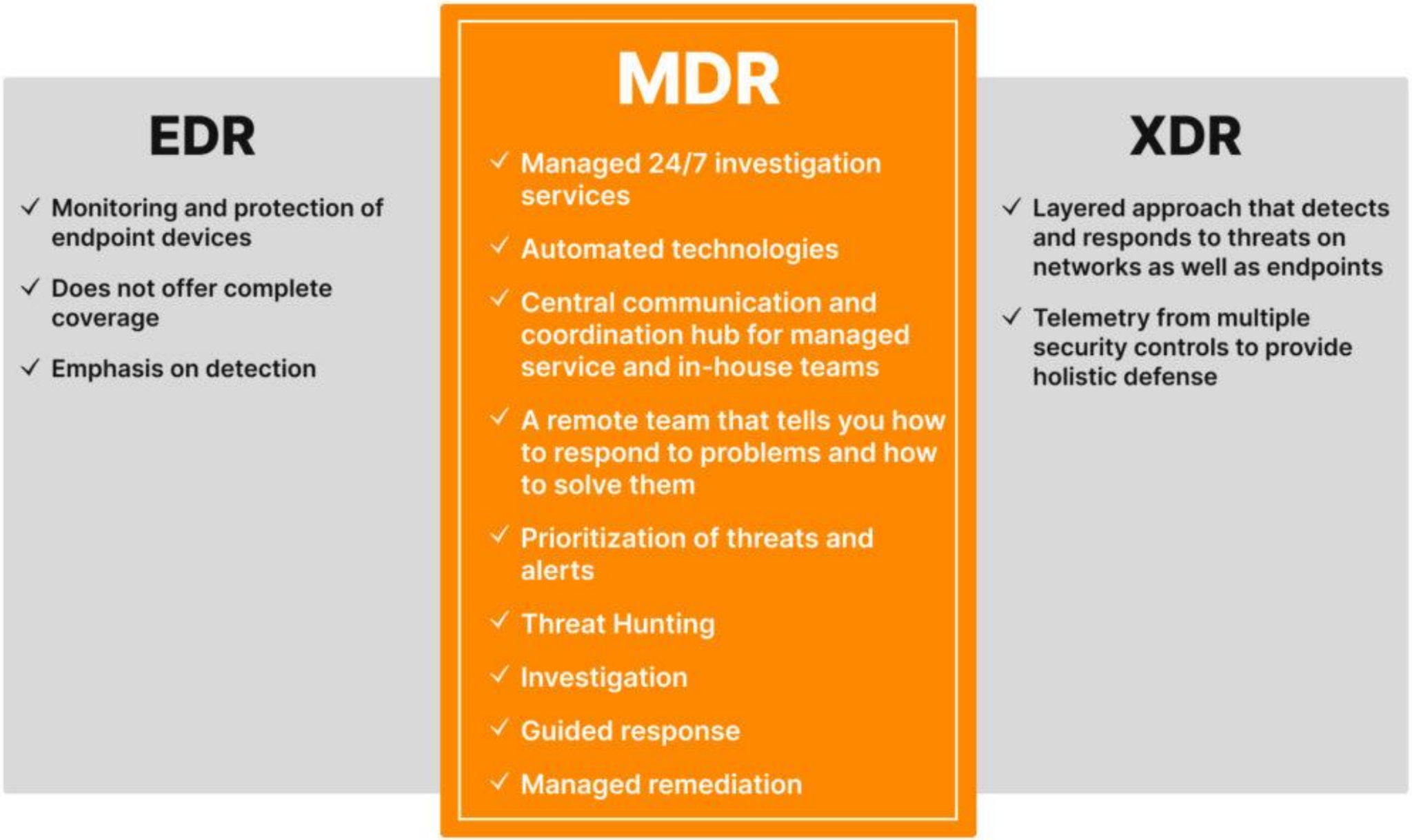
Both users & IT

Medical vendors using old Windows OS

Never ending patching work

Ever rising new attacks

Ever revolving technologies



Risk is escalating: Users want more and more features

Money perspectives

- Need money for
    1) Hardware & Software
    2) IT resource ie head count
    3) Salary increment
- We vs Boss = IT vs Management (non IT)
- Cost centre vs Revenue generation

Agenda

- Existing landscape
  - Cyber attack like cancer
  - Healthcare attacks and success case
- Challenges and difficulties
  - People: Phishing, User & IT staff
  - Technology: Vendor, Upgrades, New tech
  - Resources: Ever growing needs, Money
- ***Road ahead***
  - Back to basic
  - Management awareness
  - External engagement & sharing

Back to basics

Seven Habits of Cyber Security

1. Security Policy and Security Management

- Define and document the security requirements with respect to cyber security risks
- Review and update regularly the security requirements and security policy
- Disseminate regularly the information on the latest security policy to staff members

2. Endpoint Security

- Install security software such as anti-virus and anti-malware software
- Keep the definition file and patches of security software up-to-date
- Keep the operating system and software of the endpoints up-to-date
- Login with a non-privileged and non-administrator account for daily usage

3. Network Security

- Protect organisation network with a firewall and minimise network ports exposed to the Internet
- Use "DENY" as default rule on firewall, and only "ALLOW" necessary traffic
- Allow only approved IP addresses to have Internet access
- Use a secured VPN connection for remote access
- Use encrypted network protocols (e.g. HTTPS)
- Review regularly the firewall rules

4. System Security

- Perform system hardening with security policies enabled and unused services disabled
- Keep all system software including operating system, security software and patches up-to-date
- Encrypt sensitive information on the system storage
- Validate and filter input from Internet users (e.g. web server forms) properly in application to avoid SQL Injection type of attack

5. Security Monitoring

- Enable logging features in network devices (e.g. firewall) and servers
- Centralise logs within the organisation for periodic review and monitoring
- Review the logs and security alerts and respond to detected issues in a timely manner
- Monitor network traffic (e.g. Internet traffic) to detect if there is any abnormal traffic pattern

6. Incident Handling

- Develop incident response plans for handling various security incidents (e.g. ransomware, data breach, distributed denial-of-service (DDoS) attack, etc.)
- Backup systems and data regularly
- Keep backups offline (or better still offsite)
- Perform regular backup restore drills to ensure that data can be restored properly

7. User Awareness

- Remind staff members regularly on their roles and responsibilities in protecting the organisation's information assets
- Perform drills (e.g. simulated phishing attacks) to test staff readiness against common cyber attacks

GovCERT.HK

HKCERT Hong Kong Computer Emergency Response Team Coordination Centre

香港警務處 Hong Kong Police Force

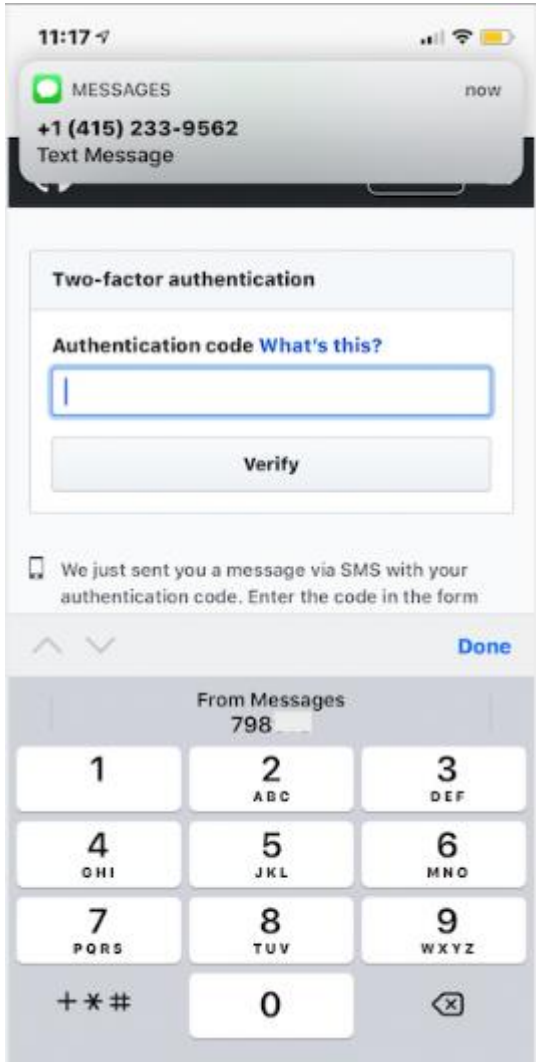
For details, please visit HKCERT website at:

www.hkcert.org

Phishing

Source: HKCERT.org

2 Factor Authentication



Microsoft Authenticator

Google Authenticator

EPP vs EDR vs XDR

Which Threat Detection Solution is Right for You?

Get management awareness

- Educate management
- Share latest news with management & IT
- Share peer’s experience and update
- Budget Cybersecurity tools, service and staff
- Table-top exercise
- Playbook

Educate management: Not just scare them

Hacked data from Cyberport released on dark web

Local | 12 Sep 2023 6:44 pm


Leverage external resources

Registration Form for the Ethical Phishing Email Campaign 2023

Home Details Start Now Contact Us

END

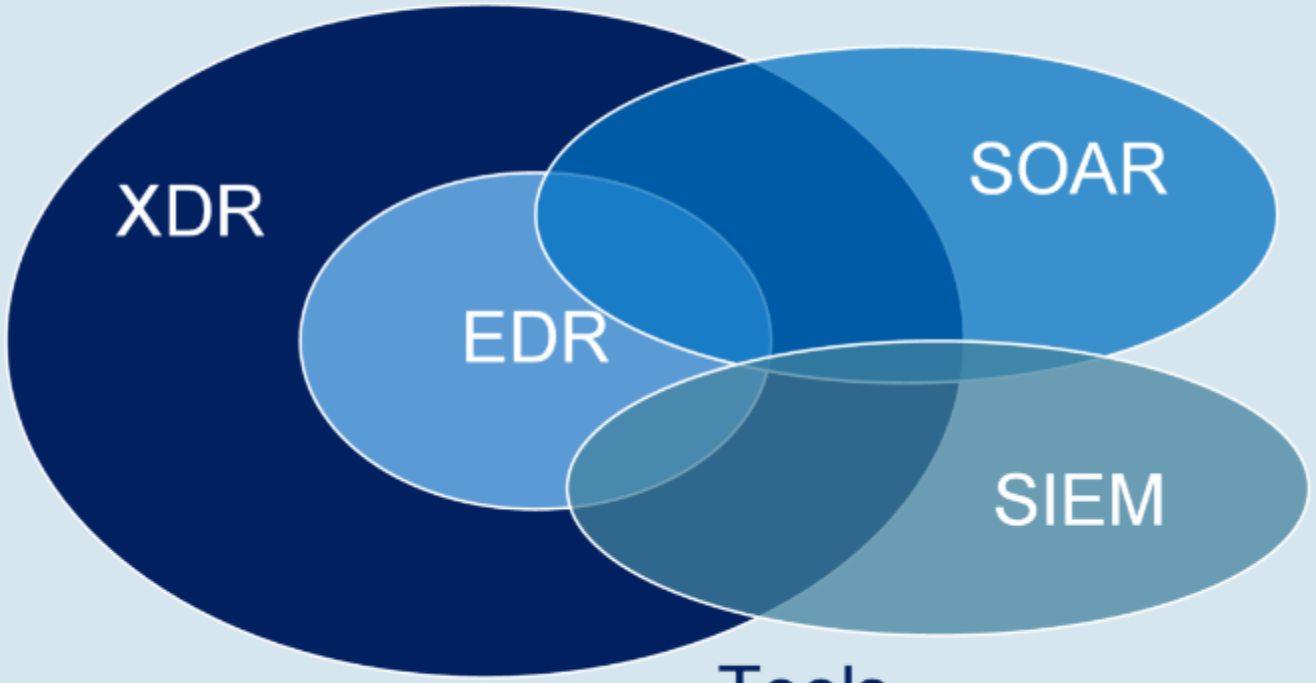
START NOW


INCIDENT RESPONSE

SOC

Services

MDR



Tools

Security Analysts

Processes

...

Experience sharing

- Join EHRSS Taskforce or Working Groups
- Join CyberSecurity Interest Group
- Join CyberSecurity events like phishing
- Gather latest CyberSecurity information trustworthy sources

Happy Ending