HISA cybersecurity

HACK ME IF YOU CAN!

Presented by

Cybersecurity Community of Practice

14 August, 2019

HIC19

#HIC19

- **Introduction** (David Bunker)
- **Workshop purpose** (David Bunker/Jorge Silveira):
  - to simplify security concepts
  - Understand ways we are at risk
  - Understand ways to protect and respond
- **Examples of breaches** in the press (James Fell)
- **Simulated experience** (Moderated by James Fell, and supported by HISA Cybersecurity CoP Steering Group Members): Attackers (Red), Defenders (Blue)
- **Wrap – up** (David Bunker)

OVERVIEW

- Wannacry cost NHS £95 million and 20,000 cancelled appointments
- NotPetya…
- Stuxnet…
- Capital One…
- How about Facebook? $5 billion fine for Cambridge Analytica data breach

WHY CYBER?

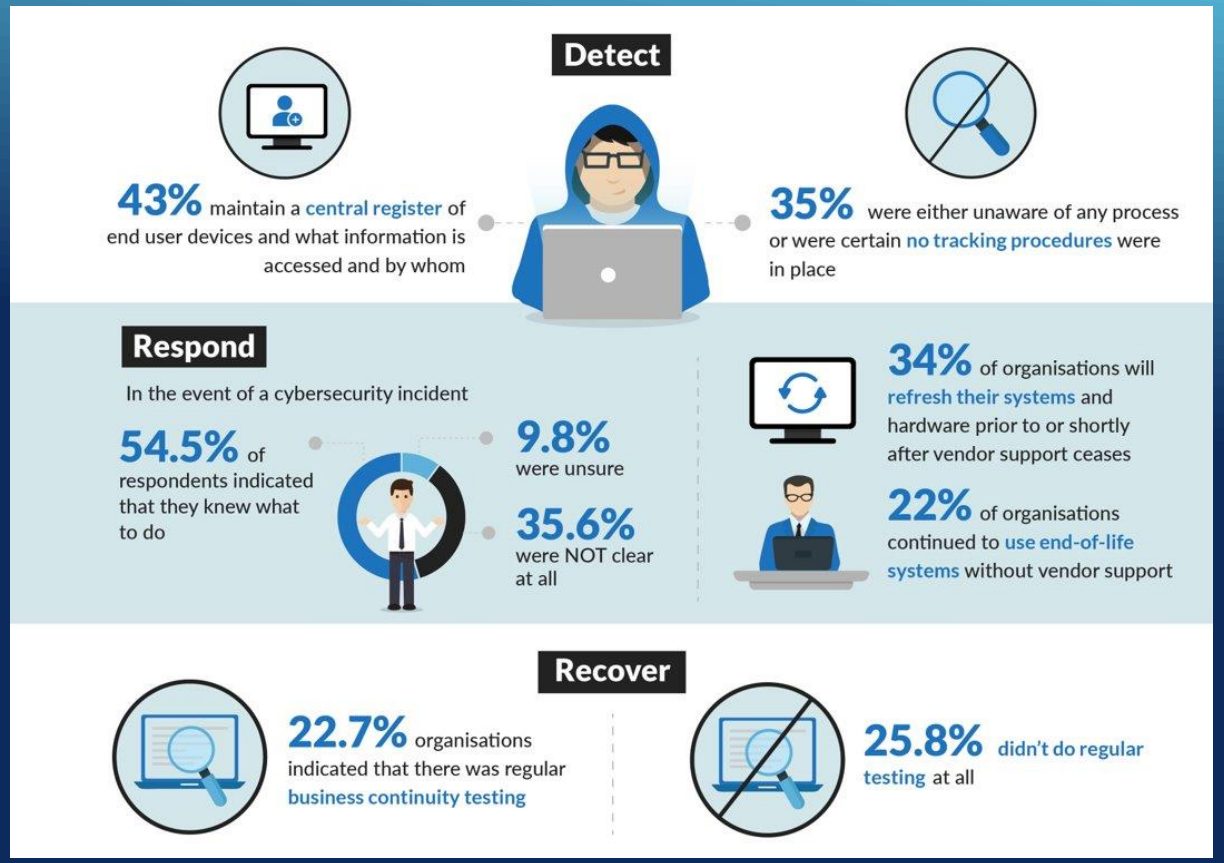
INSTRUCTIONS FOR TODAY

- **Open your Envelopes please**
  - Tables of Attackers (red hats), and Defenders (blue hats) with the objective that attackers will "launch an attack" on the defenders
  - Each table, has a set of instructions and materials to guide you through this orchestrated process. And you have Cybersecurity CoP members to assist at each table – ASK QUESTIONS!
  - **Attack teams** have a set of well known contemporary attacks they can apply, and correspondingly, **Defender teams** have information on their healthcare organisation and how you might respond based on knowledge of the attack (i.e. it will become apparent for the purpose of this workshop).
  - Each response by each team dictates how the next choice will be made.
- A time limit on each turn will be set so be ready. NOTE the egg timers!!

WHAT'S ON YOUR TABLE

- Each table has a copy of the results of the last two Cybersecurity Surveys HISA sponsored and a Cyberary (glossary of terms), just to whet your appetite.
- Defenders (blue hats) have a health organisation profile - cybersecurity maturity, IT staff experience in handling incidents and other pertinent information
- Attackers (red hats) have a profile – Organised cyber criminals
- Attackers have a set of exploits they will attempt to launch on Defenders, with more or less information on the attack target's organisation capabilities.

2017



2018

CYBERSECURITY SURVEYS


LET THE GAMES BEGIN

RED TEAM – ATTACK VECTOR

- Attack Vector 1
  - Scan the target organisations externally facing systems to identify potential vulnerabilities.

- Attack Vector 2
  - Send a spear phishing email to the CFO with a malicious attachment.

- You detect the scanning of your external websites as you have detection systems in place. But you have other priorities on your hands like EMR Go Live and Data Centre Migration projects.
- You check your detection and vulnerability management systems to determine what your exposure is and what scanning has taken place.
- You continue to configure the devices for the new EMR go-live, noting that you will check the detection and vulnerability management system later when you get time.

BLUE TEAM – INITIAL RESPONSE

- The CFO receives the phishing email and they open the attachment which deploys some malware on their computer. The CFO rings IT Service Desk complaining their computer isn't working.
  - You log an incident in your service desk system noting that the CFO opened an attachment and their computer "blue screened". IT Engineer is then tasked with resolving the issue.
  - You log an incident in your service desk system noting that the CFO opened an attachment and their computer "blue screened". You immediately triage this as a Priority 1 security incident.

BLUE TEAM – INITIAL RESPONSE

- After scanning the externally facing systems, you identify 10 critical vulnerabilities on a web server. One vulnerability allows you to remotely execute code on the server, the other allows you administrator access
  - Exploit the vulnerability on the web server to execute code remotely and deploy some ransomware.
  - Exploit the vulnerability on the web server to gain administrator access to scan the network for potentially sensitive files.

RED TEAM – ATTACK VECTOR

- As the malware has been deployed on the CFOs computer, you gain access to the Finance part of the network. Which type of malware did you design?
  - The malware you embedded in the email is designed to forensically delete recently used files but not before taking a copy first to sell.
  - The malware you embedded in the email is ransomware with a wormable component meaning it can spread across the network very quickly, encrypting systems and devices as it goes.

RED TEAM – ATTACK VECTOR

- After checking your detection and vulnerability management systems, you note suspicious behaviour on a web server.
  - You declare a cyber incident, stand-up your cyber incident response team, phone James and enact your playbook.
  - You investigate the suspicious behaviour by reading the logs on the web server.

BLUE TEAM – INCIDENT DECLARATION?

- After checking your detection and vulnerability management systems, you note suspicious behaviour on a web server.
  - You declare a cyber incident, stand-up your cyber incident response team, phone James and enact your playbook.
  - You investigate the suspicious behaviour by reading the logs on the web server.

BLUE TEAM – INCIDENT DECLARATION?

- After the IT Engineer has re-imaged the CFO's machine, they notice that several files have been deleted and are now inaccessible. The IT Engineer investigates further and identifies that there is no trace of the files existing and that a large upload to a cloud storage site has taken place recently from the CFOs machine. What do you do?

- Investigate further to determine what was taken, who did it, how it happened and root cause analysis.
- You declare a cyber incident, stand-up your cyber incident response team, phone James and enact your playbook.

BLUE TEAM – ENGINEER

- The IT Service Desk receives a number of calls relating to inaccessible patient files. A ransom note is then discovered on a desktop. Do you…

- Pay the ransom as it will be quicker to get back to normal operations. After all criminals are trustworthy
- You declare a cyber incident, stand-up your cyber incident response team, phone James and enact your playbook.

BLUE TEAM – HELD TO RANSOM

- Not a viable option!
- It is Victorian Government policy never to pay a ransom.
- Therefore, the only viable option is to declare a cyber incident…

BLUE TEAM – NOT AN OPTION

BLUE TEAM – NOT AN OPTION

- Not a viable option!
- In the real world, no cyber incident could be declared at this stage based on suspicious behaviour due to the number of false positives and error rates of such systems.
- Therefore, the only viable option is to investigate further…

BLUE TEAM – NOT AN OPTION

- Not a viable option!
- In the real world, no cyber incident could be declared at this stage based on suspicious behaviour due to the number of false positives and error rates of such systems.
- Therefore, the only viable option is to investigate further…

- Now that we know files have been stolen, we know a crime has been committed and we need to declare an incident fast.
- Further investigation should take place after an incident has been declared. So the action isn't wrong, just the order in which things need to happen.
- Therefore, declare an incident…

BLUE TEAM – NOT THE BEST OPTION…

- After deploying the ransomware on the defenders network, it encrypts multiple devices by exploiting a known vulnerability across desktops and servers which remain unpatched. These devices display a ransom note. How much would you like to hold the defence ransom for?

- 1 bitcoin
- 4 bitcoin

RED TEAM – RANSOM

- After deploying some ransomware on the web server, you execute it and it encrypts the web server and displays a ransom note. How much would you like to hold the defence ransom for?
  - 1 bitcoin
  - 4 bitcoin

RED TEAM – RANSOM

RED TEAM – PRIVILEGED ACCESS

- As you have gained privileged access to the web server, you search for sensitive files to either hold the org to ransom with or sell for future fraud. Which files would you take a copy of before deleting them?
  - 100,000 patient files including health records
  - 10,000 current and previous staff records including banking details

- As you have access to the CFOs computer, your malware reports back that you have access to several sensitive files. Which ones do you want?
  - 100,000 financial files including banking details
  - 10,000 patient files from a billing system

RED TEAM – PRIVILEGED ACCESS

- The IT Service Desk receives a number of calls relating to inaccessible patient files. A ransom note is then discovered on a web server. Do you…

- Pay the ransom as it will be quicker to get back to normal operations. After all criminals are trustworthy
- You declare a cyber incident, stand-up your cyber incident response team, phone James and enact your playbook.

BLUE TEAM – HELD TO RANSOM

BLUE TEAM – RECOVERY PRIORITY

- You have declared a cyber incident and decided not to pay the ransom (Well done!). But what is your priority in recovering from the ransomware?
  - Isolating the devices from the network to stop the ransomware spreading?
  - Ensuring you have offline backups of critical data to recover from?

- Your investigation notices that several files have been deleted and are now inaccessible. The investigation further identifies that there is no trace of the files existing and that a large upload to a cloud storage site has taken place recently from a web server. What do you do?

- Try digging further to see who did the upload, when they did it and how they did and compile a thorough report of your investigation.
- You declare a cyber incident, stand-up your cyber incident response team, phone James and enact your playbook.

BLUE TEAM – STOLEN FILES

- Now that we know files have been stolen, we know a crime has been committed and we need to declare an incident fast.
- Further investigation should take place after an incident has been declared. So the action isn't wrong, just the order in which things need to happen.
- Therefore, declare an incident…

BLUE TEAM – NOT THE BEST OPTION…

- Not a viable option!
- It is Victorian Government policy never to pay a ransom.
- Therefore, the only viable option is to declare a cyber incident…

BLUE TEAM – NOT AN OPTION

Sit back and moonwalk all the way to the bank…and try it on another health agency!

RED TEAM – JOB DONE!

Sell the stolen data on the dark web and moonwalk all the way to the bank…and try it on another health agency!

RED TEAM – JOB DONE!

- You declared an incident, got specialist forensic help the next day which determined the ransomware was deployed on a web server but because your logs are only retained for 24 hours max, you cant fully confirm how the attackers gained entry.
- You recovered the files with your offline backups, however your organisation had to use paper for a period of 48 hours. Total downtime was three days.

- How long can your org use paper for before services are affected?
- Do you all have offline backups?
- Do you have a vulnerability management system?
- Wrap-Up

BLUE TEAM – RECOVERY

- You declared an incident, got specialist forensic help the next day which determined the ransomware was deployed on the CFOs machine but because your logs are only retained for 12 hours max, you cant fully confirm how the attackers gained entry.
- You recovered the files with your offline backups, however your organisation had to use paper for a period of 48 hours. Total downtime was three days.

- How long can your org use paper for before services are affected?
- Do you all have offline backups?
- Do you have a vulnerability management system?
- Wrap-Up

BLUE TEAM – RECOVERY

- You determined that a significant amount of sensitive files were stolen and contacted the police, ACSC and the Office of the Australian Information Commissioner to report a breach. While you were able to recover the data from offline backups, some was unrecoverable. You have to undertake a significant exercise to determine who was included in the breach and issue letters to all those impacted from the CEO. The breach was on the Channel 9 news and online as well.
- Do you all have offline backups?
- Do you test the restores of those backups?
- Do you have processes in place to report breaches to the OAIC?
- Wrap-Up

BLUE TEAM – RECOVERY

WRAP -UP

Insider's Guide to Incident Response

- The Insider's Guide to Incident Response gives you an in-depth look at the fundamental strategies of efficient and effective incident response for security teams that need to do more with less in today's rapidly changing threat landscape. https://healthitsecurity.com/resources/white-papers/insiders-guide-to-incident-response

Incident Response Consortium

https://www.incidentresponse.com/

Resources | Ai Health Alliance

- Artificial Intelligence: A Potential Cybersecurity Safeguard or Viable Threat to the Healthcare Industry? From the National Law Review. Cybersecurity in Healthcare – Comparing 5 AI-based Vendor Offerings https://aihealthalliance.org/resources/ and click on Cybersecurity

RESOURCES