Mississippi State UNIVERSITY

CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 3
Cyber Incident Response

Determining the Impact of Incidents

Chapter 8

Outline

- Threat Classification
- Factors Contributing to Incident Severity and Prioritization
- Types of Protected Data
- Quiz

Threat Classification

- **Known Threats vs. Unknown Threats**
  - **Known Threats**
    - Can be detected through signature-based systems
    - Detecting known threats is only as good as the threat data that has been collected
  - **Unknown Threats**
    - Can be detected through heuristic analysis
      - This achieved by having known-good base-state of the network/systems and watching for anomalies within the base-state
    - Zero-day vulnerability
      - A flaw in a piece of software that the vendor is not aware of
    - Zero-day exploit
      - Code written to take advantage of the software flaw
    - Bug bounty
      - Vendors will pay researchers and hackers to discover vulnerabilities in their software

[1]

Threat Classification

- **Preparation**
  - **Should not rely on a single solution for protecting critical business assets and sensitive data**
  - **Should actively work to find threats that could have a negative impact on your organization**
  - **Here are two great resources to discover the latest software bugs**
    - **SANS Internet Storm Center**
    - **CERT Coordination Center at Carnegie Mellon University**
  - **Those resources will provide**
    - **New knowledge about attacker trends and techniques**
    - **Ability to potentially detect malicious traffic before it harms your organization**
    - **Time for your security team to develop controls to mitigate security incidents if a patch or counter-measure is not available**

[1,2,3]

Threat Classification

- **Advanced Persistent Threat (APT)**
  - **Continued stealthy computer hacking efforts usually coordinated and executed by an organization or government**
  - **Goal is to gain and maintain undetected persistent access to the target systems**
  - **Possible Attack vectors include**
    - **Spam messages**
    - **Infected media**
    - **Social engineering**
    - **Compromising the supply-chain**

[1]

Threat Classification

- **Advanced**
  - **Adversaries are well equipped with significant funding and formal training**
  - **High degree of coordination between technical and nontechnical sources of information**
- **Persistent**
  - **Operators are focused on specific tasks and will ignore opportunistic targets**
  - **The behavior suggests that there is an emphasis on consistency and persistence with strict rules of engagement**
- **Threat**
  - **Usually APTs are an extension of political will**
  - **APTs are difficult to handle alone**
  - **Automatic threat intelligence sharing**
    - **Many vendors automatically share threat data and their technical countermeasures for them**

[1]

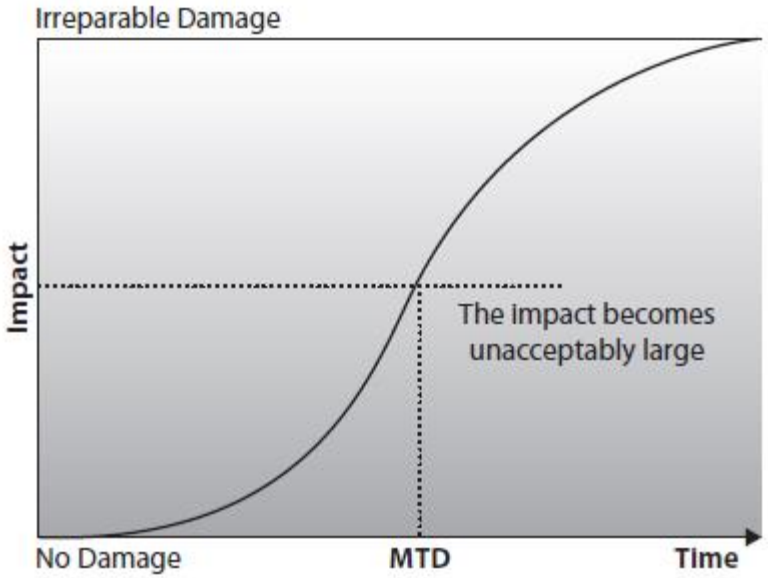
Factors Contributing to Incident Severity and Prioritization

- **Scope of Impact**
  - **A formal decision to declare an event an incident due to the event deviating enough from normal operations**
  - **The amount services have been affected**
- **Once an event is confirmed**
  - **First, Communication**
    - **Quickly decide on who needs to be contacted outside of the security group and key leadership**
    - **Ensure that any needed major changes to the organization's resources will be appropriately supported**
  - **Second, Only the IR team and decision-makers should be informed**
    - **Reduces confusion within the organization**
    - **Keeps the attacker from knowing they have been discovered**

[1]

Factors Contributing to Incident Severity and Prioritization

- **Downtime**
  - **Access to a network or a service is temporarily unavailable**
- **Maximum Tolerable Downtime (MTD)**
  - **Tolerated outage time due to an incident**



[1]

Interactive Exercise 1

What is an APT?	
What are the 5 things that contribute to the severity and prioritization of an incident?	
How does the scope of impact affect the severity and prioritization of an incident?	

[1,4]

Interactive Exercise 1 Answers

What is an APT?	Advanced Persistent Threat is the name given to any number of stealthy and continuous computer hacking efforts.
What are the 5 things that contribute to the severity and prioritization of an incident?	1. Scope of impact 2. Downtime 3. Recovery time 4. Compromise of data integrity 5. System criticality 6. The type of data
How does the scope of impact affect the severity and prioritization of an incident?	The formal determination of whether an event is enough of a deviation from normal operations to be called an incident, and the degree to which services were affected.

[1,4]

Factors Contributing to Incident Severity and Prioritization

- **MTD**
  - **If an organization cannot get production up and running within MTD window, then the organization may not recover**
  - **Business functions and assets should be placed in one of the following categories**
    - **Nonessential: ~30 days**
    - **Normal: ~7 days**
    - **Important: ~72 hours**
    - **Critical: Minutes to hours**
  - **The shorter the MTD the higher the priority of the function in questions**
  - **Items classified as critical should be addressed before those classified as nonessential**

[1]

Factors Contributing to Incident Severity and Prioritization

- **Key Performance Indicators (KPIs)**
  - Communicate with management to determine acceptable limits of downtime
  - Knowing what the KPIs are for detection and remediation will
    - Prevent confusion
    - Manage expectations
    - Demonstrate team's preparedness
- **Recovery Time Objective (RTO)**
  - The earliest time a business process must be restored after an incident
  - Period of acceptable downtime
  - RTO value is smaller than MTD value

[1]

Interactive Exercise 2

What is the MTD?	
How does the recovery time affect the severity and prioritization of an incident?	
What is the RTO ?	

[1,4]

Interactive Exercise 2 Answers

What is the MTD?	Maximum Tolerable Downtime (MTD) refers to the highest amount of outage time the organization can endure
How does the recovery time affect the severity and prioritization of an incident?	Key Performance Indicators (KPIs) utilized for detection and remediation will clear up confusion, manage expectations, and potentially allow your team to prepare correctly.
What is the RTO ?	Recovery Time Objective used to denote the earliest time or goal time within which a business process must be restored after an incident to avoid unacceptable consequences

[1,4]

Factors Contributing to Incident Severity and Prioritization

- **Data Integrity**
  - Some attackers will go after the integrity of an organization's data instead of the availability
  - Attacks on data integrity are not always easily detected
    - Malicious actors might manipulate financial transition records or personal data
    - Only a detailed inspection will illuminate possible unauthorized insertions, modifications, or deletion of data
- **Ransomware**
  - Malware disguised as files or games that is silently installed and encrypts a portion of the host machine
  - The attacker will try to demand payment from the victim in exchange for the encryption key

[1]

Factors Contributing to Incident Severity and Prioritization

- **Economic**
  - **Calculating the economic scope of an incident requires knowing the value of the asset/s involved**
    - **The value of an asset is relative to the organization**
    - **Considerations to assess the value of an asset**
      - **Effort required to develop the asset**
      - **Cost to maintain the asset**
      - **Resulting impact if the asset was lost or destroyed**
      - **Value of the asset to adversaries**
  - **Knowing the value of an asset**
    - **Organization will know how much money and time to spend on protecting the asset**
    - **E.g. if the calculated value of an organization's trade secret is X then the total cost of protecting that asset should not be larger than X** [1]

Factors Contributing to Incident Severity and Prioritization

- **System Process Criticality**
  - **Must determine essential processes for business operation**
    - **It's important to identify critical processes so that those processes are recovered first**
    - **Critical processes could include**
      - **Technical assets**
      - **Essential staff vital in the operations to get critical systems back online**
  - **Must educate members across the organization on**
    - **What the core processes are**
    - **How their work supports the goals of the processes**
    - **How they benefit from successful operations**
  - **Educating members of the organization is effective in providing a level of understanding to**
    - **Successfully respond to an incident**
    - **Recover from resulting damages**

[1]

Factors Contributing to Incident Severity and Prioritization

- **Probability**
  - The chances of a future event occurring
- **Criticality**
  - The impact of a future event
  - Usually expressed by degree such as high to low
    - **Low Criticality**
      - Indicates little impact to business operations
    - **Moderate Criticality**
      - Indicates impaired or degraded performance
    - **High Criticality**
      - Indicates a significant impairment of business functions
- **Risk Analysis**
  - Primary components are Probability and Criticality

[1]

Interactive Exercise 3

What is the RPO?	
How does the compromise of data integrity affect the severity and prioritization of an incident?	
Besides backing up your data and system configurations, what other two ways can we help ensure the integrity of our data?	
How does the system criticality affect the severity and prioritization of an incident?	

[1,4]

Interactive Exercise 3 Answers

What is the RPO?	Recovery Point Objective (RPO) identifies a point in time where data loss is acceptable.
How does the compromise of data integrity affect the severity and prioritization of an incident?	not always apparent that an attack on data integrity has taken place. This demonstrates why it's important to backup data and system configurations, and keep them sufficiently segregated from the network
Besides backing up your data and system configurations, what other two ways can we help ensure the integrity of our data?	1. File integrity checking with hashing 2. Verify your backups are not corrupted or infected with malware.
How does the system criticality affect the severity and prioritization of an incident?	you must determine which processes are considered essential for the business's operation. These processes are associated with tasks that must be accomplished with a certain level of consistency for a business to remain competitive.

[1,4]

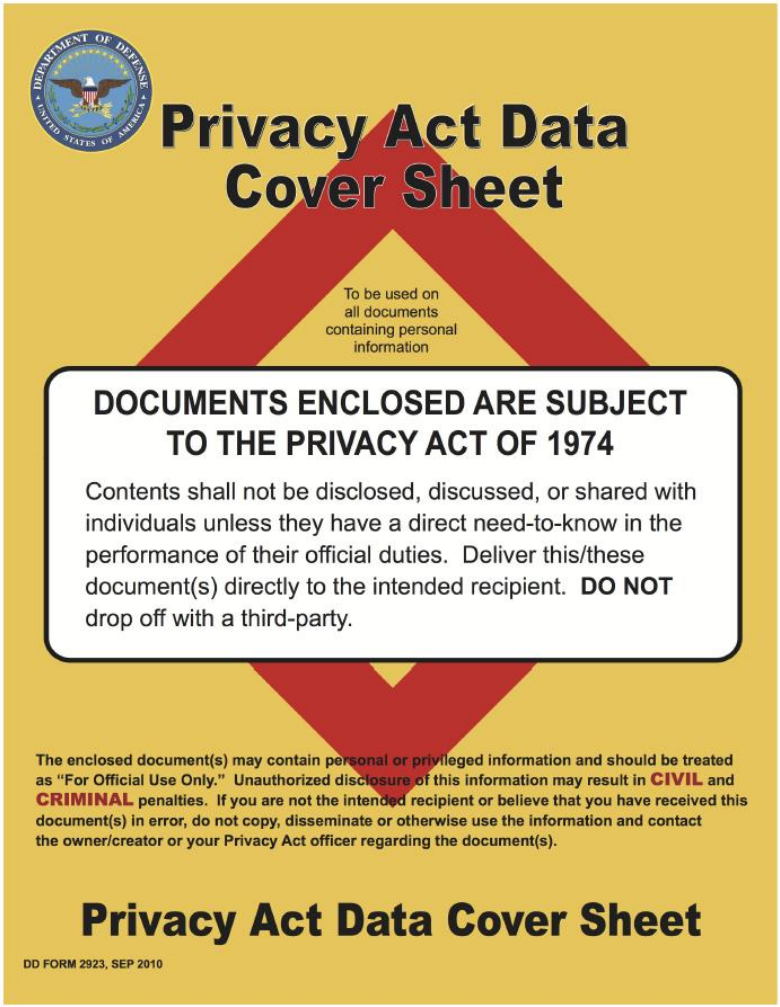
Types of Data

- **Types of Data**
  - **Some types of data require special care when storing and transmitting**
  - **Unauthorized disclosure of some types of data could have serious adverse effects on associated businesses, government, or individuals**
- **Personally Identifiable Information (PII)**
  - **Information that can be used to identify an individual such as**
    - **Biometric profile**
    - **Social Security number**
  - **Advisories often use this type of data to conduct identity theft or fraud**
  - **Privacy Act of 1974**
    - **Federal entities are required to follow strict rules regarding the collection, storage, use, and sharing of PII**

[1]

Types of Data

- PII
  - The DoD is required to have a coversheet that shows a given document contains PII
  - The figure to the right shows the DoD Form 2923, Privacy Act data coversheet



Privacy Act Data Cover Sheet

To be used on all documents containing personal information

DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974

Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. **DO NOT** drop off with a third-party.

The enclosed document(s) may contain personal or privileged information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in **CIVIL** and **CRIMINAL** penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).

Privacy Act Data Cover Sheet

DD FORM 2923, SEP 2010

[1]

Interactive Exercise 4

How can the types of data affect the severity and prioritization of an incident?

What is PII and what act establishes rules protecting it?	
What act establishes rules protecting PII?	

[1,4]

Interactive Exercise 4 Answers

How can the types of data affect the severity and prioritization of an incident?	No matter the type of data you may need to follow strict regulatory guidelines in your IR. Which might entail informing law enforcement or customers.
What is PII and what act establishes rules protecting it?	Personally Identifiable Information (PII) is information that can be used to distinguish a person's identity.
What act establishes rules protecting PII?	Privacy Act of 1974 establishes strict rules regarding the collection, storage, use, and sharing of PII when it's provided to federal entities.

[1,4]

Types of Data

- **Personal Health Information (PHI)**
  - **PHI is any data that relates to an individual's**
    - **past, present, or future physical or mental health condition**
  - **Typically this data is handled by**
    - **healthcare provider, employer, public health authority, or school**
  - **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
    - **A law that establishes standards to protect individuals' PHI**
      - **Requires appropriate safeguards to protect the privacy of PHI**
      - **Regulates what can be shared and with whom without the patient authorization**
      - **Violations have specific reporting requirements**
    - **Penalties for violation include**
      - **Fines and jail time for criminally liable groups**

[1]

Interactive Exercise 5

What is PHI?	
What act establishes rules protecting PHI?	

[1,4]

Interactive Exercise 5 Answers

What is PHI?	Personal Health Information (PHI)" is protected by the Health Insurance Portability.
What act establishes rules protecting PHI?	Accountability Act (HIPAA) of 1996. This is a law that established the standards to protect individuals' PHI. PHI is any data that relates to an individual's past, present, or future physical or mental health condition

[1,4]

Types of Data

- **Payment Card Information**
  - **Payment Card Industry Data Security Standard (PCI DSS)**
    - **Created to reduce credit card fraud and protect cardholder information**
    - **Global standard for protecting data that is**
      - **Stored, processed, or transmitted**
    - **To the right is a figure of general guidelines**
  - **PCI DSS is not a federal standard in the US**

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems aginst malware and regularly update anti-virus software or programs 6. Develop and maintain secure system and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

[1]

Types of Data

- **Intellectual Property**
  - An organization distinguishes itself from others by their individual knowledge on how to make something or by creating something unique
  - A policy should be in place to ensure employees
    - Know the latest legal guidance
    - Understand the importance of protecting intellectual property
    - Understand the consequences of unauthorized disclosure
- **Intellectual Property Laws**
  - Vary by country
  - Patents issued by the US Patent Office are only enforced in US territories

[1]

Types of Data

- **Intellectual Property Types**
  - **There are four categories of intellectual property**
    - **Patent**
      - **Provides the holder with exclusive rights to make, use, market, or sell a process or thing**
    - **Copyright**
      - **Tangible manifestation of an original creative expression**
      - **Extends to works published and unpublished**
      - **“Fair use” doctrine**
        - » **Permits limited use of copyrighted material without having to first acquire permission from the copyright holder**
        - » **Any work based on the copyrighted work can be used to justify a violation**

[1]

Types of Data

- **Intellectual Property Types**
  - **There are four categories of intellectual property**
    - **Trademark**
      - **An exclusive name or words that a business uses to distinguish itself or its product from others**
    - **Trade Secrets**
      - **Protected data on how a product is produced**
      - **The details of the secret are not documented or disclosed to any registration party**

[1]

Interactive Exercise 6

What is PCI and what standard protects it?	
What are the 4 types of intellectual property called?	
Between PII, PHI, intellectual property, and accounting data, which of the following is likeliest to require notification of government entities if it is compromised?	

[1,4]

Interactive Exercise 6 Answers

What is PCI and what standard protects it?	**Payment Card Information (PCI) is protected by The Payment Card Industry Data Security Standard (PCI DSS), which was created to reduce credit card fraud and protect card holder data.**
What are the 4 types of intellectual property called?	1) A patent: 2) Copyright 3) Trademark 4) Trade secrets
Between PII, PHI, intellectual property, and accounting data, which of the following is likeliest to require notification of government entities if it is compromised?	PHI

[1,4]

Types of Data

- **Corporate Confidential information**
  - **Information on the internal operations of a company such as**
    - **Changes to the hierarchy of the company**
    - **Marketing campaign details**
  - **Also known as proprietary information**
  - **This information is usually marked on corporate documents**
- **Accounting Data**
  - **Provides insight to the health of an organization**
  - **Access to accounting data should be on a need-to-know basis only**

[1]

Types of Data

- **Mergers and Acquisitions**
  - **Type of sensitive corporate data**
  - **Its exploitation is usually related to fraud and conspiracy**
  - **Insider trading**
    - **An employee that trades public company stock because of privileged knowledge of the company**
    - **Has civil and criminal penalties**
  - **Securities and Exchange Commission's Fair Disclosure**
    - **Dictates that if privileged knowledge is disclosed to one shareholder, then it is required to be disclosed to the public**

[1]

Interactive Exercise 7

What is corporate confidential information?

What makes information about mergers and acquisitions so sensitive? (Hint) May violate Securities and Exchange Commission's Fair Disclosure regulation	

[1,4]

Interactive Exercise 7 Answers

What is corporate confidential information?	Is any information about the internal operations of a company. EX: accounting data or merger and Acquisitions
What makes information about mergers and acquisitions so sensitive? (Hint) May violate Securities and Exchange Commission's Fair Disclosure regulation	If special knowledge about a company is disclosed to one shareholder, then it must be disclosed to the public

[1,4]

Quiz

Chapter 8

Question #1

- **1. Which of the following statements is true about a zero-day exploit?**
  - **A. It is a flaw in a piece of software of which the vendor is unaware**
  - **B. It is code written to take advantage of a software flaw unknown to its vendor**
  - **C. It is the day on which a vendor is notified of a flaw in its software**
  - **D. It is a cyber weapon developed exclusively by a nation-state adversary**

[1]

Answer #1

- **B**
  - **The code written to take advantage of a flaw that is unknown to its vendor or users is called a zero-day exploit**

[1]

Question #2

- **2. Advanced persistent threats (APTs) are best exemplified by which of the following?**
  - **A. Nation-state adversaries**
  - **B. Cybercrime syndicates**
  - **C. Hacktivist collectives**
  - **D. Script kiddies**

[1]

Answer #2

- **A**
  - **Advanced persistent threat (APT) is the name given to any number of stealthy and continuous computer-hacking efforts, often coordinated and executed by an organization or government with significant resources**
  - **Although the term can refer to certain powerful criminal organizations, nation-state adversaries is a better answer**

[1]

Question #3

- **3. All of the following are factors contributing to a determination of the scope of impact of an incident except which?**
  - **A. Recovery time**
  - **B. Downtime**
  - **C. Uptime**
  - **D. Data integrity**

[1]

Answer #3

- **C**
  - **The key factors to consider when determining the scope of impact of an incident are downtime, recovery time, data integrity, economic considerations, and system process criticality**

[1]

Question #4

- **4. Of the following types of data, which is the likeliest to require notification of government entities if it is compromised, lest your organization incur fines or jail sentences?**
  - **A. Personally identifiable information (PII)**
  - **B. Personal health information (PHI)**
  - **C. Intellectual property**
  - **D. Accounting data**

[1]

Answer #4

- **B**
  - **Personal health information (PHI) is strictly regulated in the U.S., and its disclosure could result in civil or criminal penalties**
  - **None of the other types of information listed are normally afforded this level of sensitivity**

[1]

Question #5

- **5. All of the following are types of protected intellectual property except which?**
  - **A. Trade secrets**
  - **B. Patents**
  - **C. Copyrights**
  - **D. Items covered by the "fair use" doctrine**

[1]

Answer #5

- **D**
  - **Intellectual property falls under four categories: patent, copyright, trademark, and trade secrets**

[1]

Question #6

- **6. What makes information about mergers and acquisitions so sensitive?**
  - **A. It can give an unfair advantage to the company being acquired**
  - **B. It is regulated by the PCI DSS**
  - **C. If it is disclosed to the public, it could lead to charges of insider trading**
  - **D. Its disclosure might violate Securities and Exchange Commission's regulations**

[1]

Answer #6

- **D**
  - **The Securities and Exchange Commission's Fair Disclosure regulation mandates that if special knowledge about a company is disclosed to one shareholder, then it must be disclosed to the public, so this information must be carefully controlled**

[1]

Scenario for Questions 7-10

- **You work for a large private hospital that specializes in a rare form of cancer treatment. Its reputation is such that its patients include some of the most prominent people from all over the world. Just last month, a multinational health services conglomerate quietly started an effort to acquire your hospital. Before the deal is finalized or made public, you are called in to respond to a particularly sophisticated incident after a three-letter government agency alerted your boss to a likely compromise. The threat actors appear to be targeting your account systems, but no data appears to have been modified or deleted. The initial attack vector appears to have been a previously unknown vulnerability in your perimeter firewall. It appears that the actors have been exfiltrating information from your system for several months, but this is the first you hear of it.**

Question #7

- **7. Who is the likeliest threat actor?**
  - **A. An APT**
  - **B. A cybercrime syndicate**
  - **C. A disgruntled insider**
  - **D. Script kiddies**

[1]

Answer #7

- **A**
  - **The combination of using a zero-day exploit and being on the network for months without making any demands, selling any information, or breaking anything strongly points to an advances persistent threat (APT)**
  - **This is further supported by the hospital's distinguished clientele**

[1]

Question #8

- **8. Your team has confirmed that the initial attack vector targeted a zero-day vulnerability in your firewall. What should you do next?**
  - **A. Notify the firewall vendor**
  - **B. Scan the firewall for vulnerabilities**
  - **C. Apply the latest patches to the firewall**
  - **D. Implement ACLs that mitigate the vulnerability**

[1]

Answer #8

- **A**
  - **A zero-day vulnerability is a flaw in a piece of software that the vendor is unaware of and thus has not issued a patch or advisory for**
  - **It is unlikely that you can mitigate the damage yourself, apart from switching to a different firewall**
  - **The best course of action is the notify the vendor immediately so it can develop a patch**

[1]

Question #9

- **9. which of the following factors is most important in determining the impact of the incident?**
  - **A. Systems process criticality**
  - **B. Economic considerations**
  - **C. Data integrity**
  - **D. Recovery time**

[1]

Answer #9

- **D**
  - **The attacker has been very stealthy and does not appear to have publicly released any of the harvested information. This points to an operation that is focused on surveillance rather than financial profit**
  - **Furthermore, the attacker does not appear to have modified or destroyed data or to have interfere with any critical processes**
  - **This means the best factor based on the information available is the amount of time it will take you to recover from this incident**

[1]

Question #10

- **10. In which of the following types of data is the attacker most likely interested?**
  - **A. Payment card information**
  - **B. Intellectual property**
  - **C. PII or PHI**
  - **D. Merger and acquisition**

[1]

Answer #10

- **C**
  - **The attacker does not appear to be motivated by monetary profits, so credit card information is unlikely to be the goal**
  - **The fact the attack appears to have started before the acquisition makes it less likely that the merger and acquisition information was targeted**
  - **Though it is possible that the attacker is after intellectual property regarding cancer treatments, it is more likely that an APT would be interested in PII and/or PHI about prominent world figures**

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. TruSTAR's SANS Internet Storm Center Threat Intelligence Integration. TruSTAR 2020. https://www.trustar.co/integrations/sans-internet-storm-center-integration
3. CERT/CC Coordinated Vulnerability Disclosure Since 1988. Hacker1 2016. https://hackerone.com/cert?type=team
4. friedaj friedaj, "CySA+ Chapter 8: Determining the Impact of Incidents," quizlet, 03-Mar-2018. [Online]. Available: https://quizlet.com/296891096/cysa-chapter-8-determining-the-impact-of-incidents-flash-cards/. [Accessed: 09-Feb-2021].