THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Doctor of Engineering – Cybersecurity Analytics

Cohort: DC7

CSCI 6015: Cyber Forensics

August 27, 2024

ASSIGNMENT: HOMEWORK – 1

A. Define at least three levels of classifying cyber incidents and provide a few examples for each classification.
B. Describe how the Computer Incident Response team would use this classification matrix to determine how to triage incidents and decide how to address them?
C. Describe an approach to test the effectiveness of this incident response plan.

SUBMITTED BY

Viswanath S CHIRRAVURI
G34657239
viswanath.chirravuri@gwu.edu

(Under the guidance of Professor Sean Baggott)

1A. Define at least three levels of classifying cyber incidents and provide a few examples for each classification.

Levels

The four levels of classifying cyber incidents are:

1. **P1: CRITICAL**
2. **P2: HIGH**
3. **P3: MEDIUM**
4. **P4: LOW**

Definition

P1 (CRITICAL)	P2 (HIGH)	P3 (MEDIUM)	P4 (LOW)
Severe impact incidents. These often involve critical data breaches, multiple systems compromise, significant financial loss or regulatory issues, multiple customer complaints, and that could lead to potential significant reputational damage.	High impact incidents. These typically involve disruptions to operations or compromise of a limited number of systems or data. These usually require some level of intervention to prevent escalation but are not immediately critical.	Moderate impact incidents. These involve the compromise of non-critical systems or data, leading to disruptions in certain business functions or affecting specific departments. Operations are not completely affected.	Minor incidents. These typically cause little or no damage to systems or data. These do not have impact on operations. These typically involve routine issues that can be resolved quickly and have no lasting effects.

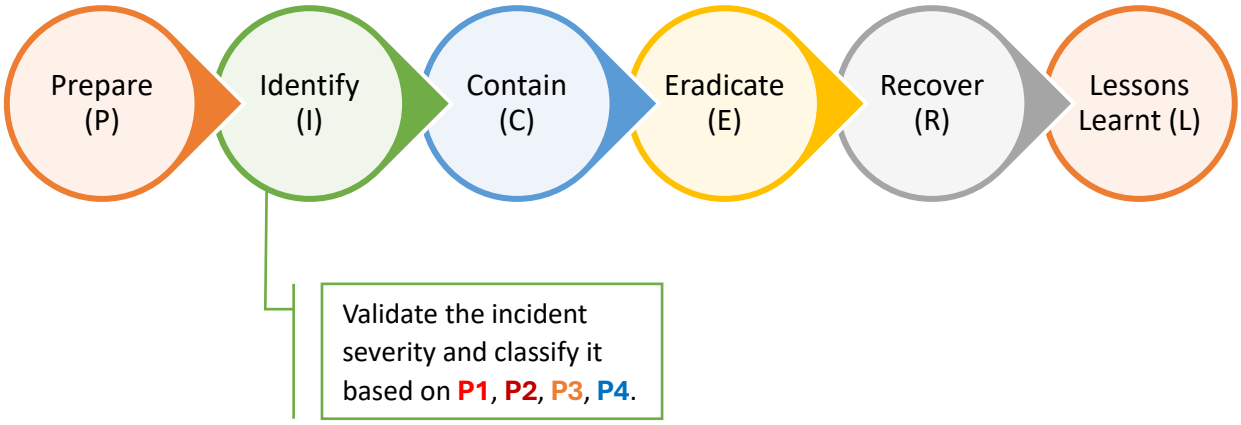
Examples

P1 (CRITICAL)	P2 (HIGH)	P3 (MEDIUM)	P3 (LOW)
Massive data breach via advanced persistent threat (APT) A major bank accidentally exposed millions of customers' credit card information stored in its private cloud. This has led to big financial and reputation losses because many people have filed lawsuits against the bank.	Ransomware A ransomware attack successfully encrypted important files, causing problems in a specific data center and disrupting business operations. The attackers are asking for a ransom to unlock the files. However, the impact is limited to a specific team or customer and hasn't widely affected everyone.	Unauthorized Access to Non-Critical Systems An unauthorized user gains access to a company's internal HR system by exploiting weak credentials. The breach allows the intruder to view non-sensitive employee information such as names, work email addresses, and job titles. While this doesn't include sensitive personal information like Social Security numbers or financial details, it disrupts the HR department's ability to operate normally.	Phishing Email Attempt An employee gets a suspicious email that appears to be from the IT department, asking them to reset their password by clicking a link. After looking into it, it turns out the email has a tracker from a vendor to validate the user's email.

Large-Scale Data Breach in Healthcare Organization A healthcare provider experiences a significant data breach where hackers access and steal sensitive patient information, including medical records and personal identification details. The breach affects a vast number of patients and compromises both medical and financial data. This incident results in substantial financial losses due to legal fees and fines, numerous customer complaints, and major reputational damage.	Email System Compromise An attacker gains unauthorized access to the company's email system, allowing them to intercept and alter email communications. This breach affects only the marketing department's email accounts, disrupting internal and external communications. While not critical to overall operations, it requires intervention to prevent further misuse of sensitive information and restore normal email functionality.	Compromised Conference Room System A company's conference room management system is hacked, allowing unauthorized access to internal meeting schedules and room booking details. This incident impacts the efficiency of meeting room management within the organization but does not affect core business operations or sensitive data. The disruption is limited to scheduling conflicts and internal communication issues.	Misconfigured Printer Settings An office printer is found to have misconfigured settings, causing it to print documents publicly accessible within the office. This results in some internal documents being printed in the wrong location but does not expose sensitive data or affect operations. The issue is minor and resolved quickly without any major impact on business activities.

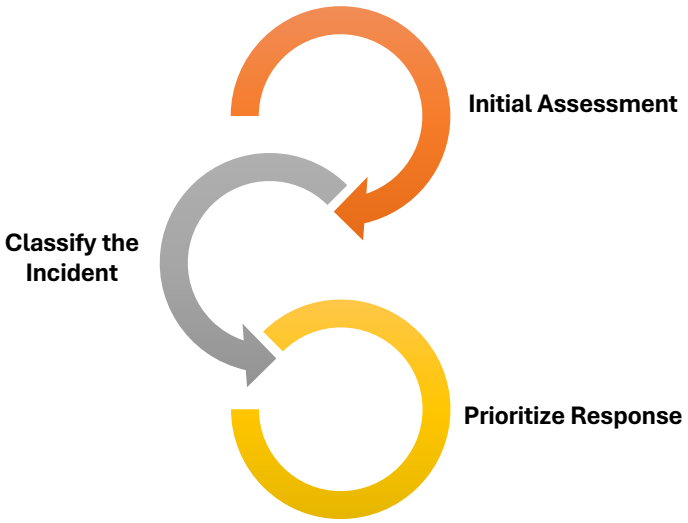
1B. Describe how the Computer Incident Response team would use this classification matrix to determine how to triage incidents and decide how to address them?

A CIRT (Computer Incident Response Team) must implement the PICERL framework, in that order, to deal with cyber incidents. That said, CIRT must follow the aforementioned classification matrix to classify the incident.



- **PREPARE**: This phase makes sure the right people are assigned to handle incidents and that they are well-trained. It ensures that processes are defined and accepted across the organization. It also uses feedback from past incidents to keep improving the process.
- **IDENTIFY**: This phase is to validate the incident and to classify it based on predefined labels.
- **CONTAIN**: This phase limits the damage of the ongoing attack by temporarily mitigating the risk of further damage.
- **ERADICATE**: This phase completely removes the attacker's payload from the ecosystem to ensure the future operations bears no impact from the previous cyberattacks.
- **RECOVER**: This phase will restore business operations in a controlled manner that will not further lead to any damage from the previous cyberattacks.
- **LESSONS LEARNT:** This phase analyzes the steps that could have prevented the cyberattack in the first place, and updates necessary policies, standards, guidelines, and procedures that lead to the normal business operations. It can also contribute to the enhancement of the preparation phase of IR process.

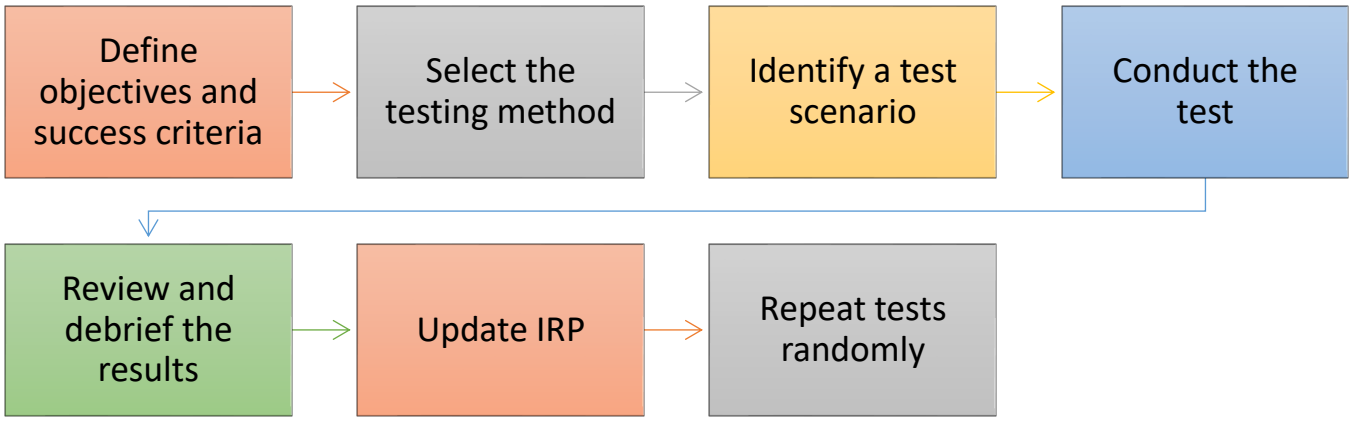
STEPS TO VALIDATE THE INCIDENT AT <u>IDENTIFY</u> PHASE



- Initial Assessment:
    - Receive Incident Report: Gather all available details about the incident, including the nature of the threat, affected systems, and potential impact.
    - Verify Authenticity: Ensure that the incident is genuine and not a false alarm.
- Classify the Incident: Assign a classification label based on the impact, urgency, and potential damage. Use the labels provided:
    - P1: CRITICAL (Severe impact incidents)
    - P2: HIGH (High impact incidents)
    - P3: MEDIUM (Moderate impact incidents)
    - P4: LOW (Minor incidents)
- Prioritize Response:
    - P1: CRITICAL: Immediate Action: Activate the incident response team (IRT), notify executive management, implement containment measures.
    - P2 (High): Prompt Action: Address the incident quickly with impacted team involved.
    - P3 (Medium): Scheduled Action: Address during regular business hours.
    - P4 (Low): Routine Action: Handle during standard operational procedures.

1C. Describe an approach to test the effectiveness of this incident response plan.

To the effectiveness of an incident response plan, one must follow this process:



Describing each one briefly:

1. **Define objectives and success criteria**: This is about how to interpret the results from the tests. For example, identify and agree upon the response time of the CIRT team members for specific classification of cyberattack.
2. **Selecting the testing method**: This is about what testing method to use to evaluate the IR process.
    a. **Table-Top**: Discussing over a meeting room with simulations in mind to evaluate the framework.
    b. **Simulation**: Hands-on driven tests in a controlled environment to evaluate the framework.
    c. **Full-scale**: Simulating a real-world cyberattack from a authorized and contracted third-party vendor.
3. **Identify and test scenario**: Pick one classification-level of cyberattack (**P1**, **P2**, **P3**, **P4**) and agree upon the associated test to perform.
4. **Conduct the test**: Launch the attack and closely monitor the behavior of every person and system involved in the attack.
5. **Review and debrief the results**: Collect feedback from people involved and discuss/debate among peers to identify changes to be made to the IRP or future tests.
6. **Update IRP**: Release new versions of the framework or policy document. Communicate and educate the changes made in the new version to the involved people.
7. **Repeat tests randomly**: Schedule future tests without prior notification of the schedule to the people involved (like a fire-drill).

***** END OF DOCUMENT *****