National College of Ireland

Project Submission Sheet

Student Name:	Pranav Prasanna Ghorpade		
Student ID:	X22197044		
Programme:	MSc. CyberSecurity	**Year:**	2023-24
Module:	Business Resilience and Incident Management		
Lecturer:	Joel Aleburu		
Submission Due Date:	09/08/2024		
Project Title:	Continuous Assessment 2 (60%)		
Word Count:	4367		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature:	Pranav Prasanna Ghorpade
Date:	09/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

[Business Resilience and Incident Management]

[Continuous Assessment 2 (60%)]

Your Name/Student Number	Course	Date
Pranav Prasanna Ghorpade/X22197044	MSc. CyberSecurity	09/08/2024

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name]	
[Insert Description of use]	
[Insert Sample prompt]	[Insert Sample response]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]

Question 1

Consequence of Cyberspace Incidents on Business Ventures

The consequences of cyber-attacks can be effectively deep and far-reaching affecting such business aspects as operations, revenues, and public image.

OPERATIONAL IMPACT: It is also known that certain kinds of cyber-attacks can impact the business operations to an extent that the down time is vast. This is especially the case with ransomware where core functions are locked in a ransom to be paid before they are unblocked. Also, the recovery process, after formulating the problem and arriving at a solution, can be quite strenuous and time-consuming and involves numerous IT services to get back to regular functioning. Perturbations can occur and they hinder economic activities and trigger a domino effect on the flow of business processes and the delivery of products and services which, consequently, poses a threat to the business's capacity to operate. [1]

FINANCIAL IMPACT: These are in several cases costly especially since more and more of the organizations' business is controlled through the internet. For the organization, there are direct costs including the ransom amounts, lawyers or legal representatives' fees, and penalties for not adhering to data protection laws. Other expenses that can be considered as indirect are fines that are incurred by the company due to business interruption, the expense incurred in making the necessary repairs, and any other expenses that would be on the increased insurance premium rates. For instance, Ponemon Institute now puts the global mean cost of a data breach at over $4 million, and these it may go higher for industries that manage on delicate data such as healthcare and finance. [2]

REPUTATIONAL IMPACT: Le noted that the loss of reputation can be tricky for a firm when it is done and can take years to be regained. This would make customers unable to trust a business with their personal data hence crossing over to other businesses that will honor their privacy, loss of business prospects, and finally, a low stock value. Gaining back people's trust may sometimes be a slow process and can entail huge spends on public relations apart from upgrading security.[1]

Overview of the Threat Landscape

Closely related to the above is the importance of comprehending the cyber threat environment Since there are always risks involved in the online environment, it is vital to know them and be prepared. Network elements are not static, which implies that new threats and threat agents who are likely to employ new tactics are ever coming into the market.

Threat Actors: Some of the most frequent threat actors are; Cybercriminals, nation-state threats, insiders, hackers, and cyber terrorists. They are primarily Economically motivated and use ransomware or phishing as their method. This involves entities whose primary motivation is due to political reasons; they can spy or launch an attack on computer-controlled systems. Insider threats are attacks carried out by people within an organization whether through negligence or being a contractor while Hacktivists attack organizations for political or social causes . [2]

Motivations: The motives of these threat actors are very diverse and range from criminals and political activists-fanatics to corporate rivals and revenge seekers. For example, ransomware is usually financially driven, while nation-state attacks can be for the purpose of sabotage or spying on facilities of significance . [2]

Tactics, Techniques, and Procedures (TTPs): The activities include malware, phishing, DoS, and vulnerability exploitation as applied by threat actors. Spear-phishing, social engineering and using zero day vulnerabilities are some of the techniques used.[2] These techniques are carried out through procedures also known as processes where concepts such as; complex coordination and advanced persistent threats (APTs) are used to target definite organizations for extended time durations .[1]

Significance of Assessing Impacts and Understanding the Threat Landscape

Assessing the impacts of cyber-attacks and understanding the threat landscape are critical for several reasons:

Proactive Defence: Anticipating such effects also allows organisations to allocate efforts and capital in cybersecurity strategically. This comprises conducting periodic security assessments, conducting awareness campaigns for employees in the organization, and putting into use modern Information technologies in the organization . [1]

Incident Response Preparedness: This help organizations to not only identify the threats current facing them but also how they can create a unique incident response plan for the threats. This preparedness can go a long way in lessening blow when it happens keeping damages and time lost to a bare minimum thus the encouragement to be prepared . [2]

Regulatory Compliance: It is worth to know that a lot of industries work under some rules and requirements, which deal with data protection. As such a clear comprehension of the threat puts businesses in the right side of the law, and makes sure that they do not incur the wrath of the law or lose sensitive information through breaches . [2]

Long-term Business Sustainability: Prevention of these threats plays a central role in the competitive security model or sustainable business security. They must create trust with their customers and sustain competitive advantage in the growing era of digital business .[1]

Question 2

1.Describe in detail, major activities of the Blue Team and their assigned roles.

The Blue Team is the defence team in an organization that works hard to shield an organization from cyber dangers. Their roles cut across all the strategies in the handling of incidents, with the aim of safeguarding the organization's assets.

Preparation: The Blue Team also ensures it has set and adheres to functional security policies as well as comprises of functional security controls and makes sure the organization is ready to handle any incidents by having an adequate common incident response plan in place. It entails training or security awareness programs to let the staff know of the risks and how they can avoid them. [3]

Detection: The Blue Team during the detection phase analyse the network traffic and system logs for such activities using SIEM, IDS, and EDR tools. They use these data points to find out the possible security incidents soon . [4]

Containment: After this, the Blue Team swings into action to neutralize the threat Before proceeding to leverage the information below; This may include disconnecting the infected systems, blacklisting the incoming traffic as well as applying security updates to the infected systems to contain the attack . [5]

Eradication: During this phase, the Blue Team's major focus is to eradicate the threat in the given environment. This involves removing the malware, closing down the exploitation breaches and putting systems back to their secure state. They may also analyse the fundamental cause of the breech to know how theissue happened . [4]

Recovery: The Blue Team's primary role is restoration after the elimination of threats in the organization's environment. This entails initiating recovery from backups, assessments to confirm system health, and verification of the systems' security before returning the systems to full use. They also persistently scan for tones of sustained menace . [5]

Lessons Learned: Daily, the Blue Team analyses the possible occurrence of an incident, what happened, and what more could be done better. This phase is especially important to the fine-tuning of the response to the incident and the readiness of measures against similar incidents .[3]

2. Specific actions/responsibilities include the following:

The red team employs the concepts of penetration testing that involves simulating an attack on the organization's defenses. Their purpose is mainly to find and take advantage of weaknesses in the system to better recreate conditions of actual attacks.

Simulating Attacks: To simulate possible attacks, the Red Team employs tactics, techniques, and procedures or TTPs like penetration testing, social engineering attacks in addition to physical intrusion. They use exploit kits, password cracking tools and bespoke malware to move beyond the defenses . [5]

Testing Defenses: In this case, the Red Team would attempt to penetrate the organization's security and expose vulnerabilities that the Blue Team might be ignorant of. It assists in ascertaining the efficiency of the existing security controls and areas of improvement where needed . [5]

Reporting and Recommendations: In a post-engagement scenario, the Red Team gives comprehensive reports and exposes aspects that were leveraged on, and where the organization stands to improve on. These are important feedbacks that the Blue Team ought to endeavour to counter in order to strengthen the security of the organization's defences . [5]

3. Interdependency of Blue Team and Red Team

It is exceptionally important for the Blue Team and the Red Team to engage in cooperation as this way, the business can be sustained, and the overall security status can be enhanced.

Feedback Loop: In the Red Team exercise, some of the observations are as follows, after the presentation it is presented to the blue team to plug those gaps and strengthen security. This forms a cycle of incremental improvement of defences whereby defences are challenged and improvement based on cyberspace attack simulations as noted in Secure Layer 7.[5]

Joint Exercises: In some cases, both teams 'engage" in the "Purple Team" study where both teams attack and defend together. Such a model is beneficial because it enables the two teams to provide feedback and learn as the procedures are being undertaken; thus, they can change strategy as they progress, making the system more secure . [3]

Enhanced Business Continuity: Making sure that the organization can quickly recover from incidents and thereby sustaining the operations of the business is the reason that both teams work as protective shields that have been put in place to rigorously test for threats as they defend the organization. These results are used in fine-tuning disaster recovery and incident response procedures.[6]

Question 3

Incident Response (IR) capability is crucial as a means of efficient protection of an organisation's business from insurgency of the cyber risks. key components include:

Incident Identification and Classification: This involve coming up with proper procedures of how to categorize or use criteria in splitting the incidents depending on the level of harm they cause. Thus, proper classification helps for quick and adequate response by which important incidents are properly prioritized and solved.[7]

Roles and Responsibilities: In scenario, it is necessary to define activities and functions of all participants in the incident response process. This also includes not only technical team but also legal, communication and management teams thus providing a technically sound, legal, communicational and management coverage to the issue . [7]

Communication and Coordination: Incident communication is crucial since it helps in the handling of the situation. Implementing the process of internal and external communication helps in the provision of the right information promptly thereby preventing wucking and confusion in responding to the event . [7]

Incident Containment and Remediation: This component is the measure to avert the incident from getting worse, for instance, one isolating the systems that are infected or applying patches. Remediation is centered on eradicating threat and bringing back the systems to their original state as they were before the incident happened . [7]

Continuous Monitoring and Improvement: Following an occurrence, it is critical to analyze the response process, evaluate the weaknesses, and update the firm's IR plan. Thus, through constant observation, signs of deviation are quickly noticed, and necessary measures are promptly taken . [8]

Fostering Methods and Techniques in Extending IR Activities in Large and Small Organisations

If many incidents are expected, it is essential to ramp up the activity levels for incident response both in more significant organizations and in smaller ones, although the approaches may vary.

Large Organizations: When it comes to large organizations, scalability is a process that includes the implementation of innovative technologies such as Security Information and Event Management systems, job automation, and cloud-based IR solutions. These organizations can also scale by assembling specialized groups with respect to some types of incidents like forensic, containment, and recovery . [8]

Small Organizations: It is not always possible for small organization to assign full time IR professionals and special team. However, they need not invest in large & independent managed IR solutions but can provide their IR scale to MSSP or can easily transit to cloud based solutions. Another way that many organisations practice is by training people to multitask in the IR process, especially in smaller entities. [9]

Continuous improvement has also been defined as a process of constant enhancement in clients, goods and services, and business processes.

Consistency is one of the critical concepts of Incident Response processes. It helps the organization to have a good posture in achieving IR goals because the organization deals with the threats of today but at the same time develops a good posture to meet future threats.

Post-Incident Reviews: The two important practices include the need to obtain permission to debrief from the affected organization, especially if the incident arose from a disaster as well as to conduct comprehensive 'what went wrong' and 'what went right' assessments. Thus, the analysis facilitates improvement of the incident response plan, gap closure and overall organisational security . [7]

Regular Testing and Simulations: Testing the IR plan on a regular basis through simulations, 'table-top' and 'real-life' is an absolute necessity. These exercises expose the plan's flaws and let the organization modify processes and equipment accordingly . [7]

Adapting to New Threats: The threat sources are dynamic in this world and so should be the incident response management and functions. A key factor of learning in organizations is the constant assessment of threats in an organization's environment and the integration of new TTPs into an organization's IR process .[9]

Question 4

Roles to be Established within Key Incidents and the Importance of System Forensic Tools

1. Incorporation of IR Roles and Specific Detailing of Each Role

Thus, role and responsibilities are one of the vital components within an incident response (IR) process. Here's a mapping of key IR roles to their specific activities during an incident:

Incident Commander: The duties of the Incident Commander include managing the whole process of the incident response plans and implementation. They oversee the activities of all the teams, make strategic decisions, and see to it that the response efforts are consistent with the organization's goals. The Incident Commander also interacts with other organizations of the company and other stakeholders to report or to request for permissions as permitted. [10]

Forensic Analyst: It would help if you considered Forensic Analysts highly involved in examining the occurrence of the misfortune. Digital forensic experts more often than not involve in the process of collecting, storing , and analyzing digital evidence. Such activities include perusing through the systems and network logs as well as other electronic traces that aim at establishing the initial point of compromise, the scope of the attackers' activities, and their methodologies. The ''Forensic Analyst'' work is useful for containment, remediation and post-incident analysis summary. [11]

Communication Lead: The Communication Lead is in charge of all the correspondence within and outside the organization in case of an incident. They make sure that all relevant information that's to be relayed to the employees, customers, or other regulatory agencies is correct. This function is most crucial for issues to do with transparency, public relations, and statutory compliance of the firm . [10]

Legal Counsel: Legal department gives the perspective of the legal consequences in relation to the incident. This involves determining legal responsibility and compliance as well as guaranteeing that activities performed in the response process are legal. They also act as a way of recording the incident for future use in case there is a lawsuit or there is a regulatory investigation coming in. [12]

IT Support: IT Support is involved in concerned technical issues pertaining to the response, like locking down the infected systems, applying security patches as well as reviving the dented functionality. They have a technical collaboration with both the Forensic Analyst and Incident Commander in relation to Containment and Remediation Procedures . [11]

2. The Evaluation of System Forensics Tools as used in Analysing and Mitigating Information Security Threats and Leaks

The tools include system forensics tools that are important in the incident response process because they contain the features that are required in the process of investigating and handling cyber incidents. These tools serve several critical functions:

Incident Identification: The forensics tools assist in the identification of the existence of a breach by analyzing system logs, network traffic among others. They can easily detect those other patterns that signify unauthorized access or any other malicious activity . [12]

Evidence Collection and Preservation: Computer forensics tools: They are also used in processing and retrieving evidence in computer related crimes in a way that does not influence the original results. This is vital especially when conducting research and in the prosecution of the case when it gets to court. Effective management of evidence entails the proper collection and storage of data in a format that would allow it to support the organization's case in courts or before regulators . [12]

Root Cause Analysis: These tools enable the forensic analysts to perform detailed analyses of the incident and get to the bottom of it and also on the modus operandi employed by intruders. Mentioned information proofs the fact that identification of the cause is an imperative step towards further preventing of similar events and performing remedial actions . [12]

Reporting and Documentation: There are also forensic tools that provide elaborate compliments that outline the findings of the search. They can be utilized for internal cases and meetings, regulatory requirements and to improve the given structure of the incident response plan. Documentation is critical in enhancing the subsequent action plans while enhancing the stability of the overall security of an organization . [11]

3. Aid of Roles and Tools to the Improvement of Business Acutenization and Handling of Incidents

Because the introduction of the new incident response roles and employment of system forensics tools are complementary, they greatly contribute for business to become more resilient. This way, organisations make certain that there are no gaps in the management of the event reducing the probability of missing out something. Anticipative tools assist by offering the right information and analysis needed for the management and containing of the event properly.

When combined, these components help firms minimize downtime, safeguard vital assets, and ensure business continuity by enabling quick and fast responses to catastrophes. The organization's incident response skills are continuously improved to tackle emerging risks, thanks to insights gleaned from forensic analysis.

Question 5

The primary role of Regulation and Operational Resilience in an incident and the significance of Threat Intelligence.

1. Impact of Threat Intelligence to the sound practice of Security Controls and Incident Handling and Operational Continuity

New threats are always emerging in the modern world, which is why threat intelligence is such an important part of a quality cybersecurity plan. It entails gathering, processing, and sharing information that relates to the likely threats in the future and those that are current depicting the ability of an organization in preventing future risks. When threat intelligence is incorporated in security activities, an organisation can obtain new threats, recognise the TTPs of attackers and adapt its protection measures.

Operational resilience which is a business’s capacity to continue operations after disruption is boosted by threat intelligence. It facilitates organizations to do a better job of managing an incident due to the timely information that can generated from the system. For example, understanding the methods thant a ransomware group such as LockBit uses helps the defense better prepare for the attacks, thus negating the attacks’ impacts. [13]

2. Role of Questions 5: Effects of compliance Standards on Operation of Businesses and Management of Incidents

Legal policies are among the critical determinants that define organisational cybersecurity and incident response systems. Other regulations that have emerged include the Digital Operational Resilience Act (DORA) in the EU, which require strong ICT risk management and operational resilience policies for organizations with this sector especially the financial institutions. These regulation help to establish that the firms are ready to responses to cyber risks and manage their impacts, thus reducing disturbances to key services. [14]

Adherence to these regulations can only be met through the employment of complex security controls, exercise of security scenarios, and evaluation of third-party risks. Though they entail subsidisation, these demands are critical for keeping the stakeholders' confidence especially in these turbulent times when business operations may be disrupted . [15]

3. Advantages of Adopting Threat Intelligence to Enhance the Results of Handling Incidents

Threat intelligence must therefore be incorporated into the incident response processes if the results are to be enhanced. This assists organizations in identifying threats and dealing with them much faster and effectively. For example, using real-time information on the current threats and threats in development can help security managers to allocate resources more efficiently, thus minimizing the time required to respond to a given threat and sanitize the organization's systems and data . [16]

Also, threat intelligence makes a positive contribution to the process of developing a management cycle for incidents. When quantitative data of threats that have occurred in the past is studied, then an organization will need to work on honing its threat detection and response mechanisms, in anticipation of future incidents. It all this not only increases security but also helps to create an Organisation's long-term ability to operate effectively when challenged. [13]

References

[1] D. Irby, "Understanding the Modern Cyber-Threat Landscape and Its Impact on Your Business Operations," SecurIT360. Accessed: Aug. 09, 2024. [Online]. Available: https://www.securit360.com/blog/understanding-modern-cyber-threat-landscape-impact-on-business-operations/

[2] C. S. E. Canada, "National Cyber Threat Assessment 2023-2024," Canadian Centre for Cyber Security. Accessed: Aug. 09, 2024. [Online]. Available: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

[3] "Red Teams vs. Blue Teams: What's The Difference? | Splunk." Accessed: Aug. 09, 2024. [Online]. Available: https://www.splunk.com/en_us/blog/learn/red-team-vs-blue-team.html

[4] "Red Team Vs. Blue Team Cyber Security." Accessed: Aug. 09, 2024. [Online]. Available: https://thecyphere.com/blog/red-team-blue-team/

[5] M. Maheshwari, "An Overview: Red Team Vs Blue team – Securelayer7," Penetration Testing and CyberSecurity Solution - SecureLayer7. Accessed: Aug. 09, 2024. [Online]. Available: https://blog.securelayer7.net/red-team-vs-blue-team/

[6] Dansimp, "Incident response planning." Accessed: Aug. 09, 2024. [Online]. Available: https://learn.microsoft.com/en-us/security/operations/incident-response-planning

[7] "Building an Incident Response Plan: Business Resilience against Cyber Threats." Accessed: Aug. 09, 2024. [Online]. Available: https://atlantsecurity.com/incident-response-plan-business-resilience/

[8] "Incident Management as a Platform: Scaling Incident Response." Accessed: Aug. 09, 2024. [Online]. Available: https://www.moxfive.com//blog/incident-management-as-a-platform-scaling-incident-response

[9] "The National Cyber Incident Response Plan (NCIRP) | CISA." Accessed: Aug. 09, 2024. [Online]. Available: https://www.cisa.gov/national-cyber-incident-response-plan-ncirp

[10] B. T. R. Viewpoint Editor at GRC, "Digital Forensics Combined with Incident Response, A significant Trend in 2023?," GRC Viewpoint. Accessed: Aug. 09, 2024. [Online]. Available:

https://grcviewpoint.com/digital-forensics-combined-with-incident-response-a-significant-trend-in-2023/
[11] E. Salfati and M. Pease, “Digital Forensics and Incident Response (DFIR) framework for Operational Technology (OT),” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST IR 8428, Jun. 2022. doi: 10.6028/NIST.IR.8428.
[12] “The Crucial Role of Digital Forensics in Effective Incident Response: 6 Key Insights - Virtual Cyber Labs.” Accessed: Aug. 09, 2024. [Online]. Available: https://virtualcyberlabs.com/digital-forensics-in-incident-response/
[13] “Top Ten Cyber Risk Predictions for 2024,” Resilience. Accessed: Aug. 09, 2024. [Online]. Available: https://www.cyberresilience.com/threatonomics/cyber-risk-predictions-for-2024/
[14] “Digital Operational Resilience Act (DORA) - European Union.” Accessed: Aug. 09, 2024. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[15] “Emerging Regulatory Focus: Operational Resilience.” Accessed: Aug. 09, 2024. [Online]. Available: https://kpmg.com/us/en/articles/2024/emerging-regulatory-focus-operational-resilience-reg-alert.html
[16] “Cyber Security Trends For 2024.” Accessed: Aug. 09, 2024. [Online]. Available: https://www.cybersecurityintelligence.com/blog/cyber-security-trends-for-2024-7287.html