National College of Ireland

National College of Ireland

Project Submission Sheet

Student Name: Matthew Browne

Student ID: x21174415@student.ncirl.ie

Programme: MSc/PGD in Cybersecurity **Year:** 1

Module: Business Resilience and Incident Management

Lecturer: Eugene McLaughlin MSc/PGD

Submission Due Date: 24th October 2025

Word Count: 7995

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 authors' 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: Matthew Browne

Date: 24th October 2025

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

Your Name/Student Number	Course	Date
Name: Matthew Browne Student Number: x21174415	MSc/PGD in Cybersecurity	24/10/2025

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
Not Applicable		

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**.

Not Applicable

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]

Not Applicable

Continuous Assessment Name	Business Resilience and Incident Management CA1
Student Name	Matthew Browne
Student ID	x21174415
Student Email	x21174415@student.ncirl.ie

Contents

Introduction

As part of my Business Resilience and Incident Management module for my PgD Cybersecurity, my assessment briefing will focus on evaluating an organization's incident response plan, I'll be looking to showcase this by using both a hypothetical and a real-world scenario. My hypothetical case will be "BestSvschools" this is a fictional made-up school I created for my analysis, and my real-world scenario will be "Munster Technological University" (MTU) which is a third level university and institution based out of Co. Cork Ireland. By using both I'll be able to demonstrate how a cyber incident was managed and then recovered from in respect of the Nist incident response life cycle ill also be able to demonstrate how educational institutions and organizations can strengthen their resilience against cybercrimes and threats, improving their security posture and incident management process and how they can align their responses and recovery plans with known frameworks such as "NIST SP 800-61r3" or "ISO".

Both my fictional and real life analysis describe and discuss the typical way in which organizations sometimes use frameworks like the NIST SP 800-61r3" to compare and contrast methods used for identification of a malicious actor like indicator of compromise , detections for indicators of compromise like there cve scores or what we might see on a server like known bad file extension types such as "crypto" (Beforecrypt.com, 2024) , the ways in which the organizations look to eradicate and contain the malicious threats and how might these organizations and educational institutions may look to fortify the defenses for the next time an incident might happen in keeping with their business continuity and disaster recovery plans.

BestSvchools is prestigious fictional second level academy based out of Ireland that processes large quantities of personally identifiable student records and data across their multifaceted IT and cloud infrastructure, this is shared across providers like Aws and Azure. BestSvchools strive every day to ensure the confidentiality of their user data, the integrity of their data at rest, in transit and in use mitigating both the known threats and the unknown threats across their hybrid infrastructure worldwide, this is also known as the "CIA Triad" (Fortinet , 2025). Munster Technological University is a third level university based out of Ireland, (MTU) just like BestSvschools it also processes large quantities of personally identifiable student records and data across their multifaceted IT and cloud infrastructure. Unlike BestSvchools, MTU was subjected to a recent cyber-attack which makes it an ideal candidate for my paper.

With cybersecurity threats occurring daily, both institutions are faced with thousands of cyber threats, exploits, vulnerabilities and threat actors attacking their Microsoft teams, SharePoint, OneDrive, Active Directory and identity and access systems both on-premises and in the cloud alongside their virtual desktop environments across Microsoft Azure and Amazon Webservices , here I'll be looking to recommend ways of strengthen their overall resilience and recovery capabilities in the name of business continuity and disaster recovery.

Question 1, Evaluation of "BestSvchools" Incident Response Plan

BestSvchools like many educational institutions provides educational services to around 12,000 + students and 300+ staff members alike through its IT Infrastructure, it hosts allot of personally identifiable information for both students and staff which vary in size like lecture records, assessment data, financial records such as payments and deposits and so on , The institution uses a combination of Microsoft 365 , Defender , Sentinel and more to record conditional access to resources and monitor for threats , although it's using a combination of services from the Microsoft security stack it doesn't have a very mature incident response plan.

BestSvchools current incident response plan incorporates some of the basic phases of the incident response lifecycle from the NIST Framework, for preparation, BestSvchools uses a Microsoft Azure backup server to back up its active directory environment and its file servers to an Azure resource vault, but in saying this it doesn't provide its technical staff with training around when to escalate issues with backups , Some of the incident response lifecycle protocols aren't clear for when something goes wrong for example when where and how to escalate a backup incident or failure this is because they don't have proper structure in their security team.

BestSvchools does operate under the detection and analysis phase of the incident response lifecycle , how it does this is it operates its own mini Security Operation Center also known as (Soc) for short it uses Microsoft technologies like Azure Sentinel for log ingestion and correlation but it doesn't once again fully operate with a standard operating procedure for this like putting classifications on alerts being generated , again not following Nist best practices , this is due to a low budget around IT spend each year and maximizing lifecycle of assets.

BestSvchools lacks protocols around the containment phase as outlined in the Nist framework, it doesn't Utilise any form of machine learning to be able to automatically identify threats or indicators of compromise this shows us that their unable to isolate assets like servers, workstations, bring your own devices and so on should they require any form of automated response to attacks , this is because there's currently no governance risk or compliance policies or strategies in place due to lack of segregation of duties in between IT Staff within the school , In BestSvchools case while recovery phases are thought about with Mabs, they are able to restore both locally on premise and in the cloud, but they don't look to eradicate issues either before or after they happen as these procedures don't happen automatically or sometimes happen at all and are often left undocumented showcasing their immaturity again this highlights the absence of governance around recording steps and procedures taken when developing out standards for staff and students to follow.

While we can see from some of the measures in place BestSvchools lacks the governance around the controls required to keep them consistent showing an immature incident response capability. Based on the "Nist SP800-61r2" (NIST Special Publication 800, 2025) BestSvchools should be looking to bring together a structure to have pre-defined roles within their Soc operations, other ways in which they can align more closely why this matter is because with Nist the school could to utilize artificial intelligence, and machine learning to leverage automated detection and response ultimately eradicating malicious actors before they happen and preventing delays to containing threats as they land on assets. While we can see that BestSvchools utilizes a portion of the Microsoft security stack like defender for workstations and servers, mabs for file and finance backups, sentinel as a Siem platform and so on they fall short in documenting their standard operating procedures for incident response and then following through with communication to teams this is evident in the way they don't have roles and levels implemented in their Soc.

BestSvchools key strengths stem from some basic cyber hygiene like integrating Microsoft Sentinel for log ingestion, foundational implementation of Microsoft Mabs for backups in cloud and on premise and then we can see some form of foundational security posture being developed but lacking follow through often evident where there is a lack of governance by stakeholders and senior management , where BestSvchools setbacks and failures are evident show when documentation is not available for incident response plans and disaster recovery scenarios , although operating a Soc there is no mention of Red or Blue teams again this was amplified by no structure to the analyzing incidents or even the combination of both with just a purple team. It was also evident that by not highlighting automated responses for recovery point objectives and recovery time objectives they weren't tracking their mean time to detect and mean time to recover metrics should they be hit by an incident this shows no accountability meaning nobody is really responsible should they face a ransomware incident.

My Recommendation's Based on "BestSvchools" Study (Fictitious).

For improving BestSvchools incident response plan they would need to look at developing out their technology integrations in line with the "Nist SP800-61r2" and " ISO/IEC 27035" , this will allow them to be clear on defining their roles within their Soc and the responsibilities of each Soc member alongside segregating out responsibilities , while they have integrated Sentinel into their technology stack there not looking at any form of SOAR capabilities which could come in the form of logic apps within Azure , this would allow them to automate some of the manual overheads and bring automation to the forefront of their incident response plan and reporting for stakeholders of the business.

Training is another area in which BestSvchools should look to adopt a more shared responsibility approach this would allow them to conduct monthly phishing exercises with students and staff and develop their techniques for assessing their risk appetite and be more responsive to future threats, being proactive and prepared is one of the phases in the Nist incident response lifecycle. While having a backup system in place is pivotal and would be classed as a preventative measure, they do not have a way of tracking their recovery point objectives and metrics for recovery time objectives this is something worth developing out to be more in line with the Nist Framework and keeping with governance risk and compliance requirement by the schools board. By making adjustments to their security posture, standard operating procedures and defensive techniques, BestSvchools can go from a reactive educational institution to a proactive one harnessing their standard operating procedures and translating them into an industry compliant, resilient and structured stakeholder friendly incident response platform allowing them to be able to protect themselves against future cybersecurity threats fortifying their security posture for a volatile threat landscape.

Question 2, Analysis of a Recent Real Cyber Incident "MTU"

It was on February 6th the Munster Technological University announced the closure of its cork's campus due a significant IT Breach which was the direct result of a ransomware attack on the university information technology systems by the group known as "BlackCat", in preparation to begin investigation with both the data protection office and An Garda Siochána. (Martin, 2023). It was on February 7th that Munster Technological University officially addressed the discovery of the incident in which that they had a significant security breach against their IT infrastructure which was affecting their telephone and voice over Ip communication systems among other things. This announcement appeared both on the rte news website and MTU website (University, 2023) (O'Donovan, 2023). Subsequently It wasn't until the 8th of February that the university acknowledged this incident existed and this only happened after an initial investigation had occurred based on the events of the 7th and 8th of February it was confirmed at this time that a group known as ALPHV (BlackCat)ransomware gang had posted 6gb of data on the dark web. (Martin, 2023) . There next incident communication bulletin update occurred on the 8th of February where the college acknowledged the incident advised its staff and students that it had discovered some of its infrastructure had been compromised but at this point in time it was not sure of the effected resources and the magnitude of individuals data accessed. (University, 2023) , this showcased a delayed reaction telling us that the containment phase was severely limited highlighting a need for monitoring capabilities around the universities infrastructure.

This incident happened during the weekend of the 9th of February , The university had also confirmed on this date the type of attack which had been launched was a ransomware attack on its IT infrastructure and telephone communications , this later appeared on an article by the silicon republic on the 9th of February (Gowran, 2023). And appeared on the MTU website as well. At this point the university did not have any clear indicators of compromise or an estimate for the mean time to recovery of their systems or the recovery point objective for their data. Their disaster recovery plan was initiated, and they were very much investigating the cause of the incident at this point in time. If we were to compare this against the Nist incident response lifecycle you could say that the university's disaster recovery plan which was initiated after the initial investigation was very much reactive rather than preventative in the first place , we would then go on to see the university go through the 7 phases of the incident response procedures and or lifecycle (TitanFile, 2023) , to this point they had prepared their statements , moved past the identification stages and begun the containment stage of the ransomware attack with support from various entities like the National Cyber Security Centre (NCSC) , high courts in Ireland and the law enforcement agencies like an Garda Siochána.

Based on responses which were posted by an MTU spokesperson they later confirmed that they had been receiving Cyber support from the National Cyber Security Centre and Legal and Compliance support from other authorities such as An Garda Síochána and the Data protection commissioner in determining the extent to which they had been compromised , this showcased how the university was integrating legal procedures and containment with technical and forensic discovery processes and procedures. (University, 2023). It was on February 11th that MTU was granted an injunction from the high court which would prevent the sale of any information discovered during the cyber-attack across the dark web and other Social media platforms which had been illegally obtained by the hackers. (University, 2023) what this meant was anyone trying to sell this information or dumping it on known forms such as reddit and other sites would be legally culpable for their actions and the high court could enforce this, this also included access on the deep web as well. This element of containment could only be described as eradicating the impact of data leakage by seeking the high court injunction they were able to reduce the risk of the data being sold and eradicate the potential of the data being dumped on the dark web by making the hackers responsible by enforceable law , the next step for the university would be the recovery stages , due to a robust backup and disaster recovery solution in place the university was able to resume normal operations by the Monday , this tells us that the university must have had some communication plans and incident response playbooks incorporated into their overall incident response plan perhaps if they had had a immutable backups stored elsewhere , a proper governance oversight of their backup infrastructure they could have restored quicker , this just highlights the need for organisations and universities alike to implement some of form of automation across their workloads to protect themselves with the use of endpoint detection and response capabilities or even a SOAR capability , all of this would have tightened the recover point objective and the recovery time objectives for MTU with respect to their incident response plans.

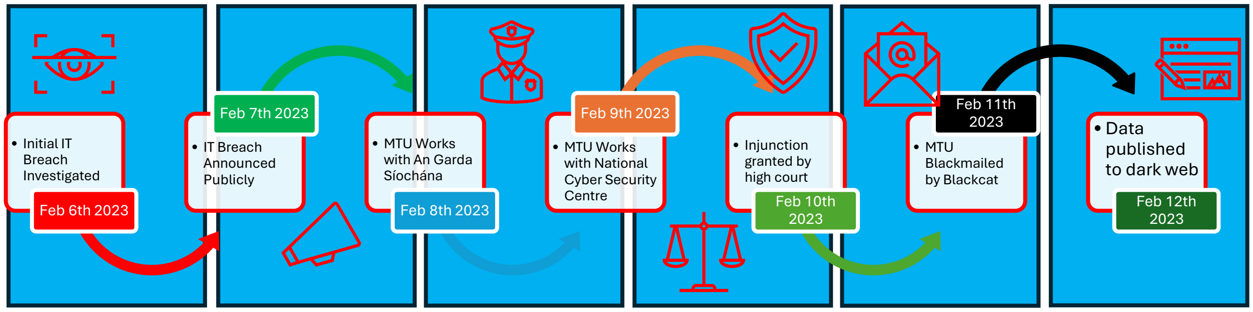
The impact was widely felt by both staff and students in which the university made a public announcement to advise both staff and students that all scheduled classes and lectures had been cancelled for the following period of at least two days , this later appeared in an article on the Irish times in which the university had advised staff and students to monitor there university email systems for updates and procedures over the coming days the attack only effected the cork campus. (RTE, 2023) (O'Brien, 2023). If we were to look at this we could describe this as an attack on the infrastructure making it unavailable if we map this back to the CIA triad (confidentiality integrity , availability) the ransomware attack affected the confidentiality of the students personally identifiable data , it also effected the integrity as the data had been encrypted with Ransomware and just for good measure the availability of the universities systems were effected as both infrastructure and communications were significantly disrupted for two plus days from my readings of multiple articles I was able to identify this attack went on for at least one week. The impact was also felt in another way Financially the incident to date has cost the Munster Technological University 3.5 million euro (University, 2022) in costs asSociated with getting a full independent review of the IT and Cybersecurity posture of the university. (Deegan, 2024) , sense the breach the university have invested a further 7 million euro in a cyber initiative to research and resolve real world problems within the Cybersecurity realm across the globe. (English, 2024).

By definition Ransomware is a type of malware attack which prevents the user or the organisation from accessing there data freely by encrypting it with a key the user or entity does not have access to therefore effecting the confidentiality of the data , meaning data is no longer confidential and has been accessed by a third party. This also means that the integrity of the data is undermined and likely compromised as the data once again is not in the same state it was before and was modified maliciously , it also effects the availability of the data as no user or entity has the ability to read , write or modify the data under normal circumstances or normal environment variables. ransomware allows an unauthorised party or hacker to demand compensation to unlock the user's data but does not guarantee after a ransom is paid that the data will remain unlocked and not exfiltrated to other platforms or Social media accounts. (The Computing Technology Industry Association, 2025)

As previously stated the chosen attack vector by the hacker group was malware , by definition malware is a software which is commonly used by criminals , threat actors and black hat hackers to purposely infect and threaten the integrity of information and computing systems around the world (The Computing Technology Industry Association, 2025) , this is a chosen method as it provides the attackers with the ability to compromise systems with different flavours of malware , in our case it was Ransomware that had been chosen. Again, ransomware allows the hackers to lock down and encrypt files to demand a ransom for releasing these files with a decryption key. Often intermediate services such as a broker are usually put in place to deal with the transaction of paying ransoms where an individual, organisation or entity opts to pay the ransom. In this case Munster Technological University did not and have not paid any ransom to date, this was published on the MTU website back in May of 2024. (University, 2025)

To date it believed that no shred of evidence exists or was provided to showcase any meaningful of personal identifiable data which could have been compromised as part of the cyber-attack on the select Munster Technological University IT infrastructure , after 16 months period of careful scanning of the dark and deep web and analysis of other Social media platform's MTU's investigations team deemed that if data was posted on the dark web it had previously been removed sense and nothing had surfaced online this was part of the lessons learned activities also mentioned and covered in the Nist incident response lifecycle. After 16-month period of investigation and analysis across the internet and combing the dark web and other social media sites, MTU have been able to conclusively state no data was compromised. (University, 2024).

Incident timeline Munster Technological University (MTU)


Initial IT Breach Investigated
Feb 6th 2023
Feb 7th 2023
IT Breach Announced Publicly
MTU Works with An Garda Síochána
Feb 8th 2023
Feb 9th 2023
MTU Works with National Cyber Security Centre
Injunction granted by high court
Feb 10th 2023
Feb 11th 2023
MTU Blackmailed by Blackcat
Data published to dark web
Feb 12th 2023

My Recommendation's Based on MTU Study (Real Life).

Based on the study I could see that MTU did have a disaster recovery solution in place but it wasn't evident from reading that they had a documented incident response plan meaning they were only half meeting the preparation phase based on the incident response lifecycle , I could also see from the study that that detection and analysis phase was lacking coordination and slightly delayed as they announced the compromise publicly a day or two later after leaks to newspapers.

Although MTU successfully contained and isolated network assets after some time , it was also evident that communication across to students and staff was inconsistent and most of the publications were made public before anyone knew what was going on this should a break in there abilities to be able to communicate across the board potentially point to no playbook for responding to queries from the press meaning reputational damage was an contributing factor to the whole investigation , while they were able to restore their systems this came at a cost as they didn't have a proper definitive recovery time objective, this effected there reputation as it took time to restore operations. The post incident report came out months later after the university worked with experts in the NCSC. This highlighted the need for a more robust incident response framework and clearer guidance going forward for monitoring systems within the university showing a lack of preparedness for incidents like this just like the Nist framework warns against for organizations. MTU should be looking to streamline their cybersecurity framework for IT Operations, adopting NIST gives them this ability to provide clearer guidance going forward, this also ensures the line up and have incident response plans and disaster recovery solutions available to them to be able to recover in a similar situation, ensuring that they don't do further damage to their reputation.

They should also have looked at separating out their physical networks using Vlans segregating out Staff and Student Network's providing a level a maturity across their networks if they ensured they were separating out student data from staff data this may have helped in preventing the spread of the ransomware , this would also have apply for their VoIP and other files and finance systems as well. Another thing MTU could have done was to ensure their backups weren't immutable to ransomware, hosting them in vaults in azure and aws with grs and zrs capabilities enabling locks add a layer of complexity ensuring relevant security controls and only authoritive writes and reads with privileged access users would have provided for an additional layer of security and a benefit to the university preventing them from being tampered against by attackers. Another element which would have provided clarity would be around the communications having clear responses and templates would have provided an added benefit to students and staff, this would have been available if only they had a proper incident response and business continuity plan. Overall, this study showed how a more proactive approach to security, proper incident response documentation and a business continuity plan would have helped with a better managed cyber incident and how coordination among its staff would have led to a better managed public media response from staff and students at the university it would have also saved the university costs associate with have to rebuild and deploy network and server components again its in the name business resilience and incident response management , this essentially ensures organizations have proper controls and procedures in place and can should an incident arise recover in an appropriate manner without reputational damage to their organization.

Question 3, Assessment of Incident Response Maturity

Case Description:

You are a security consultant brought in to assess the incident response maturity of a medium sized healthcare organization that recently experienced a ransomware attack. The organization's incident response process was informal, without documented procedures. The breach led to the encryption of patient data, disrupting their services for several days. The organization is now looking to improve its IR capabilities.

Question 3.1

From the case descriptor, were told that the healthcare organization recently suffered a cyber incident similar to what we have seen with MTU, the differentiator for this was that the organization had no formal incident response plan in place meaning they weren't following any form of framework such as Nist , Cobalt or ITIL or any sort of cyber hygiene across systems , based on the length of time the organization was affected for they also had a lack of understanding around their risk appetite as they allowed for incident to affect them for over a week plus. With the resulting factor being the confidentiality, integrity and availability of their data being subjected to malicious attackers and consequently resulting in the data being encrypted this tells us that the organization had no safeguards in place to stop it.

When we look at a scenario like this in respect of forming an incident response plan with similar medium to large scale healthcare providers the strengths and weaknesses become more evident this is a direct result of something which previously happened in Ireland like the HSE attack. The case reminds of how important it is to have a formal incident response plan as without this there's no clear line of sight in terms of an escalation process this is evident in the case descriptor as they call out "The organizations incident response process was informal".

Secondly we become aware that the organization was successfully attacked and the data was encrypted by means of saying "The breach led to encryption of patient data" , this tells us that the organization had no safeguards in place like an intrusion detection system or an intrusion prevention system , this could have come in the form of a Microsoft Sentinel Siem deployment or an endpoint detection and response solution like CrowdStrike all pointing to a limited way of monitoring the capabilities around intrusion prevention or safeguarding the patient data often a direct violation of "HIPPA" the fact that the organization speaks to be able to recover after about a week tells us that there was an absence of some backup operations and documentation this is further echoed in the statement " disrupting their services for several days" this also tells us that there is a sever lack of training around blue team (defensive) and red team (attack) exercises or maybe phishing campaigns for users of the companies' assets.

The fact that the organization is looking to improve its incident response capabilities tells us there are some strengths in the way in which there starting to look at the attack paths that's the governance side and possibly the lessons learned , this would make me believe that there starting to look to escalate and implement an incident response capabilities and by escalating these with leadership this is one way in which they can do it after they asses the weaknesses. The fact that the organization is looking now to build out its responses tells me that they want to invoke a sense of transparency across the board and by bringing in an independent consultant this is one way they can turn their weakness into a strength. One other thing we can see from the case descriptor is toward the end they highlighted the need for their incident response plan to be accessed this tells us that after the incident there are now turning to analyzing and doing lessons learned exercise allowing them to further strengthen their response capabilities going forward.

Based on the description of the case there are some key recommendations which could be put in place by a security consultant looking in from an external viewpoint. To increase the organization's security posture, they should look into either creating a framework for integrating the six phases of the incident response lifecycle or even adopt it from documents like the "NIST SP 800-61r3" publication and create their own incident response policy. The organization could also look at implementing the principal of least privilege ensuring dedicated tiering service accounts are set up based on the services requiring the account and what the use is another way of segregating these would be separation of duties ensuring that any delete or bulk delete options would require more than one user to approve the action.

Other ways the organization could look to preventing similar incidents from happening would be to implement detection and prevention techniques and software solutions , this could involve conducting vulnerability scanning across systems , automating the response with artificial intelligence and machine learning , perhaps even using software defined networking to segregate out production data from test lab data ensuring that both clinical systems like those used in hospitals and admiNistrative or test systems would remain on separate subnet's or Vlan ensuring that traffic between systems wouldn't be allowed to cross over another thing the healthcare organization could have done was to deploy honeypots to allow them to be able to understand the types of attacks and identify the indicators of compromise which could be recorded in a risk register in which they could have been learning from and adapting their defense techniques.

The fact that the systems took days to recover from the cyber incident tells us that there was no formal Soc or Siem tooling this demonstrates that the organization was very slow to deploy anything like a Microsoft Sentinel or a Splunk tool from trusted third party vendors within the ecosystem , if they had this they could have looked at bringing together the feeds or even bridging them to identify the types or ransomware attacks which were present in their environment. While a recovery process did occur we learned that this was after some time , if the organization had a azure site recovery configuration setup they could have restored operations in matter of minutes and not days , this leads us to believe they weren't meeting any form of recovery point objective or recovery time objective but then again this was evident when they said "incident response process was informal, without documented procedures" furthermore to this the organization could have done with a formal communication process instead nothing was mentioned about leading to believe there was no formal chain of command for IT Operations , something which most organizations' have in place even without a Soc.

Question 3.2

Ways in which the organization could have protected themselves in terms of the incident response lifecycle incorporating many missing elements and or steps which we could see from the scenario is if the healthcare provider started off with implementing a incident response policy , this is a simple step which would have outlined key sequences which would have needed to be followed at different role levels , if this is something they weren't comfortable with creating they could and should have adopted Nist or ISO.

Some of the more foundational ways in which they could have prevented the ransomware from spreading could have been to implement a small security operations center monitoring systems or prevention system to detect against indicators of compromise , this would have allowed them to scan there servers or workstations and prevent the ransomware from spreading , more in line with segregating and separating out roles and responsibilities the organization could have looked to implementing basic account hygiene this could have involved implementing the Microsoft Authenticator app for account login's this incorporated with least privilege and Rbac , role based access controls would have provided the organization with some basic functionalities to protect against account take overs and intrusions. As we can see the breach led to break in integrity and availability of the patient data this had some severe impacts on accessing this data, if only the organization had implemented a form of segregation across the systems this could have slowed down traversal across the network reducing the attack path.

Due to a lack of documented procedures, the response and recovery phases were slower than anticipated this was a direct result of not implementing warm or hot sites into their disaster recovery drills, having a properly identified RPO and RTO would have ensured the organization was enhancing their business continuity strategy , communication wasn't the organizations' strongest point either with no procedure in understanding how to handle crisis management the showcased just how unprepared the organization was for a cyber incident , regular blue team and red team simulations would have eased the Burdon on the organization to handle the incident a be more resilient in the future.

Often organizations' suffer from pressure management and this is no different here , it was evident from the fact it took them over a week to begin to recovering operations which tells us that the organization didn't do any form of tabletop exercises to prepare them for a similar scenario this would have helped the organization to build out baselines for their security posture and help them with scaling these into a more mature and resilient security posture as the threat landscape changed. The healthcare's overall security posture wasn't helped either by the fact that they clearly had not been audited and they were allowed an ongoing scenario where by they didn't benchmark any of their security controls this is often a big no for organizations' of this scale , the Nist Cybersecurity Framework would have helped them with identifying the data to be protected , detecting against breaches to the security baselines and rapidly responding to and recovering from these scenarios should they have opted to implement proper governance risk and compliance tooling.

Question 4, Post-Incident Review and Red/Blue Team Analysis

Case Description:

You are tasked with conducting a post-incident review after a phishing-based ransomware attack on a multinational company. The company's IR team successfully dealt with the incident, but their recovery took longer than expected, and they struggled to restore all systems.

Question 4.1

Based on the above case descriptor it highlights and states that after a cyber incident on a multinational company the companies incident response team while successfully blocking and containing the incident described it as being one which took them way longer to restore from , this tells us that the company didn't have a proper endpoint detection and response solution in place like a defender for cloud , defender for endpoint of maybe even a CrowdStrike edr product , it also tells us that the maybe there security monitoring tools wasn't as good as they expected it to be this would be evident if there visibility over the infrastructure was lacking which it must have been if their recovery processes took longer than expected.

We were also able to understand that they focused more on how the recovery process was a struggle on the system this could have included workstations, servers, or Byod devices this tells us that the processes for managing the vulnerabilities across the systems wasn't very refined and lacked coordination. Overall, one of the biggest gabs and or challenges we could see from the statement was that they "struggled to restore all systems" this tells us that due to a lack of system hardening the organization left out key protection measures to prevent their servers and workstations from being vulnerable meaning chances are they left this exposed to known zero day attacks over exposing there systems due to a lack to documented procedure possibly.

We can see that due to the severely delayed response in recovering data off the servers the organizations' clearly didn't implement any form of baselining or hardening on their systems without baselines and patching systems often get left exposed to attackers , an inventory here would have helped the organization to understand and priorities there more vulnerable assets and a raci matrix of responsibilities would have ensured that each asset was assessed addressed and taken care of prior to a breach and or attack if the organization had known about it. The statement also highlights a stark reminder of the importance of tabletop exercises blue teams struggling to find or prioritize system in the event of a disaster leads to one thing bad planning and incident response procedures, a policy for this would have helped with dealing and prioritizing systems this could have been implemented if the organization followed Nist cybersecurity framework.

Some of the ways in which the organization could look to develop out its asset management base would be to begin by creating a central repo or management console for all their assets, this could be in the form of Microsoft defender for endpoint or maybe Microsoft Intune, with the integration of Microsoft Intune the organization could have easily implemented security baselines allowing them then to track the baseline configurations across assets ensuring they remained in compliance , this could have then been accompanied by azure functions or logic apps to check for compliance across assets. Another thing the organization could have looked into doing was implementing CIS Controls they would have let the organization manage its vulnerabilities in a more effective manner. At the heart of all of this for the blue team though which would have helped was stronger monitoring capabilities by incorporating and a combination of Microsoft product security stacks and visibility dashboards this would have helped with identifying threats and being able to visualize the overall security posture , they could have opted to feed this into their Siem if they had one available.

Question 4.2

Key Requirement:

Propose how integrating a Red Team into the organization's incident response process could improve future preparedness and response. Suggest how Red Teams could help identify vulnerabilities and simulate attacks.

One of the ways in which a red team can help in a typical organization is by looking at the infrastructure in an attacker scenario rather than a defense scenario , essentially taking on the hacker mentality , red teams can often enhance the overall security posture by looking for gaps in the systems architecture and exploiting them , this is something often blue team defenders overlook and miss due to a fixation on defending rather than attacking. By using a red team an organization can simulate what an attack vector or enemy might look for in an organization's defenses. Red team members often look at the field of play and look for way in which they can enumerate , bypass and essentially compromise and break barriers in the defenses , this helps in the overall context of table top exercises , blue team defends red team attacks each side find new strategies or gaps which need to be hardened in the context of patching , system hardening and or architecture re-design all in support of making the systems and baselines more secure.

Red teams often provide benefits like simulating attack scenarios in which they can exploit vulnerabilities to gain access to systems like active directory, WordPress sites, SQL databases and so on all of this provides for a more immersive learning experience for blue team members this helps with improving the techniques blue teamers use to defend their infrastructure. By using red teamers organizations can test against the barriers and update their workbooks and playbooks in accordance with the different techniques and procedures being used. Some of the most widely used exercises for this combination would be Pen testing, Phishing attack emails and ransomware testing on files and servers. If we were to combine both blue and red teams together we would get teams which collaborate with each other known as purple teams this would allow organizations to bring together the different attack and defense techniques allowing them to update risk registers develop out playbooks and help them to classify different indicators of compromise and built out more resilient infrastructure which in turn changes the landscape from attack and defense to learn and adapt for future resilience against attackers.

By integrating both of these we can expect to learn about testing techniques used in the field by attackers and collaborating on defensive strategies used by defenders which helps with identifying incidents faster , responding to them appropriately and removing them from our networks , essentially were bringing together a shared responsibility and shared learning platform where security becomes everyone's responsibilities not just any single user , this helps us with validating and responding to incidents and where necessary respond to and update controls in place in line with Nists respond and recover functions as marked in the cyber incident response lifecycle.

Conclusion

When we look at the both BestSvchools and MTU we see many flaws in the way frameworks are integrated into the overall incident response lifecycle especially when it comes to incidents and breaches , we see that both blue and red team training is a pivotal part of the defensive strategy this is especially evident when organizations and universities are implementing the Nist lifecycle and the don't follow a chain of command or preset playbooks and runbooks , a continues governance process and oversight should be built from the ground up when developing out systems and following processes and if there are no standard operating procedures in place we see phases and lessons learned stages can be skipped if were not careful. Performing our due diligence and due care where threats are growing is a concern and the landscape is forever changing Nist provides that framework for foundational and intermediate level guidance in which organizations should follow to be able to be resilient against attacks. Both my fictional and real life case study had one exceptional and unmistakable consequence due to a key phase which is often always missed by organizations that's to ensure that you can only protect what you know if you don't know it exists how can you protect it so being proactive instead of responsive helps with aligning closer to Nist for developing the security controls and building out those baseline protections meaning your better prepared for if and when a malicious attacker tries to attack rather then being clueless.

References

Nelson, A., Rekhi, S., Souppaya, M. and Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: NIST. [online] doi:https://doi.org/10.6028/Nist.sp.800-61r3

[Accessed 13th October 2025].

Beforecrypt.com, 2024. list-of-known-ransomware-file-extensions. [Online]
Available at: https://www.beforecrypt.com/en/list-of-known-ransomware-file-extensions/
[Accessed 14 October 2025].

Deegan, G., 2024. https://www.irishexaminer.com/news/munster/arid-41340335.html. [Online]
Available at: https://www.irishexaminer.com/news/munster/arid-41340335.html
[Accessed 13th October 2025].

English, E., 2024. https://www.irishexaminer.com/news/munster/arid-41337889.html. [Online]
Available at: https://www.irishexaminer.com/news/munster/arid-41337889.html
[Accessed 14th October 2025].

Fortinet , 2025. What is the CIA Triad and Why is it important? [online]. [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/cia-triad
[Accessed 14 October 2025].

Gowran, L. M., 2023. https://www.siliconrepublic.com/enterprise/mtu-it-breach-ransomware-cyberattack-cork. [Online]
Available at: https://www.siliconrepublic.com/enterprise/mtu-it-breach-ransomware-cyberattack-cork
[Accessed 14th October 2025].

Martin, A., 2023. https://therecord.media/alphv-blackcat-posted-data-ireland-munster-technical-university. [Online]
Available at: https://therecord.media/alphv-blackcat-posted-data-ireland-munster-technical-university
[Accessed 14th October 2025].

Martin, A., 2023. https://therecord.media/alphv-blackcat-posted-data-ireland-munster-technical-university. [Online]
Available at: https://therecord.media/alphv-blackcat-posted-data-ireland-munster-technical-university
[Accessed 14th October 2025].

NIST Special Publication 800, 2025. nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf. [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf
[Accessed 13 October 2025].

O'Brien, T., 2023. https://www.irishtimes.com/ireland/education/2023/02/12/mtu-data-appears-on-dark-web-after-cyber-attack/. [Online]
Available at: https://www.irishtimes.com/ireland/education/2023/02/12/mtu-data-appears-on-dark-web-after-cyber-attack/
[Accessed 14th October 2025].

O'Donovan, B., 2023. https://www.rte.ie/news/regional/2023/0207/1354156-munster-technological-university/. [Online]
Available at: https://www.rte.ie/news/regional/2023/0207/1354156-munster-technological-university/
[Accessed 14th October 2025].

RTE, 2023. https://www.rte.ie/news/courts/2023/0211/1356002-mtu-it-breach/. [Online]
Available at: https://www.rte.ie/news/courts/2023/0211/1356002-mtu-it-breach/
[Accessed 13th October 2025].

The Computing Technology Industry Association, 2025. https://www.comptia.org/content/articles/what-is-ransomware. [Online]
Available at: https://www.comptia.org/content/guide/information-technology-terminology#section18
[Accessed 13th October 2025].

The Computing Technology Industry Association, 2025. https://www.comptia.org/content/guide/information-technology-terminology#section13. [Online]
Available at: https://www.comptia.org/content/guide/information-technology-terminology#section13
[Accessed 13th October 2025].

TitanFile, 2023. https://www.titanfile.com/blog/phases-of-incident-response/. [Online]
Available at: https://www.titanfile.com/blog/phases-of-incident-response/
[Accessed 13th October 2025].

University, M. T., 2022. https://www.mtu.ie/media/mtu-website/governance/policies-and-publications/financial-statements/english/Financial-Statements---August-2022---Signed.pdf. [Online]
Available at: https://www.mtu.ie/media/mtu-website/governance/policies-and-publications/financial-statements/english/Financial-Statements---August-2022---Signed.pdf
[Accessed 15th October 2025].

University, M. T., 2023. https://www.mtu.ie/news/major-it-breach-mtu-cork-campus-feb-2023/. [Online]
Available at: https://www.mtu.ie/news/major-it-breach-mtu-cork-campus-feb-2023/
[Accessed 15th October 2025].

University, M. T., 2023. https://www.mtu.ie/news/update-11-feb-it-breach-cork-campus/. [Online]
Available at: https://www.mtu.ie/news/update-11-feb-it-breach-cork-campus/
[Accessed 16th October 2025].

University, M. T., 2023. https://www.mtu.ie/news/update-9pm-8th-feb-it-breach-cork-campus/. [Online]
Available at: https://www.mtu.ie/news/update-9pm-8th-feb-it-breach-cork-campus/
[Accessed 16th October 2025].

University, M. T., 2023. https://www.mtu.ie/news/update-9pm-8th-feb-it-breach-cork-campus/. [Online]
Available at: https://www.mtu.ie/news/update-9pm-8th-feb-it-breach-cork-campus/
[Accessed 16th October 2025].

University, M. T., 2024. https://cybercare.mtu.ie/cyber-attack/monitoring. [Online]
Available at: https://cybercare.mtu.ie/cyber-attack/monitoring
[Accessed 15th October 2025].

University, M. T., 2025. https://cybercare.mtu.ie/cyber-attack/mtu-cyber-attack. [Online]
Available at: https://cybercare.mtu.ie/cyber-attack/mtu-cyber-attack
[Accessed 15th October 2025].

Wikipedia Contributors (2019). Health Insurance Portability and Accountability Act. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act.

[Accessed 20th October 2025].

axaxl.com. (n.d.). The Cyber Incident Response Lifecycle. [online] Available at: https://axaxl.com/fast-fast-forward/articles/the-cyber-incident-response-lifecycle

[Accessed 20th October 2025].

Cisecurity.org. (2024). CIS Controls. [online] Available at: https://learn.cisecurity.org/cis-controls-download-v8.

[Accessed 20th October 2025].

Itgovernance.eu. (2016). Business Resilience | IT Governance Ireland. [online] Available at: https://www.itgovernance.eu/en-ie/business-resilience-ie.

[Accessed 20th October 2025].

Truesec. (n.d.). Incident Response - What It Is and Why It Matters. [online] Available at: https://www.truesec.com/security/incident-response-what-it-is-and-why-it-matters.

[Accessed 20th October 2025].

SecAware (2016). ISO/IEC 27035 Security incident management. [online] Iso27001security.com. Available at: https://www.iso27001security.com/html/27035.html.

[Accessed 20th October 2025].

Faolain, A.O. (2023). Russian hacker group BLACKCAT demanded 'significant money' from MTU. [online] TheJournal.ie. Available at: https://www.thejournal.ie/mtu-cyber-attack-high-court-5992818-Feb2023/.

[Accessed 21st October 2025].

Wikipedia. (2022). Munster Technological University. [online] Available at: https://en.wikipedia.org/wiki/Munster_Technological_University

[Accessed 21st October 2025].

SecAware (2016). ISO/IEC 27035 Security incident management. [online] Iso27001security.com. Available at: https://www.iso27001security.com/html/27035.html.

[Accessed 21st October 2025].

Nelson, A., Rekhi, S., Souppaya, M. and Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: NIST. [online] doi: https://doi.org/10.6028/Nist.sp.800-61r3

[Accessed 21st October 2025].

Truesec. (n.d.). Incident Response - What It Is and Why It Matters. [online] Available at: https://www.truesec.com/security/incident-response-what-it-is-and-why-it-matters.

[Accessed 21st October 2025].

Itgovernance.eu. (2016). Business Resilience | IT Governance Ireland. [online] Available at: https://www.itgovernance.eu/en-ie/business-resilience-ie.

[Accessed 21st October 2025].