Seneca

Seneca Polytechnic

School of Information Technology Administration & Security

Building a Resilient Future: A WannaCry-Informed Cybersecurity Strategy for Group Dynamo Inc

Abraham Bolarinwa | 119532232

Leandro Delgado | 114416241

Anthony Lin | 103966248

James Williams | 181258237

CYT100NAA | Information Security

Professor Muhammad Ansari

December 5, 2024

EXECUTIVE SUMMARY

This report outlines a comprehensive cybersecurity strategy for Group Dynamo Inc., informed by lessons from the 2017 WannaCry ransomware attack. The WannaCry incident highlighted the devastating potential of cyberattacks exploiting outdated systems, poor patch management, and inadequate defences, leading to over $4 billion in damages worldwide. In response, this strategy emphasizes proactive risk management, robust defences, and incident response readiness.

Key Findings and Risks

- Critical Vulnerabilities: Outdated operating systems, unpatched software, and unsecured SMB protocols remain primary targets for attackers.
- Ransomware Threat Landscape: Evolving ransomware techniques and the increasing use of double extortion tactics pose significant risks to business continuity and data integrity.
- Human Factor: Social engineering and phishing remain prevalent attack vectors, exploiting human error to bypass technical defences.

Strategic Recommendations

To maintain a secure IT environment, it's crucial to:

- *Keep Systems Updated*: Regularly update software and hardware to patch vulnerabilities. Retire outdated systems that can't be updated to reduce risk.
- *Segment Networks and Control Access*: Isolate critical systems and limit user access to only what they need to prevent unauthorized access and lateral movement.
- *Back Up Data*: Regularly back up important data and test recovery plans to ensure data can be restored in case of a cyberattack or disaster.
- *Protect Endpoints and Perimeter*: Use advanced security tools to monitor and protect devices and network boundaries.
- *Train Employees*: Educate employees about cybersecurity threats and how to recognize and respond to them.
- *Prepare for Incidents*: Have an incident response team and plan in place to handle cyberattacks effectively.

Implementation Roadmap

The strategy proposes a phased approach over 12 months, prioritizing high-risk areas, such as patching and backup systems, followed by broader improvements in network security, training, and policy enhancements.

Expected Outcomes

By implementing this strategy, Group Dynamo Inc. aims to:

- Minimize ransomware attack risks through proactive measures.
- Enhance the organization's ability to detect, respond to, and recover from incidents.
- Build a culture of cybersecurity awareness across all levels of the organization.

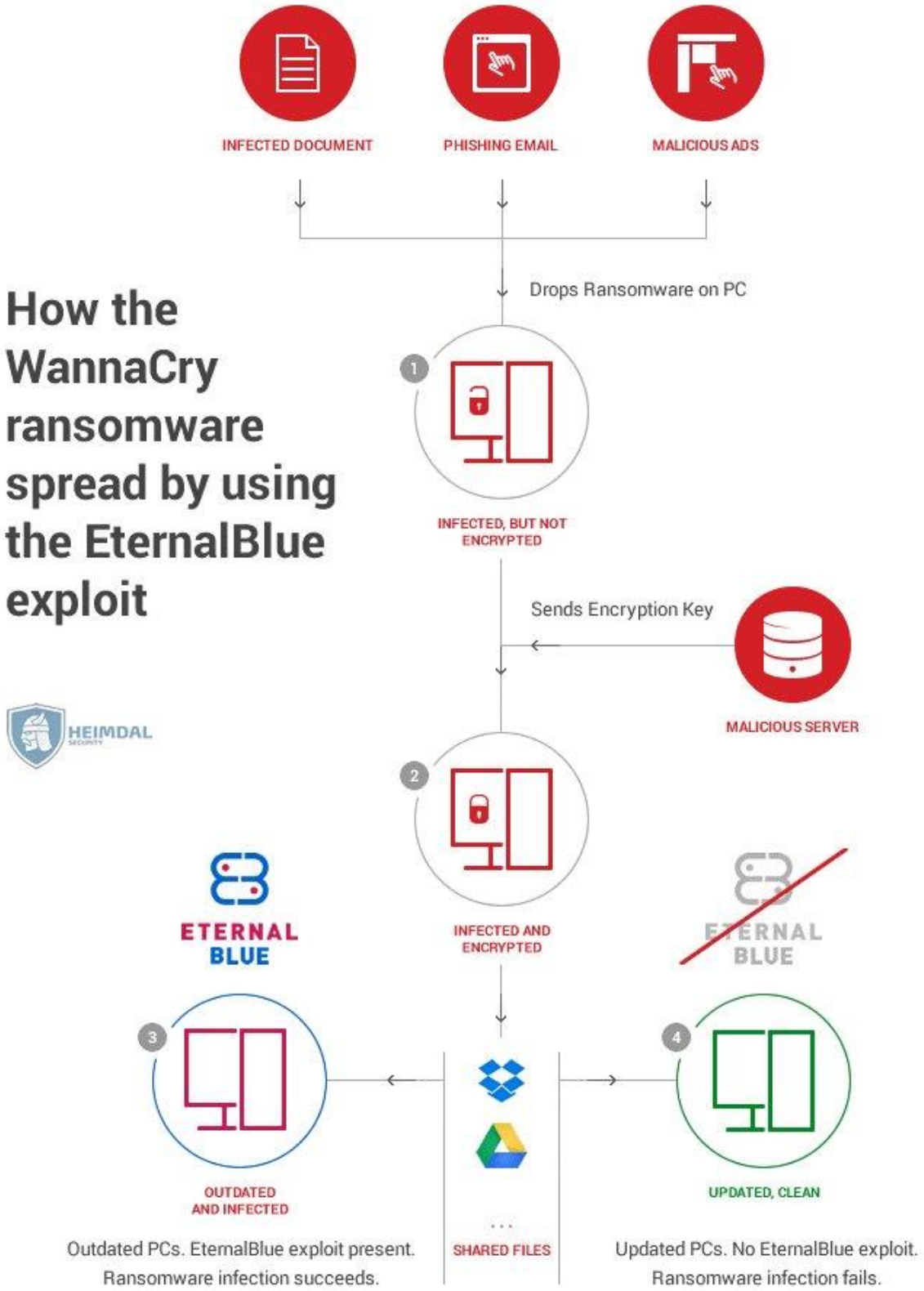
1.0 Background

EternalBlue was a piece of software developed by the National Security Agency to exploit computers (Nakashima and Timberg, 2017). It was used by the National Security agency to gain backend access to computers running on Windows operating systems by exploiting the SMBv1, Server Message Block version 1, protocol. The protocol allows Microsoft systems to communicate for purposes such as printing. EternalBlue exploited systems by sending a malicious SMBv1 packet to the target (Higgins, 2023). The Shadow Brokers are a group of hackers that appeared in 2016. The group released a variety of stolen NSA tools including EternalBlue onto the internet. The leak made sophisticated hacking tools available and enabled the creation of WannaCry (HYPR).

WannaCry is a ransomware and worm that is built upon the EternalBlue vulnerability to encrypt files and spread to other systems (NCCIC). The ransomware attack occurred in May 2017 with an estimated impact of 230 000 computers. Its impact was significant as it included Spanish telecommunication company, Telefónica, and a third of British National Health Service's hospitals. The estimated monetary impact of the WannaCry ransomware is $US 4 billion (Kaspersky).

The vulnerability exploited by the WannaCry ransomware was patched two months earlier, in March 2017, following EternalBlue's release by the Shadow Brokers. Many computer systems that were not regularly updated were still vulnerable to exploitation. The WannaCry ransomware spreads by exploiting these unpatched systems (Kaspersky). The United State attributed the WannaCry ransomware to a North Korean citizen with connections to the North Korean backed Lazarus Group (Office of Public Affairs, 2018). The WannaCry ransomware caused an estimated $4 billion in financial cost (Kaspersky). Below shows the pictorial representation of how the malware affects the device. Security researchers helped business and organizations prevent the spread of the WannaCry virus. Researchers found a domain that the malware was attempting to connect to. The domain was unregistered and when the ransomware detected that domain was active, it would not infect the machine. By registering a domain, it activated the ransomware's kill switch and prevent itself from spreading (Newman, 2017).

How the WannaCry ransomware spread by using the EternalBlue exploit



2.0 Target organization and Impact

The WannaCry ransomware attack had a global impact, affecting various sectors including healthcare, logistics, Telecommunications, defence, automotive, government, and transportation (Askarifar et al., 2018). In this report we will highlight just a few sectors.

2.1 National Health Services (NHS) England

One of the most significant and widely reported impacts of WannaCry occurred at the UK's National Health Service (NHS). The attack crippled hospital operations across the country, leading to disruptions in medical services. Over 19,000 appointments, including cancer treatments and surgical procedures, were canceled, causing serious delays and risks to patient health. Ambulances were diverted to unaffected hospitals, leading to a delay in emergency care for many patients. Moreover, the NHS staff, many of whom had to rely on paper records and manual processes to continue providing care, faced immense stress and increased workloads (NAO Comptroller and Auditor General, 2018). Therefore, this paralysis of essential services caused real damage to health systems in the face of cyberattacks. The financial cost to the NHS is estimated to have reached £92 million (approximately 120 million USD) primarily spent on recovery efforts and system upgrades due to the attack (NAO Comptroller and Auditor General, 2018). Additional resources were allocated to reinforce the cybersecurity infrastructure.

2.2 FEDEX

The global logistics giant FedEx also fell victim to the WannaCry ransomware attack, experiencing severe disruptions to its operations. FedEx's tracking systems were taken offline, preventing the company from processing shipments and orders effectively. Employees were unable to properly process internal operations such as processing and tracking packages (Culver, 2017). Beyond the immediate financial losses, FedEx also suffered damage to its reputation. Customers began questioning the company's ability to protect their digital systems, with some opting for alternative service providers (Culver, 2017).

FedEx's experience with WannaCry highlighted the importance of maintaining a firm stance on cybersecurity capable of protecting its infrastructure. Robust cybersecurity practices and

measures protect the business from ever-evolving threats and help maintain operational continuity.

2.3 Telefonica

Telecommunications giant Telefónica was another major victim of the WannaCry ransomware. Although the company took proactive measures to contain the spread of the malware such as instructing employees to disconnect their computers from the network; this action resulted in temporary operational paralysis, affecting its ability to provide customer services. The company's communication systems were disrupted, leading to delays in decision-making and interruptions to customer-facing services (Palazuelos, 2017).

While Telefónica's response minimized the overall impact, the incident revealed the vulnerability of even large, well-resourced organizations to ransomware attacks. Following the attack, Telefónica took the lessons learned to improve their processes in for future attacks. Telefónica prioritized employee training programs to educate staff on how to identify phishing attempts and better protect the company's systems from similar threats in the future (Palazuelos, 2017).

Impact of WannaCry

Over 200,000 computers in 150 countries have been impacted by a massive cyberattack in recent days. The ransomware known as WannaCry locks files on affected systems and demands a payment of $300 for their decryption.

Image credited to Stratista

3.0 Project Management Scope

3.0.1 Recommendation and Project

The security team recommended a project focused on designing and implementing security measures to protect the organization from WannaCry and other ransomware attacks

3.1 Project Objective

To design and implement a comprehensive cybersecurity strategy that ensures Group Dynamo Inc. is prepared to defend against ransomware attacks, such as WannaCry, by strengthening its security posture and enhancing its operational resilience. The strategy will encompass proactive prevention, continuous monitoring, timely detection, effective containment, and thorough recovery mechanisms to safeguard both company data and customer trust.

3.2 Project Scope

3.2.1 Implement Cybersecurity framework

- Develop a formalized cybersecurity framework tailored to the need and risk profile. include defined roles, responsibilities, and escalation paths for cybersecurity incidents
- Integrate industry standards such as NIST Cybersecurity Framework (CSF) or ISO/IEC 27001 to ensure compliance and thoroughness
- Risk Management: Conduct a risk assessment to identify assets, vulnerabilities, threats, and potential impacts
- Implement a risk treatment plan, prioritizing high-risk areas, including ransomware-specific defenses
- Defensive Measures: Focus on network segmentation, least privilege access controls, email filtering, and regular log reviews
- Ensure all communication channels, especially RDP and VPNs, are secured
- Governance: Regularly update policies and procedures to address evolving threats. Schedule periodic reviews to validate the framework's effectiveness

3.2.2 Employee training Program

- Phishing and Malware Awareness

-Design interactive, scenario-based training modules covering phishing, malware, and ransomware tactics

-Educate employees on identifying suspicious emails, links, and attachments

- Simulated Cyberattack Drills

-Conduct regular simulated phishing campaigns to assess employee vigilance and refine training

-Use advanced tools to generate detailed reports on success rates and areas needing improvement

- Role-Specific Training

-Provide targeted training for high-risk roles, such as finance and HR, which are often targeted by spear-phishing attacks

- Continuous Learning

-Offer quarterly updates on emerging threats and countermeasures to maintain awareness

3.2.3 Vulnerability Management System

- Identification and Assessment

-Deploy automated vulnerability scanners and manual penetration testing to discover system weaknesses

-Develop an inventory of assets to map vulnerabilities to specific systems or applications

- Mitigation

-Prioritize critical vulnerabilities like SMBv1 and EternalBlue exploits by disabling outdated protocols and applying immediate patches

-Adopt a zero-trust approach for additional layers of defense

- Regular Patching Schedule

-Establish a formal patch management process, ensuring timely updates for operating systems, applications, and firmware

-Include a rollback plan for patches that might introduce instability

3.2.4 Backup and Disaster Recover Solutions

- Backup Strategy

-Implement a 3-2-1 backup rule: three copies of data, on two different media types, with one offsite (preferably cloud-based)

-Encrypt backups to safeguard against unauthorized access.

- Disaster Recovery Plan (DRP)

  -Develop a clear DRP outlining steps to recover critical systems and data in case of an incident

  -Perform regular disaster recovery testing to validate the recovery time objective (RTO) and recovery point objective (RPO).

- Resilient Infrastructure

  -Use immutable backups and air-gapped storage to prevent ransomware from encrypting backups

3.2.5 Advance Threat Detection and Monitoring Tools

- Security Information and Event Management (SIEM)

  -Deploy SIEM tools to aggregate, analyses, and correlate log data from various sources, providing real-time threat detection

- Intrusion Detection and Prevention Systems (IDS/IPS)

  -Monitor network traffic for suspicious activity and automatically block known threats.

- Endpoint Detection and Response (EDR)

  -Implement EDR solutions to identify and isolate infected endpoints, limiting ransomware spread

- Threat Intelligence

  -Leverage threat intelligence feeds to stay informed about emerging threats and proactively update defenses

3.2.6 Post-Incident Analysis and Improvement

- Incident Review

  -Conduct thorough root-cause analyses after every incident to identify gaps in security protocols

  -Document findings in an incident report to improve future incident response strategies

- Lessons Learned Sessions

-Host post-incident review meetings with key stakeholders to gather insights

- Continuous Improvement

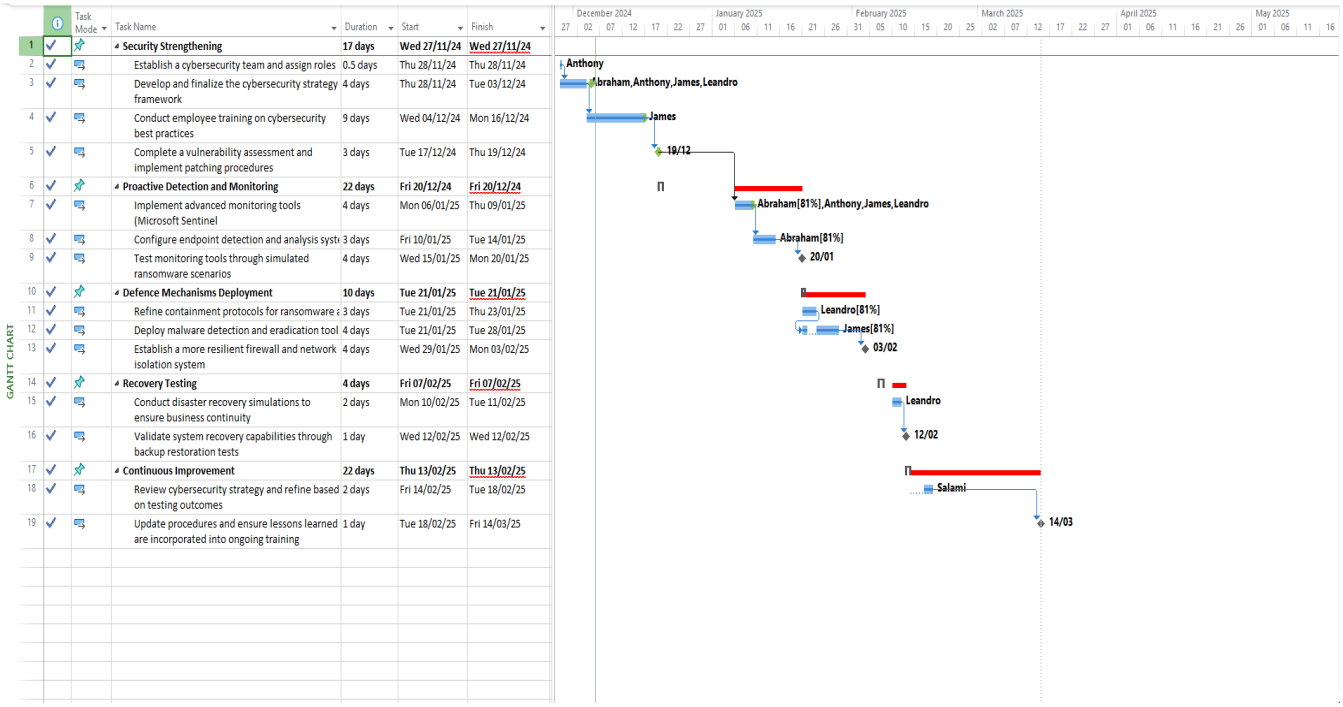
  -Update the cybersecurity framework and incident response plan (IRP) based on findings.

  -Regularly benchmark the organization's cybersecurity maturity against industry standards

Out of Scope

- Overhaul of systems unrelated to ransomware defense
- Infrastructure updates outside the scope of cybersecurity

3.3 Project Schedule Management



	Task Mode	Task Name	Duration	Start	Finish
1		**Security Strengthening**	**17 days**	**Wed 27/11/24**	**Wed 27/11/24**
2		Establish a cybersecurity team and assign roles	0.5 days	Thu 28/11/24	Thu 28/11/24
3		Develop and finalize the cybersecurity strategy framework	4 days	Thu 28/11/24	Tue 03/12/24
4		Conduct employee training on cybersecurity best practices	9 days	Wed 04/12/24	Mon 16/12/24
5		Complete a vulnerability assessment and implement patching procedures	3 days	Tue 17/12/24	Thu 19/12/24
6		**Proactive Detection and Monitoring**	**22 days**	**Fri 20/12/24**	**Fri 20/12/24**
7		Implement advanced monitoring tools (Microsoft Sentinel	4 days	Mon 06/01/25	Thu 09/01/25
8		Configure endpoint detection and analysis syste	3 days	Fri 10/01/25	Tue 14/01/25
9		Test monitoring tools through simulated ransomware scenarios	4 days	Wed 15/01/25	Mon 20/01/25
10		**Defence Mechanisms Deployment**	**10 days**	**Tue 21/01/25**	**Tue 21/01/25**
11		Refine containment protocols for ransomware a	3 days	Tue 21/01/25	Thu 23/01/25
12		Deploy malware detection and eradication tool	4 days	Tue 21/01/25	Tue 28/01/25
13		Establish a more resilient firewall and network isolation system	4 days	Wed 29/01/25	Mon 03/02/25
14		**Recovery Testing**	**4 days**	**Fri 07/02/25**	**Fri 07/02/25**
15		Conduct disaster recovery simulations to ensure business continuity	2 days	Mon 10/02/25	Tue 11/02/25
16		Validate system recovery capabilities through backup restoration tests	1 day	Wed 12/02/25	Wed 12/02/25
17		**Continuous Improvement**	**22 days**	**Thu 13/02/25**	**Thu 13/02/25**
18		Review cybersecurity strategy and refine based on testing outcomes	2 days	Fri 14/02/25	Tue 18/02/25
19		Update procedures and ensure lessons learned are incorporated into ongoing training	1 day	Tue 18/02/25	Fri 14/03/25

Phase 1: Security Strengthening

- Establish a cybersecurity team and assign roles
- Develop and finalize the cybersecurity strategy framework
- Conduct employee training on cybersecurity best practices
- Complete a vulnerability assessment and implement patching procedures

Phase 2: Proactive Detection and Monitoring

- Implement advanced monitoring tools (e.g., SIEM, IDS/IPS)
- Configure endpoint detection and analysis systems
- Test monitoring tools through simulated ransomware scenarios

Phase 3: Proactive Detection and Monitoring

- Refine containment protocols for ransomware attacks
- Deploy malware detection and eradication tools
- Establish a more resilient firewall and network isolation system

Phase 4: Proactive Detection and Monitoring

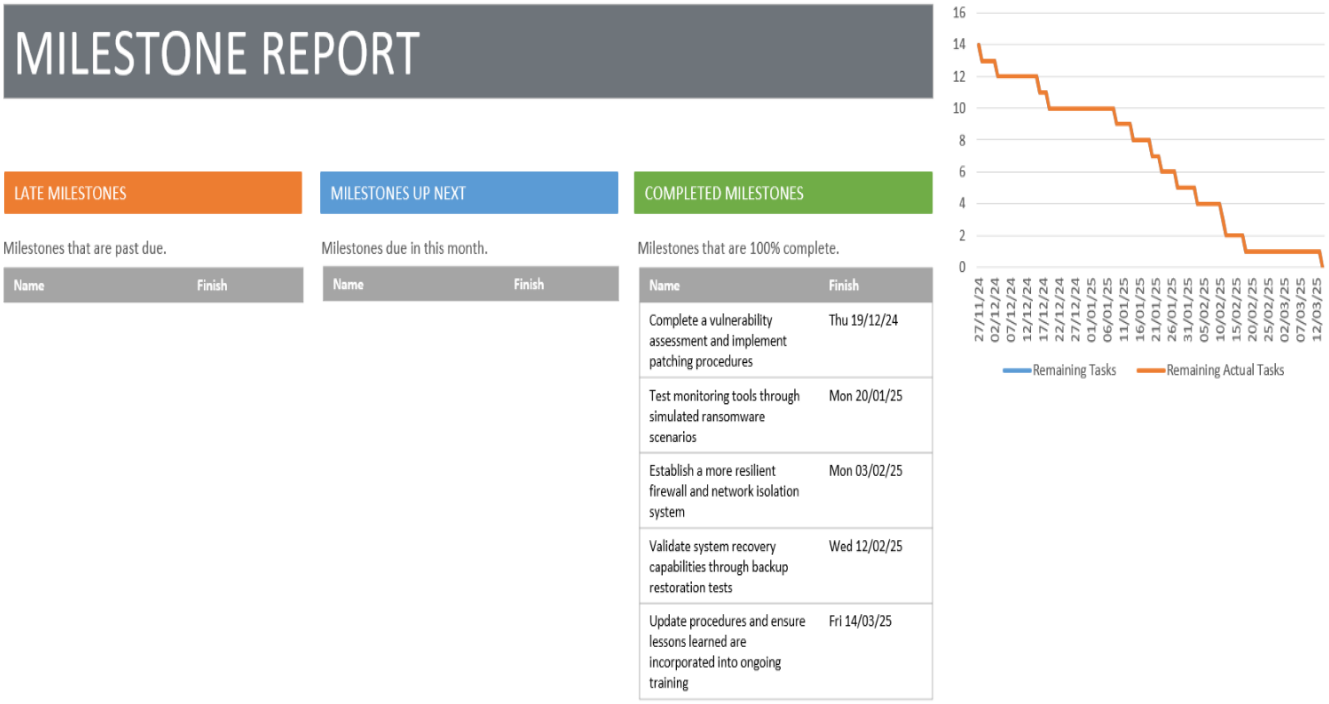
- Conduct disaster recovery simulations to ensure business continuity
- Validate system recovery capabilities through backup restoration tests

Phase 5: Proactive Detection and Monitoring

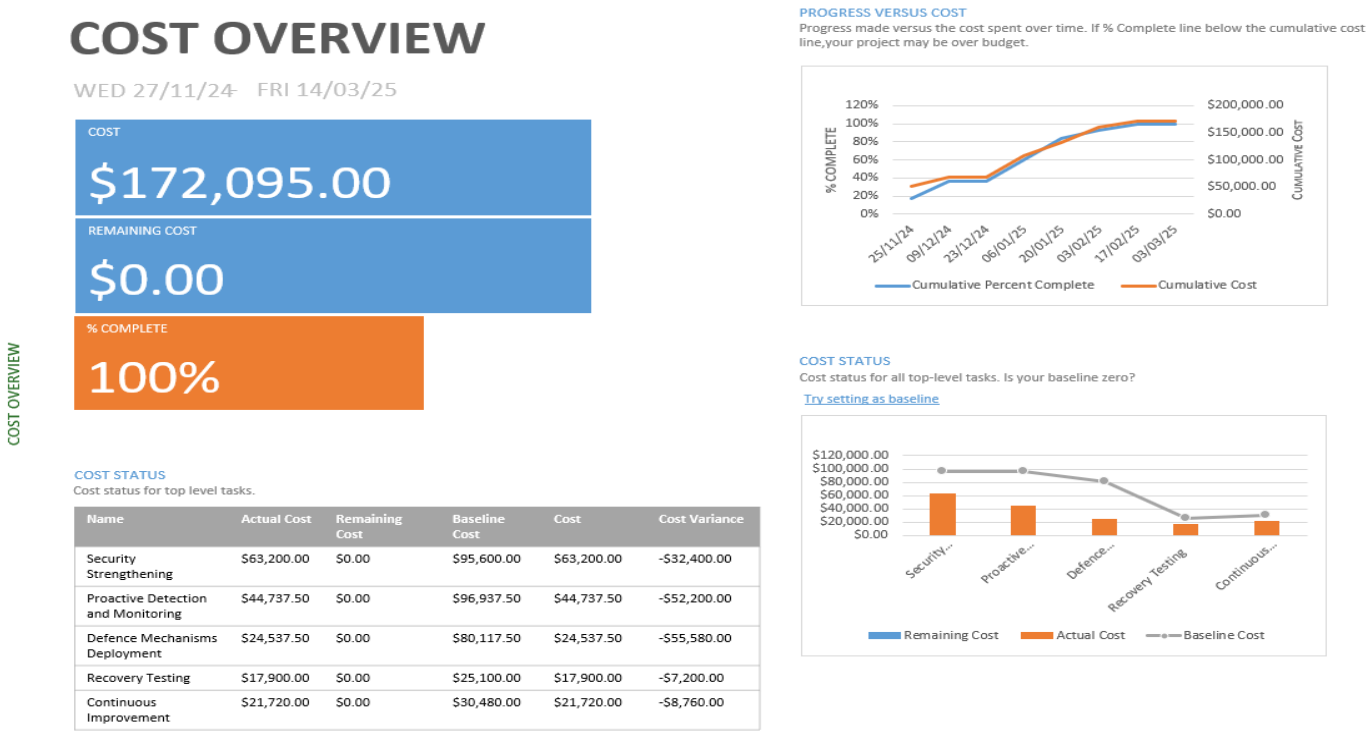
- Review cybersecurity strategy and refine based on testing outcomes
- Update procedures and ensure lessons learned are incorporated into ongoing training

Milestones

19th November 2024	Complete a vulnerability assessment and implement patches
20th January 2025	Test Monitoring tools through simulated ransomwares serious
3rd February 2025	Establish a more resilient firewall and network isolation system
12th February 2025	Validate system recovery capabilities through backup restoration tests
14th March 2025	Update procedures and ensure lesson learn are incorporated to training



3.4 Project Cost Management



3.4.1 Budget Overview by Phase

Phase	Estimated Cost

1. Security Strengthening	$63, 200.00
2. Detection & Monitoring	$44, 737.50
3. Defense Mechanisms	$24, 537.50
4. Recovery Testing	$17, 900.00
5. Continuous Improvement	$21, 720.00
Total Estimated Cost	**$172, 095.00**

3.4.2 Cost breakdown by Phase

Phase 1: Security Strengthening

- Cybersecurity team and framework development: $31,066.67
- Employee training (phishing, malware prevention): $21,066.67
- Vulnerability assessments and patch management: $10,066.67

Phase 2: Proactive Detection and Monitoring

- Deployment of SIEM and IDS/IPS tools: $24,912.50
- Endpoint detection tools (e.g., EDR solutions): $14,912.50
- Threat detection configuration and testing: $ 4,912.50

Phase 3: Defence Mechanisms Deployment

- Containment protocols development: $8,179.17
- Firewall and network isolation updates: $8,179.17
- Malware detection and eradication tools: $8,179.17

Phase 4: Recovery Testing

- Backup and disaster recovery solutions: $12,950.00
- Recovery testing and functional integrity checks: $ 4,950.00

Phase 5: Continuous Improvement

- Post-incident analysis and strategy updates: $12,860.00
- Policy and playbook revision: $ 8,860.00

3.5 Resource allocation

The resources described here are the manpower in this case the security engineer. See below the number of hours allocated to each task and percentage of work done and the start and finish date for each worker.

4.0 Key Takeaway / Lessons Learned

The WannaCry attack was a wake-up call for both private and public sector organizations around the world. It emphasized the importance of maintaining a vigilant stance on the

detection of new vulnerabilities and the critical importance of applying security patches in a timely manner. The WannaCry ransomware vulnerability was patched two months before the ransomware was first detected. The scale and the impact of the incident demonstrated the number of organizations that have not been frequently applying new secuirty patches in a timely manner thus leaving their systems vulnerable. Organizations and agencies who were impacted by the ransomware learned the importance of maintaining robust backup systems. The incident emphasized the need for a more proactive stance on cybersecurity measures such as regular system updates, employee training, and the implementation of robust backup and recovery strategies.

References

(Askarifar et al., 2018) Askarifar, S., Rahman, N. A. A., and Osman, H. (2018). A review of latest wannacry ransomware: Actions and preventions. Journal of Engineering Science and Technology Special Issue on ICCSIT 2018

(Culver, 2017) Culver, A. (2017). Fedex hit by 'wannacry' ransomware. https://www.wate.com/news/national/fedex-hit-by-wannacry-ransomware/. Accessed: 2024-11-24.

(Higgins, 2023) Higgins, M. (2023). Eternalblue: What it is and how it works. https://nordvpn.com/blog/what-is-eternalblue/. Accessed: 2024-11-24.

(HYPR) HYPR (n.d.). Shadow brokers. https://www.hypr.com/security-encyclopedia/shadow-brokers Accessed: 2024-11-24.

(Kaspersky) Kaspersky (n.d.). What is wannacry ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. Accessed: 2024-11-24.

(Nakashima and Timberg, 2017) Nakashima, E. and Timberg, C. (2017). NSA officials worried about the day its potent hacking tool would get loose. then it did. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82story.html.. Accessed : 2024 − 11 − 24.

(NAO Comptroller and Auditor General, 2018) NAO Comptroller and Auditor General (2018). Investigation: Wannacry cyber attack and the NHS. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf Accessed: 2024-11-24.

(NCCIC) NCCIC (n.d.). What is wannacry/wanacrypt0r? https://www.cisa.gov/sites/default/files/FactSheets/NCCIC Accessed: 2024-11-24.

(Newman, 2017) Newman, L. H. (2017). How an accidental 'kill switch' slowed friday's massive ransomware attack. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/ Accessed: 2024-12-05.

(Office of Public Affairs, 2018) Office of Public Affairs (2018). North korean regime-backed

programmer charged with conspiracy to conduct multiple cyber attacks and intrusions. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and Accessed: 2024-11-24.

(Palazuelos, 2017) Palazuelos, F. (2017). How the wannacry ransomware attack affected businesses in spain. https://english.elpais.com/elpais/2017/05/19/inenglish/1495181037555348.html Accessed : 2024−11−24.