Ethical Implications of WannaCry: A Cybersecurity Dilemma

Jude Osamor[1], Jane Odum[2], Celestine Iwendi[3], Funminiyi Olajide[4], Isaac Peter-Osamor[5], Victor Onyenagubom[6] and Innocent Ayodele[7]

[1]School of Computing and Creative Technologies, University of the West of England (UWE), Bristol, UK

[2]School of Computing, University of Georgia, USA

[3]School of Creative Technologies, University of Bolton, UK

[4]School of Computer Science & Engineering, University of Westminster, London, UK

[5]University of Lagos, Akoka, Nigeria

[6]Department of Computing, Teeside University, UK

[7]The Department of Engineering & Computer Science, University of Hertfordshire, UK

jude.osamor@ieee.org (corresponding author)

Abstract: The WannaCry ransomware attack of May 2017 marked a critical turning point in cybersecurity history, prompting profound ethical discussions about software vulnerability management. This comprehensive analysis examines the ethical dimensions of the WannaCry incident, focusing on the responsibilities of government agencies, technology companies, and security professionals in handling zero-day vulnerabilities. The study investigates the complex balance between national security interests and global cybersecurity while proposing ethical frameworks for future practice. Through a detailed examination of the attack's global impact and subsequent incidents, we demonstrate the ongoing relevance of lessons learned from WannaCry to contemporary cybersecurity challenges.

Keywords: WannaCry, Ethical dilemma, Zero-Day vulnerabilities, Cybersecurity ethics, National security

1. Introduction

The WannaCry ransomware incident of May 2017 represents more than just another cyberattack; it underscores a critical ethical debate in cybersecurity. The attack exploited EternalBlue, a vulnerability in Microsoft Windows systems that had been discovered and weaponized by the National Security Agency (NSA) of the United States before being leaked by the Shadow Brokers hacking group (Bright, 2017). This incident raises questions about the responsibilities of state actors in managing vulnerabilities and balancing national security interests against global cybersecurity. The ethical implications extend beyond WannaCry to include a broader history of zero-day vulnerabilities. NSA and other intelligence agencies purchase zero-day exploits from cybersecurity firms like Zerodium, which operate in a highly secretive and lucrative market. These firms acquire vulnerabilities from independent researchers and sell them to governments and corporations, often at prices reaching millions of dollars per exploit. The lack of transparency in this market raises ethical concerns, as it incentivizes withholding security flaws from software vendors, leaving users at risk. Additionally, the sale of these exploits to authoritarian regimes and cybercriminals exacerbates global cybersecurity threats, making regulation and oversight imperative. fueling a competitive market where vulnerabilities are withheld from vendors for strategic advantage. This paper will explore the history of zero-day trade and its ethical dimensions, including cases such as Stuxnet (2010), NotPetya (2017), Pegasus spyware (2021), and Log4j (2021).The rest of this paper is organized as follows: Section 2 examines the NSA's role in vulnerability hoarding and its implications. Section 3 analyzes ethical disclosure practices, considering the risks of delayed disclosure. Section 4 explores the global impact of WannaCry, particularly its economic and social consequences. Section 5 discusses the balance between national security and public safety. Section 6 broadens the discussion by examining contemporary zero-day cases, including NotPetya, Stuxnet, Pegasus, and Log4j. Finally, Section 7 provides policy recommendations for ethical cybersecurity practices, with an emphasis on international cooperation and corporate mitigation strategies. Section 3 analyzes ethical disclosure practices. Section 4 examines the global impact of WannaCry. Section 5 explores the balance between national security and public safety. Section 6 expands the discussion to contemporary zero-day cases, and Section 7 provides recommendations for ethical cybersecurity practices. Section 8 concludes the paper.

2. The NSA's Role and EternalBlue Exploitation

The NSA's involvement in the WannaCry incident presents a complex ethical case study in the management of cybersecurity vulnerabilities. During its cyber espionage efforts, the NSA discovered the EternalBlue vulnerability and made a strategic decision to retain it rather than disclose it to Microsoft (Nakashima & Timberg, 2017). This decision was guided by the perceived strategic value of the exploit for national security purposes (Shane et al.,

2017).The retention of EternalBlue by the NSA raises significant ethical considerations. On one hand, such vulnerabilities can provide tactical advantages in cyber operations, enabling intelligence gathering and potential defensive capabilities against adversarial systems. On the other hand, they also create substantial risks when compromised (Lin, 2015). The subsequent leak of EternalBlue by the Shadow Brokers transformed a closely-guarded national security asset into a global threat, demonstrating the inherent risks of vulnerability hoarding.It was highly questionable, and some may argue that it was a fundamentally bad decision by the NSA, to keep this vulnerability for itself and thus allow millions of systems worldwide to remain vulnerable to its possible exploitation. This vulnerability was exploited by cybercriminals in the WannaCry attack, representing a worst-case scenario in vulnerability management. The decision to prioritize offensive capabilities over public security ultimately contributed to one of the most devastating cyber attacks in history, raising serious questions about the ethical responsibilities of state actors in the digital age.

3. Ethical Implications of Vulnerability Disclosure

The ethical dimensions of vulnerability disclosure extend beyond simple binary choices of whether to disclose or withhold information. Responsible disclosure practices typically involve security researchers reporting vulnerabilities to vendors confidentially, allowing time for patch development before public disclosure. This approach has to be tried out by balancing user protection and preventing malicious actors from knowing and exploiting the undisclosed vulnerabilities.

3.1 The Ethics of Delayed Disclosure

The NSA's decision to withhold information about EternalBlue from Microsoft represented a significant deviation from established ethical disclosure practices (Smith, 2017). This choice prioritized potential military and intelligence advantages over the security of global computer systems. When the vulnerability eventually leaked, its impact was magnified by the lack of available patches and preparedness among potential targets.

3.2 Balancing Competing Interests

Vulnerability disclosure involves complex trade-offs between various stakeholder interests. On one hand, government agencies must balance national security objectives with public safety responsibilities. On the other hand, technology companies need to protect their users while maintaining competitive advantages. Security researchers face pressure to disclose findings responsibly while advancing knowledge in the field. The WannaCry incident demonstrates how these competing interests can lead to catastrophic outcomes when not properly balanced.

4. The Global Impact of WannaCry

The WannaCry attack's global reach demonstrated the interconnected nature of modern digital infrastructure and the potential for cascading failures across systems and borders.

4.1 Geographic Distribution

Russia and Ukraine experienced the most significant effects, representing 33.2% and 28.8% of compromised systems, respectively. India (17.6%) and Taiwan (12.8%) also faced substantial impacts. This distribution pattern reflects various factors, including the prevalence of unpatched systems and specific targeting strategies employed by the attackers. The concentration of attacks in these regions suggests that threat actors may have exploited regional cybersecurity weaknesses or targeted industries critical to these economies. Additionally, geopolitical tensions and historical cyber conflict patterns may have influenced the focus on Russia and Ukraine. In India and Taiwan, the high percentage of affected systems could be attributed to the rapid digital transformation and the widespread use of legacy infrastructure in certain sectors. Furthermore, variations in cybersecurity awareness, incident response capabilities, and the adoption of security best practices likely played a role in the observed distribution. The attackers may have also leveraged region-specific phishing campaigns or supply chain vulnerabilities to maximize their reach within these geographic areas.

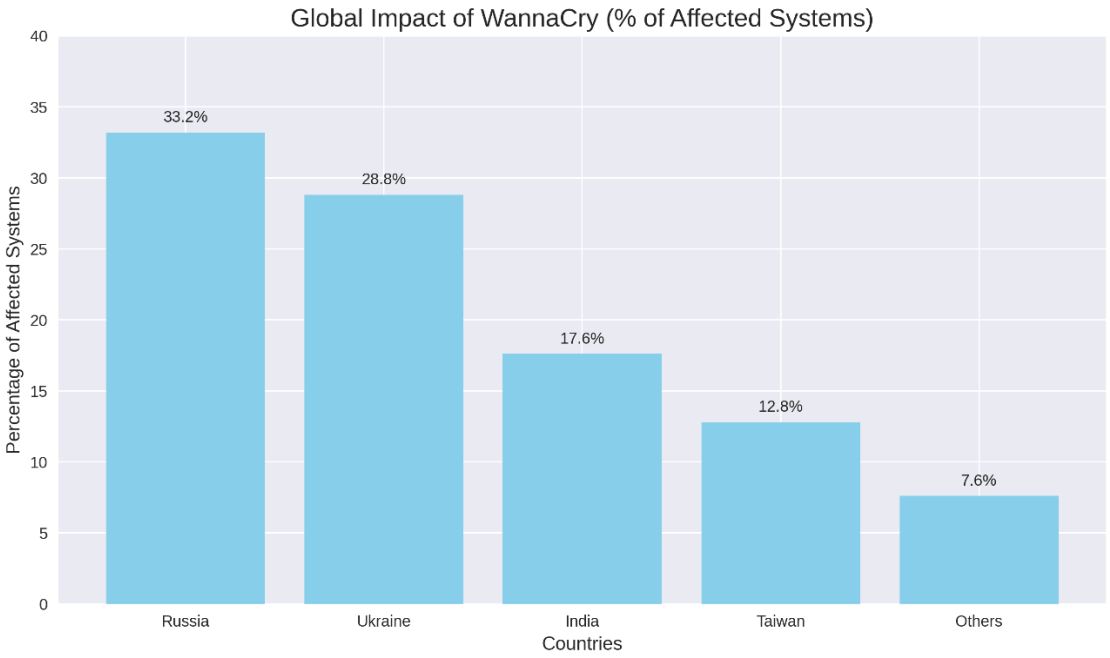

Figure 1: Global Distribution of WannaCry Infections

4.2 Temporal Progression

The attack's progression followed an exponential growth pattern typical of self-propagating malware. Initial infection rates were relatively low, with approximately 1,000 systems compromised in the first four hours. However, the infection rate accelerated rapidly, reaching 50,000 systems within 12 hours and approximately 200,000 systems across 150 countries or regions within 24 hours.

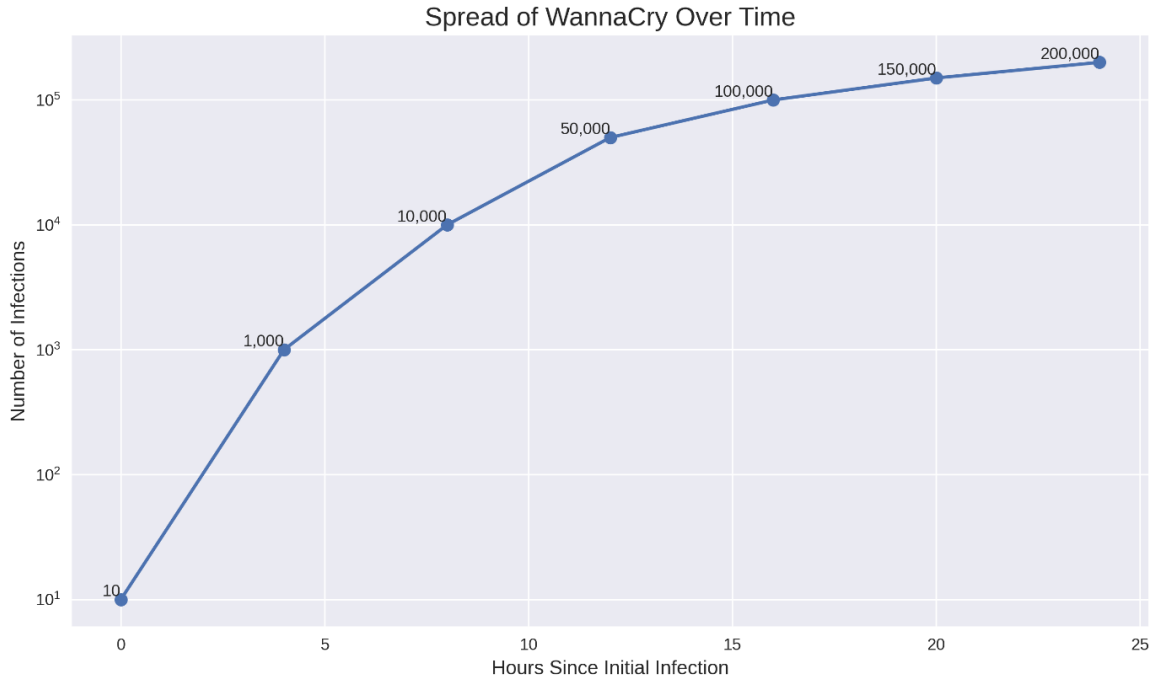

Figure 2: Timeline of WannaCry Spread

4.3 Healthcare Sector Impact

The attack's impact on healthcare systems was particularly severe. The UK's National Health Service, which was forced to cancel critical medical procedures, faced significant disruptions. The virus caused negative impact on and disrupted operations of transport systems, financial institutions, and manufacturing plants. The implications of this incident highlighted the real-world consequences of cybersecurity decisions made in the name of national security.

4.4 Economic Consequences

Financial impacts extended far beyond direct ransom payments. Organizations faced substantial costs related to system recovery, lost productivity, and implementation of enhanced security measures. Global financial losses were estimated to exceed $4 billion (Cyence & Lloyd's of London, 2017). The NSA failed in its responsibility for not disclosing the EternalBlue vulnerability, which resulted in the widespread damages.

5. The Balance Between National Security and Public Safety

The WannaCry cyberattack was an illustrative case of the dilemma usually present between national security and public safety - an issue that continues to challenge policymakers and cybersecurity professionals. Government agencies must navigate competing obligations: maintaining cyber capabilities for national defense while protecting civilian infrastructure and services.

5.1 Strategic Considerations

National security agencies argue that maintaining an arsenal of cyber capabilities, including knowledge of zero-day vulnerabilities, is essential for modern defense strategies (Singer & Friedman, 2014). These tools can provide critical advantages in intelligence gathering and potential cyber conflicts. However, the WannaCry incident demonstrated how such capabilities can become liabilities when compromised.

5.2 Public Safety Implications

The widespread impact of WannaCry highlighted the risks of prioritizing offensive capabilities over defensive measures. When vulnerabilities are kept secret for strategic purposes, they remain unpatched in civilian systems, creating widespread exposure to potential attacks (Libicki, 2019). The ultimate fallout caused wide damages to the computers worldwide

6. Contemporary Case Studies and Ongoing Challenges

Recent cyberattacks demonstrate the enduring relevance of lessons learned from WannaCry, highlighting the continuing evolution of cyber threats and the importance of ethical cybersecurity practices.

6.1 The Expanding Zero - Day Market

State actors, including Western nations, increasingly rely on the zero-day market. Companies like NSO Group (Pegasus spyware) and Intellexa (Predator) have fueled the commercialization of vulnerabilities, blurring the lines between national security and private interests. Beyond ethics, this trend endangers economic stability, trust in IT systems, and democratic values.

6.2 International Cybersecurity Agreements

The problem is if national security interests take precedence over global security, technological dominance by powerful nations such as the U.S. and China may create a new form of cyber hegemony, undermining international cooperation. For instance, the U.S. dominance in semiconductor manufacturing and China's advancements in quantum computing have shifted the balance of technological power, leading to geopolitical tensions. Similarly, the use of Israeli-developed Pegasus spyware for state surveillance has raised concerns about ethical abuses and the weakening of international privacy laws. Without stronger global agreements, the prioritization of national interests may further fragment international cyber governance, making a cooperative and balanced approach increasingly difficult to achieve. technological domination by nations such as the U.S. and China will lead to an imbalance of power with little regard for international law.

6.3 SolarWinds Supply Chain Attack (2020)

The SolarWinds incident revealed new dimensions of supply chain vulnerability. This sophisticated attack, affecting thousands of organizations through compromised software updates, demonstrated how trust relationships in software distribution can be exploited (Alshamrani *et al.*, 2021).

6.4 Colonial Pipeline Ransomware Attack (2021)

The Colonial Pipeline incident showed how cyber-attacks can directly impact critical infrastructure and essential services. The attack's disruption of fuel supplies to the southeastern United States, suffered significant operational challenges. The company was forced to shut down its pipeline operations, leading to widespread fuel shortages.

6.5 Microsoft Exchange Server Vulnerabilities (2021)

The exploitation of Microsoft Exchange Server vulnerabilities demonstrated the ongoing challenges of vulnerability management and patch deployment. This incident affected tens of thousands of organizations globally, creating a race between attackers and defenders (Orange, 2021).

6.6 Analysis of Recent Trends

Analysis of recent cybersecurity incidents reveals several interconnected patterns that demonstrate the evolving nature of cyber threats. The sophistication of attack methodologies has increased significantly, with adversaries employing multi-stage attacks that combine various technical and social engineering elements. This evolution is particularly evident in the SolarWinds attack, where attackers demonstrated unprecedented patience and sophistication in their approach to compromising target systems. The targeting of critical infrastructure has become more prevalent, suggesting a strategic shift in cyber-criminal operations. The Colonial Pipeline incident exemplifies this trend, showing how attacks on infrastructure can create cascading effects across multiple sectors of society. This targeting pattern indicates a growing understanding among threat actors of the interconnected nature of modern digital systems and their potential for creating widespread disruption. Supply chain security has emerged as a critical concern, with attacks increasingly targeting trusted relationships between software providers and their customers. The SolarWinds incident demonstrated how compromising a single trusted source can provide access to thousands of downstream targets. This trend highlights the need for more robust verification mechanisms and security controls throughout the software supply chain.The persistent challenges in vulnerability management and patch deployment, as evidenced by the Microsoft Exchange Server incidents, indicate systemic issues in how organizations approach cybersecurity. These challenges stem from complex organizational structures, resource constraints, and the increasing complexity of modern IT environments.

7. Recommendations for Ethical Cybersecurity Practices

The analysis of WannaCry and subsequent cyber-attacks provides valuable insights for developing comprehensive recommendations for ethical cybersecurity practices. These recommendations address both immediate tactical concerns and longer-term strategic considerations.

7.1 Enhanced Disclosure Frameworks

Organizations must develop and implement robust vulnerability disclosure frameworks that account for various stakeholder interests while maintaining clear ethical principles. These frameworks should establish specific criteria for evaluating vulnerabilities and determining appropriate disclosure timelines. The evaluation criteria should consider. The potential impact on public safety and critical infrastructure must be a primary consideration in disclosure decisions. This includes assessing both immediate and long-term risks to various stakeholder groups and critical systems. Organizations should develop quantitative and qualitative metrics for evaluating potential impacts, enabling more objective decision-making processes.

Technical complexity and exploitation likelihood should factor into disclosure timing decisions. Vulnerabilities that are easier to discover and exploit may require accelerated disclosure timelines, while more complex vulnerabilities might allow for longer evaluation periods. This assessment should include analysis of potential attack vectors and the technical expertise required for exploitation.

The availability and effectiveness of mitigating controls should influence disclosure strategies. Organizations should consider whether effective workarounds or temporary mitigations exist while permanent solutions are developed. This consideration helps balance the immediate need for public safety with the practical requirements of developing and testing proper fixes.

7.2 International Cooperation Mechanisms

The global nature of cyber threats necessitates enhanced international cooperation in cybersecurity efforts. This cooperation should extend beyond traditional government-to-government relationships to include private

sector entities, academic institutions, and civil society organizations. Effective international cooperation requires:

Standardized information sharing protocols must be established to facilitate rapid and secure exchange of threat intelligence and vulnerability information. These protocols should address technical, legal, and operational considerations while respecting various jurisdictional requirements and privacy concerns.

Joint response capabilities should be developed to address major cyber incidents that cross national boundaries. This includes establishing clear communication channels, defining roles and responsibilities, and creating shared resources for incident response. Regular joint exercises and simulations can help maintain readiness and identify potential gaps in response capabilities.

Harmonized regulatory frameworks should be pursued to reduce complexity in multi-jurisdictional operations. While complete standardization may not be practical, identifying and aligning core requirements can improve efficiency and effectiveness in addressing global cyber threats.

7.3 Professional Ethics Training

Cybersecurity professionals require comprehensive ethics training that addresses both technical and social aspects of their work. This training should be ongoing and evolve to address emerging challenges and technologies. Key components include:

Case-based learning should form the foundation of ethics training, using real-world examples to illustrate ethical dilemmas and their implications. The WannaCry incident and subsequent attacks provide valuable teaching materials for exploring various ethical considerations and decision-making processes.

Decision-making frameworks should be provided to help professionals navigate complex ethical situations. These frameworks should include structured approaches to evaluating competing interests, assessing potential consequences, and making defensible ethical choices.

Continuous professional development in ethics should be required to maintain relevant certifications and professional standings. This ensures that ethical considerations remain at the forefront of cybersecurity practice as new challenges emerge.

7.4 Organizational Implementation Guidelines

Implementation of ethical cybersecurity practices requires a structured approach that considers organizational context, resources, and constraints. Organizations should establish comprehensive programs that address:

Security Governance Structure: A clear governance framework should define roles, responsibilities, and accountability for ethical decision-making in cybersecurity. This includes establishing oversight committees, defining reporting relationships, and creating mechanisms for ethical review of security decisions.

Risk Assessment Processes: Organizations need robust processes for evaluating security risks that incorporate ethical considerations. These assessments should consider both technical and ethical dimensions of security decisions, including potential impacts on various stakeholder groups.

Documentation and Review Procedures: Proper documentation of security decisions and their ethical implications is crucial for maintaining accountability and enabling continuous improvement. Regular reviews of past decisions and their outcomes can help refine ethical frameworks and improve future decision-making.

8. Conclusion

The WannaCry ransomware attack represents a pivotal moment in cybersecurity history, highlighting critical ethical challenges that continue to resonate in today's digital landscape. Through careful analysis of this incident and subsequent attacks, we can identify essential principles for managing the complex relationship between national security interests and public safety.The recommendations presented in this paper provide a framework for addressing these challenges through enhanced disclosure protocols, international cooperation, and professional ethics training. However, implementing these recommendations requires ongoing commitment from all stakeholders in the cybersecurity ecosystem. As we move forward, the lessons learned from WannaCry must inform our approach to emerging cybersecurity challenges. This includes developing more robust frameworks for vulnerability disclosure, enhancing international cooperation, and ensuring cybersecurity professionals are equipped to make ethical decisions in an increasingly complex digital landscape.

References

Alshamrani, A., Myneni, S., Chowdhary, A. & Huang, D. 2021, 'A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities', IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1195-1232.

Bright, P. 2017, 'WannaCry: The ransomware worm that didn't arrive on a phishing hook', Ars Technica, viewed 25 August 2024, https://arstechnica.com/information-technology/2017/05/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/.

Cyence & Lloyd's of London 2017, 'Counting the cost: Cyber exposure decoded', Lloyd's of London, viewed 25 August 2024, https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost.

Department of Health and Social Care 2018, 'Lessons learned review of the WannaCry Ransomware Cyber Attack', NHS England, viewed 25 August 2024, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

Duan, H., Li, Z., Peng, Z. & Zhang, T. 2022, 'Towards measuring the impact of the Log4j vulnerability', arXiv preprint arXiv:2201.07706.

FIRST 2017, 'Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure', Forum of Incident Response and Security Teams, viewed 25 August 2024, https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1.

Greenberg, A. 2018, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', Wired, viewed 25 August 2024, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

He, T. 2018, 'Understanding EternalBlue: The Ransomware That Shook the World', Journal of Cybersecurity Research, vol. 8, no. 2, pp. 42-55.

Libicki, M. 2019, 'Considerations for Offensive Cyber Operations', RAND Corporation, viewed 25 August 2024, https://www.rand.org/pubs/perspectives/PE226.html.

Lin, J.C. 2015, 'Cybersecurity and National Defense: An Analysis of the Ethics of Offensive Capabilities', Journal of Military Ethics, vol. 14, no. 1, pp. 42-61.

Mimoso, M. 2017, 'NSA Exploit Among Those Used in WannaCry Attacks', Threatpost, viewed 25 August 2024, https://threatpost.com/nsa-exploit-among-those-used-in-wannacry-attacks/125773/.

Nakashima, E. & Timberg, C. 2017, 'NSA officials worried about the day its potent hacking tool would get loose. Then it did', The Washington Post, viewed 25 August 2024.

National Audit Office 2017, 'Investigation: WannaCry cyber attack and the NHS', NAO, viewed 25 August 2024, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

Orange, R. 2021, 'The Microsoft Exchange hack: What you need to know', Harvard Business Review, viewed 25 August 2024.

Palmer, D. 2018, 'WannaCry ransomware: How an NHS hospital trust is still feeling the impact', ZDNet, viewed 25 August 2024.

Shane, S., Perlroth, N. & Sanger, D.E. 2017, 'Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core', The New York Times, viewed 25 August 2024.

Singer, P.W. & Friedman, A. 2014, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, Oxford.

Smith, J. 2017, 'The impact of WannaCry on the NHS', British Medical Journal, vol. 357, p. j2689.

Tidy, J. 2021, 'Colonial Pipeline: How cyber-attack threatened US with fuel crisis', BBC News, viewed 25 August 2024.