iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.67030

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Advancing Digital Forensics and Incident Response Strategies Against Emerging Healthcare Cyber Threats

Rachael Medhurst[1], Richard Ward[2], Mabrouka Abuhmida[3]
Faculty of Computing, Engineering and Science, University of South Wales

Abstract: ***The rapid proliferation of the Internet of Medical Things (IoMT) has brought significant advancements in patient care but also introduced new cyber-related challenges. This paper focuses on cyber-related attacks on medical devices to review the Digital Forensics and Incident Response (DFIR) capabilities in the UK healthcare industry. Case studies from the United Kingdom (UK), Ireland and the United States of America (USA) have been used to highlight vulnerabilities in medical devices and healthcare IT systems, ranging from data integrity issues to large scale ransomware attacks. These attacks show the lack of sufficient information regarding the DFIR capabilities within the National Healthcare Service (NHS) in the UK, which should be assessed and continuously monitored to ensure an effective response in the event of a cyber-attack. The paper highlights the limitations of cybersecurity considerations within the healthcare industry, as well as reviewing a range of medical cyber-attacks, examining existing policies and frameworks, and discussing future DFIR capabilities in healthcare. This paper's key findings reveal gaps in current DFIR processes, including inadequate incident response plans, delayed detection of intrusions, and insufficient staff training on cybersecurity best practices. As the healthcare industry continues its digital transformation, the development and implementation of sophisticated DFIR capabilities must keep pace. A better understanding of cybersecurity challenges in healthcare and enhancing DFIR strategies will lead to improved protection of patient data and ensure the integrity of medical devices and services.***

Keywords: ***Cyber-attacks, Digital Forensic and Incident Response, DFIR, Internet of Medical Things, IoMT***

I. INTRODUCTION

The National Healthcare Service (NHS) in the United Kingdom (UK) has periodic developments to ensure patients receive necessary care. Recently, the healthcare industry has witnessed a rapid proliferation of the Internet of Medical Things (IoMT), which are designed to enhance patient care. Cost-effective Internet of Things (IoT) devices can now be integrated with medical devices, resulting in faster treatments, real-time monitoring, and personalised healthcare [1]. However, the healthcare industry has become more digitally dependent, sometimes without careful consideration of new risks and appropriate investment in cyber-security [2].

While IoMT brings efficiency to the healthcare industry, it is imperative to acknowledge the security challenges that often require Digital Forensics and Incident Response (DFIR) capabilities to determine the type of attack, how the attack occurred, what devices the attack affected, the impact to the NHS operational functions and the corresponding result to patient care. This paper examines the DFIR capabilities of cyber-related attacks on medical devices, proposes a categorisation of DFIR investigations and considers the future of healthcare DFIR.

II. CYBER SECURITY IN THE HEALTHCARE INDUSTRY

Before delving into the type of cyber-attacks within the healthcare industry, initially understanding the scale of medical devices within the healthcare industry needs to be established, and it should be noted that the NHS is a significant target for cyber-criminals [3]. "For thousands of years, healthcare was held back because we couldn't see and didn't understand the germs making us ill. Today, healthcare is held back because we don't see computer bugs, and we don't understand the risks caused by them" [4]. It has been reported that 46% of NHS IoMT devices have vulnerabilities that there is a lack of education in basic security mechanisms [5], and that only 43% of practices always change default passwords on connected medical devices and less than a third always update when a patch is available [6]. Additionally, Palo Alto Networks conducted a study of 200,000 healthcare network-connected medical infusion pumps finding that 75% of them are currently at risk, which could have catastrophic results for patients [7].

©IJRASET: All Rights are Reserved

Although incorporating training and awareness programs may not completely prevent cyber-attacks on medical devices, this knowledge would better prepare the NHS to safeguard its infrastructure and improve its response to incidents.

In addition to training and awareness programs, various preventative measures can be implemented to reduce the risk of cyber-attacks. However, it remains crucial to have structured procedures in place to respond effectively if an attack occurs. The NHS Digital website does have a 'Cyber and Data Security' page with an option for individuals to 'report an incident', where they are presented with a phone number and an email address [8]. Although it is practical to have a reporting mechanism for incidents, there needs to be a deeper understanding of the system's effectiveness, its visibility, and the measures taken after an incident has been reported. To further understand attack vectors and to determine current response capabilities, an overview of recent cyber-attacks and vulnerabilities in healthcare-related technology within the UK, Ireland and the USA will be presented.

Case studies were selected based on predefined criteria to ensure relevance and rigour. Incidents were included if they (1) occurred between 2016–2023, (2) involved NHS or comparable healthcare systems (e.g., HSE Ireland, US hospitals), (3) resulted in operational disruption, financial loss, or patient harm, and (4) had sufficient public documentation (e.g., NHS reports, peer-reviewed analyses) to evaluate DFIR processes. This approach ensures a balanced representation of attack types (e.g., ransomware, phishing) and systemic gaps (e.g., untested plans, poor communication). While the criteria prioritise incidents with public documentation, this may exclude underreported attacks. Additionally, geographic bias exists due to the focus on English-language sources, though efforts were made to include international examples.

A. IoMT Faults

In 2016, the Princess of Wales Hospital identified incorrect patient data and what was believed to be hospital workers falsifying glucometer readings. It was found that the blood glucometer meters should have been updating a web database with correct readings; however, concerns surrounding the technology used to support patients were not considered until the trial [9]. While ultimately this case was dismissed, it became apparent that the consideration of cyber-related issues (such as battery failures, device storage limitations, configuration settings or faulty devices) was not explored leading to the possible continued use of erroneous devices. With the new technology being implemented within the health industry, the consideration of IT faults, cyber-attacks and system errors should be investigated before legal proceedings start, with preventive measures implemented to minimise the chances of a cyber-incident. While the incident and the legal proceedings data are presented, there lacked information about the data integrity and incident response processes in place at that time.

B. Missing Updates

In May 2017, the WannaCry ransomware attack infected over eighty NHS trusts that had not applied a Microsoft update on their Windows 7 systems. This case meets the criteria as a high-impact ransomware attack (2017) with documented financial losses (£92M) and NHS-specific DFIR failures. Due to the unpatched operating system, more than 230,000 computers in at least 150 countries were infected, and it was estimated that this attack cost the NHS approximately £92 million due to the cancelled appointments and operations, support to recover data and to restore the systems affected by the attack [10],[11].

While there were discussions surrounding the vulnerability and that the recommended patch was not updated before the WannaCry attack, there lacked details of the DFIR capabilities and instead being more focused on the costs for the IT department to restore and recover from the incident. The National Audit Office investigated the WannaCry cyber-attack further, finding that the NHS did have a plan for responding to a cyber-attack, but it had not been tested, leading a delay in identifying, responding, and recovering from the attack [12].

C. Malware via Phishing

The Health Service Executive (HSE) is an Irish public health service that was subject to a cyber-attack called Conti in May 2021. This attack was selected due to its alignment with geographic diversity (Ireland), attack type (ransomware), and its demonstration of delayed incident detection —a critical DFIR gap.

This attack was due to a HSE employee opening a phishing email containing a malicious executable eight weeks earlier, meaning that the attack remained undetected with escalated privileges [13]. During this attack, Garda National Cyber Crime Bureau, Interpol and the National Cyber Security Centre (NCSC) supported HSE with the incident response process, which included a High Court injunction, which led to the attacker posting a link to a key that ultimately decrypted the affected files and recover computer systems.

A report detailing the Conti cyber-attack stated the impact of the incident could have been significantly greater, such as if there had been intent by the attacker to target medical devices or to destroy data, or if the ransomware spread to cloud systems [13].
Due to the decryption key being provided the HSE was able to recover from this cyber-attack within four months. However, recognising that the initial phishing email activation occurred in March and took weeks for the incident to be identified, further understanding of the incident detection mechanisms incorporated within the health industry is necessary. Incident detection should form part of the DFIR capabilities for any organisation to ensure that incidents are detected, analysed and contained to prevent and react adeptly to cyber-attacks.

D. IT System Failure

NHS England issued a formal warning over a risk to patient safety caused by a maternity IT system and a set of actions to be completed by June 2024, including checking configuration information, not copying and pasting information, ensuring all data is backed up, and updating training [3]. These cases were selected not only for direct cyber-attacks but also for systemic IT failures (e.g., NHS maternity system) that highlight vulnerabilities requiring DFIR attention, such as data integrity and monitoring gaps.
The warning was due to software that overwrote data and populated incorrect data about patients. It is a requirement of NHS users of the product to engage with their technical suppliers and consider if their local configuration is safe after a formal warning has been made [14]. However, there is a lack of auditing or continuous monitoring to ensure this, as in this example, the trusts that were using the software at the time of the alert, were still working to switch supplier [15]. To prevent incidents in the future, data integrity measures and incident detection processes should be integrated into DFIR procedures, along with audits, continuous monitoring, and appropriate governance to safeguard patients from harm.

E. Failure to Inform

A ransomware attack that targeted the Springhill Medical Centre in 2019 is believed to have contributed to the death of a newborn baby [16]. During the delivery, the baby was born with the umbilical cord wrapped around their neck, a condition that would have been detected by heart monitors due to the reduced oxygen and blood supply to the unborn baby. However, these medical devices were compromised by the ransomware attack, which ultimately resulted in brain damage and, later, the newborn's death [17]. A lawsuit against the hospital has been filed citing failure to inform the mother of the cyber-attack and negligence in patient care. Details about the incident response processes during the attack remained limited. But this case included due to its severe patient safety implications and publicly available legal proceedings highlighting communication failures. As the patient arrived on the eighth day of the attack, it suggests that the response times and communication regarding the incident were inadequate.

F. Compromising Access

CommonSpirit Health organisation was victim to a cyber-attack in September 2022. This attack was selected due to its alignment with the financial severity threshold (> $1M loss), geographic scope (U.S.), and its illustration of systemic DFIR challenges like delayed detection and opaque response processes.
The incident was identified due to the security team detecting unusual activity on the network in October. Initial steps implemented to prevent further damage including enhancing network security facilities, moving the systems offline to isolate the attack, and bringing in third-party specialists to assist in the investigation [18]. This incident led to a shutdown of the computer systems which meant that patient care, appointments and surgeries were delayed. Later, details stated that this attack accessed 623,774 patients' data records, as well as caregivers and family members. The incident response process was stated to recover by November with the estimated cost being $150 million in losses but with very little explained of the processes conducted [18]. While financial and operational impacts are well-documented, limited insights into specific DFIR processes underscore the need for improved incident reporting standards in healthcare.

G. Extortion Sites

The hacking group Black Cat advertised on an extortion site that they had a sample of data obtained from the NextGen's IT infrastructure in 2023 [19]. Although this data and advertisement was later removed, NextGen Healthcare became aware of this advertisement, which led to cybersecurity experts to investigate and remediate any breaches within their IT infrastructure to prevent any further damage. Due to this acknowledgement, action was undertaken immediately to determine any vulnerabilities and investigations took place.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

While NextGen states to have contained the threat, secured their network, and returned to normal operations, there was no evidence of access to patient data identified in that investigation. While the response was conducted upon acknowledgement, there lacked information about the DFIR capabilities and the processes that was followed. Consideration surrounding their threat monitoring tools, and DFIR capabilities should be considered as they have been attacked and unable to locate the entry point even after the data was advertised. This case was included as it exemplifies a modern extortion tactic (2023 timeframe) targeting a U.S. healthcare provider, illustrating DFIR gaps such as inadequate threat monitoring and forensic traceability despite public disclosure of the breach.

The examples throughout this section illustrate that the health industry in the UK is a significant target for cyber-attacks, which can lead to severe outcomes such as data breaches, device downtime, reduced productivity, potential harm to patient wellbeing, legal challenges, and, in the worse cases, the potential of mortality. The presented examples highlight the need for strong cyber security measures and DFIR processes to ensure reactive measures are put in place and implemented. These examples reveal the stark reality of such attacks on the industry and its IT infrastructure, and the response capabilities provided often lacked depth to be able to further understand the reactive processes after an incident, and therefore, leaving the UK health industry unable to clearly determine potential gaps and improvements for the future.

What is lacking from all examples is detailed information of DFIR capabilities, which signals a need for deeper insights into current processes to identify weaknesses and implement improvements. As the healthcare sector becomes increasingly digital, enhancing DFIR capabilities is essential to protecting patient safety and organisational integrity.

III. INCIDENT RESPONSE IN HEALTHCARE

This section illustrates key trends in attack types, financial impacts of cyber-attacks, current recovery time, and operational disruptions within the healthcare industry paragraphs must be indented.

A. Attack Types

Healthcare providers are a prime target for cyber-attacks for multiple reasons, including their expanding attack surface, lack of cyber defences, the human factor, and the heightened sense of urgency to restore confidential patient data or medical systems [20]. Efficient mitigations are required to protect the NHS against such attack vectors. Antony *et al.* [21] expressed that a proactive and moral approach to cybersecurity is necessary to maintain the resilience and integrity of healthcare systems as the industry struggles with constantly changing attack types. A proactive approach can be achieved by integrating various active mechanisms within the wider healthcare industry including backups, enhanced security controls, incident response teams, training, raising awareness, governance and compliance. While ransomware is currently the most apparent, the recognition of all attack types is required to be able to defend against such attacks efficiently.

B. Financial Impact

The increase in cyber-attacks has significantly impacted healthcare services and patient safety, resulting in a substantial financial strain on the industry. Some of the cyber-attacks previously mentioned have lacked specific cost details and others have estimated costs, that for individual cyber-attacks due to the challenges in calculating such figures. However, other cases provided estimated costs, illustrating that the recovery expenses are significant in both the UK and the USA, frequently resulting in millions being spent. Whereas, implementing preventive measures early on can help avoid catastrophic cyber-attacks and reduce additional financial burdens. The lack of early preventive measures has been presented in the 2020 Healthcare Cybersecurity Report stating that four to seven percent of a health systems IT budget is in cybersecurity compared to about 15% for the other sectors [22]. Early intervention and investment would protect the NHS from cyber-attacks, safeguarding both operations and patient wellbeing. The financial strain caused by cyber-attacks on healthcare systems underscores the urgent need for structured frameworks like ISO 27035 and robust DFIR processes to mitigate costs, enhance preparedness, and safeguard patient safety. Healthcare allocates only 4–7% of IT budgets to cybersecurity (vs. 15% in other sectors), limiting proactive defences. For example, investing in automated patch management could have prevented the WannaCry attack (costing NHS £92M) by ensuring timely Windows 7 updates.

C. Recovery Time

A full recovery typically takes between 3-6 months, with initial containment actioned as soon as possible to prevent further spread of the attack and disruption of services.

After isolating and recovering from a cyber-attack, the healthcare industry typically spends additional time, finances and resources to put further additional measures in place, including ongoing monitoring, preventive strategies, compliance checks, countermeasures, and regular reviews. Although these measures are essential after a cyber-attack, the ultimate goal is to have them in place beforehand to efficiently manage potential cyber-security threats in the healthcare industry, with ongoing monitoring in the future.

D. Operational Disruption

While cyber-attacks impose significant financial burdens on the healthcare sector, with devastating effects on the operational efficiency, and ultimately, patient wellbeing. Cyber-attacks not only compromise patient data but can also disrupt critical operations, jeopardise patient safety, and undermine public [23]. However, the healthcare industry faces unique patient linked challenges related to patients due to cyber-attacks. Although there have been no official fatalities linked to cyber-attacks in the UK, the incident at Springhill Medical Centre highlights the serious impact these attacks can have on the healthcare sector [16].

E. Summary of Current Incident Response Capabilities

Reviewing the cyber-attacks on the healthcare sector, there was notable lack of specific details regarding the DFIR capabilities, but instead, incidents were often categorised into board steps as outlined in frameworks, such as NIST Computer Security Incident Handling Guide and ISO 27035 Information Security Incident Management. Although ISO 27035 might need to be adapted to handle non-malicious incidents like system failures. The standard is primarily designed for information security incidents, but its principles are flexible.

These frameworks typically divide DFIR into categories such as Planning, Detection, Assessment, Response and Lessons Learned. However, while there is acknowledgement of the necessity of these categories, specific actions for each cyber-attack were often absent. These missing details would vary depending on factors like the type of asset, the information impacted and the nature of the attack. Gaining deeper insights into DFIR capabilities would enhance understanding of current processes and identify areas for improvement, allowing for quicker responses to cyber-attacks in the healthcare sector and reducing the financial impact of such incidents.

There are widespread cyber-attacks on the healthcare sector which can have a significant impact on essential infrastructure. These attacks highlight the need for additional resources, funding, and support to safeguard this critical infrastructure, and enhance DFIR capabilities to appropriately respond to a cyber-attack within the healthcare industry.

IV. DIGITAL FORENSICS AND INCIDENT RESPONSE CAPABILITIES IN THE HEALTHCARE INDUSTRY

The fact that over 90% of crime is recognised as having a digital element, means that the role of digital forensic will only grow [24]. The preparation for a cyber-attack within the NHS is vital, and ensuring all processes are correctly followed to protect the healthcare industry, patients, and the data. Understanding the current processes within the NHS if/when a cyber-attack is essential to determine its effectiveness and how this could be developed to better handle the continual increase of attacks. The NHS has stated that they have an Incident Response Plan in place, with the website stating that the NHS needs to be able to plan for, respond to and recover from a wide range of incidents, emergencies, or disruptive challenges that could impact on health or patient care [25]. However, the NHS's Incident Response Plan does not directly correlate to cyber-attacks and cyber-related incidents. Nevertheless, there would be a requirement for each health board to have efficient plans in place, including an Incident Response Plan, disaster recovery and business continuity that relate directly to cyber-attacks. However, in the example of the WannaCry attack, the NHS stated they had an incident response plan, but it had not been stress tested to determine the effectiveness and ensure all necessary individuals understand the steps efficiently. The WannaCry attack has highlighted that having a plan is not sufficient, regular awareness training, stress testing, audits, and updates are required to be effective in managing an incident.

The importance of developing an understanding of the cyber incident response capabilities is vital to be able to respond effectively in the event of an incident occurring against the NHS. To be able to achieve this, the NHS has incorporated Cyber Incident Response Exercises (CIRE) which aim to develop and test an understanding of how the incident response should be carried out in a health and social care setting and context [8]. There are five healthcare industry-linked exercises have been aligned with the NCSC to enable further understanding of the DFIR process that can be incorporated into the training and awareness of staff (see Table I).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Leveraging the CIRE scenarios will help ensure that health boards and individuals managing incidents are well-prepared to handle the processes efficiently and follow established health board procedures during an incident. However, integrating these scenarios requires dedicated time for conducting them, as well as additional time for training and raising awareness on managing cyber-incidents affecting the NHS. Without this training and awareness, response times may be delayed, response capabilities weakened, and the risk of further network damage and compromised patient care increased.

TABLE I
A SUMMARY OF THE NHS'S HEALTHCARE LINKED CIRE SCENARIOS [8]

Exercise	Focus	Learning Objective
1	Incident reporting and escalation	The overall focus for this exercise is to test internal escalation processes and the communication strategies in place
2	Incidence response planning and preparation	This aspect is designed to test the employee on several areas of cyber-security to identify an incident, understand the fundamentals of preparing for an incident, and how to act to prevent cyber-attacks now and in the future. This overall prepares for improved prevention and forensic readiness in the event of an incident
3	Cyber security incident response team actions and interactions	To test how your incident response team manages the incident as it develops, checking your escalation and reporting processes, and ensuring that you have a robust communication strategy
4	An incident within a GP practice	This incident focuses on the insider threat but its designed especially for GP practices
5	Co-ordinating a cyber incident alongside another major incident	To test how Cyber Co-ordination Groups can continue operating as the co-ordinating authority for a major crisis whilst itself suffering from a cyber-attack. It aims to test the resilience of business continuity plans and the effectiveness internal and external communications

There is a general understanding that IoT devices are a challenge to investigate, this is due to the devices not being standardised, the wide variety of devices, the connectivity of devices, and volatile data. Therefore, several frameworks have been developed to assist in the DFIR capabilities when investigating IoT-related devices and these will next be reviewed.

A. Digital Forensic Investigation Framework (DFiF)

The Digital Forensic Investigation Framework (DFiF) is specifically designed to focus on the process of DFIR ensuring a consistent approach to investigating digital devices while maintaining evidential integrity [26]. DFiF is aligned with ISO 27043, which specializes in incident response investigations. It emphasises several key aspects, including the appropriate handling of devices, thorough analysis, detailed reporting, and maintaining the integrity of evidence. By aligning with ISO 27043, DFiF ensures that policies, procedures, and plans for incident investigations are efficiently prepared and tested, enabling immediate action in the event of an incident.

B. Digital Forensic Framework for Smart Environments (IoTDOTS)

Smart environments, characterised by an ecosystem of interconnected devices, sensors, and systems that provide various services, are becoming increasingly prevalent. Consequently, the Digital Forensic Framework for Smart Environments (IoTDOTS) offers a structured approach to identifying, collecting, and analysing data from such environments [27]. Although the healthcare sector can be considered a smart environment due to its extensive use of technology to enhance patient care and wellbeing, it's important to recognise that medical devices may differ from traditional IoT devices, necessitating specialised investigation processes. Therefore, consideration must be given to the unique characteristics and requirements of medical devices within IoTDOTS.

C. *Forensic State Acquisition from Internet of Things (FSAIoT)*

The Forensic State Acquisition from Internet of Things (FSAIoT) framework is designed to handle the digital forensic process of IoT devices, addressing the challenges they pose while maintaining evidential integrity for potential legal proceedings. Key steps within the FSAIoT framework include the identification of IoT devices, isolation of devices, data acquisition, ensuring data integrity, analysis, and documentation of findings. Although FSAIoT is beneficial for any industry utilising IoT devices, but it does not directly apply to IoMT, where human wellbeing is in danger.

These frameworks can be utilised by organisations integrating technology into their operations, covering the requirements of DFIR capabilities from preparation to analysis and reporting. However, a consistent issue across all these frameworks is their lack of specific alignment to the healthcare sector, focusing instead on IoT devices in general. Given the wide variety of IoMT devices, their differing file systems, memory storage, connectivity, and functionality, a diverse forensic approach is necessary to handle such life supporting equipment in a different way to generalised IoT devices. This approach should be implemented and frequently updated to reflect the ongoing development of IoMT devices and their specific impacts on patient wellbeing.

A framework specifically aligned with the healthcare sector should incorporate elements from existing cyber related incident response frameworks, such as ISO 27043, ISO 27035, and Mitre Att&ck, and also integrate requirements unique to healthcare to ensure patient safety. This specialised framework should include fundamental forensic categories to be investigated, and the process for identifying the type of attack, understanding how it was executed, identifying exposed vulnerabilities, assessing affected assets, and evaluating the consequences of the incident on the medical device. This comprehensive approach would provide a full picture of the cyber-attack, ensuring thorough and effective DFIR capabilities in the healthcare sector.

V. DIGITAL FORENSIC AND INCIDENT RESPONSE CATEGORIES

The initial step in a DFIR process involves identifying where data is stored to examine these areas and answer key questions related to the cyber-attack. Digital Forensic analysis requires a comprehensive approach, so investigators must consider various forensic methodologies suitable for the investigation. Maintaining data integrity is crucial, and the least intrusive methods should be employed first to preserve evidence. This means that the following aspects of investigation should be followed (and highlighted in Fig. 1):

1) Local Device – The physical IoMT device should be examined. Given the wide range of medical devices, digital forensic investigators must adopt a flexible approach to account for varying storage types, devices, and operating systems. The forensic approach will vary depending on these factors.

2) Mobile Device – Many IoMT devices connect to a mobile device for data collection, device functionality, and reporting to medical professionals. Digital forensic investigators should therefore consider the mobile device as a potential source of evidence when responding to an incident.

3) Network & Cloud – Since IoMT devices are often network-connected, evidence may be found on network or cloud storage. Investigators should analyse network connections and cloud data for any suspicious activity that may require further examination.

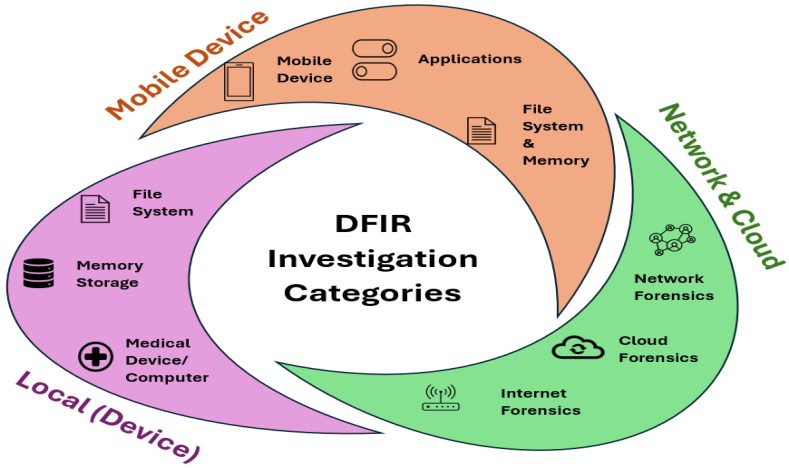


Fig. 1 A proposed categorisation for DFIR investigation of IoMT devices.

The investigation of a cyber-attack on the healthcare sector could include several categories of devices, artefacts and sources of evidence. This will enable the investigator to gather large volumes of data and potential evidence that could determine the type of attack, impact and how this was achieved. After locating such details and understanding the incident further, the methods to then protect the devices further can be conducted.

A. DFIR Process – Healthcare Sector

Several frameworks have been reviewed regarding IoT DFIR processes, encompassing broad requirements and detailed steps. While these frameworks may be relevant across various industries, it is essential to adapt and implement each phase to suit the healthcare sector specifically. This ensures that patient car e and well-being are maintained while effectively addressing cyber-attacks on the industry or medical devices.

While a generalised plan may be valuable to industries experiencing a cyber-attack, these industries typically do not handle vulnerable patients or focus on patient wellbeing. However, without a specialised and focused plan for the healthcare industry, there could be gaps that lead to medical negligence towards patients during the resolution of a cyber-attack. Therefore, without a focus driven healthcare incident response plan, there will be an impact on patient safety in the event of a cyber-incident.

VI. MEDICAL DEVICE FUTURE CONSIDERATIONS

The case studies presented in this paper have highlighted that the prospect of cyber-attacks on the healthcare sector is prevalent and the importance of cyber-security mechanisms and the incorporation of effective DFIR processes and plans cannot be underestimated. Elements such as forensic readiness, incident response, and business continuity plans are required to ensure that in the event of a cyber incident, then an effective response is actioned to return the healthcare provider to everyday functioning, and safeguard patients.

“Forensics readiness is the ability of organisations to respond quickly and collect digital evidence related to a security incident with minimal cost or interruption to the ongoing business” [29]. Without the key elements including appropriate documentation such as incident response, business continuity and disaster recovery plans that are essential, this will leave the healthcare provider unprepared in the event of an incident. Additionally ensuring these processes and plans are stress tested to confirm that individuals are as reactive and efficient as possible in the event of an incident. Other considerations should include the incorporation of efficient DFIR tools, and threat monitoring to continuously monitor systems, network, and traffic. This helps to identify any suspicious activities. Alerts are then reviewed by a Security Operations Centre analyst to determine if the alert is a true positive, or a false positive. If this was identified as a true positive, then next steps within the incident response process would be actioned to prevent further damage and disruption to the health board. After an incident has been identified, and the processes actioned, the requirement for further DFIR investigations to answer questions surrounding who, why, what, how, etc this incident has occurred. By understanding these elements this will assist in securing the device/network to prevent this from happening again in the future.

However, to be able to answer these questions, effective and efficient forensic tools are required. Due to the various IoMT devices, this can be a challenge for an individual forensic tool to be able to cater for the diverse types of medical devices available. Therefore, a variety of different forensic tools is recommended to cater for a full investigation process and to cater for a diverse range of devices. However, there is a responsibility on the investigator, to ensure that they are updating their tools to cater for new technology, file systems, storage mediums, etc. Without the developments to the DFIR tools, this will limit the capability of responding to an incident.

Additionally, there are frameworks and considerations incorporated into the NHS to help react efficiently in the event of an incident, including exercises, IoT frameworks, and the incident response reporting mechanism. It has been highlighted, that there is not a framework relating to the DFIR capabilities within the healthcare sector on IoMT devices. Having a structure framework for the healthcare industry would be beneficial as their responses and reactions may differ to other organisations and sectors. While the NCSC has developed the CIRE that the NHS can incorporate into their training and awareness. However, there is still a lack of ability to respond efficiently to these incidents, so therefore, having compulsory training implemented within the healthcare sector is vital.

VII. CONCLUSION

Over the past decade there have been critical vulnerabilities in medical devices and healthcare IT systems, ranging from data integrity issues to large-scale ransomware, that underscore the urgent need for robust DFIR capabilities in the healthcare sector.

Healthcare faces unique challenges, including the complexity of medical device ecosystems, the critical nature of patient data, and the potential for cyber incidents to directly impact patient care and safety. Effective DFIR frameworks in healthcare must address several key areas: regular vulnerability assessments and patching of medical devices, continuous monitoring and incident detection, comprehensive incident response plans with regular testing, and enhanced staff training on cybersecurity best practices. Additionally, as healthcare continues its digital transformation, improved collaboration between IT, security, and clinical teams is essential to ensure a holistic approach to cybersecurity, and importantly, sophisticated DFIR capabilities must be implemented. This evolution is crucial not only for protecting patient data but also for maintaining the integrity and safety of medical devices and healthcare services. The future of healthcare cybersecurity lies in proactive, adaptive, and comprehensive DFIR strategies that can effectively mitigate the ever-evolving threat landscape.

REFERENCES

[1] S. Razdan and S. Sharma, “Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies,” IETE Technical Review, vol. 39(4), pp. 775–788. 2021. https://doi.org/10.1080/02564602.2021.1927863
[2] WHO (2024) WHO reports outline responses to cyber-attacks on health care and the rise of disinformation in public health emergencies. [Online]. Available: https://www.who.int/news/item/06-02-2024-who-reports-outline-responses-to-cyber-attacks-on-health-care-and-the-rise-of-disinformation-in-public-health-emergencies
[3] NHS England (2024) Cyber Security. Version 1.1. [Online]. Available: https://www.england.nhs.uk/long-read/cyber-security/
[4] H. Thimbleby, Fix IT: See and Solve the Problems of Digital Healthcare. 1st ed. Oxford: Oxford University Press, 2021.
[5] Cynerio (2023) The State of NHS Trust IoT Device Security 2023. [Online]. Available: https://www.cynerio.com/nhs-trusts-iot-security-report-cynerio-only
[6] Capers, Z. (2022) More Healthcare Devices Means More Cyberattacks - How Weak Medical IoT Security Threatens Patient Care. Available: https://www.capterra.com/resources/medical-internet-of-things-iot-security/
[7] Palo Alto Networks (2022) Palo Alto Networks Announces Medical IoT Security to Protect Connected Devices Critical to Patient Care. [Online]
[8] Available: https://investors.paloaltonetworks.com/news-releases/news-release-details/palo-alto-networks-announces-medical-iot-security-protect
[9] NHS Digital (2025) Cyber Incident Response Exercise (CIRE). [Online]. Available: https://digital.nhs.uk/cyber-and-data-security/training/cyber-incident-response-exercise
[10] H. Thimbleby, “Misunderstanding IT: Hospital cybersecurity and software problems reach the courts,” Digital Evidence and Electronic Signature Law Review, vol. 15, pp. 11-32. 2018. https://doi.org/10.14296/deeslr.v15i0.4891,
[11] W. Smart (2018) Lessons learned review of the WannaCry Ransomware Cyber Attack. [Online]. Available: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
[12] Cyber Security Policy (2018) Securing cyber resilience in health and care: Progress update October 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf
[13] National Audit Office (2017) Investigation: WannaCry cyber attack and the NHS. [Online]. Available https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ PwC (2021) Conti cyber attack on the HSE. [Online]. Available: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf
[14] S. Trendall (2023) NHS issues warning over potential serious risks to patient safety posed by issues with maternity IT system. [Online]. Available: https://www.publictechnology.net/2023/12/08/health-and-social-care/nhs-issues-warning-over-potential-serious-risks-to-patient-safety-posed-by-issues-with-maternity-it-system/
[15] C. Lydon (2024) Euroking Patient Safety Alert: 13 Trusts Switch Supplier. [Online]. Available: https://www.digitalhealth.net/2024/04/euroking-patient-safety-alert-13-trusts-switch-supplier/
[16] K. Poulsen, R. McMillan and M. Evans (2021) A Hospital Hit By Hackers, A Baby In Distress: The Case Of The First Alleged Ransomware Death. [Online]. Available: https://www.namd.org/journal-of-medicine/2789-a-hospital-hit-by-hackers-a-baby-in-distress-the-case-of-the-first-alleged-ransomware-death.html
[17] S. Alder (2021) Lawsuit Alleges Ransomware Attack Resulted in Hospital Baby Death. [Online]. Available: https://www.hipaajournal.com/lawsuit-alleges-ransomware-attack-resulted-in-hospital-baby-death/
[18] S. Alder (2023) CommonSpirit Health Reports $150 million Loss Due to Ransomware Attack. [Online]. Available: https://www.hipaajournal.com/commonspirit-health-reports-150-million-loss-due-to-ransomware-attack/
[19] K. Trupplaar (2023) 1M NextGen Patient Records Compromised in Data Breach. [Online]. Available: https://www.darkreading.com/application-security/1m-nextgen-healthcare-patient-records-stolen-
[20] A. Al Qartah, "Evolving Ransomware Attacks on Healthcare Providers," MSc Cybersecurity dissertation, Utica College, ProQuest Dissertations & Theses, Aug. 2020.
[21] A. Antony, S. M. Thomas, T.K. Varghese and V. Padman, “Ransomware Attacks on Healthcare Systems: Case Studies and Mitigation Strategies,” preprint, 2023. http://dx.doi.org/10.13140/RG.2.2.34192.17928
[22] S. Morgan (2020) The 2020 Healthcare Cybersecurity Report. [Online]. Available: https://www.herjavecgroup.com/wp-content/uploads/2019/12/Healthcare-Cybersecurity-Report-2020.pdf
[23] P. Mee and E. Southerlan (2023) Seriousness of Cyberattacks in Healthcare Cannot be Ignored [Online]. Available: https://www.oliverwyman.com/our-expertise/perspectives/health/2023/oct/seriousness-of-cyberattacks-in-healthcare-cannot-be-ignored.html
[24] National Police Chiefs’ Council (2020) Digital Forensic Science Strategy. [Online]. Available: https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[25] NHS England (2022) NHS England Incident Response Plan (National). Version 4.0. [Online]. Available: https://www.england.nhs.uk/wp-content/uploads/2017/07/B0992i-incident-response-plan-national-v4.pdf

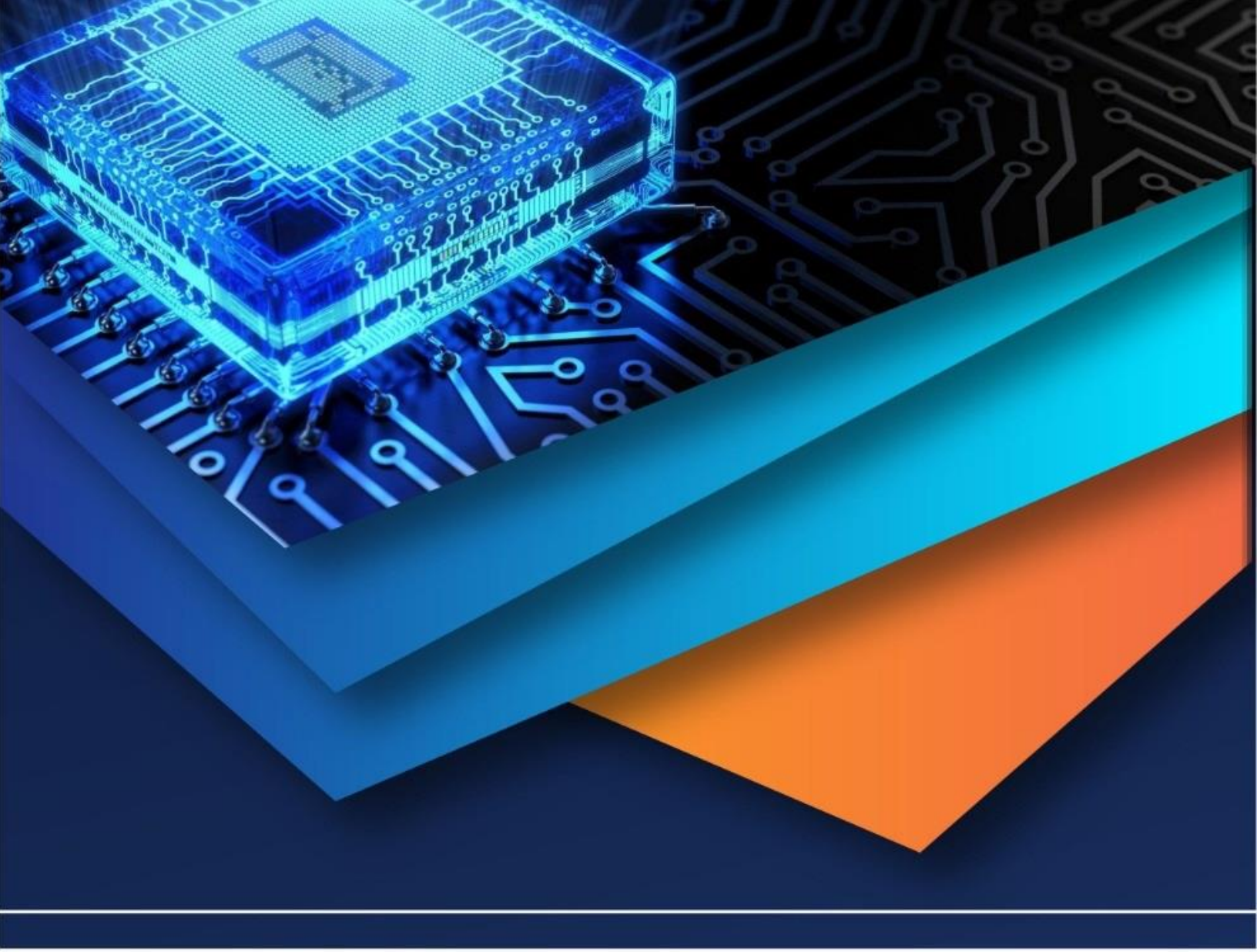
[26] V.R. Kebande and I. Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, Vienna, Austria, pp. 356–362. 2016. https://doi.org/10.1109/FiCloud.2016.57

[27] A. Goudbeek, K.-K.R. Choo and N.-A. Le-Khac, "A Forensic Investigation Framework for Smart Home Environment," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, New York, NY, USA, pp. 1446–1451. 2018. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00201

[28] C. Meffert, D. Clark, I. Baggili and F. Breitinger, F., "Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition," Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM, Reggio Calabria Italy, pp. 1–11. 2017. https://doi.org/10.1145/3098954.3104053

[29] C. Vidal and K.-K.R. Choo, Cloud security and forensic readiness, in The Cloud Security Ecosystem, ScienceDirect: Elsevier, pp.401-428, 2015. https://doi.org/10.1016/C2014-0-00456-X

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)