





Research Article

Healthcare Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure

Ying He ¹, Leandros Maglaras ², Aliyu Aliyu ² and Cunjin Luo ^{3,4}

¹School of Computer Science, University of Nottingham, Nottingham, UK

²School of Computer Science and Informatics, De Montfort University, Leicester, UK

³School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK

⁴Key Lab of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou, China

Correspondence should be addressed to Cunjin Luo; cunjin.luo@essex.ac.uk

Received 4 December 2021; Revised 16 January 2022; Accepted 18 January 2022; Published 23 February 2022

Academic Editor: Thippa Reddy G

Copyright © 2022 Ying He et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The healthcare information system (HIS) has become a victim of cyberattacks. Traditional ways to handle cyber incidents in healthcare organizations follow a predefined incident response (IR) procedure. However, this procedure is usually reactive, missing the opportunities to foresee danger on the horizon. Cyber threat intelligence (CTI) contains information on emerging attacks and should be ideally utilized to inform the IR procedure. However, current research shows that the IR has not been effectively informed by CTI, especially in healthcare organizations. This paper fills in this gap by proposing a proactive IR response procedure based on the National Institute of Standards and Technology (NIST) IR methodology. This paper then presents the NHS WannaCry case study to demonstrate the use of the proposed IR methodology. We collate cyber security advisories from different CTI sources such as US/UK CERT to protect interconnected systems and devices from Ransomware attacks. This research provides novel insights into the IR in healthcare through embedding CTI advisories into IR processes and concludes that our proposed IR procedure can be used to counteract WannaCry Ransomware using CTI advisories. It has the significance of transforming the way of IR from reactive to proactive using the CTI in healthcare.

1. Introduction

Cyber security attacks such as Ransomware [1] have caused major incidents to the Critical National Infrastructure (CNI) within various industries, especially in healthcare [2]. Existing work shows that a staggering 34% of ransomware attacks are targeted at healthcare organizations [3]. Recent research shows that over the past five years time, thousands of healthcare-related data breaches have been reported, affecting more than 154 million health records in total [4]. A typical example is the WannaCry malware, one of the most historic ransomware attacks, that had targeted the UK National Health Service (NHS) causing 19,000 appointments to be canceled, costing the NHS £20 million between 12 May 2020 and 19 May 2020 and £72 million in the subsequent cleanup and upgrades to its IT systems [5].

Healthcare organizations are a favored target as it has many critical systems within their medical infrastructure [6-11]. Once a healthcare organization is infected with ransomware, healthcare services will fail to operate as expected [3] and human lives will be jeopardized. It is imperative to defend against the threats such as ransomware, especially in healthcare.

Traditional ways to handle adverse events in healthcare organizations follow a predefined incident response (IR) procedure, which includes preparation, detection and analysis, containment, eradication, and recovery, and post-incident activities [12-14]. What is not so readily considered is that countermeasures themselves can have unintended consequences, whether in crime prevention, physical security [15], or cybersecurity [16]. What is even less often considered is the fact that countermeasures can actually

cause harm, whether to the infrastructure or to some or all of its users. This harm can be as minor as the disruption and additional security burden of using a system to the negative impact on entire groups of users, forcing them to leave the system/service or placing them in a position where they are more physically or psychologically impacted [17].

However, most organizations are still adopting a reactive method [18], which obscures their capability to foresee potential security attacks in the future. Emerging threats need to be handled with a proactive approach [19]. CTI is the provision of evidence-based knowledge about impeding threats aiming to support organizations' security defense at strategic, operational, and tactical levels. A proactive approach relies on the CTI as a consultative practice, built with people processes, and technology to achieve continuous improvement of cyber security.

To address this challenge, this research proposed a proactive IR procedure through embedding the CTI that contains information on emerging attacks, root causes, affected assets, the course of actions. This allows the organizations to be well aware of the emerging attacks, get prepared and respond to those attacks proactively. This paper then presents the NHS WannaCry Ransomware case study to demonstrate the use of the proactive IR procedure. This paper makes the following contributions,

1. Reviews the current IR literature and practices and identifies the gap of the research in IR informed by CTI;
2. Proposes a proactive IR methodology that is informed by CTI, through embedding CTI into the traditional IR procedure;
3. Presents the NHS WannaCry case study to demonstrate the use of the proposed proactive IR procedure.

The remainder of this paper is structured as follows. Section 2 presents related work of cyber threat intelligence, security incident response, and Ransomware. Section 3 introduces the proactive incident response (IR) methodology. Section 4 applied the proactive IR methodology to analyse the NHS WannaCry Ransomware case study. Section 5 concludes the research and outlines future work.

2. RELATED WORK

This section introduces related work in cyber threat intelligence (CTI), security incident response (IR), and Ransomware. TABLE 1 provides a summary of related work.

2.1. Cyber Threat Intelligence (CTI). CTI contains information such as attack vectors, attack actors, victims, courses of actions, affected organisations and is presented in the form of CTI feeds using different standardised languages (e.g. MAEC, STIX, TAXII, CYBOX) [20]. The security communities have established CTI platforms (e.g. UK/US Cert, Microsoft, MISP, and MITRE) to facilitate threat exchange [21]. Proactive defense should be ideally informed by CTI [22]. The detective and preventive capabilities needed to resolve attacks have been improved by CTI as it has provided

advisories and security recommendations during security operations. The knowledge base of threat information and the way in which data is represented concludes the successfulness of the CTI within the cyber domain. This purpose is served by the use of taxonomies [23], CTI sharing standards [20], and ontologies [24] in security defence.

CTI is classified into four different types, namely Strategic, Operational, Tactical, and Technical threat intelligence [21]. Strategic Threat Intelligence [25] can help the decision-makers understand current and identify further risks related to the aims of an organisation. It is consumed by the board level of decision-makers is often short and concise, focusing on business impact and risk. Operational Threat Intelligence [26] provides information on the details of the incoming attack, the identity, and capability of the attack actor, and also the probability of the attack. This information is consumed by the security managers and the incident response team lead. Tactical Threat Intelligence provides details on the threat actors, their tools, and methodologies, which is also known as the Tactics, Techniques, and Procedures (TTPs) [27]. It is consumed by architects, internet administrators, security analysts, etc. Technical Threat Intelligence involves the technical details of an attacker's capabilities for example their tools, Command and Control (C2) channels, and infrastructure. It is usually consumed by staff at the first line of defense i.e. SOC analysts.

2.2. Security Incident Response (IR). Security incident response procedure includes preparation, detection and analysis, containment, eradication and recovery, and post-incident activities [12,13,14,28]. The Preparation stage establishes the incident response capability that will enable the organization to be ready to respond when an adverse event occurs. Main activities include the preparation of the communication routes and facilities, hardware, software, network diagrams, security plans, and predefined mitigation strategies. In the detection phase, organizations use precursors and indicators (e.g. information collected from log files, intrusion detection systems, and antivirus software) to detect incidents. Accurately detecting and assessing possible incidents have proven to be difficult, especially when determining the type, extent, and magnitude of it due to the high volumes of potential incidents. Their intrusion detection systems [29] can receive thousands if not millions of alerts per day. The majority of incidents require containment before performing the eradication and recovery as it may reduce the resources used and the damage caused to the business processes. Various containment strategies are available and predefined. After major incidents have occurred, organizations should hold a "lessons learned" meeting with all parties involved [14,30]. The meeting will help the organization when improving its security measures and the incident response handling itself.

2.3. Ransomware. Ransomware [31] is a variation of malicious software that once installed will encrypt files on a machine. The attacker will then demand a ransom to which the victim will have to pay to get their files decrypted back to

TABLE 1: Proactive Incident Response (IR) informed by Cyber Threat Intelligence (CTI) in the context of counteracting ransomware

	Author(s)	Description
CTI	Barnum [20]	Standard description of CTI using structured threat information expression
	Tounsi and Rais [21]	A survey on technical threat intelligence and its CTI sharing platforms
	He et al. [22]	Proactive cyber defence strategy through feeding CTI into IR processes
	Burger et al. [23]	Taxonomy model for cyber threat intelligence information exchange technologies
	Qamar et al. [24]	Data-driven analytics for CTI through mapping CTI feeds to Web Ontology Language (OWL) ontologies
	Dog et al. [25]	Strategic cyber threat intelligence sharing and a case study on IDS logs
	Li et al. [26]	Operational threat intelligence and a comparative analysis of CTI
	Maymí et al. [27]	Tactical threat intelligence (tactics, techniques, and procedures)
IR	Cichonski et al. [12]	NIST IR model: computer security incident handling guide
	Souppaya and Scarfone [13]	NIST malware incident prevention and handling
	Ahmad et al. [14]	A case study on information systems and security incident response processes
	Moreno et al. [28]	IR processes enhanced by blockchain technologies
	Grispos et al. [30]	IR processes (follow-up stage) improved by Agile methodology
Ransomware	Field [5]	NHS WannaCry ransomware incident investigation and response
	Brewer [34]	Ransomware IR detection, prevention, and cure
	Hassan [32]	Ransomware IR definition and its variants
	Kyurkchiev et al. [33]	CryptoLocker ransomware analysis and investigation

their original form. It can deny legitimate users access to systems or data. It blocks access to the systems or data and threatens to release the victim's data unless a ransom is paid. Such attacks typically use a Trojan as their attacking method. The Trojan can be disguised as a legitimate file waiting to be downloaded and opened by the users. There are various variants of ransomware such as Petya, Locky, and Samas [32].

Two types of ransomware making headlines all across the world in recent months are called CryptoLocker [33] and CoinVault. Both types of ransomware operate, in the same way, as they infect a computer as soon as an unsuspecting user clicks an unknown link or opens up an attachment sent via email. The high profile Ransomware is the UK NHS WannaCry [5]. Several hospitals and GP surgeries were forced to shut down their entire IT systems over the weekend, after ransom notes from hackers appeared on computer screens, threatening to delete all of their files within seven days unless a ransom of \$300 in bitcoin currency was paid. It can be distributed through spam emails and fake ads, which trick users into downloading the virus onto their computer. It then sets about creating encrypted copies of files on the victim's computer, and deleting the originals, leaving the victim with only the encrypted copies, which cannot be accessed without a decryption key.

3. Proactive IR Methodology

In this section, we propose the proactive IR methodology by mapping the National Institute of Standards and Technology (NIST) IR methodology [12,13] to the extracted CTI advisories from different sources including US CERT [35–37]. and industrial best practices. Through embedding CTI into the IR lifecycle, organisations can benefit from an informed IR with the CTI advisories from different sources. organisations should be able to take this information and map it to their own IR processes to enhance their networks, systems and applications security against potential attacks. Fig. 1 provides an overview of

our proposed proactive IR procedure with actions in different stages of IR. The IR procedure starts from Planning & Preparation, finishing in the stage of Post-incident Activity. We have listed the actions required to be taken in each of the IR stages. The actions include both the ones from NIST and newly added ones derived from CTI advisories. The rest of this section detailed the actions in different stages.

3.1. Planning & Preparation. The Preparation stage establishes the security plan and incident response capability that enables the organisation to be ready to respond to an incident. It helps to prevent incidents by ensuring sufficient security for systems, networks, and applications. The initial preparation phase involves the creation of an incident response team and acquiring the necessary tools and resources, as well as implementing a set of controls on their assets, some of which will be based on the risk assessment results in an attempt to limit the number of incidents that have already been identified. This stage identifies the facilities needed throughout the life cycle. An incident reporting mechanism facility should be implemented, allowing individuals or teams to declare a potential incident to a wider view of people or a person of higher authority. This can be done via phone numbers, email addresses, online forms, security management systems, etc. Issue tracking system facilities can be implemented, containing information about the case owner, case status update as well as for the uses of report generating and learning purposes. This stage should prepare software and hardware to analyse and mitigate incidents. For example, a clean image of the operating system, fresh application installations, digital forensic software, additional workstations, servers, and networking equipment. Organisations should also consider implementing systems purely for backups and to analyse incidents in a controlled environment. Incident analysis resources should also be incorporated in the preparation stage such as risk assessment.



FIGURE. 1: Proactive Incident Response (IR) informed by Cyber Threat Intelligence (CTI)

Network diagrams and a list of critical assets should also be identified. This will allow for the addition of specific security controls based on high-end organisational-assets. System and staff training is also required. The incident response team can play a key role in the risk assessment and training process.

CTI can strengthen the Preparation capacity by providing additional information on emerging threats that the organizations are facing. Such CTI can be obtained from different sources, such as CTI advisories provided by US/UK

CERT, security incident reports, and CTI sharing platforms. The CTI advisories especially those within the same industry or business domain can help the organizations prepare tailored IR plans and capacity to counteract emerging threats and proactively react to the incidents.

3.2. *Detection.* The detection of an incident can be via a variety of forms, each with a varied level of detail and fidelity. One form of incident detection uses automated capabilities,

for example, network/host-based intrusion detection systems [38,39], antivirus software, and log analyzers. Another uses manual needs, such as users reporting problems. Some incidents have blatant signs that can be easily detected, for example, a defaced website, yet others are almost impossible to detect. An organization will typically receive high volumes of potential incidents. Their intrusion detection sensor alerts can receive thousands if not millions of alerts per day. Precursors and indicators are two categories that can show signs of an incident. A precursor is “a sign that an incident may occur in the future”. Whereas, an indicator is “a sign that an incident may have occurred or may be occurring now”. These precursors and indicators can be obtained from antivirus software, file integrity checking software, and intrusion detection prevention systems. Log files can also be used for detection purposes and they can be obtained from the operating system, services and application logs, and network device logs.

CTI sources can provide an exhaustive list of indicators. These indicators are usually publicly available via the CTI advisories provided by US/UK CERT. These indicators can also be downloaded from CTI sharing platforms such as MISP [40]. Those can then be used to update the signatures of the IDPS, allowing the IDPS to detect emerging threats proactively. Some CTI sharing platforms provide enabling functionalities to continuously feed updated indicators to the IDPS and other monitoring systems.

3.3. Analysis & Assessment. Once an incident has emerged, the incident response team should work quickly to analyze and validate it, making sure to follow pre-defined processes and documenting every step taken. When the incident becomes apparent to the team, performing rapid initial analysis should be performed to determine the incident scope. For example, which networks, systems, or applications are affected; how the incident is occurring (e.g., what tools or attack vectors are being used, what vulnerability is being exploited (5)); and who or what originated the incident. The initial information produced from this analysis enables the team to prioritize subsequent activities (e.g., containment strategy of the incident and further analysis regarding the effects of the incident).

When analyzing the incidents, the precursors or indicators may not be accurate. For example, intrusion detection systems regularly produce false positives – incorrect indicators. This shows the difficulties that incident response teams face, especially when every indicator has to be examined to determine whether it is legitimate. Additionally, thousands of indicators are identified every day, making it an extremely daunting task to identify the real security indicators. Even an indicator has shown to be accurate, it still does not necessarily conclude that an incident has occurred. For example, the modification of a critical file may not be a security incident but a human error. Some incidents do not have clear symptoms, for example, one-character modification within a file name.

The incident response team may be unable to fully determine the cause and nature of an incident. This could have

major effects on the organization, for example not having enough information to make decisions on whether to contain or eradicate the incident. In this scenario, organizations should seek assistance from CTI sources such as US-CERT, and CTI sharing platforms to determine the full scope and cause of the incident. There are also criteria such as YARA rules available from CTI sources to identify and verify an incident.

3.4. Containment & Eradication. Incident containment can reduce the resources used and the damage caused. The majority of incidents require containment. Organisations should implement containment techniques to provide additional time to develop a tailored remediation strategy. For example, Sandboxing is a containment technique that allows the organisation to monitor the activity and gather more evidence. The decision-making process is a crucial part of containment for example whether to shut down a system, disconnect it from a network and disable functions. Pre-determined strategies and procedures make containing the incident easier. Within these strategies, the organisation should define acceptable risks. The criteria should be documented clearly to facilitate containment decision-making. Criteria for determining the appropriate strategy include potential damage to and theft of resources; the need for evidence preservation; service availability (e.g. network connectivity, services provided to external parties); time and resources needed to implement the strategy; effectiveness of the strategy (e.g. partial or full containment); and duration of solution (e.g. incident related components to be removed urgently, within 5 hours (temporary) or permanent solution).

Information about the attacking host and the incident-related components could be from the CTI. Once the attacker’s IP address and the incident have been identified, a CTI search could lead to more information about the attack such as attack vectors and threat actors of similar attacks. The use of CTI sources, for example, the national vulnerability databases (NVD) is key to identifying the attacker host. CTI communities have collected and consolidated related incidents from numerous organizations into a database. This shared information can be presented in several ways, such as real-time blacklists and trackers.

Eradication deletes the incident-related components and disables all user accounts that were infected, as well as mitigates all the identified vulnerabilities that were exploited. During the eradication process, identifying all the victim hosts within the organisation is important so they can be remedied. Eradication can also be performed during the recovery stage. Organisations can check the CTI sources for possible eradication solutions.

3.5. Recovery. Within recovery, the administrator will restore systems back to their normal state and confirm that the systems are functioning normally; and if applicable, remediate vulnerabilities to prevent similar incidents. The recovering process may involve the use of clean versions disks when restoring, rebuilding the system from scratch,

replacing comprised files with clean versions, installing patches, changing passwords, tightening security parameters, high-level logging, and network monitoring. CTI sources can be consulted regarding the backup and recovery of data in different categories.

3.6. Post-Incident Activity. The post-incident activity aims to improve technology and learn lessons. After major incidents have occurred, organizations should hold a “lessons learned” meeting with all parties involved. The meeting will help the organization when improving its security measures as well as the incident response handling itself. The question that could be answered in the meeting includes, exactly what happened; how well did staff and management perform in dealing with the incident; were the documents procedures followed, were they adequate? what would the staff and management do differently next time if a similar incident occurs; what corrective actions can prevent similar incidents in the future; what indicators or precursors should be watched for in the future to detect similar incidents; what additional tools or resources are needed to detect, analyze, and mitigate future incidents?

CTI advisories from US/UK CERT provide recommendations (e.g. in the form of a business continuity plan) on what can be improved in order to prevent a similar incidents in the future. Such information is also available in the CTI course of action attributes in the format of CTI feeds shared by different CTI platforms.

4. Case Study

This section uses the NHS WannaCry Ransomware case study to demonstrate the use of the proactive IR procedure proposed in Section 3. In the study, we collate cyber security best practices and advisories to protect interconnected systems and devices from Ransomware. CTI can be used in numerous ways to help an organisation defend against the incidents [41]. However, there is limited research in applying CTI to counteract Ransomware. This section maps the relevant CTI information about Ransomware to our proposed IR procedure by following the NIST IR methodology [12,13]. The information provided in this case study covers the basics of Ransomware as well as cyber security best practices and general prevention techniques. We followed our proposed proactive IR procedure to examine how NHS has reacted to the WannaCry Ransomware attack and identify the opportunities where can be improved using the proactive procedure. This is achieved through mapping the proposed proactive IR procedure to the NHS WannaCry Ransomware Investigations Report [42] and Ransomware CTI advisories [35-37]. Fig. 2 presents the NHS WannaCry Ransomware attack IR procedure, including the actions evidenced by NHS, the missed actions, and the added proactive actions from CTI advisories. TABLE 2 elaborates the proactive actions in Figure 2. As we can see, the NHS has not fully addressed all actions in a traditional IR life cycle. The key missing items are, a clear security plan in the planning & preparation stage, the indicators, and precursors

in the detection stage, the lack of central directions on the mitigation strategy in the containment & eradication stage. NHS seems to have done well in the recovery and post-incident activity stages. NHS could have benefited from additional CTI sources to enable a proactive IR. The reports warning ransomware risks can improve NHS’s awareness in the planning & preparation stage, the indicators and precursors identified from CTI can be fed into their detection stage. By checking the impact score of ransomware incidents and the YARA rules from CTI sources can help identify and verify the incident, the CTI advisories (i.e. MS17-010 SMB) provide solutions for containment & eradication and recovery. CTI advisories on business continuity plans can have improved the IR capacity as part of the post-incident activity.

5. Discussion

The healthcare information system (HIS) has become a victim of the cyber attacks, such as the UK NHS WannaCry Ransomware attack. Cyber-attacks have been categorised as a Tier One Priority Risk in the UK National Security Strategy [19]. The UK government has established the National Cyber Security Centre (NCSC) to proactively mitigate cyber security risks. These initiatives recognise the importance of tracking and forecasting upcoming changes in the cyber landscape in order to proactively respond to potential cyber threats. This requires the organisation to be well aware of the threat landscape while responding to the emerging threats [24, 43, 44].

CTI can be used in numerous ways to help an organisation defend against the incidents, however, there is limited research found applying CTI into IR especially in healthcare. Our proposed proactive IR procedure contributes to the national strategy on cyber security through the research of proactive incident response informed by CTI. Proactive incident response can enhance the organisations’ capability in defending against attacks. Being aware of the threat landscape can reduce the uncertainty in making security decisions in IR processes [21].

Within the traditional IR, the preparation phase involves the creation and training of an incident response team, acquisition of the necessary tools and resources, the implementation of a set of controls on their assets based on the risk assessment. The detection and analysis stage collects and correlates the precursors, indicators, and log files to determine an incident and define the scope. The containment eradication and recovery phase include the incident response team attempting to mitigate the incident by containing it through defined strategies; eradicating by deleting the incident-related components from systems, networks, and applications then ideally recovering from it. The final post-incident activity includes a report issued by the organisation, detailing the cause of the incident as well as costs and steps that should be taken to prevent incidents in the future.

Throughout this phase, there tends to be a cycle of activities back to the detection and analyses, see figure 5.1. For example, to see if additional hosts are infected by malware



FIGURE 2: Ransomware (WannaCry) Proactive IR informed by CTI

while eradicating the incident (5). Once the incidence is handled adequately,

There have been extensive CTI sources into the IR life cycle including preparation, detection, analysis, containment, eradication, and recovery of incidents. It will be important for an organisation to map their IR to CTI in order to get better coverage and ultimately provide a more robust security system. Teams within the organisation have the job of creating or implementing a vulnerability-free

system to protect their assets. There are numerous CTI sources that provide incidents information regarding assets, the exploited vulnerability (e.g. NVD [45]), and emerging threats (e.g. through US/UK CERT advisories, CTI sharing platforms) and security recommendations (e.g. security incident reports). Organisations should take advantage of this information to strengthen their IR capacity [46].

Our proposed proactive IR methodology addresses this challenge by embedding CTI into each stage of the

TABLE 2: Cyber Threat Intelligence (CTI) advisories for Ransomware (WannaCry) Incident Response (IR)

WannaCry IR stages	CTI advisories
Planning and preparation	NHS has taken inadequate actions against the alerts published in July 2016 warning that cyberattacks could jeopardise access to critical patient record systems. NHS will benefit from ransomware CTI advisories [35–37] on how to prevent such incidents; example solutions include rehearsing the IR plan before implementing it straight away.
Detection	The WannaCry incident report does not indicate whether NHS has used a monitoring system to identify the indicators. NHS can use the ransomware CTI advisories [35] to identify and feed indicators into the monitoring system through signature updates. Indicators include but are not limited to mssecsvc.exe, diskpart.exe, lhdfgui.exe, ransomware07_no_detection.exe, and WCry_WannaCry_ransomware.exe.
Analysis and assessment	NHS confirmed the WannaCry incident and identified the scope and impact. NHS can still benefit from CTI advisories [35–37] for the verification. The CTI advisories show that the impact can be “temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organisation’s reputation” [35].
Containment and eradication	NHS lacked central direction and formalised process to respond to WannaCry incident. They failed to shut down/isolate the systems in time. Example solutions from CTI advisories are to apply MS17-010 SMB vulnerability dated March 14, 2017; enable spam filters to prevent phishing emails; and manage the use of privileged accounts.
Recovery	NHS worked with the IT suppliers to recover the system. CTI advisories [35–37] also provide a list of solutions to consider, e.g., backing up sensitive and important data regularly and testing the backups to ensure they work correctly upon use.
Lessons learned	NHS learned the lessons from this incident; they conducted causal analysis and took actions to improve the security controls and policies. CTI advisories [35–37] also provide some solutions like implementing a business continuity plan.

traditional IR processes. It fills in the gap of CTI utilization in order to strengthen the IR capacity. The practitioners can benefit from informed IR decision-making using the CTI. This research also uses a case study to demonstrate the feasibility of the proactive IR methodology. The disadvantages are the lack of practical application in real practices and the lack of detailed explanation for each item in different IR stages. For example, cost estimation is embedded in the risk assessment item in the preparation stage but not displayed in the high-level proactive IR processes.

6. Challenges and Future Directions

The incident response includes the proper deployment of strategies, policies, and hardware and software security solutions in the organization [47]. The process of deciding which countermeasures and security policies will be applied against cyberattacks using CTI should take into account also the cost-perspective of the company. Even by applying a standard password policy that forces complex passwords, the company would increase the security budget due to extra costs induced from password creation and storage [48]. As stated in [49], correct modeling of the behavior of attackers and general users and proper calculation of the cost associated with the behavior of each entity could result in cost-efficient security policies.

Incident response of an organization could become more efficient by taking into account supply chain management, emerging technologies, privacy preservation techniques and even business analytics. The authors in [50] investigated the perspective of exploiting information analysis using BA inside Incident response plans in order to address the dynamic and uncertain cybersecurity threat environment. This

initial analysis could lead to the incorporation of BA into IR. Moreover, supply chain cybersecurity analysis can be used in order to calculate attack propagation and cascading effects [51]. This analysis can further improve IR and future work on this area is very promising especially if emerging technologies like blockchain or 5G are also taken into account [52–54]. Finally, secure arrangements for IoT healthcare privacy-preserving data collection must be taken into account when selecting the proper security solutions [55].

Regarding our proposed proactive IR procedure, our future work will focus on applying it in real practice in healthcare organisations. We will also consider integrating the proactive IR procedure with existing IR products used in Healthcare such as Security Information and Event Management (SIEM), Intrusion Detection Systems, Orchestration Automation and Response (SOAR) [18], and Security Operations Centre (SOC) in healthcare. This involves a careful mapping of CTI to each different component of the existing IR products. Future work will also consider expanding the current proactive IR processes by elaborating the items listed in each IR stage.

7. Conclusions

CTI contains knowledge of impending attacks, such as threat vectors, threat actors, victims profiles, courses of action, etc. and is shared via different CTI platforms such as UK/US Cert, Microsoft, MISP, and MITRE, with the intention to create a proactive line of cyber defense and should be ideally used to inform incident response, however, there is limited research in applying CTI into IR especially in healthcare. This paper addresses this gap by proposing a proactive IR procedure that is embedded with CTI. We examined

different stages of the IR procedure and identified the points where CTI can be fed into the IR processes. This paper then presented the NHS WannaCry Ransomware case study to demonstrate the use of the proposed proactive IR procedure. This research has significance for the IR practices within healthcare organizations. The practitioners can use the proposed proactive IR procedure to counteract Ransomware and other security-related adverse events in a systematic manner. Healthcare organizations can benefit from an informed proactive IR using CTI.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, "Unveil: a large-scale, automated approach to detecting ransomware," in *Proceedings of the 25th USENIX Security Symposium USENIX Security 16*, pp. 757–772, Austin, TX., August 10–12, 2016.
- [2] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. K. R. Maddikunta, and S. Singh, "A review on cyber crimes on the internet of things," arXiv:2009.05708, 2020.
- [3] F. Donovan, "Healthcare industry takes brunt of ransomware attacks," [Online]. Available: <https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks>, 2019.
- [4] J. G. Ronquillo, J. Erik Winterholler, K. Cwikla, R. Szymanski, and C. Levy, "Health it, hacking, and cybersecurity: national trends in data breaches of protected health information," *JAMIA Open*, vol. 1, no. 1, pp. 15–19, 2018.
- [5] M. Field, *Wannacry cyber attack cost the nhs£ 92m as 19,000 appointments cancelled*, The Telegraph, 2018.
- [6] C. Luo, H. Soygazi, H. Janicke, and Y. He, "Security defense strategy for intelligent medical diagnosis systems (IMDS)," in *Proceedings of the 41th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 23–27 July 2019.
- [7] Y. He and C. Johnson, "Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization," *Informatics for Health and Social Care*, vol. 42, no. 4, pp. 393–408, 2017.
- [8] Y. He and C. Johnson, "Improving the redistribution of the security lessons in healthcare: an evaluation of the generic security template," *International Journal of Medical Informatics*, vol. 84, no. 11, pp. 941–949, 2015.
- [9] M. Evans, Y. He, L. Maglaras, I. Yevseyeva, and H. Janicke, "Evaluating information security core human error causes (is-heck) technique in public sector and comparison with the private sector," *International Journal of Medical Informatics*, vol. 127, pp. 109–119, 2019.
- [10] M. Evans, Y. He, C. Luo et al., "Real-time information security incident management: a case study using the is-heck technique," *IEEE Access*, vol. 7, pp. 142147–142175, 2019.
- [11] M. Evans, Y. He, C. Luo, I. Yevseyeva, H. Janicke, and L. A. Maglaras, "Employee perspective on information security related human error in healthcare: proactive use of is-heck in questionnaire form," *IEEE Access*, vol. 7, pp. 102087–102101, 2019.
- [12] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, *Computer security incident handling guide*, NIST Special Publication, vol. 800, no. 61, pp. 1–147, 2012.
- [13] M. Souppaya and K. Scarfone, *Guide to malware incident prevention and handling for desktops and laptops*, NIST Special Publication, vol. 800, p. 83, 2013.
- [14] A. Ahmad, S. B. Maynard, and G. Shanks, "A case analysis of information systems and security incident responses," *International Journal of Information Management*, vol. 35, no. 6, pp. 717–723, 2015.
- [15] S. Dekker, *The field guide to understanding 'human error'*, CRC Press, 2017.
- [16] S. L. Pfleeger and R. K. Cunningham, "Why measuring security is hard," *IEEE Security & Privacy Magazine*, vol. 8, no. 4, pp. 46–54, 2010.
- [17] Y. T. Chua, S. Parkin, M. Edwards et al., "Identifying unintended harms of cybersecurity countermeasures," in *Proceedings of the 2019 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–15, IEEE, Pittsburgh, PA, USA, 13–15 Nov. 2019.
- [18] C. Islam, M. A. Babar, and S. Nepal, "A multi-vocal review of security orchestration," *ACM Computing Surveys*, vol. 52, no. 2, p. 37, 2019.
- [19] P. Hammond, *National Cyber Security Strategy 2016 to 2021*, Her Majesty's Government, London, 2016.
- [20] S. Barnum, *Standardizing cyber threat intelligence information with the structured threat information expression (stix)*, Mitre Corporation, vol. 11, pp. 1–22, 2012.
- [21] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, pp. 212–233, 2018.
- [22] Y. Ying He, L. A. Maglaras, H. Janicke, and K. Jones, "An industrial control systems incident response decision framework," in *Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 761–762, IEEE, Florence, Italy, 28–30 Sept. 2015.
- [23] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, pp. 51–60, ACM.
- [24] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaar, and B.-T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Computers & Security*, vol. 67, pp. 35–58, 2017.
- [25] S. E. Dog, A. Tweed, L. Rouse et al., "Strategic cyber threat intelligence sharing: a case study of ids logs," in *Proceedings of the 2016 25th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–6, IEEE, Waikoloa, HI, USA, 1–4 Aug. 2016.
- [26] V. G. Li, M. Dunn, P. Pearce, D. McCoy, G. M. Voelker, and S. Savage, "Reading the tea leaves: a comparative analysis of threat intelligence," in *Proceedings of the 28th Security Symposium (Security 19)*, pp. 851–867.
- [27] F. Maymí, R. Bixler, R. Jones, and S. Lathrop, "Towards a definition of cyberspace tactics, techniques and procedures," in *Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*, pp. 4674–4679, IEEE, Boston, MA, USA, 11–14 Dec. 2017.
- [28] J. Moreno, M. A. Serrano, E. B. Fernandez, and E. Fernández-Medina, "Improving incident response in big data ecosystems by using blockchain technologies," *Applied Sciences*, vol. 10, no. 2, p. 724, 2020.

- [29] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016.
- [30] G. Grispos, W. B. Glisson, and T. Storer, "Enhancing security incident response follow-up efforts with lightweight agile retrospectives," *Digital Investigation*, vol. 22, pp. 62–73, 2017.
- [31] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Network Security*, vol. 2016, no. 9, pp. 5–9, 2016.
- [32] N. A. Hassan, *Ransomware families Ransomware Revealed*, pp. 47–68, Springer, 2019.
- [33] N. Kyurkchiev, A. Iliev, A. Rahnev, and T. Terzieva, "A new analysis of cryptolocker ransomware and welchia worm propagation behavior. some applications. iii," *Communications in Applied Analysis*, vol. 23, no. 2, pp. 359–382, 2019.
- [34] R. Brewer, "Cyber threats: reducing the time to detection and response," *Network Security*, vol. 2015, no. 5, pp. 5–8, 2015.
- [35] U. S. CERT, "Indicators associated with WannaCry ransomware," [Online]. Available: <https://www.us-cert.gov/ncas/alerts/TA17-132A>, 2017.
- [36] Stop Ransomware, "Ransomware," [Online]. Available: <https://www.us-cert.gov/security-publications/Ransomware>, 2019.
- [37] Petya Ransomware, "Alert (TA17-181A). Petya ransomware," [Online]. Available: <https://www.us-cert.gov/ncas/alerts/TA17-181A>, 2017.
- [38] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020.
- [39] A. Ahmim, M. A. Ferrag, L. Maglaras, M. Derdour, and H. Janicke, "A detailed analysis of using supervised machine learning for intrusion detection," in *Strategic Innovative Marketing and Tourism*, pp. 629–639, Springer, 2020.
- [40] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP: the design and implementation of a Collaborative threat intelligence sharing platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 49–56.
- [41] M. Conti, T. Dargahi, and A. Dehghantanha, *Cyber threat intelligence: challenges and opportunities*, Springer, 2018.
- [42] D. of Health, *Investigation: WannaCry cyber attack and the NHS*, [Online]. Available: <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>, 2018.
- [43] S. Samtani, K. Chinn, C. Larson, and H. Chen, "Azsecure hacker assets portal: cyber threat intelligence and malware analysis," in *Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, pp. 19–24, IEEE, Tucson, AZ, USA, 28–30 Sept. 2016.
- [44] S. Samtani, R. Chinn, H. Chen, and J. F. Nunamaker Jr, "Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence," *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1023–1053, 2017.
- [45] M. A. Williams, S. Dey, R. C. Barranco, S. M. Naim, M. S. Hossain, and M. Akbar, "Analyzing evolving trends of vulnerabilities in national vulnerability database," in *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data)*, pp. 3011–3020, IEEE, Seattle, WA, USA, 10–13 Dec. 2018.
- [46] B. Ndiabanje, K. Kim, Y. Kang, H. Kim, T. Kim, and H. Lee, "Cross-method-based analysis and classification of malicious behavior by api calls extraction," *Applied Sciences*, vol. 9, no. 2, p. 239, 2019.
- [47] L. Maglaras, M. A. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis, "Threats, protection and attribution of cyber attacks on critical infrastructures," *arXiv:1901.03899*, 2019.
- [48] L. Maglaras, H. Janicke, and M. A. Ferrag, "The cost perspective of password security," in *Handbook of Research on Multimedia Cyber Security*, pp. 319–330, IGI Global, 2020.
- [49] S. Gong and C. Lee, "Cyber threat intelligence framework for incident response in an energy cloud platform," *Electronics*, vol. 10, no. 3, p. 239, 2021.
- [50] H. Naseer, S. B. Maynard, and K. C. Desouza, "Demystifying analytical information processing capability: the case of cybersecurity incident response," *Decision Support Systems*, vol. 143, p. 113476, 2021.
- [51] A. Yeboah-Ofori and S. Islam, "Cyber security threat modeling for supply chain organizational environments," *Future Internet*, vol. 11, no. 3, p. 63, 2019.
- [52] L. Maglaras and I. Kantzavelou, *Cybersecurity Issues in Emerging Technologies*, CRC Press, 2021.
- [53] W. Wang, C. Qiu, Z. Yin et al., "Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, p. 1, 2021.
- [54] H. Xiong, C. Jin, M. Alazab et al., "On the design of blockchain-based ecdsa with fault-tolerant batch verification protocol for blockchain-enabled iomt," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2021.
- [55] J. Song, Z. Han, W. Wang, J. Chen, and Y. Liu, "A new secure arrangement for privacy-preserving data collection," *Computer Standards & Interfaces*, vol. 80, p. 103582, 2022.