Title Page (with Author Details)

Agile Incident Response (AIR): Improving the Incident Response Process in Healthcare

Ying He, School of Computer Science, The University of Nottingham, Nottingham NG8 1BB, United Kingdom, ying.he@nottingham.ac.uk

Efpraxia D. Zamani, Information School, The University of Sheffield, Sheffield S1 4DP, United Kingdom, e.zamani@sheffield.ac.uk

Stefan Lloyd, School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, United Kingdom, stefanlloyd7581@gmail.com

Cunjin Luo, School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, United Kingdom; Key Lab of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou 646000, Sichuan Province, China, cunjin.luo@essex.ac.uk (corresponding author)

Abstract

Recent industrial reports show an increased number of cybersecurity incidents, which inflict significant financial losses. Although organisations have been increasing their investments towards information security, incidents continue to occur. Most organisations adopt traditional linear incident response (IR) frameworks to prevent, detect, contain, eradicate and learn lessons from information security incidents. However, due to their rigidness, such linear frameworks are often ineffective. In this study, inspired by the Agile Manifesto, we propose the Agile IR Framework to refine, adjust, and improve the current linear IR process. We use the IR framework of UK's National Health Service (NHS) as an illustrative case, critically analysing the current linear IR framework and demonstrating how it can be transformed into a hybrid IR framework. Using an illustrative case study from the healthcare domain, this study contributes to the incident response literature by showcasing how the integration of Agile principles in archetypical linear IR processes can improve incident response.

Key words: Security Incident, Incident Response, Agile methodologies, Healthcare, Information Security

Agile Incident Response (AIR): Improving the Incident Response Process in Healthcare

Abstract

Recent industrial reports show an increased number of cybersecurity incidents, which inflict significant financial losses. Although organisations have been increasing their investments towards information security, incidents continue to occur. Most organisations adopt traditional linear incident response (IR) frameworks to prevent, detect, contain, eradicate and learn lessons from information security incidents. However, due to their rigidness, such linear frameworks are often ineffective. In this study, inspired by the Agile Manifesto, we propose the Agile IR Framework to refine, adjust, and improve the current linear IR process. We use the IR framework of UK's National Health Service (NHS) as an illustrative case, critically analysing the current linear IR framework and demonstrating how it can be transformed into a hybrid IR framework. Using an illustrative case study from the healthcare domain, this study contributes to the incident response literature by showcasing how the integration of Agile principles in archetypical linear IR processes can improve incident response.

Keywords: Security Incident, Incident Response, Agile methodologies, Healthcare, Information Security

1. Introduction

The 2018 United Kingdom (UK) Breach report shows that networked systems are increasingly susceptible to cyber criminals, who breach organisations and inflict significant financial losses (Department for Digital, Culture, Media and Sport, 2018). Across sectors, attacks of the healthcare sector account for 18% of incidents with an upward trend on a yearly basis (Symantec, 2018). Successful breaches have various negative impacts. Some, such as ransomware attacks will cause a massive business disruption (O'Dowd, 2017). There is almost a guaranteed reduction in productivity and business process failures, which results in revenue losses (Connolly & Wall, 2019). Organisations that permit the use of personal devices for organisational purposes (e.g., Bring-Your-Own-Device schemes) (Baillette et al., 2018) and those that use cloud-based services record the most security breaches (Roumani & Nwankpa, 2019). Depending on the nature of organisational data, the impact can be even greater. Therefore, in order to combat attacks and information system breaches, businesses and organisations have been increasing their investments in protecting their cyber space (The UK Breach Report, 2018; Department for Digital, Culture, Media and Sport, 2018).

Much of the expenditures on cyber security is allocated to Incident Response (IR) teams (Steinke et al., 2015), who are responsible for reducing the impact of breaches and helping the business resume operations as soon as possible (Wiik et al., 2005). To date, there is extensive research on improving IR processes (e.g., Bartnes et al., 2016; Evans, He, Maglaras, et al., 2019; Grispos et al., 2017; He & Janicke, 2015; He & Johnson, 2015; Menges & Pernul, 2018; Skopik et al., 2016; Tøndel et al., 2014). Most IR processes and frameworks are linear in nature, where the completion of one aspect of the response must be completed before moving onto the next (Grispos et al., 2014), such as the ones proposed by The National Institute of Standards and Technology (NIST) (Cichonski et al., 2012), CREST (Creasy, 2013), The International Organization for Standardization (ISO) (British Standards Institution, 2016) and Mitropoulos et al. (2006). Typical IR frameworks contain five phases: preparation; detection and analysis; containment; eradication and recovery (which can constitute separate phases); and post incident review (or follow up). However, linear IR approaches are usually time-consuming, ineffective in responding to large scale attacks, over-complex when handling sophisticated incidents, and lack learning opportunities (Grispos et al., 2014; He & Janicke, 2015). As a result, and as incidents become more and more sophisticated, linear models become less and less efficient and don't offer the appropriate level of responsiveness (Werlinger et al., 2010).

In this study, we address the above-mentioned challenges and explore how a linear IR framework can shift to a more agile one. We propose the Agile Incident Response (IR) Framework, inspired by the Agile Manifesto (Beck et al., 2001) and we incorporate agile principles into IR processes to break them down into smaller, more manageable parts, focused around specific tasks, which can be prioritised and continuously delivered over shorter iterations. The Agile philosophy is widely and successfully applied in Software Engineering (e.g., Colomo-Palacios et al., 2018; Gupta et al., 2019; Tam et al., 2020), and have been shown to reduce large project failures, by providing constant monitoring and continuous improvement throughout the project (Laanti et al., 2011). Most importantly, it incorporates quick feedback and continuous adaptation (Serrador & Pinto, 2015), both of which can support IR teams to respond to incidents whilst minimising information loss and service disruption. Equally, compared to linear methodologies, agile approaches emphasise learning and feedback (Grispos et al., 2017), which are essential for counteracting future incidents.

Using the UK's National Health Service (NHS) as an illustrative case, we explore how a linear IR model in a large organisation may be changed to a hybrid IR framework through targeted adaptations of the linear model's major components. In doing so, we assess the NHS' current IR Framework and identify which components can be adapted and how. We then evaluate the Agile IR Framework and propose a hybrid IR approach, whereby the linear IR process is augmented using Agile-inspired components. Our findings show that, among the main shortcomings of the NHS' current IR Framework are that it lacks a clear process for collecting forensically sound evidence and it does not require the involvement of asset owners during Incident Analysis. Our study contributes to the IR literature from the following perspectives. First, it extends previous studies by following a systematic approach for the integration of the Agile principles within linear IR processes. While previous studies (e.g., Anderson, 2017; Grispos et al., 2014, 2017) have proposed similar concepts, there is lack of holistic research to formally build Agile principles into IR processes. Second, the majority of research on the use of Agile for IR focuses primarily on Industrial Control Systems (ICS) (e.g., He & Janicke, 2015; Smith et al., 2021). However, ICS comprise of information systems and physical components. Therefore, research focus is placed primarily on the latter to mitigate against disasters and loss of life (Kondo et al., 2018), while security solutions are typically designed for a specific industrial control environment or a particular security issue (Asghar et al., 2019). Our study extends such previous work by focusing on the entire IR process. While our case study is drawn from the healthcare sector, our contributions extend to other information-sensitive large organisations.

Our study has important practical implications. We offer insights and tangible recommendations for improving the IR process. Namely, we argue for the integration of Agile Principles within linear IR processes, against the backdrop of a collaborative effort throughout the process. Coupled with lightweight retrospectives and the participation of forensic specialists, hybrid approaches can support organisations to return to a business-as-usual state sooner, whereby the incremental approach for resolving information security breaches instils flexibility and responsiveness, and technical excellence supports the collection of valuable evidence and the deterrence of future incidents.

The remainder of this paper is structured as follows. Section 2 presents related work on IR approaches and background information on the Agile principles. In Section 3 we present our Agile Incident Response (IR) Framework. In Section 4, we evaluate the NHS' IR Framework against the Agile IR Framework. In Section 6 we discuss the theoretical and practical implications of our work and we conclude our paper by recommending avenues for future research.

2. Theoretical Foundation

2.1. The Incident Response Lifecycle and Current Challenges

Incident Response (IR) models are widely used across various industries. Typical IR frameworks are those proposed by NIST (Cichonski et al., 2012), CREST (Creasy, 2013), ISO (British Standards Institution, 2016) and Mitropoulos et al. (2006), where each of these contains the following phases: preparation; detection and analysis; containment; eradication and recovery (which can constitute

separate phases); and post incident review (or follow up). As such, while there are different IR models, which exhibit some minor differences, the archetypical IR Framework (Figure 1) entails that IR starts with the preparation phase, where the organisation considers the potential types, the impact, and the likelihood of breaches for their assets, and develops the relevant policies for each of these breaches (Blum, 2020). During detection and analysis, the organisation will assess the incident, and whether it constitutes an actual threat. If it does, and depending on the severity, the IR team will trigger the appropriate response policy (Lamis, 2010), which leads to the containment phase. During containment, the objective is to stop the attack from impacting any additional organisational resources and creating further damage. This often means that the organisation will need to make some decisions, e.g., what are the acceptable risks, and for this purpose, it is expected that the organisation will have predefined strategies (developed during the preparation phase) for decision-making for the containment of incidents (Akkuzu et al., 2018). After successful containment, the organisation should be able to eradicate the breach and recover to a 'business as usual' (BAU) state (Thompson, 2018). Finally, there should be a follow-up phase for a post-incident review, in order to reflect on the breach and the outcomes of the incident response, which helps the organisation learn, update its IR policies and future-proof its assets (Mitropoulos et al., 2006).

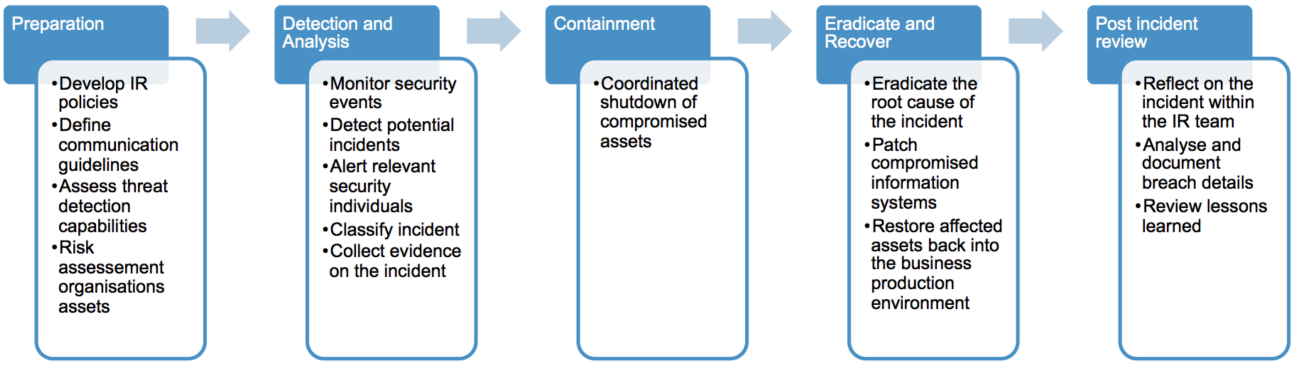

Figure 1. The Archetypical Incident Response Framework

Existing research has heavily criticised these approaches, specifically for being too linear, as they do not reflect the concurrent lifecycle of real world incident handling (Ahmad et al., 2012; Grimes, 2007; Werlinger et al., 2010), which further prohibits capturing insights into the root causes of incidents (Casey & Nikkel, 2020; Shedden et al., 2011). There are several limitations of the linear IR processes. First, *linear processes are time consuming*. Existing evidence suggests that the structured approach makes the process too rigid to be effective (Information Security Media Group, 2013). In other words, linear processes exhibit a "progression flaw" (Grispos et al., 2014, p. 3), where if one phase cannot be completed – or takes too long, then the entire cycle of the process may halt while the incident is still occurring. This allows the attack to cause further damage. Attackers often use automated tools to extend and scale up their attacks (Wiik et al., 2005), while the unavailability of information systems across the organisation may result in significant reputational damage, information, data and financial losses (Khan et al., 2021). As such, short response times are crucial during incidents to stop the attack. *Second, linear processes are ineffective in responding to large scale attacks and can become over-complex when handling sophisticated incidents*. Such attacks and incidents are often unpredictable, both in their occurrence and in the way they unfold. However, linear, plan-driven approach are generally less accommodating to changes (He & Janicke, 2015; He & Johnson, 2015), thus can hardly handle unpredictable situations of large scale attacks and sophisticated incidents. Third, *linear processes lack of learning opportunities* during the IR processes. While the archetypal IR framework entails a post-incident review, where the team is doing a follow up to identify root causes and lessons learnt and work towards updating and improving their future response policies (Mitropoulos et al., 2006), in reality, studies show that organisations often skip incident learning because incident teams are more focused on containment, eradication, and recovery (Ahmad et al., 2012; Grimes, 2007; Tan et al., 2003; Werlinger et al., 2010). Yet, omitting the root cause analysis undermines the organisation's

digital forensic capabilities (Jaatun et al., 2009; Papastergiou et al., 2020), which impedes future incident resolution and demonstrating due diligence (Casey & Nikkel, 2020). As a result, traditional linear IR processes cannot provide the required speed and support for handling and managing contemporary incidents.

2.2. Incident Response Frameworks in Healthcare Settings

Globally, most healthcare organisations have adopted linear IR Frameworks because these tend to offer a structured approach to incident response. For example, in the USA, the NIST framework has been adopted by 57.9% of healthcare organisations, whereas others have adopted the HITRUST, Critical Security Controls, ISO and COMBIT, with 16.9% of them not having adopted any framework (HIMSS, 2018). In the UK, the NHS uses the Information Security Incident – Good Practice Guide (Heathcote, 2017b) for incident management across its organisations. The framework is used by both small and large NHS organisations and outlines the process that needs to be implemented and the key activities that need to be followed across its five phases for handling incidents and minimising the immediate and long-term business impact of incidents on NHS organisations. In Ireland, the Health Service Executive (HSE) has adopted the "Incident Management Framework 2018" (HSE, 2018), which comprises of six phases, including preparation; incident identification and immediate actions; initial reporting and notification; categorisation and initial assessment; review and analysis; and improvement planning and monitoring and all health services at all levels within HSE are required to align their processes for incident response. Finally, in China, the security management of Chinese healthcare organisations complies with the GB/T 22239-2019 (Code of China, 2019). This standard uses a five-level information security classification system and embeds the incident response process in the organisation, focusing however exclusively on the technical aspects and missing follow up activities.

While the above presentation is not exhaustive, it illustrates in general terms the nature of the usual IR frameworks and the processes implemented within healthcare settings. The common denominator across the aforementioned IR frameworks is that they all follow linear IR processes and therefore exhibit the weaknesses earlier discussed in §2.1.

To address these weakness in IR, scholars have proposed building IR frameworks on the basis of Agile principles (Grispos et al., 2014, 2017). In what follows, we first discuss the Agile Principles and we then focus on how these have been implemented for Incident Response.

2.3. The Agile Principles

The Agile principles were first introduced as an alternative to the more structured methodologies, with the aim to accommodate changes and bring products faster to market (L. Williams & Cockburn, 2003). These principles place the emphasis on working collaboratively with customers (internal or external) and prioritising a working product over documentation (Beck et al., 2001). As a result, adopting an Agile methodology entails working iteratively, and breaking down a project into smaller, more manageable pieces of work, which are focused on delivering increments of the product and specific user functionalities, which can be prioritised over shorter iterations, e.g., two weeks (Cram & Marabelli, 2018). In addition, Agile methodologies are open to changing requirements throughout the process (Dingsøyr et al., 2012).

Against this background, the benefits of using Agile methodologies are well documented. Such methodologies improve productivity and response times (Ghobadi & Mathiassen, 2017), resulting in quicker return on investment (Sidky et al., 2007). The close collaboration among teams facilitates quick resource reallocation when needed to achieve each iteration's goals (Baham et al., 2017; Lindstrom & Jeffries, 2004). This optimisation of resources ultimately leads to increased productivity (Hemon-Hildgen et al., 2020). Furthermore, Agile approaches allow the prioritisation of the more critical aspects of a project, which addresses the risk of the project slowing down due to bottlenecks issues (Baham et al., 2017) and waiting times (Lindstrom & Jeffries, 2004), as there are few or no dependencies among the self-managed teams. Coupled with the quicker response times, teams can deliver the features that provide greater business value, better product quality and improve customer satisfaction (Dingsøyr et

al., 2012).

While the benefits of Agile methodologies are plenty, it is not always easy to implement them within larger organisations. Within large organisations, the multiple teams need to enjoy a closed loop communication process and increased trust among them in order to coordinate effectively across interdependent processes, while they have to incorporate feedback mechanisms within their processes to maintain oversight (Bjørnson et al., 2018). Along the same lines, scholars have further highlighted the importance of organisational change and organisational culture when moving from structured to Agile methodologies (Gupta et al., 2019; Tolfo et al., 2011), whereby Tolfo et al. (2011) have argued that large organisations need a cultural shift and clear buy-in from management in order to truly embrace Agile principles. Indeed, without management support, Agile methodologies risk abandonment as employees may lose focus and motivation (e.g., Dennehy & Conboy, 2019).

2.4. Implementing the Agile Principles for Incident Response

First developed for the world of Software Engineering, the Agile principles have been widely adopted across numerous fields, such as Business and Government (Janssen & van der Voort, 2020), as their benefits are transferrable in other areas. Specifically, He et al. (2015) have illustrated how Agile methodologies can be applied within the context of industrial control systems, and Grispos et al. (2014) have discussed the merits of adapting linear incident response processes by incorporating agile principles within existing frameworks.

The implementation of Agile principles can help address the limitations of the linear IR processes. First, as far as the response time is concerned, Agile methodologies are designed specifically for fast responses, which are critical for security incidents. Second, Agile principles are more effective in responding to large scale of attacks and handling sophisticated incidents because the Agile methodology promotes an iterative and incremental approach that can reduce uncertainty. Agile methodologies emphasise individuals and the interactions among them over processes and tools. This can be particularly beneficial during an incident, because people are one of the key factors for the success or failure of security incident investigations (Grispos et al., 2017; He & Janicke, 2015). In addition, the continuous attention to technical excellence can enhance efficiencies and effectiveness (Grispos et al., 2014). Similarly, the emphasis that Agile places on collaboration supports incident response teams towards developing a deep understanding of the organisational processes with the view to prepare for a potential incident, to effectively contain it and help recovery efforts (He & Johnson, 2015). Third, Agile principles create learning opportunities during the IR processes. Goncalves and Linders (2015) draw attention to a core feature of Agile methodologies, that of conducting retrospectives and which is directly applicable to incident response (Grispos et al., 2014, 2017). Retrospectives were initially introduced as a way for incorporating feedback within each iteration and improvements into the development lifecycle (Gupta et al., 2019), and it is a core activity for learning and improving team performance. In their work, Goncalves and Linders (2015) formalise this by providing guidelines on how best to conduct retrospectives, thus increasing the benefits for the organisation and maximising the business value. Applying the lightweight retrospectives in incident response can support incident response teams to enhance feedback and follow-up efforts. Grispos et al. (2017) evaluated this approach with a Fortune 500 Financial organisation's security incident response team, and concluded that the more formal retrospectives were potentially more beneficial compared to lightweight Agile ones. However, in their study, Grispos et al. (2017) focused solely on the follow-up phase of incident response rather than the entire process and therefore it is unclear whether and to what extent an organisation could benefit from the implementation of Agile methodologies across the entire process of incident response.

To date, there have been limited efforts to build the Agile principles into incident responses processes. However, we posit that there are benefits to be reaped by adopting more Agile methodologies for responding to incidents, because such methodologies hold great potential for improving the linear Incident Response success against the growing number of cyber threats. Namely, the weaknesses that linear Incident Response frameworks tend to exhibit, such as poor efficiency, can be improved by

applying the Agile principles.

3. The Agile Incident Response (IR) Framework: Applying the Agile Principles in Incident Response

In this section we conceptually develop the Agile Incident Response (IR) Framework. We use the archetypical IR framework (Figure 1) as the baseline and we augment it with the Agile principles for the purpose of improving existing linear and more structured practices. We do so by drawing from the Agile principles, existing academic and industry literature (e.g. incident response guidelines from NIST (Cichonski et al., 2012), CREST (Creasy, 2013) and the ISO (British Standards Institution, 2016)) on incident response. The proposed framework is further enriched by our consulting experience in the cybersecurity area, as the first author has extensive consulting experience, working collaboratively on cybersecurity with industrial partners from the sectors of aviation, telecom and industrial control systems and has worked in one of the Academic Centres of Excellence in Cybersecurity Research, recognised by the UK's National Cyber Security Centre. This approach allows us to identify both the successes and the failures that have been documented and experienced while implementing Agile principles and methodologies during incident response across various industries. Therefore, our Agile IR Framework encapsulates an informed approach towards the adoption of the Agile values for cybersecurity.

The values that underpin the Agile Manifesto set out the goals of Agile Methodologies and at the same time provide guidance on how to implement the methodology itself (Larson & Chang, 2016). We thus present the conceptual development of the Agile IR Framework by unpacking and elaborating how the Agile principles can inform the archetypical IR framework.

3.1. Responding to Changing Requirements

During an incident, the threat landscape changes rapidly. New threats may be introduced while a complex incident is still unfolding. For example, an advanced persistent threat (APT) can persist within an information system and create back doors, through which new threats (e.g., malwares) can be introduced to the system. This then leads to changed requirements, because the IR team will need to address the original threat as well as the newly introduced malware, and potentially re-prioritise their course of action. To do this, IR teams must react promptly. However, existing linear frameworks recommend IR teams to go through a rigid process of detection and analysis, containment, eradication, recovery and post incident reflection (Figure 1) (British Standards Institution, 2016; Chichonski et al., 2012; Creasy, 2013). This requires that a phase is completed before the IR team can move onto the next phase. This can be problematic when there are new developments during complex incidents, such as additional compromised assets being identified during the eradication phase. The whole process will have to take a backwards step and be restarted from the detection phase, while the new asset is being brought up to the same stage of the process.

To address this, and inspired by the Agile principle of responding to changing requirements (Beck et al., 2001), Grispos et al. (2014) propose the incorporation of iterations, which allow addressing an incident in increments. These iterations further allow IR teams to react quickly to the changes occurring due to the breach and move away from the linear processes, which hackers can easily predict (He & Janicke, 2015).

This principle is represented in our framework via the addition of the cyclical arrows that allow moving backwards to previous phases (Figure 2). Tracing these arrows, and on the basis of the added components within the phases of the Detection and Analysis, Containment, and Eradicate and Recover, IR teams can investigate any compromised assets if and when these are identified without having to trigger the entire process from the beginning or halting operations elsewhere. The team can then iteratively evaluate and reprioritise those assets, based on which actions can be estimated and assigned (i.e., the time required for asset resolution). As such, changing requirements is embraced throughout the process through the addition and reprioritisation of assets at any point during the incident lifecycle: during the Detection and Analysis phase, the IR team may prioritise assets; during

the Containment phase, actions can be estimated and assigned to team members; during the phase of Eradication and Recovery, the IR team will eradicate the root causes of the incident, iteratively.

3.2. Early and Continuous Delivery

The implementation of iterations within an incremental approach can result in the earlier recovery of subsystems and individual assets, which in turn results in satisfying stakeholders (i.e., employees and external customers) through early and continuous delivery (Beck et al., 2001).

According to linear IR processes, while newly compromised assets are being analysed, contained and restored, previously detected compromised assets need to be kept contained, and therefore offline. This is time consuming and is considered inefficient. However, within the context of an iterative and incremental process, IR teams can iteratively re-evaluate and reprioritise assets and return those that no longer pose a threat to the production environment. In more detail, tracing the arrows in Figure 2, the IR process continues prioritising assets during the Detection and Analysis phase ('prioritise assets'), which allows the IR team during the Containment phase to identify the assets required for the investigation ('estimate and assign action'), reinstate non-critical assets and return the assets to stakeholders for use in day-to-day business processes in the Eradicate and Recover Phase ('restore the affected assets as and when they become available'), thereby reducing incrementally the overall impact of the breach.

Having said that, over-responding to changes can have a negative impact on success rates and costs (Boehm, 2002). Continuous changes in focus may negatively impact efficiency and overall quality and IR teams must make sure they are responding to significant changes rather than minor ones (Ahmad et al., 2012), which could potentially threaten the overall success of the incident recovery and returning to BAU.

3.3. Technical and Non-Technical Professionals Must Work Together

A key part of Agile is customer satisfaction through valuable product, which is achieved in part through the close collaboration of stakeholders with the development team (Beck et al., 2001). We thus propose that the IR team must be able to communicate and collaborate effectively with necessary stakeholders from across the organisation in order to successfully respond to changes, add value to the process, and ultimately satisfy their needs (He & Janicke, 2015).

Stakeholders are considered, including all those individuals who are involved in the incident: the asset owners who are subject experts for their systems and assets, the IT department that provides technical knowledge for mitigation, forensic specialists who are responsible for the collection of forensically sound evidence, and the legal team who will pursue legal action against the attackers if and when identified. The IR teams will need to tap into this collective knowledge in order to deal with the incident and recover the compromised assets. Therefore, they will need to work closely with the aforementioned stakeholders. Such collaboration reduces uncertainty because all stakeholders share a similar understanding regarding the circumstances of incidents. Most crucially, the IR team will need to work even more closely with those who are asset owners for prioritising assets and achieve faster incremental recovery.. For example, these stakeholders will be responsible for evaluating asset recovery based on their own expert knowledge (Grispos et al., 2014). In other words, asset owners will need to be actively involved and be considered as customers of an information system, participating in user acceptance testing.

On the same note, Agile methodologies place the emphasis on the interactions among individuals rather than on the tools and the processes they may use (Beck et al., 2001), because it is through these interactions that information can be best communicated (Larson & Chang, 2016). The same holds true for the IR process, which relies on the individuals involved and the ways they interact. Indeed, Ahmad et al. (2012) have highlighted how IR teams tend to experience lack of communication between the different security functions, which in turn contributes to incidents due to inconsistent and untimely responses. In addition, collaboration among stakeholders has become increasingly important for incident response because the detection of an incident may very well rely on their tacit knowledge,

rather than merely the expertise of the IR team (Werlinger et al., 2010). In other words, working in siloes does not allow for efficient recovery from incidents as it means knowledge and expertise are not pooled together to address the problem from the different perspectives of all involved.
This further highlights the need for collaboration among all relevant personnel in order to effectively and efficiently respond to security incidents, making incident response a prime candidate for the adoption of the collaborative aspects of Agile methodologies. To address the aforementioned issues, we include in the Detection and Analysis and the Post Incident Activities phases the components of 'Identify all Stakeholders and IR team members' and 'Perform retrospectives including all stakeholders involved', respectively, as shown in Figure 2.

3.4. Creating Learning Opportunities (Post Incident Learning)

Linear IR frameworks include post incident reviews, which aim at drawing lessons learned and improving the overall response process for the future. However, it has been questioned as to whether organisations place adequate importance in this phase: reviews tend to take place only for very high impact incidents, they are usually lengthy and often there is no feedback mechanism attached to them, i.e., lessons learned are not implemented (Ahmad et al., 2012).
Practically speaking, during post incident reviews, stakeholders, or their representatives, need to be involved in post incident review sessions and work together with the security team. This would help with extracting valuable knowledge from across the affected areas of the organisation, and with transferring lessons learned across relevant teams and departments. Naturally, the post-incident review actions need to be implemented and policies and processes need to improved and aligned on the basis of the lessons learned, to avoid future incidents and/or minimise their impact (He & Janicke, 2015; He & Johnson, 2015).
Borrowing concepts from Agile methodologies, the above are more easily achieved through retrospectives. Becoming more effective through reflection is a core activity in Agile methodologies, and typically carried out through retrospectives at regular intervals (Gupta et al., 2019). Designing the post-incident review in the fashion of a retrospective can provide the IR team with a lightweight structure, which will allow its members to focus on the people and processes involved (Goncalves & Linders, 2015). By asking questions such as 'what went wrong', 'what went well', 'what could be improved', can further help them identify the root cause of the incident, and ultimately ascertain and develop more targeted actions for future improvement.
Retrospectives are further beneficial for collaboration, as they bring organisational members together from different teams and departments, who may not typically interact outside of the context of an incident. Through this collaboration, effective retrospectives can improve the data collection post-incident, especially as far as security controls and security incident response-related process changes are concerned, which are captured during these sessions. Therefore, thanks to their lightweight and collaborative nature, retrospectives can become the mechanism that supports organisational learning and dissemination across the organisation, which lengthy investigations and formal reports often fail to do (He & Johnson, 2015).
To incorporate the above in our proposed framework (Figure 2), in the Post Incident Activities phase, we include the components of 'Perform retrospectives including all stakeholders involved' and 'Identify any necessary policy or procedure amendments', to account for reflective learning. Then, in the Preparation phase, we include the component 'Implement actions based on lessons learned from previous incidents' to account for the implementation of the drawn lessons learned from the retrospective.

3.5. Continuous Attention to Technical Excellence (Digital Forensics)

Currently, most incident response practices lack forensic investigation (Ahmad et al., 2012; Papastergiou et al., 2020), especially when it comes to attacks and intrusions to database systems (Al-Dhaqm et al., 2020). Historically, forensic investigations within organisations have not been up to standards for pursuing legal action (Nnoli et al., 2012; Papastergiou et al., 2020). This is because such

investigations typically focus primarily on the Detection and Analysis phase, because the value of the investigation is itself undermined by the linearity of IR processes, whereby emphasis is placed at front-end of the process (i.e., Preparation, Detection and Analysis, Containment), rather than on the learning element (Papastergiou et al., 2020, 2019).

However, gathering evidence from across all IR phases is invaluable. During a security breach, a forensic investigation can find various artefacts, such as deleted files and metadata (Ho et al., 2018) which can be used to gain insights into file operations and other patterns (Singh & Gupta, 2019). These artefacts can support the IR team's understanding as to why and when the breach occurred, and how the attackers were able to get around the existing information security defences. Equally, the product of the forensic investigation can be used for the identification of said attackers and therefore will be a critical tool for any future criminal investigations of the security breach. As such, by gathering evidence throughout the IR process, facilitates on the one hand the apprehension of the attacker, while on the other hand indirectly discourages attacks (Bakhshi, 2019) by increasing the overall costs of an attack, as future attackers will need to spend more resources in covering their tracks.

This holistic understanding can be seen as the equivalent to continuous attention to technical excellence (Grispos et al., 2015), heralded in the Agile principles (Beck et al., 2001). We implement this in our framework through the inclusion of the 'Detect incident and collection forensic evidence' component during the Detect Incident Phase (Figure 2), and which, keeping with the Agile spirit, remains activated until the last phase of incident response.

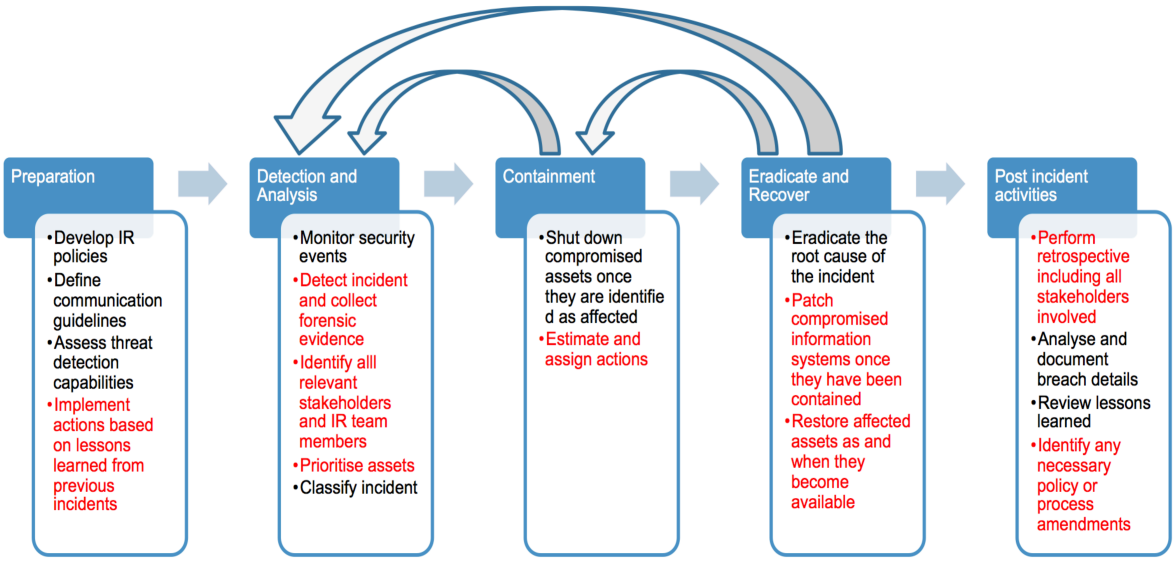

Figure 2. Agile Incident Response (IR) Framework (Agile-inspired components are noted in red; cyclical arrows indicate iterations).

In summary, implementing an iterative and incremental approach to IR will provide the necessary flexibility which is necessary for responding to sudden and therefore unforeseen changes typically occurring when handling an incident, and as a result, it will facilitate returning to BAU sooner. Coupled with greater and more meaningful collaboration, IR teams can become more efficient and successful and, ultimately, support the organisation reflect on and learn from the successes and failures of the incident process, and therefore improve. However, embracing these Agile principles can be a challenge, especially when it comes to large organisations, where bureaucracy may be an impediment to the implementation of more horizontal processes; yet, it is imperative if IR is to be transformed into a more effective and value-driven process.

4. Application of the Agile IR Framework in the Healthcare Sector: the case of NHS England

To illustrate the usefulness of the Agile IR Framework and how it can improve linear IR processes, we theoretically apply it within the context of the healthcare sector and specifically within the NHS. We do so by first presenting NHS' current IR framework, drawing out its strength and weakness. We then present how the organisation can implement the Agile principles within its IR processes through targeted adaptations and modifications, thus allowing the NHS to reinforce its current framework.
We focus on the NHS because it constitutes a large healthcare organisation with a complex IT infrastructure, a network of Information Security teams, and its processes are underpinned by the requirement to comply with international security standards (Evans, He, Luo, et al., 2019). This means that, on the one hand, IR requires the coordination of different parties from across the organisation, and on the other hand, that NHS has today quite a mature incident management framework, evidenced in the official documentation (Heathcote, 2017b), which allows us to assess several aspects of its IR processes. We specifically focus on the larger NHS organisations, because typically it is those that have IR teams and IR procedures in place, whereas in smaller organisations these are often undertaken by third-party providers. In addition, other organisations may develop and use their own policies and procedures for handling incidents, as for example the NHS North West London Collaboration of Clinical Commissioning Groups (NWL CCG) (NHS NWL, 2018); however, such policies tend be specific to individual, smaller groups (as in the case of NWL CCG which applies solely to those entities commissioned by NHS NWL) and thus they do not readily apply to the wider NHS.
Therefore, for the purposes of our analysis, we chose NHS' official documentation titled "Information Security Incident – Good Practice Guide" (Heathcote, 2017b), as it applies for information security incident management within the NHS. To complement our understanding and provide a more thorough analysis, we further draw from the "Hardware and Software Security - Good Practice Guide" (Heathcote, 2017a), NHS England's Information Security Policy (NHS England, 2018) and published research in relation to incident management and information security breaches.

4.1. A critical review of the NHS incident management framework

The NHS has adopted the incident management framework documented in the "Information Security Incident – Good Practice Guide" (Heathcote, 2017b), which describes specific processes for minimising the immediate and long-term business impact of cybersecurity incidents. The framework contains detailed instructions that both small and large NHS organisations are required to follow in case of an information incident.
The "Information Security Incident – Good Practice Guide" begins by indicating its scope of application, which includes any information security incidents affecting NHS IT systems or services used for storing, processing and transmitting NHS information. The Guide comprises of the phases of Incident Reporting, Incident Analysis, Incident Response, Responding and Closure of Incident, and Lessons Learnt and Follow on Actions; in essence, it outlines a high level linear process, alike the archetypical linear IR framework and almost identical to the NIST IR framework (Chichonski et al., 2012).
In what follows, we analyse the five main activities identified by the Good Practice Guide. We focus on identifying the strong and weak points and on the potential challenges they may pose to the organisation, which we summarise in Table 2. We then map these activities against the Agile IR Framework in order to illustrate the steps that can be taken towards adopting the Agile principles for incident response. These are summarised in Table 2.

4.1.1. Information Security Incident Reporting (IRP)

The Guide emphasises having a simple and clear reporting process to boost the speed of response. To this end, it advises the use of bespoke IR IT systems for gathering and reporting information throughout the IR process, without making any specific recommendations. This allows the NHS organisations make their own choices. However, public organisations are under pressure to reduce their operational costs (Gantman & Fedorowicz, 2020); as a result, this flexibility, under the burden of cost cutting, may drive NHS organisation to decide against the use of any reporting tool, irrespective of sophistication or the

type of solution (e.g., bespoke or off-the-shelf software), with adverse effects on the IR process on its speed and efficiency.
NHS organisations are required to create a single reporting point for all incidents. Keeping this phase simple reduces the chances of reporting to the wrong team. The requirement is that all incidents are reported via telephone, with email reporting being optional. Reporting via telephone could be a risk, whereby some information may be lost or forgotten after the telephone conversation. However, the Guide also requires that some essential information is captured in hard copy, too, namely the date and location of the incident, a summary of it and its type of the incident, and contact details to follow up. This information is used for progressing to the Incident Analysis stage.
Finally, the Guide advises testing the process annually through tabletop, walkthroughs and real-time live tests to ensure that the organisation handles incidents effectively.

4.1.2. Information Security Incident Analysis (IA)

Incident analysis begins with assessing the severity of the incident, thus assigning a priority to it. The Guide does not formally acknowledge that more than one asset can potentially be compromised. However, having multiple compromised assets is common and the most efficient way to return to BAU is to prioritise the most business critical assets (Thompson, 2018). Contrary to that, the Guide suggests that NHS organisations restore all affected services and assets together, which inescapably will result to longer downtime.
According to the Guide, the stakeholders included in Incident Analysis are from IT, Operations, Legal, Human Resources, Police Authority, and Forensic Specialists. This approach indicates a collaborative effort, which is expected to contribute to a successful incident response (Menges & Pernul, 2018; Skopik et al., 2016). The expectation is that between these teams, there will be pooled knowledge that can assist and support the IR team. Having said that, the identified stakeholders do not necessarily bring input from asset owners, who can contextualise the Incident Response and are better positioned to appreciate the business impact of the incident and offer accuracy to the severity assessment.
The analysis process provides a sound base for responding on the basis of the Incident Reporting phase, as it uncovers the scale of the incident and allows for potential reassessment later on. Yet, the severity assessment is conducted by the NHS organisation rather than an NHS standard method, which will prove problematic if the incident affects multiple organisations, because it may result to different local assessments, and in turn, to inefficient collaboration across organisations.
The possibility of criminal activity requires that evidence collection occurs in a forensically sound manner, which explains the inclusion of Forensic Specialists. This ensures a correct chain of custody that increases the potential for criminal convictions and award of damages if the attackers are identified, and acts as a deterrent for future attacks (Bakhshi, 2019). However, the Guide offers no tangible information as to what constitutes forensically sound evidence collection. This is challenging, especially when considering that it is often later in the IR process that the IR team is able to identify signs of criminal activity (Lamis, 2010; Thompson, 2018).

4.1.3. Information Security Incident Response (IR)

Incident Response involves primarily individuals and teams with technical knowledge who will directly respond to the incident. As such, the same challenges exist, i.e., stakeholders with tacit knowledge regarding directly or indirectly affected assets are excluded.
The Guide outlines the exact IR activities to be undertaken and begins by indicating the need for a responsible person, overseeing the IR. This reduces uncertainty among those involved and supports the coordination of activities and the allocation of resources.
Within the IR activities, the Guide includes a root cause analysis, thus benefiting the IR process itself, and Post Incident activities, too. However, on the one hand, it is unclear what information should be gather for the root cause analysis, while it prioritises resolving the incident as quickly as possible. The combined effect of these two issues can easily result to taking shortcuts and conducting a poorly executed root cause analysis. A minimum expectation for the root cause analysis would remove this.

Another important step is the identification and management of risks resulting from the incident in order to determine whether changes in services are needed to negate the effect of the incident possible without operating under increased risks.
The Guide finally suggests the implementation of recovery actions without indicating what these might be. It does not refer to containing compromised assets either. Containment prevents further damage, it is usually done before any resolution efforts have started, and it is included in all linear IR frameworks (British Standards Institution, 2016; Chichonski et al., 2012; Creasey, 2013). This omission is worrying considering that attackers often enter information systems via low-risk assets and then navigate to high risk ones, e.g., health records; however, containment of compromised assets reduces such risks significantly (Akkuzu et al., 2018).

4.1.4. Reporting and Closure of Incident (RC)

As part of IR, the NHS organisation prepares two reports. The first report is prepared early on and contains information regarding the incident's severity, the proposed response and the investigation activities. Its purpose is to determine the required resources for the IR process. The report is then communicated to the organisation's Senior Management for approval and oversight. At this stage, however, this initial report can be a time-consuming process. While the report is being prepared and waiting for approval, the incident worsens, especially if compromised assets are not contained. In addition, if the report is prepared by those involved in the IR, this may entail inefficient allocation of resources, as it takes the focus away from resolving the incident. Other means, such as a conference call, could easily replace the need for the preliminary report.
The second report is produced after IA and IR are complete. The report draws input from all relevant stakeholders and provide an in depth understanding of the incident and the IR. However, the distribution path of the report is unclear. Appropriate distribution would mean that the report is read by those who can enact changes, those who can learn from others' mistakes and inefficiencies during the IR, and those who can provide insights regarding the organisation's future operations. Therefore, a careful distribution path could result to significant improvements in the overall process or lead to policy changes (Mattord & Whitman, 2014; Whitman, 2004).

4.1.5. Learning from Incidents & Follow on Actions (LI&FA)

The Guide recognises learning as an important part of IR. For this reason, it requires that the second report should incorporate the lessons learned from responding to the incident. This section comprises the views of the stakeholders involved in the response in order to identify a full range of potential improvements, and it is then used to form the follow on actions. Such follow on actions can be changes in policy, IT system changes and updates, changes in procedures and processes, or new and updated information security training. The Guide provides no tangible advice for assessing and evaluating existing security controls of previous IR updates. However, it does highlight that the NHS organisation should analyse incidents for any trends and this can be very useful as it can indicate whether there are any missing controls, which result in repeated incidents.

Table 1. Summary of NHS incident management framework critical review

Phase	What works well	What requires improvement	What is missing
Information Security Incident Reporting (IRP)	• Clear reporting process • Single reporting point for centrally handling incidents • Incident reporting in hard copy • Annual testing of the IR procedures	• Non-binding advice for a reporting tool	
Information Security Incident Analysis (IA)	• Forensically evidence needs to be collected if there is indication of criminal activity. • Expects collaborative effort for IA (IT, operations, legal, HR, police, forensic specialist) • Expects coordination if the incident is at the organisational boundaries or involves more than one organisation. • Asset prioritisation • Pre-defined severity scale • Data classification (sensitive, PII)	• Signs of criminal activity may show in later stages (forensic evidence may be lost/destroyed during IR) • Unclear if the forensic specialist will be involved during the IR • Asset prioritisation is aimed at one incident affecting one asset: not all assets are identified and prioritised • The severity assessment is conducted locally	• Advice on how to collect forensically sound evidence • Asset owners not involved in IA • Standard way to assess severity
Information Security Incident Response (IR)	• Requirement for a risk assessment before implementing changes • Designation of a responsible person for IR: supports central coordination, oversight, resource allocation • Root cause analysis	• Unclear responsibility allocation to individual IR members • Restoring all affected services simultaneously results in longer downtime	• Asset containment • Minimum expectations for the root cause analysis
Reporting and Closure of Incident (RC)	• One initial report on severity (proposed response activities) • One detailed report on IR with input from relevant stakeholders	• The initial report is time-consuming and inefficient resource allocation as the incident may be worsening	
Learning from Incidents & Follow on Actions (LI&FA)	• Lessons learnt should lead to changes, updates, additions to the existing IR, IT system configurations, procedures, policies, standards or guidelines to mitigate future incidents • The detailed report should be purposefully disseminated for follow on actions. • Stakeholders to be involved during incident learning to identify potential improvements.	• The identified proposes/required changes may not be implementable in their full extent due to budget/resource constraints and other priorities	• Indication as to who should be the recipient of the report for contributing on follow on actions • Advice on how to evaluate security controls and previous IR revisions (whether and how they have been implemented in practice).
Note: Incident Reporting (IRP); Incident Analysis (IA); Incident Response (IR); Reporting and Closure of Incident (RC); Learning from Incidents (LI&FA)			

4.2. Developing the NHS Agile IR framework

Our critical review of the NHS Incident Management Framework shows that it is quite efficient in many respects. For example, comprising a single reporting point reduces the risk of unreported incidents and mistakes in the reporting process, while ensures that IR will be triggered as soon as possible. However, we have also identified several weaknesses, as for example the non-binding advice regarding the use of reporting tools.

In this section, we offer recommendations for improving the NHS incident management guidance. As shown in Table 2, we do this by a) maintaining the components of the NHS framework that work well (column "component" in Table 2), b) mapping them against the major phases of the archetypical linear IR framework to clarify where in the IR process are positioned (column "phase" in Table 2) and c) incorporating components from the Agile IR framework within the relevant phases to address the previously identified weakness of the NHS framework (recommendations in italics noted in Table 2).

To begin with, the first recommendation is the incorporation of a digital forensics specialist in the team and the IR process (Detection and Analysis phase) to address the current lack of clarity around evidence collection and the potential collateral consequences. Such a role will enable identifying what data could potentially be relevant for identifying the attacker and thus support in the apprehension effort, constitute evidence within the context of a prosecution, holding the attacker accountable and claiming damages if relevant. The Association of Chief Police Officers (ACPO) (J. Williams, 2012) offers a set of clear guidelines for evidence collection during cyber security incidents and it is one of the most widely cited and applied guides (Horsman, 2020). Using the best practices detailed in the ACPO's guide suggests that the IR team will comply with current legislation and policies. It also increases the chances that the IR team will not taint the evidence, and that the evidence will be admissible in court.

The second recommendation requires the inclusion of all stakeholders, i.e., asset owners in the IR process, and specifically in the IA phase for the purposes of drawing input from them. The NHS framework does not require, nor indicate their involvement, however not including all stakeholders in the IR process leads to inconsistent and untimely IR, thus contributes negatively to incidents (Ahmad et al., 2012). In contrast, their participation in IA will help build an IR that incorporates tacit knowledge held by different groups across the organisation, which can prove critical later on for resolving the incident, during the risk assessment etc. (Werlinger et al., 2010).

Our third recommendation is the introduction of a formal Containment phase, which presently is lacking from the NHS framework and which is nevertheless essential during a breach. A Containment phase provides the IR team with valuable time to analyse the incident and identify viable solutions that will work correctly first time (Khan et al., 2019). In an of itself, containment is reactive; however, it also allows for asset prioritisation during Eradication and Recovery, because the IR team can freely focus on those requiring immediate attention (Khan et al., 2021), or being business critical, rather than focusing on all assets equally, potentially leading to a prolonged impact on business. Therefore, restoring assets as soon as they become available is our fourth recommendation, because this will allow the organisation to return to BAU sooner, restoring services as soon as they become available. On the one hand, initiating Containment once an asset has been identified as compromised should be easy to do and should take place automatically. On the other hand, the plan to resolve the incident must keep adapting to include resolutions for the potentially increasing number of affected assets. This can be challenging; however, the incorporation of a formal Containment phase, coupled with a slightly reimagined Eradication and Recovery phase will allow for incremental progress, which is a major Agile principle for improving efficiency and timeliness to incident recovery.

Our fourth recommendation is to implement iterations to ensure early and continuous delivery, where the IR process continues prioritising assets during the Detection and Analysis phase. This allows the IR team to identify the assets required for the investigation during the Containment phase and reinstate non-critical assets and return the assets to stakeholders in the Eradicate and Recover Phase. This way, it Iteratively re-evaluates and reprioritise assets and returns those that no longer pose a threat to the production environment, thereby incrementally reducing the overall impact of the breach.

The Agile IR framework places an emphasis on learning during and through the Post-Incident Activities. Our recommendation is for transforming the cumbersome Learning from Incidents & Follow on Actions with the use of retrospectives and information security training across the organisation. The retrospectives are a way for providing all people involved in the IR with the opportunity to reflect on how they believe the process went (Goncalves & Linders, 2015; Grispos et al., 2017). The result will be a discussion that highlights the positive aspects of the process that need to be continued, alongside the negatives, which need to be addressed for future incidents. Involving *all stakeholders* once again increases the sense of teamwork when it comes to incident response and incorporates knowledge and experiences from different parts of the organisation, thus improving the IR for the future. The actions from the retrospectives must be monitored and seen through to completion to realise the full benefits of the retrospectives. In addition, meta-retrospectives should be introduced to look at the outcomes from all incident-based retrospectives, which will formally identify trends, consistent points of failure that need to be addressed and formally lead to follow on actions. They will also help to identify whether the actions from retrospectives are successful at improving the organisations control environment or incident response success.

Coupled with the idea of increased collaboration is the recommendation of distributing IR reports to all stakeholders affected. This can be done by sending these reports to the business owners and senior stakeholders within the NHS organisation who are best placed to distribute them further to relevant teams and individuals, since the report may contain business sensitive information. The findings and learning from each incident, however, should be shared widely.

Table 2. Mapping the NHS IR process against the Agile IR framework.

Phase	Component (recommendations noted in italics)	Rationale
Preparation	• Clear reporting process • Single reporting point for centrally handling incidents • Incident reporting in hard copy • Annual testing of the IR procedures	
Detection & analysis	• Forensically evidence needs to be collected if there is indication of criminal activity. • *Forensically examine and collect evidence according to the ACPO guidelines (J. Williams, 2012)* • *Include a forensic expert within the core IR team* • Collaboration for IA (IT, operations, legal, HR, police, forensic specialist) • Coordination if the incident is at the organisational boundaries or involves more than one organisation • Designation of a responsible person for IR: supports central coordination, oversight, resource allocation • *Include stakeholders (asset owners) in IR and specifically request for input during IA* • Pre-defined severity scale • Data classification (sensitive, PII) • Root cause analysis • Asset prioritisation	• The ACPO provides guidance for law enforcement and IR teams for the investigation of cyber security incidents and crimes. Collecting evidence following this guide ensures compliance with current legislation and policies. • A forensic expert will provide up-to-date, accurate legal knowledge and expertise to the IR team an incident response team to ensure it has the necessary breadth of expertise (Gurkok, 2017). • Not including all stakeholders in the IR process leads to inconsistent and untimely IR, thus contributes negatively to incidents (Ahmad et al., 2012); the inclusion of all stakeholders helps incorporate tacit knowledge held by different groups across the organisation, which may be critical for IR (Werlinger et al., 2010).
Containment	• *Containment plans should be predefined and all compromised assets should be isolated within a sandbox environment until the incident has been resolved* • Risk assessment before implementing changes	• Containment facilitates decision-making: it allows the organisation to take a calculated risk for shutting down, maintaining and restoring services; it reduces the likelihood of the incident overwhelming the organisation and compromising further assets (Akkuzu et al., 2018); it provides enough time for the IR.
Eradication & Recovery	• *Restore affected assets as and when they become available*	• This allows for an incremental approach to recovery and earlier move to BAU where systems get restored as soon as restored

Post incident activities	• One initial report on severity (proposed response activities) • One detailed report on IR with input from relevant stakeholders • *Specifically request input from stakeholders (asset owners)* • *The detailed report should be distributed to senior stakeholders for improved overall awareness within the organisation and follow on actions* • *Implement retrospectives and meta-retrospectives and include all individuals and teams involved in the IR* • Lessons learnt should lead to changes, updates, additions to the existing IR, IT system configurations, procedures, policies, standards or guidelines to mitigate future incidents	• To increase interaction between the IR team and other teams • To increase overall awareness within the organisation • Light-weight retrospectives can be more effective and can improve data collection post-incident which will enable the organisation to improve the IR process (Grispos et al., 2017) • Retrospectives can support organisations understand better the root cause of the incident.
Iterations	• *Implement iterations between the Detection & analysis, Containment and Eradication & Recovery stages.* • *Iteratively re-evaluate and reprioritise assets and return those that no longer pose a threat to the production environment.* • *In the Detection and Analysis phase, the IR process continues prioritising assets during the Detection and Analysis phase ('prioritise assets'),* • *In the Containment phase, the IR team identifies the assets required for the investigation ('estimate and assign action').* • *In the Eradicate and Recover Phase, the IR processes reinstate non-critical assets and return the assets to stakeholders for use in day-to-day business processes ('restore the affected assets as and when they become available'.*	• *Implementing iterations between the Detection & analysis, Containment and Eradication & Recovery stages enables early and continuous delivery* • *Implementing iterations can reduce incrementally the overall impact of the breach.*
Note: Incident Reporting (IRP); Incident Analysis (IA); Incident Response (IR); Reporting and Closure of Incident (RC); Learning from Incidents (LI&FA)		

5. Discussion

Information security breaches are one of the main challenges for organisations today in the area of cybersecurity (Khan et al., 2021), and this can be of particular concern for healthcare organisations that handle PII and sensitive data. Typically, healthcare organisations tend to employ linear IR frameworks to respond to information and data breaches. However, while such linear frameworks offer structure in the response, they are not efficient and effective when addressing sophisticated incidents, especially those that can propagate and infect additional assets in the system (Anderson, 2017; Grispos et al., 2014, 2017; He & Janicke, 2015). Our analysis shows that there are several limitations because, by design, linear IR approaches are usually time-consuming, ineffective in responding to large scale attacks, over-complex when handling sophisticated incidents, they discourage collaboration among experts and stakeholders, and they lack learning opportunities.

In this study, we build on the archetypical linear IR lifecycle (Mitropoulos et al., 2006) and the Agile principles (Beck et al., 2001; Grispos et al., 2014, 2015), and develop the Agile IR framework, in order to address these challenges. To date, while there have been some efforts to build Agile principles into IR processes, most typically such studies either target individual phases of the IR process or argue in favour of agile as a more high level concept, without detailing what tasks and activities needs to be undertaken so as to develop a holistic approach that could be adopted by organisations (Anderson, 2017; Casey & Nikkel, 2020; Grispos et al., 2014).

Linear IR processes require that IR teams focus on one phase at a time, whereby once a phase is complete, it cannot be revisited. As such, iterations and updates in the response are not supported by rigid linear approaches. However, our critical review of the NHS Incident Management Framework illustrates that being able to update the response strategy by iterating between phases is vital. Such an approach allows the components of the agile IR process to function together in order to quickly restore assets and business-critical services. This is achieved because Agile approaches allow the organisation to prioritise and restore business-critical services and assets (including compromised ones) as soon as they become available, rather than waiting until an entire phase is complete. In addition, as Smith et al. (2021) note, during information security breaches, teams need to update and adapt their response strategy on the basis of the evolving requirements. Particularly during large scale attacks, the ability for iterations is of paramount importance, because it is during such attacks that security requirements continuously evolve (Hadar & Hassanzadeh, 2019). In contrast, focusing on completing one stage at a time while an incident is still unfolding, i.e., a more rigid approach, often results in halts in the IR lifecycle and in the attack further propagating across networks and systems (He & Janicke, 2015; He & Johnson, 2015).

Next, linear IR processes are predictable in what they entail regarding defences against cyber-attacks. However, sophisticated cyber-attacks are not as unpredictable, which suggests that linear process are unable or at least less effective in "protecting the remaining infrastructure and business functions in the context of fast-pivoting and multipronged cyber-attacks" (Smith et al., 2021, p. 2). Naseer et al. (2021) further highlight that what is needed is enhanced cybersecurity awareness and understanding the behaviour of the adversary, in order to respond to such threats. By comparison, agile methodologies, as shown by our findings, can address such issues, because not only they can accommodate changes and handle unforeseen situations in shorter cycles, but also they incorporate post-incident activities.

Such post-incident activities support developing enhanced cybersecurity awareness across the organisation. Existing literature indicates that organisations often skip learning by the incident because IR teams typically focus on containment, eradication, and recovery (Ahmad et al., 2012; Grimes, 2007; Tan et al., 2003; Werlinger et al., 2010). In addition, while the archetypal IR framework entails a post-incident review during which the IR team does a follow up to identify root causes and lessons learnt (Mitropoulos et al., 2006), this review is often cumbersome. Our critical review of the NHS Incident Management Framework illustrates that the numerous reports required by post-incidents activities and the lack of clarity can potentially divert attention away from the focus of the primary activity. In

fact, linear IR frameworks seem to discourage learning opportunities during the IR processes. By comparison, Agile principles build such opportunities in the IR processes by adopting the retrospectives approach (Gupta et al., 2019). Such retrospectives favour a lightweight approach and avoid extensive documentation. While Grispos et al. (2017) evaluated empirically this approach, their findings are specifically focused on the follow-up phase of incident response rather than the entire process. Our analysis extends this work by focusing on the entire IR process and showing how retrospectives can support gauging lessons learned easily, where these inform and are informed by stakeholders from across the organisation.

Potentially, the greatest benefit of an agile IR process is the promotion of collaboration across various teams and the organisation. Our analysis shows that existing IR processes prohibit fruitful collaboration because they require that only the core IR team is involved in incidents, potentially communicating with a short list of key stakeholders. This most typically leads to negative results, where, for example, digital forensics evidence may be disregarded and even destroyed. In addition, domain knowledge from critical asset owners may not be actively considered and opportunities for capturing and distributing lessons learned can be lost. Our critical review of the NHS Incident Management Framework allowed us to identify the expected collaborative efforts across the IR process, particularly during the incident analysis phase from different teams including IT, operations, legal, HR, police, and forensic specialist. Our findings suggest that adopting agile principles can address this and offer a platform for close collaboration, quick resource allocation, which ultimately support achieving each iteration's goals (Baham et al., 2017; Lindstrom & Jeffries, 2004). Further, they can support the cross fertilisation of expertise and experience, which then facilitate the integration and contextualisation of knowledge, and resolve current incidents and prevent future incidents.

Based on this analysis, we develop the following three propositions:

Proposition 1: The integration of Agile Principles within linear IR processes can enable organisations return to BAU sooner.

The proposed Agile IR framework is underpinned by the Agile values and principles and focuses on responding to changes, early and continuous delivery of restored assets and services in a BAU state, collaboration among stakeholders, learning, and technical excellence (i.e., digital forensics). Assessing this framework against the background of the NHS Incident Management Framework's critical review illustrates that its components, and the way they function together are particularly supportive of an iterative and incremental approach to incident resolution. Restoring compromised assets as soon as they become available allows the organisation to prioritise and restore business-critical services first; incorporating light-weight retrospectives supports learning and feedback loops and moves away from cumbersome processes that discourage rather than support learning from incidents; collaboration with critical stakeholders allows integrating and contextualising knowledge that can be crucial for resolving current incidents, prorating assets and preventing future incidents. Similar effects have been observed in other disciplines, as for example in software engineering (Abrahamsson et al., 2002) and the information systems project management (Dennehy et al., 2019; Dennehy & Conboy, 2018, 2019), governance (Janssen & van der Voort, 2020) and supply chain management (Dubey et al., 2020), to name only a few.

Proposition 2: Effective IR requires a collaborative effort throughout the process.

The Agile principles entail strong collaborative spirit that spans across the various teams and the organisation. This collaboration aims at providing timely response to continuous changes in the environment, as well as producing a result that is valuable and fit for purpose (Batra et al., 2017). Within the context of information security, this can be understood as responding early to an information security breach, adapting the IR to the requirements of the incident while the latter may still be unfolding, and for the purpose of resolving it with minimum losses (financial, informational, etc.). Our critical review shows that the lack of collaboration can lead to negative results, such as loss of potential forensic evidence, loss of tacit knowledge from critical asset owners, and inability to

capture and distribute the lessons learned from the incident back to the organisation. Furthermore, Stacey et al. (2021) argue that collaboration and engagement between management, stakeholders and those delivering the cybersecurity agenda and response it is crucial for sensing, evaluating and responding to required changes.

Proposition 3: Favouring lightweight retrospectives over cumbersome reporting can improve learning from incidents.

Agile methodologies favour lightweight approaches throughout and processes and products that work and are fit for purpose over extensive documentation (Beck et al., 2001). This is often misinterpreted as Agile methodologies requiring no documentation at all. Contrary to that, the Agile principles suggest that it is excessive documentation that needs to be avoided because it can potentially divert attention away from the focus of the primary activity (Pries-Heje & Baskerville, 2017). Reviewing the linear IR framework and the NHS framework shows that cumbersome learning activities that require extensive documentation are counterintuitive to learning. Typically, they necessitate a lot of details, numerous reports and lack clarity with regards to their structure, i.e., what exactly should be assessed and evaluated. This often results in delays, propositions that are difficult or impossible to be implemented due to budgetary and other constraints and, in turn, little value in the Post-Incident activities (He & Janicke, 2015; Shedden et al., 2011). Replacing these with retrospectives can significantly support extracting lessons learned from the incident because retrospectives, in their simplicity, have a clear approach to evaluating the team's experiences and viewpoints with regards to what worked well and what worked less well, with the view to improve the latter in the future (Gupta et al., 2019; He & Johnson, 2015).

5.1. Theoretical Implications

Previous studies have long argued for the suitability of the Agile principles for incident response (e.g., Anderson, 2017; Grispos et al., 2014, 2017; He & Janicke, 2015). However, to date there have been limited efforts to formally build Agile principles into IR processes, and typically such efforts have not been holistic or systematic, but rather they focused on parts of the IR process. For example, Grispos et al. (Grispos et al., 2014, 2015) argue for a more agile approach to IR but do not develop a framework that directly indicates core activities or components for the different phases. Others (e.g., Casey & Nikkel, 2020; He & Janicke, 2015; He & Johnson, 2015) focus more on the learning activities of the Post-Incident phase and the missed opportunity to learn due to the lack of forensic analysis. As such, our first contribution is to integrate the existing studies of the IR processes and agile principles, proposing the Agile IR framework that can refine, adjust, and improve the current linear IR process. We contribute by focusing on the key areas of the IR process that require strengthening and by augmenting them with Agile-inspired components. As such, each of these focal components corresponds to an Agile principle (Beck et al., 2001), but most crucially, formally incorporates critical IR functions, previously missing from the archetypical linear IR lifecycle: 'responding to changes' enables the addition and prioritisation of the newly infected assets at any point during the incident lifecycle (Neubauer & Heurix, 2008); 'early and continuous delivery' enables iterative revaluation and prioritisation of assets and returns those no longer needed to the production environment, hence incrementally reducing the impacts on businesses (Grispos et al., 2015); 'collaboration between stakeholders' enables tapping into valuable knowledge from disparate sources (Bernard, 2007); 'incident learning' enables team reflection to become more effective in the future (He & Janicke, 2015; He & Johnson, 2015) (He et al., 2014); 'continuous attention to technical excellence', brings in the digital forensics expertise to support the forensic investigation (Grispos et al., 2017; Horsman, 2020; Tan et al., 2003).

Our second contribution derives from the assessment of the Agile IR framework against the backdrop of our critical review of the NHS Incident Management framework. Through this evaluation we show that the Agile principles can be incorporated into linear frameworks, whereby organisations can choose some but not necessarily all of the Agile principles. We consider that in the case of IR in large

organisations, such hybrid approaches have the added benefit of allowing the organisation to develop a tailor-made approach, according to their specific resources and in line with their culture, that still allows them to support their IR efforts. Therefore, our study complements existing research on IR and information security by combining two different paradigms that have long existed separately. We acknowledge that combining structured and less structured approaches is not a novel approach in other knowledge fields. For example, in Information Systems Project Management, hybrid approaches have been showing their potential for quite a while (e.g., Gill et al., 2018; e.g., Poba-Nzaou et al., 2014), particularly for larger projects, where the software development and project management lifecycles can follow different methodologies (e.g., Scrum for the first and Waterfall for the second) and still harmoniously co-exist in order to maximise the benefits for the project.
We thus set up a foundation for the research community to conduct further research on Agile IR and further elaborate, refine and adapt the current AIR framework.

5.2. Practical Implications

Our study has important practical implications. The implementation of an incremental approach to resolving information security breaches instils flexibility and responsiveness, thereby supports faster return to BAU, which is the crux of IR (Shukla et al., 2019). The focus on technical excellence, and specifically on digital forensic analysis and the inclusion of a forensic specialist can support organisations in two different ways. First, it cannot be emphasised enough that it is this type of expertise that will allow an organisation to identify and collect the necessary evidence, which can then lead to the identification of the perpetrator and subsequent potential damage claim (Al-Dhaqm et al., 2020; Horsman, 2020; Khan et al., 2019). Second, while it may be argued that such a measure increases costs, in the aggregate, developing digital forensic capabilities can only be beneficial for the organisational in the long run and decrease costs. On the one hand, it indirectly increases the costs for attackers, who will need to commit more resources (time, effort, hardware etc.) towards covering their attacks before, during and after the attack, thereby acting as a deterrent for would-be attackers (Brewer et al., 2019). On the other hand, following an information security breach, especially when PII and sensitive data is involved, organisations rarely consider the full breadth of costs, and these costs often exceed financial ones, involving regulatory and reputational ones, which may difficult to recover from (Furnell et al., 2020).
We consider that large organisations, and particularly healthcare organisations have most to benefit from our work. Papastergiou et al. (2020) discuss that the sector of healthcare, like most critical information infrastructures, faces an increasing amount of cyberthreats, yet healthcare organisations still follow in their majority linear IR processes. We identify a number of weaknesses, and provide tangible recommendations for addressing them, by illustrating their application through our critical review of the NHS Incident Management framework and subsequent evaluation of our Agile IR framework. In the first instance, these recommendations can aid the NHS in creating a more efficient IR process, by improving the control environment, and allowing for necessary adaptations if and when necessary. At the same time, considering that several national healthcare systems, such as the Chinese and the Irish, similarly follow linear IR processes (Code of China, 2019; HSE, 2018), we posit that our recommendations are applicable beyond the confines of the NHS. Importantly, we argue that the general industrial guidelines and best practices, such as the National Institute of Standards and Technology (Chichonski et al., 2012), CREST (Creasey, 2013) and the International Standard for Information Security Incident Management (British Standards Institution, 2016) can also benefit from the proposed Agile IR framework. These guidelines are all based on the archetypical linear IR approach, aiming to provide organizations with guidance in establishing IR capabilities. The coupling of the Agile IR framework with industrial guidelines and best practices has the potential to transform the way of incident response from linear to hybrid or agile, and provide a number of benefits, as for example faster return to BAU and superior lessons learned processes.
While we identify the above benefits and implications for the information security sector, it would be inappropriate not to recognise some of the challenges we foresee in the implementation of the Agile

principles in linear IR processes. Our overarching aim for mapping the NHS Incident Mapping framework onto the Agile IR framework was to arrive to recommendations that constitute minor refinements rather than overhauls, which can nevertheless improve the efficiency and effectiveness of the IR in order to provide benefits to the NHS. However, this does not mean that implementing the Agile principles and moving from the linear to a more agile methodology will be an easy process; instead, most of these recommendations will require a mindset shift within the organisation, and this will be more difficult for very large organisations and/or regulated sectors, because the complexity of the processes involved increases exponentially (Moyón et al., 2020). 'Becoming Agile' requires a concentrated effort, with top management support (Dennehy & Conboy, 2019; Denning, 2019), who will be responsible for creating a supportive and nurturing environment so that the necessary changes can be implemented and followed through (Mergel et al., 2018). In the first instance, our proposition with regards to collaboration (Proposition 2) can support changing mindsets; collaboration facilitates moving from traditional 'command and control' approaches to more collaborative working and trust building among team members, both of which are valued and needed in Agile environments (Rezvani & Khosravi, 2019). There also needs to be a degree of trust at senior management that everyone involved will do what they have committed to do, as constant managerial oversight will reduce the speed of the process (Denning, 2019), and in some cases, it may even result in the disillusionment with Agile principles (Dennehy & Conboy, 2019). Without these as prerequisites, Denning (2019) argues that, efforts to move to more agile approaches are likely to fail.

5.3. Limitations and Directions for Future Research

Our study comes with some limitations. The Agile IR framework has been built based on drawing from the Agile Manifesto, existing academic and industry literature and our own experience in cybersecurity. Due to the nature of the topic, it is very difficult to empirically evaluate the Agile IR framework and report findings. To do this, it would require an organisation to experience an information security breach and be willing to share, even anonymously, the outcome of the IR process. However, this could theoretically jeopardise a potential forensic investigation. We consider that future work in this area can consider the evaluation of the framework via expert panel review by experienced industry practitioners in incident response from critical infrastructure sectors, as for example the healthcare sector. Such an approach will add depth to the framework itself and rich insights with regards to potential enablers and inhibitors for its implementation.

In addition, to indirectly assess the viability and usefulness of our framework, we conducted a critical review of the NHS Incident Management framework, i.e., a single IR process from a specific sector. This has its implications in the sense that our findings are more relevant to the healthcare sector, as the NHS framework is widely similar to those frameworks used by other national healthcare services (e.g., USA, China, Ireland). Examining multiple frameworks would have allowed the comparison across them and contrasting how the Agile IR could potentially work in different organisational contexts.

With regards to future research, it would be particularly useful and interesting to examine the change management initiatives within large organisations in their journey to adopt agile principles for their cybersecurity programmes. Considering that large organisations tend to have more bureaucratic environments, it would be interesting to explore how different parts of the organisation can interface within the Cybersecurity area and whether and to what extent there are differences to the hybrid approaches elsewhere observed (e.g, Gill et al., 2018; Poba-Nzaou et al., 2014; Schuh et al., 2017).

6. Conclusions

Information security breaches are continuously increasing, and attacks are becoming more and more sophisticated. However, current Incident Respond processes tend to follow a linear path, which is not conducive to how a breach unfolds in real life: unexpected, fast-spreading, and multi-faceted. In this paper, we presented an approach for the implementation of Agile principles into the archetypical IR processes for responding to information security breaches. We develop an Agile IR framework that aims to support the quick and targeted reaction of the organisation with the overarching objective to

bring the organisation to its business-as-usual state as fast as possible, and with as little as possible losses. Our work sets up a foundation for the research community to conduct further research on Agile incident response through elaborating or adapting the current framework. We also show that the Agile principles can be combined within a more linear IR approach through targeted refinements and additions to the baseline IR, while allowing for the incremental progress of the response. However, what is probably more important is the management support as moving from structured approaches to agile principles can be a challenging endeavour even the more adaptable organisations. A greater degree of trust and a move away from the traditional command and control approach are needed to allow the freedom to use an agile process.

Highlights

- Linear IR models are inefficient in responding to the changing threat landscapes.
- We develop the Agile IR framework underpinned by the Agile principles.
- We illustrate how Agile can improve IR processes in healthcare.
- We provide a set of recommendations for strengthening existing linear IR processes.
- Management support can facilitate moving to agile methods for IR.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61803318).

References

Abrahamsson, P., Salo, O., Ronkainen, J., & Warsta, J. (2002). *Agile Software Development Methods: Review and Analysis*. VTT Technical Research Centre of Finland. VTT Publications 478, Otamedia 2002. http://arxiv.org/abs/1709.08439

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Akkuzu, G., Aziz, B., & Liu, H. (2018). Feature Analysis on the Containment Time for Cyber Security Incidents. *2018 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)*, 262–269. https://doi.org/10.1109/ICWAPR.2018.8521252

Al-Dhaqm, A., Razak, S. A., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020). Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access*, *8*, 145018–145032. https://doi.org/10.1109/ACCESS.2020.3008696

Anderson, K. (2017). Using agility to combat cyber attacks. *Journal of Business Continuity & Emergency Planning*, *10*(4), 298–307.

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, 106946. https://doi.org/10.1016/j.comnet.2019.106946

Baham, C., Hirschheim, R., Calderon, A. A., & Kisekka, V. (2017). An Agile Methodology for the Disaster Recovery of Information Systems Under Catastrophic Scenarios. *Journal of Management Information Systems*, *34*(3), 633–663. https://doi.org/10.1080/07421222.2017.1372996

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management*, *43*, 76–84. https://doi.org/10.1016/j.ijinfomgt.2018.07.007

Bakhshi, T. (2019). Forensic of Things: Revisiting Digital Forensic Investigations in Internet of Things. *2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, 1–8. https://doi.org/10.1109/ICEEST48626.2019.8981675

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*, 32–45. https://doi.org/10.1016/j.cose.2016.05.004

Batra, D., Xia, W., & Zhang, M. (2017). Collaboration in Agile Software Development: Concept and Dimensions. *Communications of the Association for Information Systems*, *41*, 429–449. https://doi.org/10.17705/1CAIS.04120

Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R. C., Mellor, S., Schwaber, K., Sutherland, J., & Thomas, D. (2001). *Manifesto for Agile Software Development*. https://agilemanifesto.org/

Bernard, R. (2007). Information Lifecycle Security Risk Assessment: A tool for closing security gaps. *Computers & Security*, *26*(1), 26–30. https://doi.org/10.1016/j.cose.2006.12.005

Bjørnson, F. O., Wijnmaalen, J., Stettina, C. J., & Dingsøyr, T. (2018). Inter-team Coordination in Large-Scale Agile Development: A Case Study of Three Enabling Mechanisms. In J. Garbajosa, X. Wang, & A. Aguiar (Eds.), *Agile Processes in Software Engineering and Extreme Programming* (pp. 216–231). Springer International Publishing. https://doi.org/10.1007/978-3-319-91602-6_15

Blum, D. (2020). Institute Resilience Through Detection, Response, and Recovery. In D. Blum (Ed.), *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment* (pp. 259–295). Apress. https://doi.org/10.1007/978-1-4842-5952-8_9

Boehm, B. (2002). Get ready for agile methods, with care. *Computer*, *35*(1), 64–69. https://doi.org/10.1109/2.976920

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime Prevention: Theory and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-31069-1

British Standards Institution. (2016). *ISO/IEC 27035-1:2016 (ISO27035 Standard) Information Security Incident Management*.

Casey, E., & Nikkel, B. (2020). Forensic Analysis as Iterative Learning. In M. M. Keupp (Ed.), *The Security of Critical Infrastructures: Risk, Resilience and Defense* (pp. 177–192). Springer International Publishing. https://doi.org/10.1007/978-3-030-41826-7_11

Chichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide. NIST Special Publication* (800 (61); pp. 1–147).

Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Code of China. (2019). *GB/T 22239-2019 Information security technology—Baseline for classified protection of cybersecurity*. https://www.codeofchina.com/standard/GBT22239-2008.html

Colomo-Palacios, R., Fernandes, E., Soto-Acosta, P., & Larrucea, X. (2018). A case analysis of enabling continuous software deployment through knowledge management. *International Journal of Information Management*, *40*, 186–189. https://doi.org/10.1016/j.ijinfomgt.2017.11.005

Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Cram, W. A., & Marabelli, M. (2018). Have your cake and eat it too? Simultaneously pursuing the knowledge-sharing benefits of agile and traditional development approaches. *Information & Management*, *55*(3), 322–339. https://doi.org/10.1016/j.im.2017.08.005

Creasey, J. (2013). *Cyber security incident response guide*. CREST.

Creasy, J. (2013). *Cyber Security Incident Response Guide—Version 1*. CREST. https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

Dennehy, D., & Conboy, K. (2018). Identifying Challenges and a Research Agenda for Flow in Software Project Management. *Project Management Journal*, *49*(6), 103–118. https://doi.org/10.1177/8756972818800559

Dennehy, D., & Conboy, K. (2019). Breaking the flow: A study of contradictions in information systems development (ISD). *Information Technology & People*, *33*(2), 477–501. https://doi.org/10.1108/ITP-02-2018-0102

Dennehy, D., Kasraian, L., O'Raghallaigh, P., Conboy, K., Sammon, D., & Lynch, P. (2019). A Lean Start-up approach for developing minimum viable products in an established company. *Journal of Decision Systems*, *28*(3), 224–232. https://doi.org/10.1080/12460125.2019.1642081

Denning, S. (2019). Lessons learned from mapping successful and unsuccessful Agile transformation journeys. *Strategy & Leadership*, *47*(4), 3–11. https://doi.org/10.1108/SL-04-2019-0052

Department for Digital, Culture, Media and Sport. (2018). *Cyber Security Breaches Survey 2018*. Gov.UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Dingsøyr, T., Nerur, S., Balijepally, V., & Moe, N. B. (2012). A decade of agile methodologies: Towards explaining agile software development. *Journal of Systems and Software*, *85*(6), 1213–1221. https://doi.org/10.1016/j.jss.2012.02.033

Dubey, R., Bryde, D. J., Foropon, C., Tiwari, M., Dwivedi, Y., & Schiffling, S. (2020). An investigation of information alignment and collaboration as complements to supply chain agility in humanitarian supply chain. *International Journal of Production Research*, 1–20. https://doi.org/10.1080/00207543.2020.1865583

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Zamani, E. D., & Maglaras, L. A. (2019). Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique. *IEEE Access*, *7*, 142147–142175. https://doi.org/10.1109/ACCESS.2019.2944615

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, 74–89. https://doi.org/10.1016/j.cose.2018.09.002

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6–12. https://doi.org/10.1016/S1361-3723(20)30127-5

Gantman, S., & Fedorowicz, J. (2020). Determinants and Success Factors of IT Outsourcing in the Public Sector. *Communications of the Association for Information Systems*, *47*(1). https://doi.org/10.17705/1CAIS.04712

Ghobadi, S., & Mathiassen, L. (2017). Risks to Effective Knowledge Sharing in Agile Software Teams: A Model for Assessing and Mitigating Risks: Risk management in agile software development. *Information Systems Journal*, *27*(6), 699–731. https://doi.org/10.1111/isj.12117

Gill, A. Q., Henderson-Sellers, B., & Niazi, M. (2018). Scaling for agility: A reference model for hybrid traditional-agile software development methodologies. *Information Systems Frontiers*, *20*(2), 315–341. https://doi.org/10.1007/s10796-016-9672-8

Goncalves, L., & Linders, B. (2015). *Getting value out of agile retrospectives: A toolbox of retrospective exercises*. Ben Linders Publishing.

Grimes, J. (2007). *National Information Assurance Approach to Incident Management*. Committee for National Security Systems.

Grispos, G., Glisson, W. B., & Storer, T. (2014, August). *Rethinking Security Incident Response: The Integration of Agile Principles*. 20th Americas Conference on Information Systems (AMCIS 2014), Savannah, Georgia, USA. http://eprints.gla.ac.uk/114468/

Grispos, G., Glisson, W. B., & Storer, T. (2017). Enhancing security incident response follow-up efforts with lightweight agile retrospectives. *Digital Investigation: The International Journal of*

Digital Forensics & Incident Response, *22*(C), 62–73. https://doi.org/10.1016/j.diin.2017.07.006

Grispos, G., Glisson, W., & Storer, T. (2015, June 26). Security Incident Response Criteria: A Practitioner's Perspective. *Americas Conference on Information Systems (AMCIS 2015)*. https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/35

Gupta, M., George, J. F., & Xia, W. (2019). Relationships between IT department culture and agile software development practices: An empirical investigation. *International Journal of Information Management*, *44*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.09.006

Gurkok, C. (2017). Cyber Forensics and Incidence Response. In *Computer and Information Security Handbook* (pp. 603–628). Elsevier. https://doi.org/10.1016/B978-0-12-803843-7.00041-7

Hadar, E., & Hassanzadeh, A. (2019). Big Data Analytics on Cyber Attack Graphs for Prioritizing Agile Security Requirements. *2019 IEEE 27th International Requirements Engineering Conference (RE)*, 330–339. https://doi.org/10.1109/RE.2019.00042

He, Y., & Janicke, H. (2015, September 1). Towards Agile Industrial Control Systems Incident Response. *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) (ICS-CSR)*. https://doi.org/10.14236/ewic/ICS2015.11

He, Y., & Johnson, C. (2015). Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template. *International Journal of Medical Informatics*, *84*(11), 941–949. https://doi.org/10.1016/j.ijmedinf.2015.08.010

Heathcote, A. (2017a). *Hardware and Software Security. Good Practice Guide*. NHS Digital. https://technodocbox.com/Network_Security/68832843-Hardware-and-software-security.html

Heathcote, A. (2017b). *Information Security Incident. Good Practice Guide*. NHS Digital. https://technodocbox.com/Data_Centers/69196057-Information-security-incident.html

Hemon-Hildgen, A., Rowe, F., & Monnier-Senicourt, L. (2020). Orchestrating automation and sharing in DevOps teams: A revelatory case of job satisfaction factors, risk and work conditions. *European Journal of Information Systems*, *29*(5), 474–499. https://doi.org/10.1080/0960085X.2020.1782276

HIMSS. (2018). *2018 HIMSS Cybersecurity Survey*. HIMSS. https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Ho, S. M., Kao, D., & Wu, W.-Y. (2018). Following the breadcrumbs: Timestamp pattern identification for cloud forensics. *Digital Investigation*, *24*, 79–94. https://doi.org/10.1016/j.diin.2017.12.001

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports*, *2*, 100076. https://doi.org/10.1016/j.fsir.2020.100076

HSE. (2018). *Incident Management Framework*. Quality Assurance and Verification Division, HSE. https://www.hse.ie/eng/about/qavd/incident-management/hse-2018-incident-management-framework-guidance-stories1.pdf

Information Security Media Group. (2013). *The Need for Speed: 2013 Incident Response Survey*. Bank Info Security. https://www.bankinfosecurity.com/handbooks/need-for-speed-2013-incident-response-survey-h-44

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1), 26–37. https://doi.org/10.1016/j.ijcip.2009.02.004

Janssen, M., & van der Voort, H. (2020). Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic. *International Journal of Information Management*, *55*, 102180. https://doi.org/10.1016/j.ijinfomgt.2020.102180

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). DATA BREACH MANAGEMENT: AN INTEGRATED RISK MODEL. *Information & Management*, *58*(1), 103392. https://doi.org/10.1016/j.im.2020.103392

Khan, F., Kim, J. H., Moore, R., & Mathiassen, L. (2019, July 4). Data Breach Risks and Resolutions: A Literature Synthesis. *25th Americas Conference on Information Systems (2019)*. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/14

Kondo, S., Sakashita, H., Sato, S., Hamaguchi, T., & Hashimoto, Y. (2018). An application of STAMP to safety and cyber security for ICS. In M. R. Eden, M. G. Ierapetritou, & G. P. Towler (Eds.), *Computer Aided Chemical Engineering* (Vol. 44, pp. 2335–2340). Elsevier. https://doi.org/10.1016/B978-0-444-64241-7.50384-0

Laanti, M., Salo, O., & Abrahamsson, P. (2011). Agile methods rapidly replacing traditional methods at Nokia: A survey of opinions on agile transformation. *Information and Software Technology*, *53*(3), 276–290. https://doi.org/10.1016/j.infsof.2010.11.010

Lamis, T. (2010). A forensic approach to incident response. *2010 Information Security Curriculum Development Conference*, 177–185. https://doi.org/10.1145/1940941.1940975

Larson, D., & Chang, V. (2016). A review and future direction of agile, business intelligence, analytics and data science. *International Journal of Information Management*, *36*(5), 700–710. https://doi.org/10.1016/j.ijinfomgt.2016.04.013

Lindstrom, L., & Jeffries, R. (2004). Extreme Programming and Agile Software Development Methodologies. *Information Systems Management*, *21*(3), 41–52. https://doi.org/10.1201/1078/44432.21.3.20040601/82476.7

Mattord, H. J., & Whitman, M. E. (2014). *Business Continuity State of the Industry Report*. Elsevier.

Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. *Computers & Security*, *73*, 87–101. https://doi.org/10.1016/j.cose.2017.10.009

Mergel, I., Gong, Y., & Bertot, J. (2018). Agile government: Systematic literature review and future research. *Government Information Quarterly*, *35*(2), 291–298. https://doi.org/10.1016/j.giq.2018.04.003

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*, *25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Moyón, F., Méndez, D., Beckers, K., & Klepper, S. (2020). How to Integrate Security Compliance Requirements with Agile Software Engineering at Scale? In M. Morisio, M. Torchiano, & A. Jedlitschka (Eds.), *Product-Focused Software Process Improvement* (pp. 69–87). Springer International Publishing. https://doi.org/10.1007/978-3-030-64148-1_5

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 113476. https://doi.org/10.1016/j.dss.2020.113476

Neubauer, T., & Heurix, J. (2008). Defining Secure Business Processes with Respect to Multiple Objectives. *2008 Third International Conference on Availability, Reliability and Security*, 187–194. https://doi.org/10.1109/ARES.2008.174

NHS England. (2018). *Information Security Policy*. NHS England. https://www.england.nhs.uk/wp-content/uploads/2016/12/information-security-policy-v4.0.pdf

NHS NWL. (2018). *Information Security Policy*. NHS North West London Collaboration of Clinical Commissioning Groups. https://www.england.nhs.uk/wp-content/uploads/2016/12/information-security-policy-v4.0.pdf

Nnoli, H., Lindskog, D., Zavarsky, P., Aghili, S., & Ruhl, R. (2012). The Governance of Corporate Forensics Using COBIT, NIST and Increased Automated Forensic Approaches. *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, 734–741. https://doi.org/10.1109/SocialCom-PASSAT.2012.109

O'Dowd, A. (2017). Major global cyber-attack hits NHS and delays treatment. *BMJ*, *357*, j2357. https://doi.org/10.1136/bmj.j2357

Papastergiou, S., Mouratidis, H., & Kalogeraki, E.-M. (2020). Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. *Evolving Systems*. https://doi.org/10.1007/s12530-020-09335-4

Papastergiou, S., Mouratidis, H., & Kalogeraki, E.-M. (2019). Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE). In J. Macintyre, L. Iliadis, I. Maglogiannis, & C. Jayne (Eds.), *Engineering Applications of Neural Networks* (pp. 476–487). Springer International Publishing. https://doi.org/10.1007/978-3-030-20257-6_41

Poba-Nzaou, P., Marsan, J., Pare, G., & Raymond, L. (2014). *Governance of Open Source Electronic Health Record Projects: A Successful Case of a Hybrid Model*. 2798–2807. https://doi.org/10.1109/HICSS.2014.350

Pries-Heje, J., & Baskerville, R. (2017). The translation and adaptation of agile methods: A discourse of fragmentation and articulation. *Information Technology & People*, *30*(2), 396–423. https://doi.org/10.1108/ITP-08-2013-0151

Rezvani, A., & Khosravi, P. (2019). Emotional intelligence: The key to mitigating stress and fostering trust among software developers working on information system projects. *International Journal of Information Management*, *48*, 139–150. https://doi.org/10.1016/j.ijinfomgt.2019.02.007

Roumani, Y., & Nwankpa, J. K. (2019). An empirical study on predicting cloud incidents. *International Journal of Information Management*, *47*, 131–139. https://doi.org/10.1016/j.ijinfomgt.2019.01.014

Schuh, G., Rebentisch, E., Riesener, M., Diels, F., Dolle, C., & Eich, S. (2017). Agile-waterfall hybrid product development in the manufacturing industry—Introducing guidelines for implementation of parallel use of the two models. *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 725–729. https://doi.org/10.1109/IEEM.2017.8289986

Serrador, P., & Pinto, J. K. (2015). Does Agile work? — A quantitative analysis of agile project success. *International Journal of Project Management*, *33*(5), 1040–1051. https://doi.org/10.1016/j.ijproman.2015.01.006

Shedden, P., Ahmad, A., & Ruighaver, A. (2011). Informal Learning in Security Incident Response Teams. *ACIS 2011 Proceedings*. https://aisel.aisnet.org/acis2011/37

Shukla, M., Johnson, S. D., & Jones, P. (2019). Does the NIS implementation strategy effectively address cyber security risks in the UK? *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–11. https://doi.org/10.1109/CyberSecPODS.2019.8884963

Sidky, A., Arthur, J., & Bohner, S. (2007). A disciplined approach to adopting agile practices: The agile adoption framework. *Innovations in Systems and Software Engineering*, *3*(3), 203–216. https://doi.org/10.1007/s11334-007-0026-z

Singh, B., & Gupta, G. (2019). Analyzing Windows Subsystem for Linux Metadata to Detect Timestamp Forgery. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics XV* (pp. 159–182). Springer International Publishing. https://doi.org/10.1007/978-3-030-28752-8_9

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Smith, R., Janicke, H., He, Y., Ferra, F., & Albakri, A. (2021). The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. *Computers & Security*, *109*, 102398. https://doi.org/10.1016/j.cose.2021.102398

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management*, *58*, 102298. https://doi.org/10.1016/j.ijinfomgt.2020.102298

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., Zaccaro, S. J., Dalal, R. S., & Tetrick, L. E. (2015). Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *IEEE Security Privacy*, *13*(4), 20–29. https://doi.org/10.1109/MSP.2015.71

Symantec. (2018). *Cyber Security and Healthcare: An Evolving Understanding of Risk*. https://docs.broadcom.com/doc/2018-istr-executive-summary-for-healthcare-professionals-en

Tam, C., Moura, E. J. da C., Oliveira, T., & Varajão, J. (2020). The factors influencing the success of on-going agile software development projects. *International Journal of Project Management*, *38*(3), 165–176. https://doi.org/10.1016/j.ijproman.2020.02.001

Tan, C., Ruighaver, A., & Ahmad, A. (2003, January 1). *Incident Handling: Where the need for planning is often not recognised.* 1st Australian Computer, Network and Information Forensics Conference.

Thompson, E. C. (2018). *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*. Apress.

Tolfo, C., Wazlawick, R. S., Ferreira, M. G. G., & Forcellini, F. A. (2011). Agile methods and organizational culture: Reflections about cultural levels. *Journal of Software Maintenance and Evolution: Research and Practice*, *23*(6), 423–441. https://doi.org/10.1002/smr.483

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42–57. https://doi.org/10.1016/j.cose.2014.05.003

Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management & Computer Security*, *18*(1), 26–42. https://doi.org/10.1108/09685221011035241

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43–57. https://doi.org/10.1016/j.ijinfomgt.2003.12.003

Wiik, J., Gonzalez, J. J., & Kossakowski, K.-P. (2005). Limits to Effectiveness in Computer Security Incident Response Teams. *23rd International Conference of the System Dynamics Society*.

Williams, J. (2012). *ACPO good practice guide for digital evidence* (No. 5). Metropolitan Police Service, Association of chief police officers. Police Central e-Crime Unit. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Williams, L., & Cockburn, A. (2003). Agile software development: It's about feedback and change. *Computer*, *36*(6), 39–43. https://doi.org/10.1109/MC.2003.1204373

CRediT Author Statement

Ying He: Conceptualization, Methodology, Investigation, Validation, Resources, Project administration, Supervision, Writing - original draft, Writing - review & editing.
Stefan Lloyd: Conceptualization, Methodology, Investigation, Writing - original draft.
Efpraxia D. Zamani: Methodology, Validation, Writing - original draft, Writing - review & editing.
Cunjin Luo: Conceptualization, Validation, Writing - original draft, Writing - review & editing, Funding acquisition