Enhancing Security Incident Response Follow-up Efforts with Lightweight Agile Retrospectives

George Grispos[a,*], William Bradley Glisson[b], Tim Storer[c]

[a]*School of Interdisciplinary Informatics, University of Nebraska at Omaha, Omaha, NE, United States*
[b]*School of Computing Science, University of South Alabama, Mobile, AL, United States*
[c]*School of Computing Science, University of Glasgow, Glasgow, Scotland*

Abstract

Security incidents detected by organizations are escalating in both scale and complexity. As a result, security incident response has become a critical mechanism for organizations in an effort to minimize the damage from security incidents. The final phase within many security incident response approaches is the feedback/follow-up phase. It is within this phase that an organization is expected to use information collected during an investigation in order to learn from an incident, improve its security incident response process and positively impact the wider security environment. However, recent research and security incident reports argue that organizations find it difficult to learn from incidents.

A contributing factor to this learning deficiency is that industry focused security incident response approaches, typically, provide very little practical information about tools or techniques that can be used to extract lessons learned from an investigation. As a result, organizations focus on improving technical security controls and not examining or reassessing the effectiveness or efficiency of internal policies and procedures. An additional hindrance, to encouraging improvement assessments, is the absence of tools and/or techniques that organizations can implement to evaluate the impact of implemented enhancements in the wider organization. Hence, this research investigates the integration of lightweight agile retrospectives and meta-retrospectives, in a security incident response process, to enhance feedback and/or follow-up efforts. The research contribution of this paper is twofold. First, it presents an approach based on lightweight retrospectives as a means of enhancing security incident response follow-up efforts. Second, it presents an empirical evaluation of this lightweight approach in a Fortune 500 Financial organization's security incident response team.

Keywords: Security Incident Response, Security Investigations, Case Study, Retrospectives, Incident Learning.

*Corresponding author
Email addresses: grisposg@acm.org (George Grispos), bglisson@southalabama.edu (William Bradley Glisson), timothy.storer@glasgow.ac.uk (Tim Storer)

1. Introduction

Information security incidents continue to escalate in today's highly integrated business environments. According to a recent survey, a quarter of all businesses in the United Kingdom detected a security incident in the previous twelve months (Klahr et al., 2016). The consequences of such incidents for an organization can include significant financial losses, a loss of customer confidence and a reduction in business reputation (Ponemon Institute, 2015). In an effort to address information security incidents, many organizations have chosen to create security incident response teams (Killcrece et al., 2003; Mitropoulos et al., 2006). The objective of a security incident response team is to minimize the damage from a security incident, and to allow an organization to ultimately learn about the cause of the incident and how it can be prevented in the future (Mitropoulos et al., 2006).

In the past decade, several security incident response processes and best practice guidelines have been published in industry (Grance et al., 2004; International Organization for Standardization and International Electrotechnical Commission, 2011; Northcutt, 2001) and academia (Mitropoulos et al., 2006; Prosise et al., 2003; Vangelos, 2011), defining how organizations can investigate and manage a security incident. Typically, these incident response approaches consist of six phases: *preparation*, which leads to the *detection* of an incident, followed by its *containment* which, in turn, allows security incident response teams to *eradicate*, *recover* and then, potentially, provide *feedback* information into the next preparation stage. The final phase within many security incident response approaches is the feedback/follow-up phase (Mitropoulos et al., 2006; Northcutt, 2001). Information collected during an investigation is used in this phase to learn wider lessons from the security incident, with the aim of preventing a reoccurrence of the incident (He, 2014; Mitropoulos et al., 2006). Incident learning is usually accomplished through a series of formal reports, meetings and presentations to management (Northcutt, 2001). Lessons learned can include actions taken during the investigation, enhancing existing security controls and identifying modifications to security incident response processes (Mitropoulos et al., 2006).

Although security incident response approaches stress the importance of incident learning, researchers have observed that many organizations find it difficult to learn from security incidents (Ahmad et al., 2012; Shedden et al., 2010, 2011). A contributing factor is that although many incident response approaches incorporate a feedback/follow-up phase, these approaches provide very little practical information about the tools or the techniques that can be used to extract lessons learned from an investigation (He et al., 2014). As a result, organizations tend to focus on improving technical controls and do not reassess the effectiveness of internal policies and procedures, which could also have contributed to the incident or obstructed investigative efforts (He et al., 2014). Moreover, if an organization does extract lessons learned from

an investigation, there is currently very limited tool or technique support for organizations to evaluate if these enhancements have actually been implemented in the wider organization (Grispos, 2016).

Retrospectives are an agile practice commonly used by software development teams (Derby et al., 2006). The purpose of a retrospective is to provide a lightweight approach to identify what worked and what did not work during the previous development iteration and use this information to reflect on and improve the processes used by the development team (Derby et al., 2006; Pham, 2011). In fact, previous research supports the idea that retrospectives can have a positive effect on agile development processes improvement (Maham, 2008; McHugh et al., 2012; Tiwari and Alikhan, 2011). This information prompted the hypothesis that *integrating lightweight agile retrospectives, in a security incident response environment, will enhance feedback and/or follow-up efforts.* In order to address the hypothesis, the following research questions were identified:

1. What components of a retrospective need to be modified for use in security incident response?
2. Do retrospectives assist with identifying and documenting additional information about a security investigation that, otherwise, may not be documented within a corresponding investigation record?
3. Do retrospectives assist a security incident response team in identifying and documenting security controls?
4. Do retrospectives assist a security incident response team in identifying and documenting security incident response-related process changes?
5. To what extent can a meta–retrospective highlight how many security controls and security incident response-related process changes are actually implemented within an organization?

Hence, this work investigates the impact of integrating lightweight agile retrospectives into a security incident response environment with the aim of implementing a process of on-going and incremental improvement. In addition to implementing retrospectives in a security incident response environment, a retrospective of retrospectives (hereafter referred to as a meta–retrospective) was also implemented in the same environment. The purpose of the meta–retrospective was to evaluate if any security controls and/or security incident response-related process improvements, identified during a retrospective, were actually implemented within an organization. The research contribution of this paper is twofold. First, it presents an approach based on lightweight retrospectives as a means of enhancing security incident response follow-up efforts. Second, it presents an empirical evaluation of this lightweight approach in a Fortune 500 Financial organization's security incident response team. The results of this evaluation indicate that it is a plausible solution for driving the development of lessons learned in security incident response.

Highlights of the retrospective/meta-retrospective implementation in this case study involving the Fortune 500 organization revealed:

- In one hundred forty-eight (148) out of the three hundred and twenty-four (324) retrospectives conducted, more information was revealed when compared with the corresponding record of the actual investigation (see Table 5 for further details). This indicates that more relevant information is often available, which can be identified and documented through further reflection and consideration.
- Security incident handlers in an organization need to communicate with a wide range of individuals internally and externally (see Section 4.1 for details). This finding suggests the importance of up-to-date contact lists, alternative contact mechanisms (potentially out-of-band channels) and a routinized way to document who was contacted and what was discussed or decided.
- In twenty-five (25) out of the three hundred and twenty-four (324) retrospectives conducted, a single security control could have prevented a security event/incident from occurring. In four (4) other retrospectives, two security controls could have prevented the security event/incident from occurring. See Table 3 and associated discussion for further details.
- The retrospectives implementation also revealed that process changes were required and, in certain cases, that completely new processes needed to be developed to assist incident handlers investigating similar future security events/incidents.
- Security incident handlers lost opportunities to investigate because relevant data sources were not always preserved (for example, Lotus Notes email, virtual machines) for a variety of reasons. This indicates a need for improved communication and coordination when an incident occurs, and for improved processes to 'freeze' relevant data sources.
- The meta-retrospectives implementation revealed that forty-two (42) out of the sixty-five (65) potential improvements identified using the retrospectives were implemented. However, the meta-retrospectives also identified that fifteen (15) out of the sixty-five (65) recommendations could not be made until they were escalated to senior management within the Information Security unit. See Table 4 for more details.
- Six (6) out of the sixty-five (65) security control and process changes identified in the retrospectives resulted in 'No Changes' being made within the organization. This is largely because the organization's security incident response team does not have authority over all the processes within the organization.

Overall, those involved in the retrospective implementation perceived the following benefits/advantages:

- That additional information was captured through the retrospectives, including information regarding data sources, contact information, and process changes/improvements.

- The retrospectives helped to provide a 'safety-net mechanism' to help document security control modifications. They also assisted with the identification of important stakeholders whose assistance could be required in resolving investigations quicker and more effectively in the future.
- Provided a mechanism for incident handlers to identify and document security incident response-related process improvements to help investigators in the future.

The remainder of this paper is structured as follows. Section two discusses relevant previous work and section three describes the research methodology. Section four presents the data collected using the retrospectives and the meta–retrospectives, along with an analysis of the results. Section five discusses the implications of the research findings and section six draws conclusions and presents future work.

2. Related Work

In today's digitally integrated environment, it is understandable that organizations are examining different security incident response approaches, for the purpose of formalization (Killcrece et al., 2003). As a result, a consensus as to the standardization, effectiveness and efficiency of these approaches is yet to emerge (Killcrece et al., 2003; Alberts et al., 2004; Wiik et al., 2005). While numerous security incident response processes have been discussed in the literature, Hove et al. (2014) argue that many organizations find it difficult to implement established security incident response processes. This is evident in an analysis of empirical case studies conducted, in various organizations, which have identified several problems and challenges with these approaches.

Grimes (2007) argued that traditional security incident response models have become outdated and are no longer suited to manage today's security incidents. Werlinger et al. (2010), add that current security incident response tools do not appropriately support the highly collaborative nature of security investigations and that incident handlers often need to develop their own tools to perform specific tasks. Tan et al. (2003) explored the factors that influenced information security managers to avoid conducting investigations subsequent to a security incident. Tan et al. (2003) reported that their studied organization had no clear definition for the term 'security incident'. As a result, incident handlers did not realize what security problems were actually 'incidents' and were slow to react to real security incidents. Hove et al. (2014) studied three large organizations with the purpose of investigating the plans and procedures for handling security incidents within the studied organizations. Hove et al. (2014) identified that although the organizations have plans and procedures in place, based on industry best practices, many other procedures were missing from the studied organizations. For example, in two of the organizations, security incident reporting procedures were not established while the other organization did not appear to have enough staff to respond to incidents efficiently (Hove et al.,

2014). Grispos et al. (2017b) investigated the ability for employees to identify a security incident in technology–focused and non–technology–focused business units within an organization. The results of this study indicated that there are opportunities to improve security incident recognition and reporting within the organization. These include focusing education initiatives on activities that will provide employees with information on 'what to do' and 'when to do it' when they identify or detect an incident and clarifying corporate policy with regard to incident reporting (Grispos et al., 2017b).

Several researchers focused on how current approaches do not adequately support security incident learning (Ahmad et al., 2012; Shedden et al., 2010, 2011; Tan et al., 2003; Jaatun et al., 2009). Ahmad et al. (2012) argue that the 'feedback' phase is often skipped because security incident response teams are too focused on containment, eradication, and recovery. In a study involving the petroleum industry, Jaatun et al. (2009) explained that while learning from security incidents was considered important, organizations found it difficult to implement the concept in practice. Jaatun et al. (2009) go on to argue that organizations must be prepared for incident learning and this includes obtaining managerial commitment and the willingness to commit resources to facilitate learning from security incidents. This is a view that is shared by Tan et al. (2003), who also noted that their studied organization was not prepared to gather data or learn from security incidents. While the above researchers have argued that organizations need to do more to effectively learn from a security incident, Shedden et al. (2010) argue that current best practices and approaches do not provide enough guidance and support as to how this can be achieved. In another publication, Shedden et al. (2011) state that "researchers and practitioners must accept that informal activities will occur below the surface in security incident response"; hence, security incident response approaches should be less formal and cater to informal learning approaches. The authors go on to report that within their studied organization, incident handlers were undertaking informal learning through conversation and observation. While Shedden et al. (2011) propose that security incident learning should be informal within organizations, very few informal tools have been proposed in the literature to help organizations undertake security incident learning.

In order to address some of these problems, Grispos et al. (2014) proposed the integration of agile principles into security incident response processes as one solution to strengthening an organization's security incident response posture. Grispos et al. (2014) argue that the agile principles, such as iterative and incremental incident handling, reducing uncertainty, and continuous attention to technical excellence could enhance real–world security incident response efficiencies and effectiveness. Grispos et al. (2015) also proposed Security Incident Response Criteria (SIRC) for the evaluation of security incident response tactics being implemented in practice. Four of the criteria: dynamic stakeholder involvement, multidisciplinary security incident response teams, short investigation lifecycle times and incident learning throughout the incident lifecycle can be closely aligned to agile practices and principles. From an industrial control system perspective, He and Janicke (2015) discussed how security incident re-

sponse processes might benefit from the integration of agile principles. He and Janicke noted that future work should investigate mapping traditional incident response processes to agile methodologies in order to determine which methodology would be more suited for security incident response (He and Janicke, 2015). A limitation of these proposals is that they do not investigate specific agile practices in real-world incident scenarios.

The last principle within the Agile Manifesto proposes that "at regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly" (Beck et al., 2001). The basis for this principle is that no software development process is perfect and that agile development teams will encounter new and unique situations whenever they take on software projects (Shore, 2007). As a result, agile development teams are encouraged to continually inspect, reflect and adapt their development processes to match their changing environments (Maham, 2008; Shore, 2007). A common technique used by agile development teams to achieve this objective is the *retrospective* (Derby et al., 2006). Agile development teams will typically undertake a retrospective at the end of the development iteration (Derby et al., 2006). The purpose of the retrospective is to identify what 'worked well' and 'what did not work well' during the most recent development iteration (Derby et al., 2006). Development teams can also use retrospectives to determine if there is anything they can learn from their experience that will improve the next iteration (Pham, 2011). Agile teams can also use retrospectives to understand the reasons behind missed targets, finding ways to improve responses to customers and re-building damaged relationships (Derby et al., 2006).

Several studies have examined the positive effect of retrospectives on agile development teams (Maham, 2008; McHugh et al., 2012; Tiwari and Alikhan, 2011). Maham (2008) studied how a Scrum team performed retrospectives after a three-week Sprint. The results from the study showed that the team members highlighted what had worked well and what could be improved on from the previous Sprint. Areas of improvement were then prioritized and implemented in the next Sprint (Maham, 2008). Tiwari and Alikhan (2011) changed the scope and method of retrospectives and decided to include customers in the practice, instead of just the development team (Tiwari and Alikhan, 2011). The perceived benefit of this modification was that it would provide customers with an opportunity to hear first-hand about the team's performance in the previous iterations (Tiwari and Alikhan, 2011). Tiwari and Alikhan reported that after a few retrospectives, the customers noted that they felt like they were a part of the agile team and could contribute towards the development of their product (Tiwari and Alikhan, 2011). McHugh et al. (2012) studied three separate agile teams to examine if agile practices enhanced trust among team members. All three teams agreed that retrospectives provided transparency and visibility regarding the achievement of Sprint goals.

Multiple agile teams can often be working on the same product or project. Often, each team will do their own retrospective and then look to conduct a retrospective of retrospectives (Gonçalves and Linders, 2013). Gonçalves and Linders (2013) describe a retrospective of retrospectives as a method of im-

proving collaboration between the various agile teams. Retrospectives of retrospectives can also be viewed as a tool for sharing information between teams (Gonçalves and Linders, 2013). While retrospectives and meta-retrospectives have been used to inspect and adapt agile development processes, minimal research has examined the integration of these two agile practices in a security incident response context.

3. Research Methodology

In order to empirically evaluate the use of retrospectives as a method for enhancing the feedback/follow-up phase within security incident response, a case study was conducted in Fortune 500 Financial organization. The case study was completed between February 2014 and March 2015. The name of the organization is being withheld to ensure organizational anonymity. Therefore, the names of organizational documents and processes have been altered and the results of data collected in the organization are presented anonymously. Maintaining organizational anonymity helps attain sensitive material, while creating an environment that is conducive to the presentation of this information. The case study utilizes a mixed method approach to the collection of data (Oates, 2005). The overall data flow and the data collection process executed in the case study is illustrated in Figure 1 - Research Process.

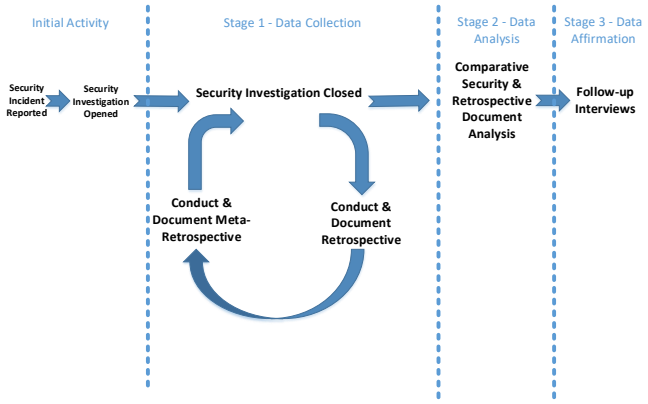

Figure 1: Research Process

The organization's Information Security Incident Response (ISIR) team uses a customized security incident response process. This process consists of four phases: incident detection and reporting; recording, classification and assignment; investigation and resolution; and incident closure. For the purposes of this discussion, these activities are represented in Figure 1 as Security Incident Reported, Security Investigation Opened and Security Investigation Closed. In this environment, a Security Incident Handler (SIH) facilitates and coordinates the organization's response to a security incident. At the 'incident closure' stage

of the process, SIHs are prompted to document findings obtained from a security investigation in an investigation record, which is then stored in a database. Documentation is typically done throughout the investigation, as well as at the closure of the incident.

The first stage in the research process (Stage 1 – Data Collection) monitors the security investigation record database, in order to identify and document when an investigation record was closed by a SIH. The identification of a closed investigation record prompts the second step in the first stage of the data collection. This involves the primary author performing face-to-face retrospectives with the SIH identified from the investigation record. A pragmatic decision based on time constraints, data richness and potential data depth prompted the use of questions as a method for conducting the retrospectives. The advantage of using open-ended questions is that in-depth information can, potentially, be obtained from participating individuals which encourages clustering and pattern identification which is needed to identify improvement actions (Oates, 2005). The questions used in the retrospectives with the SIHs were as follows:

1. Which information assets did you need to investigate in this security event/incident?
2. Which information asset could you not investigate in this security event/ incident?
3. Who did you need to communicate with during this security event/ incident?
4. Who could you not communicate with during this security event/incident?
5. What security controls could have prevented the security event/incident from occurring?
6. What process changes would assist investigating a similar security event/ incident in the future?

In this case study, responses to the retrospective questions were initially recorded by hand and then digitally documented. Each retrospective lasted approximately ten minutes and was conducted at the SIH's desk. In software development, retrospectives are typically held at the end of a development iteration (Derby et al., 2006). However, unlike agile software development, where work is broken down into iterations, security incident response investigations generally stop at the end of an investigation (i.e. the end of the process lifecycle) (Mitropoulos et al., 2006). Therefore, the retrospectives within a security incident response lifecycle were undertaken at the end of each security investigation. It was anticipated that a retrospective would typically be conducted within one–to–three days after the closure of an investigation record. In practice, approximately 92% of the retrospectives were held within this time frame and the longest time between the closure of an investigation and a retrospective was seven days.

The ISIR team was allotted four weeks to implement any security controls and/or security incident response-related process changes identified in the retrospective. After this time period, the third step in the first stage of the data collection process is to conduct a meta–retrospective. The meta–retrospectives are

conducted to evaluate if the security controls and/or security incident response-related process changes identified during the retrospectives were implemented within the organization. The meta–retrospective consist of asking two questions:

1. Have the security controls you identified in the retrospective been implemented? If No, why not?
2. Have the process changes you identified in the retrospective been made? If No, why not?

A meta–retrospective was only undertaken when a SIH identified either a security control and/or process change during the initial retrospective. Hence, meta–retrospectives were undertaken with the same SIH involved in the initial retrospective. Each meta-retrospective lasted approximately five minutes and was conducted at the SIH's desk. The SIH's responses were initially recorded by hand and then digitally documented.

The second stage of the research process (Stage 2 – Data Analysis) is a comparative document analysis (Oates, 2005). This analysis incorporates the retrospectives and the corresponding investigation records. The document analysis aspect of this case study was conducted in March of 2015 and involved examining the answers from the retrospective questions with the information documented in the corresponding investigation record. The comparative analysis involved examining all of the investigation records and retrospectives that were undertaken in the organization. The purpose of the document analysis was to determine if a particular retrospective identified more or less information when compared to its associated investigation record.

At the conclusion of the document analysis, the third stage of the research process (Stage 3 – Data Affirmation) uses semi–structured interviews to clarify the impact that the retrospectives have on the organization. The interview instrument establishes the participant's credentials and then proceeds to inquire about what worked well, what did not work well, and process modifications. The interview instrument in this case study consisted of both open-ended and closed questions. To mitigate researcher bias in terms of reliability and viability, the interview instrument was validated by two security professionals (Kitchenham and Pfleeger, 2002). An information security manager and a senior security analyst validated the instrument by taking the interview and providing feedback. The feedback from these individuals ranged from simplifying open-ended questions to adding response options to closed questions. This validation was only conducted once due to time constraints. Interviews were undertaken with individuals who had participated in the retrospectives. In addition, the organization's security incident response policy owner was also interviewed. Although this individual did not participate in the retrospectives, he/she had an overview of how the retrospective was implemented within the organization. The interviews were conducted at the participant's desk within the organization. All responses to the individual questions were initially recorded by hand and then digitally recorded soon after the interview was completed, typically within an hour. The results were then examined by hand to identify trends, patterns, and anomalies.

The scope of this research is limited from the following perspectives. This research consists of a single case study in a Fortune 500 Financial organization based in the United Kingdom. Hence, factors potentially impacting the case study include international, national and local regulatory requirements, along with societal and organizational cultural issues. It should also be noted that the primary researcher was embedded in the organization for several months along with being the primary data collector. Hence, the potential influence and impact of the primary researcher has to be acknowledged.

4. Data Collection and Analysis

This section presents the results of the data collection from the implementation of the retrospectives and meta-retrospectives within the Fortune 500 Organization.

4.1. Retrospectives

Three hundred and twenty-four (324) retrospectives were conducted between February 2014 and March 2015. All of the retrospectives were conducted with six different Security Incident Handlers (SIHs). A summary of the data collected using the retrospectives is presented in Table 1 and discussed in more detail below.

Question Number	Retrospective Data	Total
1	Assets Investigated	502
2	Assets Not Investigated	22
3	Individuals/Groups Communicated	737
4	Individuals/Groups Not Communicated	5
5	Security Controls Identified	36
6	Process Changes Identified	29

Table 1: Retrospectives Summary

Question one was answered in all three hundred and twenty-four (324) retrospectives. A total of five hundred and two (502) information assets were identified in this question. For the purpose of this work, an information asset is defined as any tangible or intangible system or data that has value to an organization (International Organization for Standardization and International Electrotechnical Commission, 2013). The collected data indicates that more than half (280 assets) of the investigations involved the organization's email assets and associated logs. An example investigation from the email group could perceivably be an inquiry into potential data leakage via the email service. Furthermore, the SIHs also indicated that access to security-specific assets was also needed in their investigation, with 162 such assets being involved these investigations. The remaining assets identified through this question include data repositories and databases (18 assets), network devices, servers and logs

(15 assets), third-party assets (9 assets), organization-specific assets (7 assets), desktops and laptops (6 assets) and Intranet/Internet-based assets (5 assets).

For question two, the SIHs indicated that there were eighteen (18) investigations where they encountered problems investigating an asset or assets. The answer provided in the remaining three hundred and six (306) retrospectives was "none". The SIHs indicated that they had encountered problems investigating nine (9) individual information assets. In total, twenty-two (22) assets were identified as not being investigated from eighteen (18) retrospectives, with three (3) of these information assets identified in more than one (1) retrospective. Table 2 – Information Assets Not Investigated provides an overview of the information assets, which the SIHs indicated during the retrospectives they could not investigate along with the reason.

The table shows that SIHs could not investigate a variety of information assets. These include virtual machines that have since been deactivated and deleted, expired email accounts and missing email attachments due to expired retention periods. One observation from Table 2 is that the ability to investigate an asset is largely due to factors outside of the control of the SIHs. For example, in nine (9) investigations the SIHs required access to a Lotus Notes mail file. However, the retention period for these mail files had expired and was no longer available for examination. It is also worth noting that in one retrospective, one of the SIHs indicated that the reason why they could not investigate the contents of the Windows Registry was due to limited tool access. This supports previous findings that individuals within security incident response, often need specialized tools and/or they have to develop their own tools to perform specific exploratory tasks (Werlinger et al., 2010).

The third retrospective question was answered in all three hundred and twenty-four (324) retrospectives. The SIHs indicated that, in addition to the individuals affected by an incident and the individuals within the security incident response team, they needed to communicate with fifty-five (55) different individuals or teams during an investigation. In total, seven hundred and thirty seven (737) names of individuals or teams were provided in response to this question. The data collection from this question indicated that the SIHs needed to communicate with individuals affected by a security incident, relevant managers or team leaders in three hundred and twenty-three (323) investigations. Moreover, individuals within the Physical and Information Security unit were required in one hundred and fifty-four (154) investigations, and individuals within the Email and Information Technology (IT) Services unit in one hundred and twenty-nine (129) investigations. In addition, the SIHs required the assistance of external individuals, including third-party vendors, were required for forty-two (42) investigations, legal and regulatory teams in fifty-eight (58) investigations, customer-facing units in twenty-one (21) investigations, and software development/support units in ten (10) investigations. The results from this retrospective question support previous findings that security incident response teams often need to collaborate with a variety of individuals and organizational teams during an investigation (Grispos et al., 2017a; Werlinger et al., 2007).

With regard to question four, the SIHs identified five scenarios where com-

Information Asset Name	Total	Reason Provided
Deleted Email Messages	1	The Email Recovery Unit could not recover the deleted emails needed for the investigation.
Email Attachments	3	Email attachments that were required for the investigation were no longer available because the data retention period had expired.
Encrypted File Contents	4	The decryption key was no longer available because the retention period had expired.
Laptop Computer	1	The Security Incident Handler was not requested to perform a deeper analysis.
Email Account	1	The email account could no longer be accessed as it was disabled after the individual left the organization.
Lotus Notes Mail File	9	Data retention period had expired at the time of the investigation.
Organization-specific Asset	1	The system owner was not available during the course of the investigation.
Virtual Machines	1	The virtual machines were deactivated and deleted before they could be investigated.
Windows Registry Settings	1	A lack of available tools.
Total	**22**	

Table 2: Information Assets Not Investigated

munication was a problem during an investigation. A total of four individuals were identified through this question, with one individual being identified twice. In four retrospectives, the individuals were asset owners and their assistance was required to gather data from the asset. In the fifth retrospective, an individual's assistance was required because he/she was a managerial figure for an individual affected by an investigation. The communication problems were generally caused by outdated contact information (four investigations) and absent individuals, away on vacation (one investigation).

With regard to question five, the SIHs indicated that in thirty (30) investigations, security controls could have prevented the security event/incident from occurring. In the remaining retrospectives, the SIHs indicated that no security control could have prevented the incident (179 investigations) or the question was not applicable (115 investigations). Thirty-six (36) security controls were identified from the thirty (30) retrospectives. Within twenty-five (25) retrospectives, a single security control was identified, which could have prevented the security problem, while in four (4) retrospectives, the SIHs indicated that two (2) security controls would be required. In one (1) retrospective, three (3) security controls were identified. The security controls identified by the SIHs, in response to this retrospective question, have been mapped to eight out of the fourteen relevant domains within the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002, Information Security standard (International Organization for Standardization and International Electrotechnical Commission, 2013). Table 3 – Security Controls Identified, categorizes the number of controls identified using relevant domains from the ISO/IEC standard.

The table shows that nineteen (19) out of the thirty-six (36) security controls identified from question 5 are related to 'Access Control' and 'Operations Security'. This result reflects an opportunity for the organization to strengthen security controls in these domains with the objective of preventing security incidents in the future. The results also show a preference for restricting access to assets through the enforcement of enhanced access controls.

Within question six, the SIHs identified twenty-nine (29) process changes from twenty-eight (28) retrospectives. Within twenty-seven (27) retrospectives, the SIHs identified a single process change. While in one (1) retrospective, two (2) process changes were identified. The twenty-nine (29) process changes can be categorized into one of four types. Four (4) of the process changes involved the creation of a new process, while eleven (11) of the process changes involved enhancing existing processes. Eight (8) of the process changes identified by the SIHs involved the introduction of new tools and/or methods to assist the security incident response team with future investigations. Six (6) process changes involved modifications to existing processes owned by other teams within the organization.

4.2. Meta-Retrospectives

Meta–retrospectives were initiated for forty-eight (48) out of the three hundred and twenty-four (324) retrospectives undertaken within the organization

ISO/IEC Domain Name	Total	Example Control
Access Control	9	Define administrative permissions for virtual machines used in test development servers
Asset Management	2	Check all hardware for CD media prior to sending for recycling
Communications Security	1	Enhanced logging on Network File System share
Cryptography	2	Transport Layer Security to be implemented between organisation and third-party involved in incident
Human Resources Security	4	Education re-enforcement surrounding Secure Remote Access Service tokens and PIN numbers
Information Security Policies	4	Creation of new lock-down standard for web server security
Operations Security	10	Block access to specific file-upload portal on web gateway
Supplier Relationships	4	Third-party involved to implement technical and procedural controls
Total Security Controls	**36**	

Table 3: Security Controls Identified

between February 2014 and March 2015. These meta-retrospectives were used to 'follow-up' on the implementation of sixty-five (65) security controls and/or security incident response process changes identified during the initial retrospective. These security control and process changes are broken down as follows:

- Within twenty (20) retrospectives, the SIHs identified only a security control and no process changes. Twenty-three (23) security controls were identified in these twenty (20) retrospectives.
- Within eighteen (18) retrospectives, the SIHs identified only a process change and no security controls. Eighteen (18) process changes were identified in these eighteen (18) retrospectives.
- Within ten (10) retrospectives, the SIHs identified both a security control and a process change. Thirteen (13) security controls and eleven (11) process changes were identified in these ten (10) retrospectives.

Hence, the forty-eight (48) meta–retrospectives were conducted to investigate if the security controls and process changes identified in the retrospectives

had been implemented and, if not, determine why the change was not implemented. The results from the meta–retrospectives inquiries are categorized in the following manner:

- **Change Made (CM)** – the proposed security control or security incident response-related process change was implemented within the organization at the time of the meta-retrospective.
- **Change On-going (CO)** – the implementation of the proposed security control or security incident response-related process change was on-going at the time of the meta-retrospective.
- **Change After meta-retrospective (CA)** – the implementation of the proposed security control or security incident response-related process change was initiated during or after the meta-retrospective.
- **Escalated to Management (EM)** – the implementation of the proposed security control or security incident response-related process change was escalated to senior information security management for progression.
- **No Changes (NC)** – the proposed security control or security incident response-related process change was not implemented.

Table 4 summarizes the results of the 48 meta–retrospectives. The figure shows that forty-two (42) out of the sixty-five (65) security control and process changes identified in the retrospectives were either implemented (Change Made) in the organization or their implementation was considered 'Change On-going' at the time of the meta-retrospective. Two (2) enhancements (one security control and one process change) resulted in no changes being implemented at the time of the meta-retrospective. However, in both these meta-retrospectives, the SIHs started to take actions to implement these controls and changes shortly after the meta-retrospective. One possible explanation is that the act of undertaking a meta-retrospective may have prompted the SIHs to remember to take an action with regards to the implementation of these enhancements.

Meta-retrospective Type	**CM**	**CO**	**CA**	**EM**	**NC**	**Total**
Only Security Control(s)	15	5	1	2	0	**23**
Only Process Change(s)	5	2	1	6	4	**18**
Combination	10	5	0	7	2	**24**
Total	**30**	**12**	**2**	**15**	**6**	**65**

Key: *CM = Change Made; CO = Change On-Going; CA = Change After Meta-Retrospective; EM = Escalated to Management; NC = No Changes.*

Table 4: Summary of Meta-Retrospectives Results

The results from the meta-retrospectives also identified that a security incident response team can face numerous challenges when attempting to implement

security controls and process-related changes. During the meta-retrospectives, the SIHs indicated that fifteen (15) out of the sixty-five (65) enhancements had to be escalated (EM, in Table 4) to senior management within the Information Security unit, who are responsible for operational security within the organization. In all fifteen (15) cases, senior management either assisted in the implementation of the proposed changes or continued to champion the changes on behalf of the SIHs. This finding suggests that although an organization's security incident response team may have the responsibility to ensure that an organization can learn from a security incident, the team may not necessarily have the authority to change security controls to prevent a recurrence.

Similarly, not all security controls and process changes identified by a security incident response team will be implemented within an organization. Six (6) out of the sixty-five (65) security control and process changes identified in the retrospectives resulted in 'No Changes' (NC, in Table 4) being made within the organization. However, in all six (6) cases, these retrospectives involved process changes and not security controls. According to the SIHs, the primary reason these changes were not made was because the security incident response team does not have authority over all the processes within the organization. As a result, if the SIHs propose changes to processes owned by other organizational teams, it is dependent upon that particular team to decide whether it will modify its process to satisfy the security incident response team's requests. For example, an SIH identified that enhanced logging for a web-based system would assist with investigating the system. However, while the system's owners acknowledged the potential benefit, a business decision was made not to implement more detailed logs and the risk associated with this decision was accepted by the organization.

4.3. Analysis

In order to determine if retrospectives can enhance feedback/follow-up efforts during security incident response, quantitative data was collected from the organization's security incident response database. In addition, qualitative data was collected through interviews with relevant individuals.

4.3.1. Investigation Record Analysis

At a high-level, the analysis of the retrospectives and investigation records revealed that more 'information items' were identified using the retrospectives. The term 'information item' is used in this context to describe an information asset, individual, organizational team, security control or process change identified in either the retrospective or investigation record. The results of the analysis show that one hundred forty-eight (148 (46%)) out of the three hundred and twenty-four (324) retrospectives contained more information about an investigation when compared with the corresponding record. One hundred and fifty-one (151 (47%)) out of the three hundred and twenty-four (324) retrospectives identified the same information as the relevant record. However, the analysis also revealed that twenty-five (25 (7%)) of the investigation records contained

more information than their corresponding retrospective. Table 5 – Investigation Records vs. Retrospective Data, presents a comparison of the 'information items' identified from each retrospective question with the investigation record.

The table shows that five hundred and two (502) information assets were identified using the retrospectives. In comparison, the corresponding investigation records contained information about four hundred and twenty-four (424) information assets. Overall, sixty-five (65) retrospectives contained more information about information assets required for a security investigation than what was documented in the investigation records. Seventy-eight (78) additional information assets were identified from the sixty-five (65) retrospectives. Moreover, two hundred and fifty-nine (259) retrospectives and investigation records contained the same assets.

With regards to information assets that could not be investigated, the investigation record analysis revealed that eleven (11) retrospectives contained more information about the assets, which could not be investigated, than the corresponding investigation records. Twenty-two (22) information assets were identified during these eleven (11) retrospectives, while only eleven (11) assets were documented in the investigation records. The analysis also revealed that seven (7) retrospectives and investigation records contained the same information about assets, which could not be investigated.

With regard to the individuals or teams required during a security investigation, the comparative analysis showed that eighty (80) retrospectives identified more information about individuals and groups involved in an investigation, when compared to the corresponding investigation record. Ninety-four (94) individuals and groups were identified in these eighty (80) retrospectives. However, the comparative analysis also revealed that twenty-five (25) investigation records contained more information about individuals and teams communicated with, than the corresponding retrospective. Thirty-four (34) individuals and groups were documented in the investigation records, but were not identified using the retrospectives.

Regarding the fourth retrospective question, the comparative analysis revealed that, in four (4) out of the five (5) retrospectives, more information about individuals and groups, where communication was a problem, was identified by using the retrospectives than in the investigation records. In the fifth instance, the information identified from the retrospective was also found in the corresponding investigation record.

The comparative analysis of the security control information revealed that eleven (11) security controls were documented within the investigation records, while twenty-five (25) additional security controls were identified using the retrospectives. Hence, more security controls were identified using the retrospectives than the corresponding investigation record. Moreover, six (6) retrospectives and investigation records contained the same security control. With regards to security incident response-related process changes, the analysis showed that while twenty-nine (29) changes were identified using the retrospectives, only three (3) of these modifications were documented within the investigation records. Therefore, twenty-six (26) additional process changes were identified

Retrospective Question	Investigation Record	Retrospective Data	Difference
1	424 Information Assets	502 Information Assets	+78
2	11 Information Assets	22 Information Assets	+11
3a	601 Individuals or Groups	695 Individuals or Groups	+94
3b	76 Individuals or Groups	42 Individuals or Groups	-34
4	1 Individual or Group	5 Individuals or Groups	+4
5	11 Security Controls	36 Security Controls	+25
6	3 Process Changes	29 Process Changes	+26

Table 5: Investigation Records vs. Retrospectives Data

using the retrospectives.

4.3.2. Interview Analysis

Seven individuals were interviewed and the answers are summarized below. Initial questions established the participant's current role, within both the organization and the security incident response team. Additional questions asked participants about using retrospectives to identify 'what worked well', 'what did not work well', along with security controls and security incident response-related process changes.

Interviewee Demographics

Participants identified themselves as information security managers, senior security analysts and security analysts. One individual was a trainee information security analyst. These individuals assume various roles, which include managers who enforce the organization's security incident response process, as well as analysts who manage security events and incidents. When the participants were asked if they were involved in any post-investigation activities within the organization, six out of the seven respondents indicated that they were involved in various post-investigation activities. These activities included improving and reviewing security policies and controls, analyzing security incident risk and escalating security recommendations to other stakeholders. Two participants added that, in addition to these activities, retrospectives were also a post-investigation activity. This result suggests that retrospectives have not been completely recognized as a post-investigation activity, even though they were undertaken at the completion of all the investigations during the case study.

Identifying 'What Worked Well'

When the interviewees were asked about using the retrospectives to identify 'what worked well', the predominant answer was that this part of the retrospective helped to capture additional information that can be used to identify frequency of asset use and stakeholder involvement. One individual added that this part of the retrospective had helped to identify the individuals and teams that the security incident response team must ensure are available to assist with future investigations. The suggestion was that building stronger relationships with these units would assist in resolving investigations quicker and more effectively in the future. One information security manager also argued that this part of the retrospective provided SIHs a second opportunity to document investigation information which may have been missed during the initial investigation. When asked if there was a disadvantage to using the retrospective to identify 'what worked well', all seven respondents indicated there was no disadvantage. In fact, all seven participants stated that this part of the retrospective provided an additional avenue for the SIHs to identify and document information that may otherwise not be documented. When asked about the overall impact of using the retrospectives to identify assets investigated and people with whom they communicated with during an investigation, the respondents indicated that it

could, potentially, enhance important asset information acquisition and identify required investigation stakeholders.

Identifying 'What Did Not Work Well'

When queried about using the retrospective to identify 'what did not work well', five interviewees stated that this part of the retrospective has helped to identify and capture information, which would otherwise not be documented. One of the interviewees indicated that SIHs do not document information about individuals they do not talk to or assets they cannot investigate, due to time pressures. However, the individual went on to state that capturing this information can help with identifying gaps in the process of obtaining access to key information assets and stakeholders, which could be required for future investigations. All seven interviewees indicated that there were no disadvantages to using a retrospective to identify information about 'what did not work well' during an investigation. When asked to discuss the overall impact of the question 'what did not work well', the interviewees generally agreed that this part of the retrospective has provided an opportunity for SIHs to stop and reflect about 'what went wrong' in the investigation and to document additional information.

Identifying Security Controls

When the interviewees were queried about using the retrospective to identify security controls that can be improved, they indicated that the retrospective provided a 'safety-net mechanism' to help document security control modifications. One information security manager indicated that while this is a process requirement, in reality, this does not always occur. These comments support the results presented in Section 4.3.1, which indicated that security controls are not always documented in the investigation record. When questioned further on this matter, interviewees stated that this information was not documented because of limited knowledge surrounding security controls. The interviewees went on to acknowledge that while it is important to document this information, their limited knowledge about security controls affected their capability to identify modifications. One interviewee suggested that this part of the retrospective becomes a group activity. The idea was that individuals, within the incident response team, have varied levels of security control knowledge and that collective input would be more affective at identifying improvements. This suggestion emulates the Agile Manifesto, which encourages providing individuals with the environment and support they need to reach specific objectives (Beck et al., 2001). Similarly, undertaking a group retrospective could provide an incident response team with the right environment to expand their knowledge and assist with the identification of security controls.

Identifying Security Incident Response Process Changes

When asked about using the retrospective to identify security incident response related process changes, the interviewees were unanimous that the retrospectives assist with the identification of process changes. Two individuals

indicated that this type of information was important to document, but the organization's process did not require the security incident response team to document this information. The two individuals went on to state that the process of conducting a retrospective assisted with capturing this information, which would otherwise not have been documented within the organization. One of the information security managers added that they did not expect any security incident response-related process changes to be recorded in the investigation record. This is because SIHs are likely to be more focused on eradicating and recovering from security problems, rather than deciding on how to improve processes. Hence, the manager stated that this part of the retrospective provided a mechanism that prompted SIHs to stop and think about how they can improve the way they conduct security investigations, therefore, identifying and documenting process modifications. Six out of the seven interviewees indicated that there was no disadvantage to using the retrospectives to identify and document security incident response-related process changes. However, one individual noted that the activity was less important than identifying security controls and suggested a monthly retrospective implementation targeting process changes.

Other Factors Influencing Retrospectives in Security Incident Response

Towards the conclusion of the follow-up interview, the participants were talking about their opinion regarding other factors that have contributed to the successful or unsuccessful attempt to use retrospectives within security incident response. Five interviewees argued that a SIH's knowledge of an organization's security controls and security incident response-related processes was a key factor in their inability to identify modifications. These individuals added that if an SIH does not know about a specific security control or the existence of a particular process, it could be difficult to suggest improvements. Hence, educating and training security incident response teams was considered a critical factor to help SIHs identify modifications through retrospectives. Two individuals stated that the success of a retrospective was also dependent on how quickly it was undertaken at the closure of an investigation. These two individuals indicated that the retrospectives should be undertaken swiftly at the conclusion of an investigation, however, both individuals concluded that this might not always be feasible. This is because a security incident response team may have to manage multiple investigations at any given time, and the priority will be to close the investigation and move onto the next problem. As a result, retrospectives may not be a priority when multiple incidents are affecting an organization. From a managerial perspective, one of the information security managers argued that security incident response teams needed to 'buy-in' into the idea of using retrospectives as a method for conducting follow-ups in security incident response. The manager added that "a security incident response team, together with their managers, need to want to improve and without the will to want to improve, there is no point in undertaking the retrospectives".

5. Discussion

Responding to and learning from security incidents is a critical component of the Fortune 500 Financial organization's information security posture. Although the organization's security incident response team closely follows best practice guidelines, the case study findings suggest that retrospectives can help enhance how the team identifies security control and security incident response process changes. However, the case study findings suggest that the retrospective implementation in the organization have also affected and been affected by a process culture in the organization, can assist with the implementation of best practices, and influenced information dissemination and security incident learning.

5.1. Process Culture

The investigation record analysis revealed that more information was documented in the retrospectives regarding assets that could not be investigated and individuals where communication was a problem. During the follow-up interviews, one of the interviewees suggested that SIHs do not document this information in the investigation record because of time pressures. However, the individual went on to state that capturing this information could help with identifying gaps in the security incident response process. These observations provide an indication that a process culture exists within the organization and that this type of culture influences the SIH's ability to conduct follow-ups to security incidents. Deal and Kennedy (2000) argue that a process culture is very common in financial organizations and employees tend to focus on doing tasks correctly according to a process. However, difficulties can arise because of problems with systems and processes currently used in a process-driven organization (Deal and Kennedy, 2000). Within the Fortune 500 organization, SIHs are expected to conduct thorough and conclusive security investigations. However, the case study has highlighted that this is not always possible because assets and/or individuals needed may be unavailable to the investigator. The process challenges arise because the organization's security incident response process does not take into consideration deviations from 'normal' investigative events. As a result, the process is expected to work all the time and does not account for assets or individuals being unavailable. Even though the SIHs recognize that these resources may help them learn from an incident, without a process deviation, assets may not be investigated and incident causes may not be correctly identified.

Another problem with a process culture is the lack of immediate feedback from processes implemented within an organization (Deal and Kennedy, 2000). Consequently, employees do not actually know if the process is actually working to achieve the particular objective (Deal and Kennedy, 2000). The case study results suggest that retrospectives could be one solution to this problem. A security incident response team could receive feedback about its incident response process by implementing retrospectives at regular intervals to evaluate if the process is achieving its objectives. Focusing the retrospectives on specific

aspects of the process such as assets needed, individuals whose assistance was required and security controls to prevent an incident reoccurrence means that SIHs can identify if the process is working and improve those areas which are not working correctly.

5.2. Assistance with Implementation of Best Practices

A commonly cited process for security incident response best practice is the National Institute of Standards and Technology (NIST) Special Publication 800-61 (Grispos, 2016). The purpose of this publication is to provide organizations with guidance in establishing security incident response capabilities, in order to handle incidents efficiently and effectively (Grance et al., 2004). The last phase within the NIST process is the Post-Incident Activity phase. According to the NIST guide, in this phase, an incident response team should hold a lessons learned meeting to reflect on new threats and technology and to identify lessons learned (Grance et al., 2004). The guide goes on to state that this meeting provides an opportunity for an incident response team to review what occurred, what was done to intervene and how well that intervention worked in the context of the incident. However, apart from suggesting a meeting, the guide does not provide any practical information on how these questions can be answered. The lightweight retrospectives process could provide one solution to this problem. As the case study results have shown, this lightweight process could be used to drive post-incident meetings in order to collect information that will help answer the the queries posed in the NIST guide.

5.3. Information Dissemination

While the case study results suggest that the retrospectives approach can assist with the implementation of incident response best practices, the approach could also be used to disseminate information learned from security incidents. Researchers (Grispos et al., 2015; He and Johnson, 2012) have generally argued that organizations find it difficult to disseminate information from security incidents. These researchers go on to state that information that is learned from a security incident investigation is usually not documented or often, when it is documented, does not reach management to instigate change (He et al., 2014; He and Johnson, 2012). In concert with these concerns, He et al. (2014) argue that there is no systematic or standardized way to disseminate or manage information dissemination in security incident response. While a detailed report could be produced for management, these individuals may find it difficult to digest the information in the report because of the interrelated information it will contain (He, 2014). Moreover, these reports are likely to be written for an administrative purpose rather than 'engineering purposes' and, as a result, can not be used to improve assets or processes affected by an incident (He and Johnson, 2012). The case study results suggest that retrospectives could provide an alternative lightweight mechanism to support information dissemination, in security incident response, for engineering purposes. As the case study has shown, the retrospective questions can be tailored to collect specific information that

is useful to a security incident response team and its managers. This information can provide insight into improving security controls and security incident response-related processes.

5.4. Incident Learning

While the retrospectives could be used to improve information dissemination and feedback from a security incident response process, the information collected using retrospective can also be used for wider organizational incident learning. By extension, this can be considered one of the objectives of the case study; additional information captured using the retrospectives can be used by a security incident response team to learn about a security incident. Cooke defines incident learning as "the collection of organizational capabilities that enable an organization to extract useful information from incidents of all kinds and use this information to improve organizational posture over time" (Cooke, 2003). However, one observation made during the case study was that the organization's security incident response team did not frequently use this information for the purpose of incident learning. Even though the team had this additional information at their disposal very few actions were taken to extend learning from particular incidents. While further investigation is needed to determine why limited incident learning occurred using the retrospective information, managers did use the same information for metric reporting to high-level management to show organizational performance. Hence, based on Cooke's definition, the retrospectives information is being used by managers for incident learning.

6. Conclusions and Future Work

Undertaking a security investigation within organizations is an increasingly challenging and complex task. The results from this research facilitated initial answers to the proposed research questions. In reference to the first question, the results identified two retrospective components that needed to be modified for use within a security incident response process. First, unlike agile development where retrospectives are undertaken throughout a software project, the security incident response retrospectives were only conducted at the end of an investigation. Second, the retrospectives conducted in a security incident response process were undertaken with selective individuals and not the entire security incident response team. Only the individuals who were involved in an incident response participated in the retrospective.

In regard to the second research question, retrospectives assist with identifying and documenting additional information about a security investigation which may, otherwise, not be documented within a corresponding investigation record. The results from the comparative document analysis demonstrate that retrospectives assist with identifying and documenting additional information about a security investigation. One hundred and forty-eight (148) out of the three hundred and twenty-four (324) retrospectives contained more information than the corresponding investigation records. More specifically, the retrospectives contained information about an additional seventy-eight (78) assets that

were investigated; eleven (11) assets that were not investigated; ninety-four (94) individuals or teams with whom the SIHs needed to communicate and four (4) individuals or teams with whom the SIHs could not communicate during an investigation. However, the analysis also showed that a retrospective is not a replacement for investigation documentation. Twenty-five (25) security investigation records were found to contain additional investigation information when compared to the information identified using the retrospective.

Regarding the third research question, retrospectives assist a security incident response team to identify and document security controls. The analysis has shown that twenty-five (25) additional security controls were identified and documented using the retrospectives rather than the corresponding investigation records. In regard to the fourth research question, retrospectives assisted a security incident response team in identifying and documenting security incident response-related process changes. The analysis has shown that twenty-six (26) security incident response-related process changes were identified and documented using the retrospectives, but were not documented in the investigation records.

With regards to the fifth research question, meta–retrospectives highlight how many security controls and security incident response-related process modifications are implemented within an organization. The analysis from the meta–retrospectives show that forty-two (42) out of the sixty-five (65) security control and process changes were either implemented in the organization or their implementation was considered 'on-going' at the time of the meta-retrospective. Two further adjustments were implemented after the specific meta-retrospective was undertaken. In both of these cases, no changes were implemented prior to the meta-retrospective and the changes within the organization were only instigated during the meta-retrospective. In addition, the meta-retrospectives highlighted that fifteen (15) out of the sixty-five (65) security control and process changes had to be escalated to management. These managers then either assisted with the implementation of the security control and process modification or continued to champion its implementation. Finally, six out of the sixty-five (65) security control and process changes identified, in the retrospectives, resulted in no changes within the organization.

Hence, the results from the experiment support the proposed hypothesis that the implementation of lightweight agile retrospectives, in a security incident response process, can enhance feedback and/or follow-up efforts. In addition, the results from the experiment indicate that retrospectives can be used to enhance the data collected during future security investigations. The data collected by the retrospectives include assets investigated and not investigated; identification of individuals and teams where there were communication issues; needed security controls, and modifications to the security incident response process. Improvements in these areas can potentially enhance overall investigation information, data capture from security controls, and influence modifications to security incident response processes. While this lightweight retrospective approach was demonstrated in a Fortune 500 Organization, the method is, plausibly, applicable to a range of organizations.

Future work will evaluate the research results on a much grander scale. The experiment will be extended to investigate security incident response retrospectives in a variety of organizations and industries. Other industries, of particular interest, include highly regulated domains, such as healthcare and critical infrastructure environments. The research expansion allows for a comparison of the financial organization's results with the results from other industries and organizations. Future research will explore additional agile practices such as 'pair programming' and 'product backlogs' to determine enhancement potential in multiple environments.

Acknowledgements

The authors would like to thank the anonymous reviewers for their feedback on this work. The authors would also like to thank Eoghan Casey for his advice and recommendations during the peer-review process.

References

Ahmad, A., Hadgkiss, J., Ruighaver, A.B., 2012. Incident Response Teams – Challenges in Supporting the Organisational Security Function. Computers & Security 31(5), 643–652.

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., Zajicek, M., 2004. Defining Incident Management Processes For CSIRTS: A Work in Progress. Technical Report. DTIC Document.

Beck, K., Beedle, M., Bennekum, A.V., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., 2001. Manifesto for Agile Software Development `http://www.agilemanifesto.org`.

Cooke, D., 2003. Learning from Incidents, in: 21st System Dynamics Conference, NYC, New York, pp. 1–30.

Deal, T.E., Kennedy, A.A., 2000. Corporate Cultures: The Rites and Rituals of Corporate Life. Da Capo Press.

Derby, E., Larsen, D., Schwaber, K., 2006. Agile Retrospectives: Making Good Teams Great. Pragmatic Bookshelf Raleigh.

Gonçalves, L., Linders, B., 2013. Getting Value out of Agile Retrospectives. Lulu Publishers.

Grance, T., Kent, K., Kim, B., 2004. Computer Security Incident Handling Guide, in Special Publication 800-61. Technical Report. National Institute of Standards and Technology.

Grimes, J., 2007. National Information Assurance Approach to Incident Management. Technical Report. Committee for National Security Systems.

Grispos, G., 2016. On the Enhancement of Data Quality in Security Incident Response Investigations. Ph.D. thesis. University of Glasgow.

Grispos, G., Garcia-Galan, J., Pasquale, L., Nuseibeh, B., 2017a. Are you ready? towards the engineering of forensic-ready systems, in: IEEE 11th International Conference on Research Challenges in Information Science, Brighton, United Kingdom.

Grispos, G., Glisson, W., Storer, T., 2014. Rethinking Security Incident Response: The Integration of Agile Principles, in: 20th Americas Conference on Information Systems, Savannah, Georgia, USA, pp. 1–10.

Grispos, G., Glisson, W.B., Bourrie, D., Storer, T., Miller, S., 2017b. Security Incident Recognition and Reporting (SIRR): An Industrial Perspective, in: 23rd Americas Conference on Information Systems (AMCIS 2017), Boston, USA.

Grispos, G., Glisson, W.B., Storer, T., 2015. Security Incident Response Criteria: A Practitioner's Perspective, in: 21st Americas Conference on Information Systems, San Juan, Puerto Rico, USA, pp. 1–10.

He, Y., 2014. Generic Security Templates for Information System Security Arguments: Mapping Security Arguments within Healthcare Systems. Ph.D. thesis. University of Glasgow.

He, Y., Janicke, H., 2015. Towards Agile Industrial Control Systems Incident Response, in: Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research, British Computer Society. pp. 95–98.

He, Y., Johnson, C., 2012. Generic Security Cases for Information System Security in Healthcare Systems, in: System Safety, incorporating the Cyber Security Conference 2012, 7th IET International Conference on, IET. pp. 1–6.

He, Y., Johnson, C., Renaud, K., Lu, Y., Jebriel, S., 2014. An Empirical Study on the Use of the Generic Security Template for Structuring the Lessons from Information Security Incidents, in: Computer Science and Information Technology (CSIT), 2014 6th International Conference on, IEEE. pp. 178–188.

Hove, C., Tårnes, M., Line, M.B., Bernsmed, K., 2014. Information Security Incident Management: Identified Practice in Large Organizations, in: IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on, IEEE. pp. 27–46.

International Organization for Standardization and International Electrotechnical Commission, 2011. ISO/IEC 27035 - Information Security Incident Management. Technical Report. ISO/IEC.

International Organization for Standardization and International Electrotechnical Commission, 2013. ISO/IEC 27002 - Code of practice for information security controls. Technical Report. ISO/IEC.

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.

Killcrece, G., Kossakowski, K.P., Ruefle, R., Zajicek, M., 2003. State of the Practice of Computer Security Incident Response Teams (CSIRTs). Technical Report. DTIC Document.

Kitchenham, B.A., Pfleeger, S.L., 2002. Principles of Survey Research: Part 3 – Constructing a Survey Instrument. ACM SIGSOFT Software Engineering Notes 27(2), 20–24.

Klahr, R., Amili, S., Shah, J.N., Button, M., Wang, V., 2016. Cyber Security Breaches Survey 2016. Technical Report. H.M. Government, Ipsos MORI Social Research Institute and University of Portsmouth.

Maham, M., 2008. Planning and Facilitating Release Retrospectives, in: Agile, 2008. AGILE'08. Conference, IEEE. pp. 176–180.

McHugh, O., Conboy, K., Lang, M., 2012. Agile Practices: The Impact on Trust in Software Project Teams. IEEE Software 29(3), 71–76.

Mitropoulos, S., Patsos, D., Douligeris, C., 2006. On Incident Handling and Response: A State-of-the-Art Approach. Computers & Security 25(5), 351–370.

Northcutt, S., 2001. Computer Security Incident Handling: Step by Step, A Survival Guide for Computer Security Incident Handling. Technical Report. SANS Institute.

Oates, B.J., 2005. Researching Information Systems and Computing. Sage.

Pham, A., 2011. Scrum in Action:: Agile Software Project Management and Development. Cengage Learning.

Ponemon Institute, 2015. Global Report on the Cost of Cyber Crime. Technical Report. Ponemon Institute.

Prosise, C., Mandia, K., Pepe, M., 2003. Incident Response & Computer Forensics. McGraw-Hill, Inc.

Shedden, P., Ahmad, A., Ruighaver, A., 2010. Organisational Learning and Incident Response: Promoting Effective Learning Through the Incident Response Process, in: 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth, Western Australia, pp. 131–142.

Shedden, P., Ahmad, A., Ruighaver, A.B., 2011. Informal Learning in Security Incident Response Teams, in: 2011 Australasian Conference on Information Systems, pp. 1–12.

Shore, J., 2007. The Art of Agile Development. O'Reilly Media, Inc.

Tan, T., Ruighaver, A., Ahmad, A., 2003. Incident Handling: Where the Need for Planning is Often Not Recognised, in: 1st Australian Computer, Network & Information Forensics Conference, pp. 1–10.

Tiwari, G., Alikhan, Z., 2011. From Team to Wow Team: An Agile Team's Journey, in: AGILE'11 Conference, pp. 296–301.

Vangelos, M., 2011. Incident Response: Managing, in: Encyclopedia of Information Assurance.. Taylor & Francis, pp. 1442–1449.

Werlinger, R., Botta, D., Beznosov, K., 2007. Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis, in: Proceedings of the 3rd Symposium on Usable Privacy and Security, ACM. pp. 149–150.

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.

Wiik, J., Gonzalez, J.J., Kossakowski, K.P., 2005. Limits to Effectiveness in Computer Security Incident Response Teams, in: Boston, Massachusetts: Twenty Third International Conference of the System Dynamics Society, pp. 1–26.