Folk Risk Analysis: Factors Influencing Security Analysts' Interpretation of Risk

Andrew M'manga
Department of Computing and Informatics
Bournemouth University
Fern Barrow, Poole, UK
ammanga@-bournemouth.ac.uk

Shamal Faily
Department of Computing and Informatics
Bournemouth University
Fern Barrow, Poole, UK
sfaily@-bournemouth.ac.uk

John McAlaney
Department of Psychology
Bournemouth University
Fern Barrow, Poole, UK
jmcalaney@-bournemouth.ac.uk

Christopher Williams
Defence Science and Technology Laboratory
Porton Down, UK
cwilliams@mail.dstl.gov.uk

ABSTRACT

There are several standard approaches to risk analysis recommended for use in information security, however, the actual application of risk analysis by security analysts follows an opaque mix of standard risk analysis procedures and adaptations based on an analyst's understanding of risk. We refer to these approaches as *Folk Risk Analysis*. To understand folk risk analysis, we present the results of a study where Distributed Cognition and Grounded Theory were used to elicit factors influencing risk interpretation by security analysts, and the constrained conditions to risk decision making they encounter.

1. INTRODUCTION

A fundamental challenge in designing systems for security analysts is understanding how they make decisions about security risk. One approach to addressing this challenge lies in the identification and understanding of factors that influence the analyst's interpretation of risk and the appreciation of constraints in the analyst's operations; these can uncover the analyst's translation of risk. Risk analysis is rarely a straight forward or rational process, and by understanding the risk analysis practices that analysts deploy, system designed can better address them [27, 35].

This paper aims to contribute to system design for security by increasing the visibility of decision making activities security analysts carry out during risk analysis. A large proportion of an analyst's activities revolves around directly or indirectly eliciting and analysing risks. Activities range from intrusion detection and incident response, to systems administration [22]. In a bid to preserve consistency, we focused our study's scope on risk analysis undertaken during vulnerability analysis.

The work was motivated by the question: how do security analysts make decisions about risk, given that risk analysis, is rarely a rational process? Our findings show that decision making on risk is a matter a consolidated effort between analysts, artefacts, and facilitated by communication and awareness. In addition, we identify that these factors are insufficient in addressing constraints resulting from goal conflicts when context is not considered in specifying security requirements.

The rest of the paper is structured as follows; we consider the related work on risk and risk perceptions, and activities of security analysts in Section 2, before presenting our study approach and data collection method in Sections 3 and 4 respectively. We analyse the data in Section 5, present the findings in Section 6, and discuss them in Section 7. Conclusions and future work are discussed in Section 8.

2. RELATED WORK

2.1 Risk and Risk Analysis

Risk is a term traditionally designated as the possibility of objective danger that could not be traced back to wrongful conduct [19], but is now synonymous with some form of threat, danger or hazard. Techno-scientific approaches to risk expand on this synonym by incorporating the probability of harm occurring, i.e. the product of the probability and consequences (the magnitude and severity) of an adverse event [8]. Two forms of risk are dominant in the literature: objective risk and perceived risk [24].

Objective risk appeals to the techno-scientific definition of risk in that it is stated scientifically and capable of measurement; this definition provides the basis for risk analysis and management techniques used by security analysts. Perceived risk relates to the subjective assumptions people hold about future events. Perceived risk is characterised by theories around risk compensation, e.g. [12, 34, 2] which describe how different people have different propensities to take risk,

this propensity is influenced by the potential rewards of risk taking, and that risk perceptions vary not just by individual, but also by culture.

Risk management processes put objective risk to action. The premise behind management processes is that the use of predetermined sets of procedures can help manage and reduce risk, but an analyst's failure to understand and follow these procedures is a recurring problem in security [30]. Moreover, risk management processes are optimal only in static, well-ordered situations where risk has been pre-defined and, if too much trust is placed in these processes, the resulting outputs may increase residual risk [17].

2.2 Decision Making and Risk

The related work concerning decision making and risk appears to be concerned with perceived rather than objective risk, and the incoherent nature of risk perception and interpretation for decision making.

Beautement et al. [5] discuss factors that influence decision making in security compliance by employees. They introduced the term compliance budget, by which they argued that security compliance is a finite resource and the lengths at which a person is willing to comply depends on the perceived reward to the individual. Although this work is not primarily concerned with security analysts, it does raise the intriguing question of whether security analysts view aspects of risk analysis as tradable resources and, if so, how these might be identified.

Asgharpour et al. [4] identified that the communication of risk is an important factor in computer security. However, they state that the interpretation of risk by communicating parties differs based on the mental models (understanding) used to translate risk terminology from expert to non-expert. This, in turn, renders the goal of risk communication ineffective when there is a mismatch.

2.3 The Work of Security Analysts

D'Amico et al. [11] reviewed security analysts work processes when defending against attacks by analysing workflows, decision processes and cognitive demands. They identified that security analysis activities flow through three stages of cognitive data fusion and three stages of situation awareness. However, their findings appear limited to the cognitive challenges the analysts encounter and do not consider their socio-technical challenges.

Werlinger et al. [37] report on incidence response practices of security analysts. They identify the tasks, skills, strategies and tools analysts use to understand security incidents. Botta et al [7] continue from this by using Distributed Cognition to study group dynamics in Information Security Management (We define Distributed Cognition in Section 5). Their aim was to verify the influencers of Distributed Cognition in Information Security Management, and the factors leading to its failure. Their results, however, did not identify independent constraints that could lead to Distributed Cognition failures and only highlighted the lack of its influencing norms and cues.

Sundaramurthy et [31] also address the issue of failure with security analysts by using Grounded Theory to investigate factors leading to security analyst's burnout in Security Operation Centres (SOC). They identify several human, technical and managerial factors affecting the morale of the analysts and suggest solutions. For validation, they present some of their anthropological work [32], where they studied the functioning of three different SOC's.

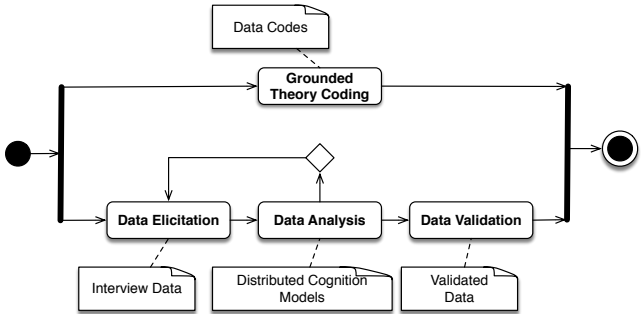

Figure 1: Study Approach

The main distinction between our work and the related work is that we do not only investigate risk analysis activities leading to decision making, but we also identify factors constraining analysts decision making on risk from a socio-technical perspective. Outside security literature, we note that Eiser et al. [13] provides a good coverage on the interpretation of risk from a natural disaster perspective.

3. APPROACH

The approach taken followed the series of activities illustrated in the Activity diagram in Figure 1. We began the study with data eliciting interviews on vulnerability analysis with security analysts. The interview data collected was analysed and based on descriptions and illustrations (Figures 8, Appendix A) of work processes given by the analysts, Distributed Cognition models were produced. The Distributed Cognition models were then presented to the analysts for validation. Where inconsistencies were identified, corrections were suggested. In parallel to the elicitation and creation of the Distributed Cognition models, we coded and qualitatively analysed the data collected using Grounded Theory.

4. DATA COLLECTION

4.1 Participants

We interviewed ten security analysts from three different organisations. The organisations were recommended to us by contacts that later introduced us to the organisations. Organisations were selected on the basis of having a security team that carried out vulnerability analysis.

Organisation A was a Higher Education Institution with three permanent information security analysts supported by team members from their IT (Information Technology) services department, e.g. the Linux, Windows, and Oracle server teams. P1 and P2 (Participant) was a security analyst and security manager in the permanent security team respectively, while P3 to P5 were analysts from the support teams. The professional experience of participants within Organisation A ranged from two to over seven years in the organisation, and they were responsible for over 1000 servers.

Organisation B was an information security practice with a core team of information security analysts. P6 was the organisation technical director and P7 the head of group IT. P6 and P7 had eleven and two years of professional experience in the organisation respectively and were responsible for approximately 150 servers.

Organisation C was a public sector organisation; the three security analysts (P8 - P10) interviewed were primarily focused on external engagements. Their work entailed vulnerability assessment, information assurance, and penetration testing. Their professional experience in the organisation ranged from eighteen months to five years.

4.2 Interview Method

All interviews were carried out over a period of four months based on participant availability. Each interview was semi-structured and driven by the goal of understanding the steps taken during vulnerabilities analysis. The interviews were held at the participant's place of work; examples of guiding questions asked included:

- What guidelines do you follow to help you manage risk?
- How do you select vulnerabilities to act upon when time and resources are limited?
- Are vulnerabilities identified as high or critical by the scanners representative of your work environment?
- How do you identify false positives, and how do you share information?
- What were the occasions when you had to accepted risk?
- What kind of constraints have you experienced during your work?

Using a participant information sheet each participant was made aware of the purpose of the study beforehand, the ethical procedures to be followed and written consent was sought before interviews could begin. Each interview lasted approximately an hour, and was recorded and later transcribed. The transcripts were coded and managed using Nvivo 11 Computer-Assisted Qualitative Data Analysis Software (CAQDAS) tool. Throughout the paper, we present interview extracts as told by the participants to illustrate our findings.

5. DATA ANALYSIS

5.1 Distributed Cognition

Distributed Cognition is a cognitive theory based on the idea that cognition is not limited to an individual's inner mental processes but facilitated by external structures such as artefacts and the social context [16]. Whereas traditional cognition solely focusses on an individual's inner decision making abilities, Distributed Cognition considers cognition as shared among individual's, with external structures, and the relation between past and present events in facilitating decision making. This focus helps examine the socio-technical system of which analysts are a part.

An aeroplane's cockpit is a typical example of Distributed Cognition at work. Whereas the actual flying of a plane would be very difficult, the cockpit relieves the pilots load through the careful positioning and operations of its controls. For example, communication to the passengers and crew is facilitated through an intercom, the flaps are controlled by buttons, and wheels by gear levers as the pilot remains sitting. The cockpit is a socio-technical system and cognition is distributed among its artefacts and individuals (co-pilot) to achieve a common goal. From a Human Computer Interaction (HCI) perspective, Andrews et al. [3] discuss analysts use of to-do notes stuck on a computer monitor to relieve memory load and in turn, elevate awareness. Here the notes are as an external cognitive artefact, reducing the analyst's cognitive limitations.

Blandford and Furnis [6] identified that although Distributed Cognition had been in use for several years, it lacked standard representational models to support its perspective on interaction. To address this, they developed Distributed Cognition for Teamwork (DiCoT): an approach for building models that capture information flow, physical layout, social structures and artefacts of systems [6, 23]. Borrowing from DiCoT, five models were developed from the collected interview data. The interview data consisted of verbal descriptions of work processes and illustrations drawn by the analysts during the course of the interview. Figure 8 in Appendix A is one of the illustrations produced by the analysts. Unlike Blandford and Furniss who mainly developed their own diagrams, we chose to use UML [21] due to its ubiquity and recognition within the IT practitioners community. The five models we developed were:

1. A high level model describing the overall activities and goals during vulnerability analysis.
2. A communication flow model illustrating communicating parties in vulnerability analysis.
3. An external awareness model highlighting third party information used to assist in vulnerability analysis.
4. A vulnerability analysis model highlighting the steps taken in vulnerability analysis.
5. A vulnerability response model highlighting decision processes in addressing identified vulnerabilities.

We now present the generalised version of these Distributed Cognition models.

5.2 Distributed Cognition Models

5.2.1 High Level Model

The high level model in Figure 2 summarises the main vulnerability analysis activities taking place in the study organisations. The analysts typically concerned themselves with proactive and reactive vulnerability analysis.

Proactive analysis entailed planned system vulnerability scans where no malicious activities were apparent. These were either regular weekly to monthly scans, or ad-hoc scans were undertaken when new services and systems were coming online.

Reactive analysis took place after malicious activities had been detected. For example, Organisation A decided to carry out a full network scan soon after its website had been

Table 1: Security Analyst Teams

Teams	Scan	Analysis	Management
Analysts	P2,P8,P9,P10	P3,P4,P5,P7	P1, P6

defaced. Nessus [33] was a common tool for vulnerability detection in the organisations. Like most tools, Nessus had its shortcomings that resulted in false positives. The most prevalent of these was a false positive called backporting on Linux servers. The analyst's knowledge and experience to identify false positives and the use of a variety of awareness sources played an important part in vulnerability analysis. While vulnerability remediation was the analyst's overall goal, this was sometimes hindered by constraints later described in Section 6.2.

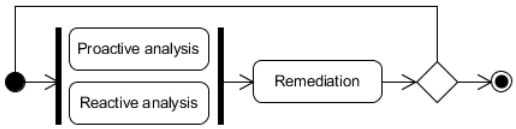

Figure 2: High Level Model

5.2.2 Communication Flow Model

The communication flow model in Figure 3 illustrates the passing of information used for decision making between the analysts. It was noted that, in most cases, analysts belonged to one of three teams (Table 1). The first was the *Scan* team; they were responsible for configuring the scan parameters and scanning the network infrastructure. The Scan team monitored false positives and passed all scan results to the Analysis team. The *Analysis* team was responsible for verifying the findings, identifying, and applying remediations. Feedback was given to the Scan team on false positives, false negatives, and selected responses to vulnerabilities. In situations of high uncertainty, the Analysis team sought approval from the *Management* team before taking action. The Management team provided guidance to the other teams, action approvals, requests justifications, and monitored activities. Members of this team had significant experience in one or both of the other teams.

A common trend in the organisations was the use of a collaboration and workflow management tools to support communication, e.g. the ServiceNow product suite [29]. These facilitate the posting and tracking of jobs and completion status. From the communication flow, we see a consolidated effort of passing information between teams to analyse and act on vulnerabilities. Each team has a unique role and speciality, and they depend on communication tools to assist in the process.

"They notify me from the system, and when the change is happening, I get notified as well. It's when they log it, so the system itself notifies me when a change is going to happen" [P2].

5.2.3 External Awareness Model

The external awareness model in Figure 4, focusses on information that aided the analyst decision making. Other than the vulnerability analysis reports produced by the scanners, the analysts appeared to be highly dependent on information produced by sources external to the organisations for their awareness, risk analysis and decision making.

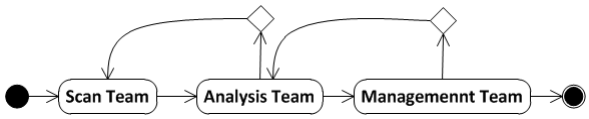

Figure 3: Communication Flow Model

"There are CERTs that will send us notifications on malicious activity on the network if we sign up to them..." [P1].

Though this is not an exhaustive list, the external sources of awareness identified from the interviews were penetration test and vulnerability analysis findings from third parties, CERT notifications, information from the general media, and updates from vendors and threat intelligence communities. False negatives in scans were usually discovered using external sources.

"...we identified new vulnerabilities so they were, therefore, no tests for them in Nessus...Pen testing teams have identified some of these by trying our system" [P7].

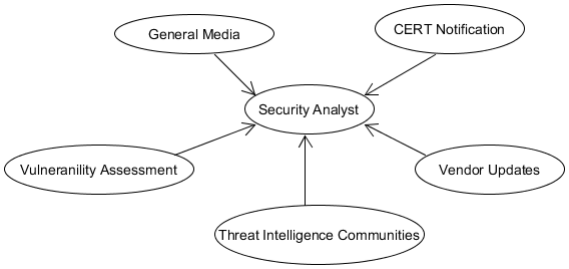

Figure 4: External Awareness Model

5.2.4 Vulnerability Analysis Model

The vulnerability analysis model in Figure 5 illustrates the activities the analysts took to identify and validate vulnerabilities and the tools used to assist them in the process.

As indicated in Section 5.1, Distributed Cognition emphasises that cognition is not limited to an individual but facilitated by external structures. The vulnerability analysis process illustrated this through the tools used by the analysts. For example, the analysts appeared to use more than one tool to verify vulnerabilities.

"We manually scan for vulnerabilities using Kali Linux, and then we verify the findings using Nessus as a backup" [P8].

The analysts also appeared to use a combination of tools to check and verify false positives.

"Over time we have identified certain vulnerabilities where we do not agree with the rating in Nessus. We will then write exceptions in our system to change them. So when the XML report is presented to our system, it knows that rating is wrong" [P7].

"As Nessus doesn't link scans, I keep a record of the false positives in my Excel spreadsheet so if I see the vulnerability occur again, I know to ignore it" [P2].

Once false positive filtering was completed by analysts, an updated file was produced for remedial action. The common trend was to address the critical and high vulnerabilities as early as possible and leave other activities for later.

"If we got high or critical vulnerability that is found we immediately raise a ticket into our support desk and we will prioritise that to be fixed within 48 hours if possible...The rest of them we lump into one ticket which we work on over the rest of the month" [P7].

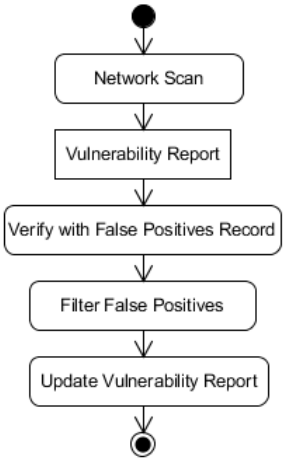

Figure 5: Vulnerability Analysis Model

5.2.5 Vulnerability Response Model

The vulnerability response model in Figure 6 illustrates the steps analysts took to identify and apply suitable vulnerability responses. The response process first identified who was using the vulnerable software and its purpose.

"My team needs to investigate, how did it occur? What vulnerabilities were associated? What exploit kits went on the machine? What was the capability? What else could have happened? Did that machine have access to other networks that held sensitive data?" [P1].

The analysts then checked for the availability of patches and tested their compatibility in a test environment. In the event that patches were unavailable, could not be applied or tests had failed, alternative approaches to mitigating risks had to be identified. These could be blocking ports or other forms of isolating vulnerable services.

"We cannot control the plugins, and if we enforce Wordpress updates, the plugins will stop working. We have worked around the problem by hosting the Wordpress websites off a non-organisation domain" [P5].

When alternative mitigation strategies were unavailable or unachievable, the risk was tolerated and monitored until a strategy could be found.

"In that six months, we went and investigated alternative ways of mitigating the risk and found there were no cost-effective ways of doing that. We are happy to carry that risk until a new system comes in, but for now, we are monitoring" [P6].

5.3 Application of Grounded Theory

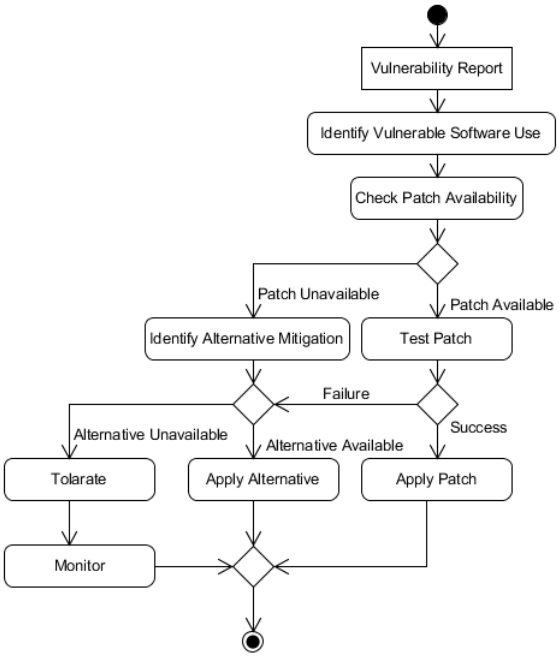

Figure 6: Vulnerability Response Model

Grounded Theory [10] was used as a complementary research methodology as this has been used effectively to direct researchers in identifying social phenomena associated with security practices [1, 14]. While techniques such as Soft Systems Methodology can equally be used to uncover human activity and relations in socio-technical systems, it lacks the inductive abilities to interrogate data through thematic analysis and identify significant patterns.

Grounded Theory employs the constant comparative method where data collection, coding and memoing take place simultaneously. Emerging themes are constantly tested as codes are generated [18]. By following this, data coding did not wait for all fieldwork to be completed and theory generation evolved as coding progressed [25].

The Strauss-Corbin approach to Grounded Theory subjects elicited data to rounds of *Open*, *Axial*, and *Selective* coding.

5.3.1 Open Coding

During the Open coding phase, elicited data is broken down into blocks of concepts based on their characteristics and variations. Concepts are the categorisation of ideas contained in the data [10]. To illustrate; the following two interview quotes were assigned the code *Assistive Tools,* based on the secondary tools the analysts used in addition to the main ones.

"What we wanted was just a high level report...We need something to present to management...I felt I couldn't manipulate it in Nessus" [P2].

In this quote, the analyst was justifying the reason they exported data from Nessus to Excel. They felt they required a tool that could easily manipulate data into visual reports for management use.

"We have an XML feed out into our in-house built system

Open Coding	Axial Coding	Selective Coding
Internal Awareness	Awareness	Remediation
External Awareness		
Standards and Guidelines		
Proactive Remediation	Remediation	
Reactive Remediation		
Feedback	Communication	
Information Sharing		
Third Party Dependency	Constraints	
Business Process Requirement		
Insufficient Privileges		
Project Management		
Data Encryption		
Assistive Tools	Tool Capabilities	
Vulnerability Analysis		
Vulnerability Scans		
Mental Models	Individual Capabilities	
Roles and Responsibilities		
Experience and Training		

Figure 7: Grounded Theory Code Summary

from Nessus. With the XML feed, it keeps a track of how many of each category that we had..." [P7].

In this quote, the analyst was explaining how an in-house built system was used to aid in tracking identified vulnerabilities by severity. While Nessus only presented the latest scan results, this tool maintained multiple scan results fed from Nessus.

Transcript data (interview quotes) may be assigned more than a single code if other salient concepts are justifiable [20]. Consequently, we also assigned the code *Information Sharing* to P2's quote above as it expressed the sharing of information within the organisation. After de-duplicating and merging of related codes, a total of 18 codes were elicited; these are listed in the Open coding column in Figure 7.

5.3.2 Axial Coding

In Axial coding, data codes from Open coding are pieced together by identifying relationships between the concepts. Much of the Axial coding takes place in parallel with Open coding as relationships often become visible during this stage [10]. The output of this stage was the assignment of six Axial codes illustrated under the Axial coding column in Figure 7.

5.3.3 Selective Coding

Selective coding entails defining the Core Category (central phenomenon) and basic social process. The Core Category represents the main theme with greatest explanatory relevance and highest potential for connecting other categories [10]. The Core Category that emerged from our analysis was *Remediation* as it best defined the activities of the Basic Social Process which was identified as *the requirements for vulnerability identification and remediation.*

6. FINDINGS

As a result of Grounded Theory, four groups of factors emerged that influenced the analyst's interpretation of risk, and five conditions constraining the analyst's decision making. We describe these in the sub-sections that follow.

6.1 Risk Interpretation Influencers

In Section 1, we stated that risk analysis is rarely a rational process. Therefore, this implies that, for analysts to make decisions on risk, they require factors that promote a sense of rationality in the face of uncertainty. We identify these factors as *risk interpretation influencers*. These may begin to explain how analysts make rational decisions on risk while using non-standardised approaches. Just as the presence of these factors augments the interpretation of risk, their absence limits interpretation.

6.1.1 Awareness

Awareness is defined as having knowledge or perception of a situation. The analysts reported the need for awareness to understand situations and make decisions on risk [11].

Awareness was gleaned from sources inside the organisations by the sharing of information between colleagues.

"Mostly it is a shared as a ticket simply saying, hey guys, we have identified this information, do you know about it?" [P7],

or from third parties as identified in Section 5.2.3:

"We rely on the scanner, on its results depending on its rules. What we will also do is have an intel feed. So based on this we get a different view of vulnerabilities even if Nessus is reporting it as medium or low" [P6].

The use of standards and guidelines was also perceived as a means to promote awareness.

"We have a detailed assessment because we use ISO 27001. Management has awareness of this, so they use it too as an extra source of awareness" [P6].

"We use a version of Cyber Mission Impact Assessment in vulnerability analysis" [P9].

The effects of low awareness for risk interpretation were evident when [P2] was asked on the level of trust they placed in scan results.

"I do not have the awareness of all the systems, maybe if I had been here an awful lot longer. It's all context oriented" [P2].

6.1.2 Communication

Communication provided assistance to the analysts in understanding risk, both as information shared and feedback; the exchange of information and reports promoted clarity for informed decision making [36, 7]. An Analysis team analyst highlighted the importance of communication in the following quote with their Scan team.

"What we do now, is we send them a list of the servers we have updated and we tell them every package that was updated is now not vulnerable up to the day they were patched" [P5].

Communication was facilitated either by email or more advanced collaborative tools depending on the organisation and team.

"We communicate through our system which logs everything. So our team also feeds the scanning team. If we see a lot of false positives, we tell them to add it to their list" [P7].

The analyst further cited regular communication with the management teams as assurance they were doing things correctly.

"Mostly it is via a bi-weekly meeting, but if it is something very important, then we have a distribution group and we will discuss it by email" [P7].

6.1.3 Tool Capabilities

Tool capabilities define the effectiveness of the tools used by the analysts in the identification and verification of vulnerabilities. Through these capabilities, the analysts were able to ascertain the presence of risks. Rarely was a single tool sufficient to validate the presence of vulnerabilities.

"Nessus gives me the vulnerable software version but it does not give me the complete version number. Nagios does that..." [P2].

Where tool-support was not available, the impact was usually evident;

"Without creating and updating the spreadsheet, I have no way of knowing if it's a false positive or not" [P2].

6.1.4 Individual Capabilities

Despite the presence of tools to identify and validate vulnerabilities, the responsibility for decision making about risk lay primary on the analyst's personal capabilities. These capabilities were considered the combination of factors such as experience and training.

"A lot of the decisions are based on the experience of people in that group and their knowledge of risk and the business...but we are relying on expertise and awareness of those people" [P6].

"There was one the other day to do with exploiting Java code through a certain call. Now I wasn't sure whether that call was used or not because most of it is in the vendor supported side of things...I just patched it anyway" [P5].

The impact of limited individual capabilities was observed also when [P2] explained the level of trust they placed in scan results.

"As far as I am concerned, we have to take the scan results as almost gospel" [P2].

6.2 Constrained Conditions to Risk Decision Making

Goal conflict situations were identified that forced analysts to address risks under constrained conditions. Risk interpretation influencers did not address the conflicts suitably, resulting in difficult decision making. The constrained conditions usually resulted in the failure to enforce security objectives due to the effects of contextual mismatches that were not carefully considered during the specification of security and organisational goals. As a result of Grounded Theory coding, five classifications of the goal conflicts emerged. We present the five goal conflicts leading to constrained decision making below.

6.2.1 Business Process

A business process is defined as an activity or set of activities that accomplish specific organisational goals. The Business Process goal conflict was identified, when analysts were constrained in addressing and acting upon a risk due to the requirements of essential business processes. In one reported event, an analyst had to allow lower security configurations for some users, as the higher ones were in conflict with the user's requirements. In another event, users required new business processing tools that seemed harmless on their own, but their overall security implications, when used with other tools, were unclear.

"Sometimes the application team will say, can we have this application, please. I was installing it and one of the application steps was disable SE Linux. So I asked my boss about this and he said go ahead but write them a note that you are not happy about it" [P5].

"The developer team are using software which they use for their internal collaboration and they want to use video, but we are unsure how they are going to use the video...we are going to review it in six months and if we find that they are using it in a way that is a risk to the business...we would shut it down despite the fact that it is a good tool to them" [P7].

The remarks and actions taken by the analysts indicate the acceptance of risk, although [P7] took the extra step of defining the risk acceptance time frame.

6.2.2 Data Encryption

The data encryption goal conflict was identified, when the analyst's addressing of risk was constrained by legal, standard or contractual obligations to protect data, versus the requirement to share to achieve a business objective. For instance, an organisation may implement the security goal to encrypt all transmissions of personal identifiable data as one way of conforming with the data protection act [9]. However, goal conflicts arise when this information has to be shared with entities lacking encryption capabilities. An analyst expressed how a third party IT support service they used had requested the transfer of user validation data unencrypted, while another expressed how they had resorted to unencrypted data transfers with clients that had no encryption capabilities.

"We send them a list of our user's names and their details so they can change the password. If a user calls up saying they want to change their password, we ask them some security questions...We were asked to send this through an unencrypted document...We said we are sorry, we refuse to do that because we will be breaking data protection laws" [P5].

"We do have challenges around client capabilities. So if we want to send an encrypted message and they do not have PGP or an encrypted Dropbox, then we have to come to an agreement on how to share that information" [P6].

The quotes show that the two analysts chose to act differently based on their understanding of the situation and the sensitivity of the data.

6.2.3 Project Management

Time, cost and human resource are vital ingredients of a successful project. Without these, projects risk failure [28]. The Project Management goal conflict arose when resource allocations were not in line with the maintenance of security goals. Systems typically have an end of life where replacements are required due to advances and improved security. When this point is reached, time and resources are required to upgrade systems and maintain security goal.

An analyst described the continual running of an outdated and unpatched Windows 2003 servers, as they lacked the time and personnel to oversee their migration. Similarly, another analyst described permitting the use of an outdated version of the secure socket layer (SSL) for a specified period, due to the time updating work was going to take.

"We know we have a number of 2003 servers that need to migrate to the latest version of Windows server and the reason that does not happen overnight is because of a conflict of interest in terms of products but also because of the services that sit on these" [P1].

"We found that fixing it was going to take a significant amount of time while there was a new system being built in six months, so it would be better spending the time configuring the new system correctly" [P6].

6.2.4 Insufficient Privileges

Risk analysis depends on privileged access to devices and services for assessment and remediation. Studies have shown that privileged access is essential [26], but may sometimes be difficult to obtain [15]. The Insufficient Privileges goal conflict was identified based on access restrictions. In one instance, the organisational Bring Your Own Device (BYOD) policy restricted the amount of access analysts had, as devices were personally owned. While in another, the conflict was a result of access restrictions set by vendors on their products.

"That scan will hit our entire infrastructure but we focus on the stuff that is in our control. So we scan the organisation servers...desktops, the network routers and switches and essentially anything connected to our network. Anything that falls outside stuff that is managed by IT, like personal laptops, is hard to remediate" [P1].

"We use Qualys for our external servers and website, but Qualys tend to talk back to its cloud service (vendor run) ...If you have a Qualys system on your network, it belongs to them so you cannot change the system configuration" [P7].

6.2.5 Third Party Dependency

Third party dependency goal conflicts were situations when a constraint arose as a result of a third parties failure to provide complete support for their products and services. A notable number of IT products and services in use are either wholly outsourced from third parties or provided by a group of third parties. Established vendors like Microsoft and Oracle usually supports their services and make updates available routinely or on request. Less established vendors and open source projects prefer a collaborative approach maintaining different parts of products and systems. Analysts identified that although the use of such collaborative products was essential, problems ensued when some collaborators stopped supporting the products.

"We have a product that uses Apache and there is a vulnerability that needs to be patched in Apache. Unfortunately, it is vendor supported, and the vendor does not support that version of Apache, so we have got to accept it, to be in line with the vendor application" [P4].

"Glassfish used to be an open source project and was bought out by Oracle. The product we have has the open source side of things. We had a CVE come the other day which said, to fix, we have to move to a new version supported by Oracle. We cannot do that because the vendor only supports the open source version of it" [P4].

7. DISCUSSION

The work was motivated by the question: how do security analysts make decisions about risk, given that risk analysis is rarely a rational process? Our findings show that decision making on risk is a matter of consolidated effort between analysts, artefacts, and facilitated by communication and awareness. This interplay was uncovered by the socio-technical research approach taken using Distributed Cognition. Through this, the research focus moved from the limited analysis of the analysts, to a wider context where the roles in facilitating risk analysis and decision making in the socio-technical environment were considered. From the Distributed Cognition models developed, significant aspects of risk analysis where highlighted that would have otherwise been overlooked. These include the use of primary and secondary tools to improve vulnerability analysis, the coordinated roles that teams play, the vital role that technology-facilitated communication plays, and the distribution of information from external sources to improve awareness.

Although Distributed Cognition brought the interactions between analysts and artefacts during risk analysis to light, it is not suitable for data interrogating. Grounded Theory was used as a complementary research methodology to address this need. Traditional Grounded Theory requires multiple interviews be taken before theoretical saturation is reached. However theoretical saturation was reached by the seventh interviews as the primary methodology was Distributed Cognition uncovering the interplay in the socio-technical environment.

As an overall, coding identified that the analyst's main objective was to remediate vulnerabilities. To achieve this, four risk interpretation influencers; Individual Capabilities, Tool Capabilities, Communication and Awareness were used. While most of these are within individual or organisational control, such as the improvement of tools, training and communication to improve risk analysis, there is little that can be done to improve awareness from external sources or guarantee that sources will have essential information when required.

Conditions that constrain risk decision making were identified from analysis and five categories emerged from coding; Business Process, Data Encryption, Project Management, Insufficient Privileges and Third Party Dependency. The five are not presented as an exhaustive list and may differ in other studies. We identified that these conditions are a result of goal conflict resulting from mismatches in security and organisational requirements when the context is not carefully considered in planning. Our assumption was that constraints the analyst's encounter would originate from external sources. However, the findings show that the main constraints the analyst's encountered, were problems originating from within the organisations.

We believe that if careful consideration is given to context when planning security and organisational goals, the constraints can be controlled or avoided. For example, if an organisation plans to use a particular application for their business processes, they may want to identify the security requirements and other factors that may have implications

in the enforcing of the requirements in the short and long term. In other words, defining security requirements has far-reaching implications than the identification of vulnerabilities and controls. Goal conflicts that introduce security risks should be understood and considered early in requirements analysis.

8. CONCLUSIONS AND FUTURE WORK

In this paper, we illustrated how Distributed Cognition and Grounded Theory can be used to identify the understanding and approach to risk analysis used by security analysts. In doing so, we have presented the idea of *folk risk analysis*: a non-standardised approach used in risk analysis based on one's understanding. We have identified factors that influence risk interpretation and constraints encountered.

Our findings suggest the need to consider methods of promoting risk interpretation influencers when designing interactive systems for analysts. It must also be understood that the identification and implementation of security requirements is not an end in itself, but the wider implications of goals and context must be taken into account.

The constraints identified, helped us address the earlier posed questions from the work by Beautement et al [5]. Do security analysts view aspects of risk analysis as tradable resources, and how may these be identified? We have established that security analysts are willing to trade compliance aspects of risk analysis. e.g. the willingness to remove encryptions when clients lack the capability.

A limitation of our work is that it focuses only on the vulnerability analysis practices of security analysts, whereas risk may be analysed in a variety of ways depending on the security practice employed.

In future work, we will incorporate the risk interpretation influencers and methods for identifying goal conflicts into formative evaluation guidelines when designing for security analysts. We will also carry out additional interviews with analysts concerned with other security activities that entail some form of risk analysis. This will increase the generalisability of our findings.

9. ACKNOWLEDGMENTS

We are grateful to all participants in this study for the time and expertise they shared. The research was funded by Bournemouth University studentship DSTLX1000104780R_BOURNEMOUTH_PhD_RBDM. We are grateful to DSTL for their sponsorship of this work.

10. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] J. Adams. *Risk*. UCL Press, London [England] : Bristol, PA, 1995.

[3] C. Andrews, A. Endert, and C. North. Space to think: large high-resolution displays for sensemaking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 55–64. ACM, 2010.

[4] F. Asgharpour, D. Liu, and L. J. Camp. Mental models of security risks. In *International Conference on Financial Cryptography and Data Security*, pages 367–377. Springer, 2007.

[5] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 workshop on New security paradigms*, pages 47–58. ACM, 2009.

[6] A. Blandford and D. Furniss. DiCoT: a methodology for applying distributed cognition to the design of teamworking systems. In *International Workshop on Design, Specification, and Verification of Interactive Systems*, pages 26–38. Springer, 2005.

[7] D. Botta, K. Muldner, K. Hawkey, and K. Beznosov. Toward understanding distributed cognition in IT security management: the role of cues and norms. *Cognition, Technology & Work*, 13(2):121–134, 2011.

[8] J. A. Bradbury. The policy implications of differing concepts of risk. *Science, technology & human values*, 14(4):380–399, 1989.

[9] G. Britain. *Data Protection Act*. Stationery Office, London, 1998.

[10] J. M. Corbin and A. L. Strauss. *Basics of qualitative research: techniques and procedures for developing grounded theory*. Sage Publications, Inc, Los Angeles, Calif, 3rd ed edition, 2008.

[11] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth. Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In *Proceedings of the human factors and ergonomics society annual meeting*, volume 49, pages 229–233. SAGE Publications Sage CA: Los Angeles, CA, 2005.

[12] M. Douglas and A. Wildavsky. *Risk and culture: An essay on the selection of technological and environmental dangers*. Univ of California Press, 1982.

[13] J. R. Eiser, A. Bostrom, I. Burton, D. M. Johnston, J. McClure, D. Paton, J. Van Der Pligt, and M. P. White. Risk interpretation and action: A conceptual framework for responses to natural hazards. *International Journal of Disaster Risk Reduction*, 1:5–16, 2012.

[14] I. Flechais and M. A. Sasse. Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. *International Journal of Human-Computer Studies*, 67(4):281–296, 2009.

[15] A. Ghosh, P. K. Gajar, and S. Rai. Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4):62–70, 2013.

[16] J. Hollan, E. Hutchins, and D. Kirsh. Distributed cognition: toward a new foundation for human-computer interaction research. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 7(2):174–196, 2000.

[17] G. Klein. *Streetlights and shadows: Searching for the keys to adaptive decision making*. MIT Press, 2011.

[18] S. M. Kolb. Grounded theory and the constant comparative method: Valid research strategies for educators. *Journal of Emerging Trends in Educational Research and Policy Studies*, 3(1):83, 2012.

[19] D. Lupton. *Risk*. Routledge, 1999.

[20] M. B. Miles and A. M. Huberman. *Qualitative data analysis: an expanded sourcebook*. Sage Publications, Thousand Oaks, 2nd ed edition, 1994.

[21] R. Miles and K. Hamilton. *Learning UML 2.0*. O'Reilly, Beijing ; Sebastopol, CA, 1st ed edition, 2006. OCLC: ocm69706455.

[22] C. L. Paul and K. Whitley. A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In *Human aspects of information security, privacy, and trust*, pages 145–154. Springer, 2013.

[23] A. Rajkomar and A. Blandford. Understanding infusion administration in the ICU through distributed cognition. *Journal of biomedical informatics*, 45(3):580–590, 2012.

[24] Royal Society, editor. *Risk assessment: report of the a Royal Society Study Group*. The Royal Soc, London, 1983. OCLC: 10394029.

[25] J. Saldana. *The coding manual for qualitative researchers*. Sage, 2015.

[26] R. S. Sandhu and P. Samarati. Access control: principle and practice. *IEEE communications magazine*, 32(9):40–48, 1994.

[27] B. Schneier. The psychology of security. In *International Conference on Cryptology in Africa*, pages 50–79. Springer, 2008.

[28] K. Schwalbe. *Information technology project management*. Course Technology, Cengage Learning, Boston, MA, seventh edition edition, 2014.

[29] ServiceNow. ServiceNow | Work at Lightspeed.

[30] D. W. Straub and R. J. Welke. Coping with systems risk: security planning models for management decision making. *MIS quarterly*, pages 441–469, 1998.

[31] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan. A human capital model for mitigating security analyst burnout. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 347–359, 2015.

[32] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann. A Tale of Three Security Operation Centers. In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, pages 43–50. ACM, 2014.

[33] Tenable Network Security. *Nessus web site*. Mar. 2017.

[34] M. Thompson, R. Ellis, and A. Wildavsky. *Cultural theory*. Westview Press, 1990.

[35] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[36] R. Werlinger, K. Hawkey, and K. Beznosov. Security practitioners in context: their activities and interactions. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems*, pages 3789–3794. ACM, 2008.

[37] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 18(1):26–42, 2010.

11. APPENDIX A

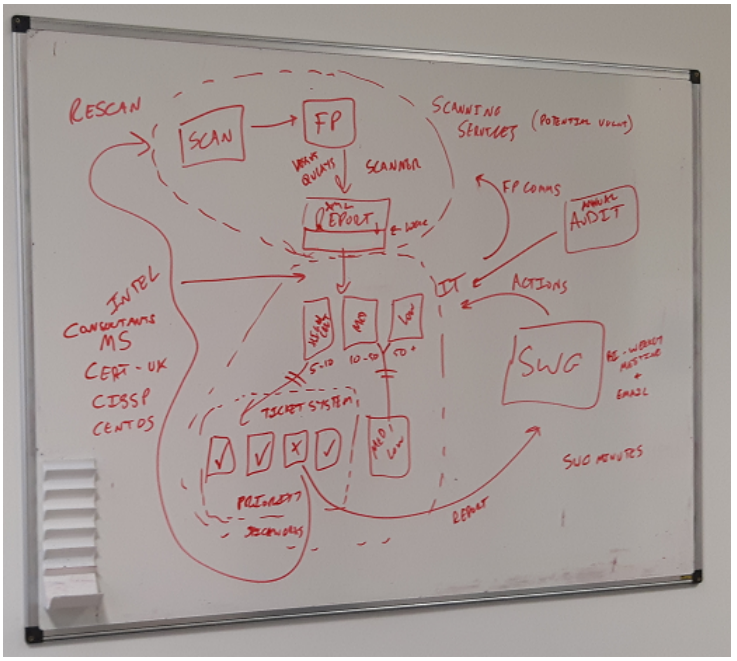

Figure 8: Sample Illustration of Work Process