Investigating the work practices of network security professionals*

Muhammad Adnan, Mike Just, Lynne Baillie, Hilmi Gunes Kayacik
Interactive and Trustworthy Technologies Group
Glasgow Caledonian University, UK

Structured Abstract:

Purpose - The purpose of this paper is to investigate the work practices of network security professionals and to propose a new and robust work practices model of these professionals.

Design/methodology/approach - The proposed work practices model is composed by combining the findings of ten notable empirical studies performed so far this century. The proposed model was then validated by an online survey of 125 network security professionals with a wide demographic spread.

Findings - The empirical data collected from the survey of network security professionals strongly validate the proposed work practices model. The results also highlight interesting trends for different groups of network security professionals, with respect to performing different security-related activities.

Research limitations/implications - Further studies could investigate more closely the links and dependencies between the different activities of the proposed work practices model and tools used by network security professionals to perform these activities.

Practical implications - A robust work practices model of network security professionals could hugely assist tool developers in designing usable tools for network security management.

Originality/value - This paper proposes a new work practices model of network security professionals, which is built by consolidating existing empirical evidence and validated by conducting a survey of network security professionals. The findings enhance the understanding of tool developers about the day-to-day activities of network security professionals, consequently assisting developers in designing better tools for network security management.

1. Introduction

In an era of global reliance on networked systems, information security becomes a major concern for most organisations (Goel and Shawky, 2009; Dlamini *et al.*, 2009). Despite the recent economic recession, the IT security market saw an increase of 12% in 2010 to 16.5 billion US dollars, and is expected to exceed 125 billion globally by 2015 (Posey *et al.,* 2014). The individuals who are at the forefront of the battle of protecting the organisational assets against unauthorised use and access are known as network security professionals. However, little is known about the work practices of these professionals. A deep understanding about the work practices of network security professionals could vastly benefit tool developers in designing effective and efficient tools for network security management (Goodall *et al.,* 2009; Shiravi *et al.,* 2012).

The definitive published version is available here: http://dx.doi.org/10.1108/ICS-07-2014-0049 to be cited as
Muhammad Adnan , Mike Just , Lynne Baillie , Hilmi Gunes Kayacik , (2015) "Investigating the work practices of network security professionals", Information & Computer Security, Vol. 23 Iss: 3, pp.347 - 367

A number of studies have been performed to examine the day-to-day activities of network security professionals. However, considerable gaps and inconsistencies remain in terms of the number of activities as well as in their descriptions. Further, previous studies have been limited to samples sizes of as few as two participants, which meant that they could not present any statistically verifiable results.

To address the limitations of existing empirical studies, we created a new work practices model to describe the high-level tasks of network security professionals, developed by merging the findings of several existing empirical studies. To confirm the robustness of the proposed model, it was validated with a survey of 125 network security professionals. Thus, the proposed model provides a broad understanding of the tasks performed by network security professionals by utilising the existing empirical evidence and complimenting it with new empirical data. In addition, the results of the survey also highlight work practice trends for different groups of network security professionals, defined by the job titles of the respondents, their daily exposure to network security, sector and size of their organisations and security management model (SMM) employed by their organisations.

2. Defining a network security professional

Defining a network security professional on the basis of job titles is a natural first approach. In such a scenario, one might consider only those with the keywords “network security” or “security” within their job titles. In reality, the network security industry is much more complex. D’Amico *et al.* (2008) note that job titles vary considerably across organisations and there is a lack of functional job descriptions of a network security professional. Previous research established that the management of network security varies considerably across organisations. For this purpose, some organisations have dedicated security staff and formal computer security incident response teams (CSIRTs); whereas, in other organisations no formal CSIRT exists and the existing IT staff also perform security-related activities (Killcrece *et al.,* 2003b; Hawkey *et al.,* 2008). To address this lack of common descriptions and to account for general IT staff (e.g. network managers and systems administrators) responsible for network security management, we avoid a reliance on job titles and define network security professionals as *“individuals who perform network security-related activities as a part of their job”*. A main contribution of this paper is to identify and define these activities.

In support of our argument, some existing empirical studies (e.g. Botta *et al.,* 2007 and Goodall *et al.,* 2009) also treated general IT staff as their targeted subjects when investigating the work practices of network security professionals. In addition, the results from our online survey confirm that individuals without the word “security” in their job titles also spend a considerable amount of time performing security-related activities on a daily basis.

3. Review of previous work practices studies

A number of empirical studies have been conducted to examine the work practices of network security professionals. Some of these studies focused on specific types of network security professionals (e.g. intrusion detection analysts and incident response practitioners), while other studies took a broader perspective. This paper reviews ten notable empirical studies performed so far this century, focusing on the work practices of “modern-day” network security professionals.

Biros and Eppich (2001) performed a cognitive task analysis, asking intrusion detection analysts to answer a set of questions from which they identified four major decision steps that take place after an alert was received. The authors did not formally name nor describe the activities, though from our analysis (see Section 4.1), the answers to these questions map to three different activities: *triage, incident verification* and *incident assessment*. In addition, the number of participants involved in their study was not disclosed. Komlodi *et al.* (2004) also investigated the work practices of intrusion detection analysts by conducting 9 contextual interviews from which they summarise the intrusion detection process as three main phases: monitoring, analysis and diagnosis, and response. From our analysis, these three phases map to seven different activities (see Table I (b)). On the one hand, they extend the findings of Biros and Eppich (2001) by identifying more activities. However, they neglected to identify the activity of *triage*. Thompson *et al.* (2006) and Goodall *et al.* (2004; 2009) similarly investigated the work practices of intrusion detection analysts. Thompson *et al.* (2006) performed a literature review and analysed empirical data from 2 interviews, describing it as a cognitive task analysis from which they summarise the intrusion detection process as four main phases: pre-processing information, monitoring the network, analysing attacks and responding to attacks. Similar to Komlodi *et al.* (2004), these four phases also map to seven different activities in our model (see Table I (c)). However, the activities identified by Thompson *et al.* (2006) differ considerably from the activities identified by Biros and Eppich (2001) and Komlodi *et al.* (2004). The findings from their study are based on empirical data gathered from only 2 interviews, undermining their generalisability. Finally, Goodall *et al.* (2004; 2009) use individual and focus group interviews to study the work practices of network intrusion detection analysts as well as a mailing list analysis and a confirmatory survey that generated 54 responses. Their findings summarise the intrusion detection workflow into four main phases: monitoring, triage, analysis and response. From our analysis, these four phases map to nine different activities (see Table I (d)). The findings of Goodall *et al.* (2009) are again inconsistent with the findings of all three reviewed empirical studies, targeting the work practices of intrusion detection analysts.

Killcrece *et al.* (2003a) examined the organisational structures, functions and services provided by CSIRTs. A pilot survey of CSIRTs, in which they were asked to indicate the services that they currently provide, generated 29 responses and identified twenty different services. However, the services/activities are only named, without any descriptions. In addition, there are considerable overlaps between the identified activities. For example, ‘monitoring IDS’ and ‘monitoring network and system logs’ are identified as two separate activities, which could have been easily abstracted into a single high-level activity of *monitoring*. Table I (e) provides a consolidated view of the activities identified by Killcrece *et al.* (2003a). Werlinger *et al.* (2010) also conducted a study to understand the diagnostic work during security incident response, interviewing 16 security practitioners belonging to seven different organisations. Their findings summarise the diagnostic work of IT security incident response into three main phases: preparation, anomaly detection and anomaly analysis. From our analysis, these three phases map to eight different activities (see Table I (f)). In contrast to Killcrece *et al.* (2003a), descriptions are provided for all of the identified activities. However, the activities only represent a subset of those identified by Killcrece *et al.* (2003a).

In contrast to the above empirical studies that focused on two particular types of network security professionals, the following four studies targeted more generic network security professionals. Stolze *et al.* (2003a, 2003b) conducted field observations to investigate the tasks of operators working in a security operations centre (SOC). They present a descriptive model of the tasks performed by SOC operators when processing the incoming stream of new security events. According to their model, this process occurs over five stages: new event triage, strange event analysis, pattern assessment, alert management and false positive management. From our analysis, these five phases map to four different activities in our model (see Table I (g)). Similar to Biros and Eppich (2001), insufficient information is provided about the field observations (e.g. number of participants and total observation time), making it difficult to draw reliable and generalisable conclusions. Kandogan and Haber

(2005) also employed field observations to study different aspects of the working life of network security professionals, including their day-to-day activities. They profiled two typical security administrators and described five real-life security-related case studies involving the administrators. They do not explicitly name the activities, though from our analysis, their findings map to eleven different security-related activities (see Table I (h)). However, a relatively small sample size of only two subjects limits the generalisability of their findings. Botta *et al.* (2007) relied on interviews to understand the workplace and tools of network security professionals. They conducted fourteen semi-structured interviews and identified fifteen different tasks/activities performed by network security professionals. The authors only name these activities and do not provide any descriptions, though they provide examples of how different tools are used to perform these activities. However, there are considerable overlaps between the activities. For example, they present 'verify configuration of email services' and 'patch or upgrade systems' as two separate activities, which could have been abstracted into a single high-level activity of *configuration and maintenance*. Werlinger *et al.* (2009) further extends their findings by analysing sixteen more semi-structured interviews and identifying (and describing) two additional activities, named 'develop security policies' and 'train and educate'. Table I (i) provides a consolidated view of the activities identified by these two studies. Finally, D'Amico *et al.* (2005; 2008) studied 41 computer network defence analysts, using semi-structured interviews, observations, a review of critical incidents, and a hypothetical scenario construction. They identified six main analysis roles that accounted for all of the cognitive work observed: triage analysis, escalation analysis, correlation analysis, threat analysis, incident response analysis and forensic analysis. From our analysis, these six roles map to eight different activities of network security professionals (see Table I (h)). This set of activities is again inconsistent with the findings of all of the other reviewed studies performed in this area.

Despite the undeniable contribution of the existing empirical studies, considerable gaps and inconsistencies remain in the description of the work practices of network security professionals. For example, some studies only relied on the names of the day-to-day activities and did not provide any descriptions, which can be problematic due to a lack of uniform, accepted descriptions. The inconsistencies appear in both the number of activities identified as well as in their descriptions. This necessitates the need to develop a new and consistent work practices model to describe the high-level tasks of network security professionals.

4. Proposed work practices model

4.1 Methodology

The reviewed empirical studies employed a diverse range of research methodologies, ranging from relatively informal approaches (e.g. authors' collective experience and survey follow-up discussions), to more formal, scientific methods (e.g. interviews, field observations and surveys). Thus, a good foundation of research has taken place regarding the work practices of small groups of users. We utilise this empirical evidence and create our proposed work practices model by merging, splitting, naming, renaming and rearranging the names and descriptions of the activities identified by the reviewed empirical studies. It is important to note that, to compose the proposed model, we only consider empirical studies and do not consider other literature that base their findings or recommendations on non-empirical data, e.g. CERT handbook (West-Brown *et al.,* 2003) and NIST guidelines (Cichonski *et al.,* 2012). Also, the scope of the proposed work practices model is to identify only the security-related activities of network security professionals; it does not consider generic activities such as Internet searching, project management and network design.

Merging: Where a reviewed study identified similar activities with slightly different names or descriptions, the activities were merged together and renamed appropriately. This was done both within a particular empirical study, and also to activities from multiple reviewed studies. For example, Killcrece *et al.* (2003a) identified two activities, *artefact analysis* and *virus handling*, which were merged and renamed as 'artefact handling'. In this case, the authors did not provide activity descriptions so that our decision was based upon the activity names alone. On the other hand, Komlodi *et al.* (2004) do not specifically name the activity, but categorise the inspection of artefact as one of the activities of the analysis phase. Similarly, Kandogan and Haber (2005) do not name the activity, though they observe a security administrator collecting information about MyDoom virus to understand its mechanics. The description of this activity was composed by combining the descriptions of Komlodi *et al.* (2004) and Kandogan and Haber (2005).

Splitting: Where a study identified activities that were broad in nature and we had empirical evidence from other studies suggesting that these activities are decomposable as multiple security-related activities in practice, the activity was divided into an appropriate number of small activities, and renamed accordingly. For example, Killcrece *et al.* (2003a) identified an activity, *incident handling*, where empirical evidence from other studies (e.g. Komlodi *et al.,* 2004; Werlinger *et al.,* 2010) suggested that there are multiple security-related activities as part of *incident handling*. Therefore, this activity was divided into a number of smaller activities, corresponding to three high-level activities in our model: *incident detection, incident analysis* and *incident response*.

Some of the reviewed studies described the work practices of network security professionals as phases, instead of activities. In most cases, these phases incorporated several security-related activities that were not explicitly named within the descriptions. For example, Goodall *et al.* (2009) describe 'response' as one of the four phases of the work practices of intrusion detection analysts, though further analysis identified four security-related activities. Their descriptions were compared with the findings of other reviewed empirical studies and were named as *incident containment, forensic analyses, internal feedback* and *external feedback* within the proposed work practices model.

Naming: In some cases, the studies described potential security-related activities but did not explicitly name them. Biros and Eppich (2001) and Kandogan and Haber (2005) did not name any of the activities of network security professionals. Instead, Biros and Eppich (2001) present them as four major decision steps that take place after an alert is received, which involve answering four different questions, such as 'what was the depth of the compromise?'. Kandogan and Haber (2005) describe the activities as the profiles of two security administrators and present five real-life case studies encountered by them. In such a scenario, the descriptions of the potential security-related activities were compared with the findings of other reviewed empirical studies to ascertain their validity. In a case where sufficient empirical evidence was found in favour of a description, the activity was appropriately named and described. For example Biros and Eppich (2001) describe answering the above question as one of the major decision steps taken by an intrusion detection analyst. This process was compared with the findings of other reviewed empirical studies and it was found to coincide with *incident assessment*.

Renaming: Activity renaming was usually instigated together with merging, splitting and rearranging. Though in some cases, when the majority of the reviewed studies identified an activity with similar names and one or a few studies identified the same activity with a different name, then the latter was renamed. Renaming also occurred when the description of an activity strongly suggested that the current name is inappropriate. For example, Stolze *et al.* (2003b) identified the *internal feedback* activity of the proposed model with the name of *false positive management*. However, when the description of the activity was composed by combining the findings of multiple reviewed studies, this name did not fit well with the scope of the activity.

Rearranging: In some cases, the reviewed studies identified standalone activities, but we either had considerable evidence from other studies, or it was apparent from the descriptions of the activities, that they would be better suited as sub-activities. In such a scenario, the activity under consideration was rearranged as a sub-activity of a suitable main activity. Rearranging was also performed when the reviewed studies identified an activity as a sub-activity, but we either had substantial evidence from other reviewed studies, or a strong indication from its description suggesting the opposite. In such a scenario, the activity under consideration was rearranged from a sub-activity to a main activity. For example, D'Amico and Whitley (2008) identify *incident assessment* as a standalone activity. However, the description of the activity as well as three separate studies (Komlodi *et al.* (2004); Goodall *et al.* (2009); Werlinger *et al.* (2010)) suggest that *incident assessment* is a sub-activity of a main, high-level activity of *incident analysis*, which is incorporated into our model.

4.2 Work practices model of network security professionals

Following the aforementioned methodology, ten main security-related activities were identified, which constitute our proposed work practices model of network security professionals. In addition, there are also eleven sub-activities that fall under the main activities of *incident detection, incident analysis, incident response* and *feedback*. Table I (row 1) presents the work practices model, providing a side-by-side comparison of the activities identified by the reviewed empirical studies.

[Insert Table I here]

It is important to note that while we are not concerned about the order of the activities, we present the proposed work practices model according to what seems to be a natural order for performing some specific network security tasks. For example, it would seem natural to detect an incident before its analysis. However, the reader should not take this model as strictly linear. Below, the activities of the proposed work practices model are listed, with their full descriptions. The descriptions are the same as those used as part of our survey validation (see Section 5), except that *configuration and maintenance* and *network security assessment* were slightly modified as a result of feedback from our survey of network security professionals (we explain this further in Section 5.2.3).

1. *Configuration and maintenance:* Configuration and maintenance of security infrastructure, tools or services (e.g. demilitarized zones, VLANs, IDS, anti-viruses, remote access and authentication mechanisms).
2. *Threat analysis:* Analysis of external data sources (e.g. security mailing lists, hackers' websites and news articles) to learn about new bugs, vulnerabilities or attacks; or to predict the identity, motives or sponsorship of an attacker.
3. *Network security assessment:* Assessing the security of an organisation's network based on the requirements defined by the organisation or by other applicable industry standards (e.g. ISO 27001 [1] and ICO guidelines [2]).
4. *Incident detection:* Detection of suspicious events within the monitored network. This can be divided into the following four sub-activities:

    i. *Monitoring:* Surveillance of an internal network through automated systems (e.g. IDSs, firewalls, Cacti and SmokePing) to discover potentially malicious activities.
    ii. *Received notifications:* Receiving notifications from different stakeholders (e.g. end-users, colleagues and external organisations) to discover potentially malicious activities.
    iii. *Data correlation:* Correlation of current and historical data from a single source (e.g. packet captures, network flows and IDS alerts), or correlation of data from multiple sources, to find new and unexplained patterns for further analysis.
    iv. *Triage:* Quickly dismissing a suspicious event as a false positive or prioritising it for further analysis.

5. *Incident analysis:* In-depth analysis of the suspicious incidents that have been detected. It encompasses the following three sub-activities:

    i. *Incident verification:* Analysis of data collected from multiple sources (e.g. packet captures, network flows and system logs) to establish that a compromise has actually occurred.
    ii. *Artefact handling:* Collecting copies of artefacts (e.g. computer viruses, exploits and toolkits) from compromised systems, analysing their mechanics and effects and developing response strategies.
    iii. *Incident assessment:* Examining the nature and scope of the incident, the extent of damage caused and available response strategies.

6. *Incident response:* Taking action in response to a successful intrusion. This can be divided into the following two sub-activities:

    i. *Incident containment:* Taking or assigning the appropriate measures (e.g. cleaning the infected system, disconnecting the infected node and rebuilding a system) in response to a successful intrusion.
    ii. *Forensic analysis:* Collection, preservation and analysis of evidence from a compromised system in support of a law enforcement investigation.

7. *Feedback:* Providing feedback to an internal environment and to the external community. This can be divided into the following two sub-activities.

    i. *Internal feedback:* Providing feedback to the internal environment (e.g. removing or tuning an IDS signature, adding a firewall rule and notifying a colleague).
    ii. *External feedback:* Providing feedback to the external community (e.g. informing the community or the vendor of the product about new vulnerabilities or attacks and producing technical documents).

8. *Security policy development:* Developing or auditing an organisation's security policies based on the requirements defined by the organisation or by other applicable industry standards.

9. *Development of security tools:* Development of new security tools, scripts, patches or plug-ins.

10. *Training and awareness:* Training and educating different constituents (e.g. end-users and new employees) about security issues and organisational security policies.

5. Validation of the proposed work practices model

5.1 Methodology

In order to assess the robustness of the proposed model, it was validated by conducting an online survey of network security professionals. By using a survey we can reach a wide geographical spread of professionals and a large number of responses can be collected in a short time, at a low cost. For this reason, a survey was an appropriate method to fit our purpose, which is to validate our consolidation of existing empirical evidence (primarily gathered using other research methods, e.g. interviews and field observations) in a new work practices model. Of six survey questions, five were related to participant information: job titles (question 1), daily time spent on security-related activities (question 2), sectors of their organisations (question 3), organisation size (question 4) and organisation security management model (SMM) (question 5). Question 6 was the primary question used to validate the activities of the proposed work practices model. For each activity, the respondents were asked whether the activity was 'performed by me', 'performed by a colleague' and/or 'never performed'. Respondents were then asked to specify any other security-related activities, other than the ones presented to them in our model.

5.2 Findings

The online survey generated 125 responses for the six questions. The spread of responses gathered from questions 1-5, is presented in Table II.

[Insert Table II here]

5.2.1 Job titles and daily exposure to network security

The survey received responses from individuals with 25 different job titles, which were grouped logically in Table III. 14 out of 25 job titles included the word "security" or a similar keyword (e.g. penetration tester, information assurance analyst and technical privacy leader), and were categorised as "security professionals". Similarly, 3 job titles were related to networking (e.g. network administrator and network engineer), and grouped as "network professionals". 2 job titles were related to systems (systems administrator and systems engineer), and categorised as "systems professionals". The remaining 6 job titles (e.g. technology strategist, consultant and DevOps) did not fit in any of the afore-mentioned categories, and were classified as "other".

Table III presents the relationship between these demographic groups and the amount of time they spend on performing security-related activities on a daily basis. These results highlight a reasonably close match between security title and the performance of security-related activities. For example, more than 75% of the security professionals spend more than half of their time on security-related activities, with only 13% and 15% respectively for network professionals and systems professionals.

[Insert Table III here]

5.2.2 Validation of the proposed work practices model

The results of the online survey strongly validate the proposed work practices model of network security professionals. Figure 1 presents the validation results for each activity of the model. In particular, note that all but one activity is “never performed” by less than 20% of respondents.

[Insert Figure 1 here]

5.2.3 Newly identified activities by survey respondents

In addition to validating the activities of the proposed model, 19 respondents identified 41 potentially new security-related activities, though we determined that 12 activities were too generic for our model (not specific to network security), e.g. *business continuity planning*, *project coordination* and *network design*. From the remaining 29 security-related activities, 24 were fully covered by existing activities of our model. For example, *threat intelligence gathering, network and mobile forensic* and *remote access services* are fully covered by the activities of *threat analysis, forensic analysis* and *configuration and maintenance* respectively. The remaining 5 security-related activities specified by the respondents were partially covered by 2 activities (*configuration and maintenance* and *network security assessment*) of the proposed work practices model. Therefore, the descriptions of these 2 activities were slightly modified in order to fully embrace 5 security-related activities identified by 5 different survey respondents, as described below.

Firstly, two respondents each described one additional security-related activity: “design, implementation and deployment of distributed federated identity systems” and “configuration and maintenance of policies which are not seen as security-specific but which have security as part of their role, e.g. routing policies”. Both of these activities are related to the configuration and maintenance of network security infrastructure. Our proposed work practices model had an activity, *configuration and maintenance*, to deal with the configuration and maintenance of security tools and services, but not the security infrastructure. Therefore, the description of *configuration and maintenance* activity of the proposed model was correspondingly updated (see Section 4.2).

Secondly, three survey respondents each described one additional security-related activity: “liaise with legal/regulatory functions (e.g. ICO and FCA)”, “ISO 27001 information security audit” and “IT compliance”. These three activities are related to network security audit/assessment based on the requirements defined by external regulatory authorities. The proposed work practices model had an activity, named *network security assessment*, to deal with network security audits based on the requirement defined by the organisation itself, but not the external regulatory authorities. Therefore, the description of *network security assessment* activity of the proposed model was correspondingly updated (see Section 4.2).

5.3 Work practice trends for different groups

The relatively large sample size of the online survey enables us to present the work practice trends for different groups of network security professionals. These trends could be of great interest to an individual who is investigating a particular section of the population or interested in comparing the behaviour of multiple groups. The groups (see Table II) were created on the basis of the job titles of the respondents, their daily exposure to network security, sector of their organisations, size of their organisations and SMM employed by their organisations.

In order to examine the impact of job title and daily exposure to network security on the work practices, the number of respondents answering “performed by me” [3] for each activity of the work practices model was calculated for each group. When examining the impact of size, sector and SMM employed by an organisation, the number of respondents answering “performed by me” and/or “performed by a colleague” [4] was calculated. Subsequently, a two-tailed Fisher’s exact test was performed to determine any statistically significant differences between the groups. To correct for multiple comparisons, pairwise comparisons were performed using Fisher’s exact test with Bonferroni adjusted alpha on the groups being identified as having statistically significant differences. The potential criticism against Bonferroni adjustments is that it is relatively conservative since it reduces the probability of a type I error [5], but at the expense of a type II error [6]. Therefore, the decision of whether or not to use the Bonferroni corrections depends on the circumstance of each study (Perneger, 1998). In this study (1) a large number of tests were carried out without pre-planned hypotheses and (2) it was imperative to avoid a type I error, i.e. detecting an effect that is not present. Both of these scenarios made it appropriate to use the Bonferroni corrections for pairwise comparisons within this study (Perneger, 1998; Armstrong, 2014).

In each of the subsections below, a number of statistically significant differences are identified between groups and their performance of certain activities. For example, the number of "systems professionals" who perform the *configuration and maintenance* activity is statistically significantly greater than the number of "security professionals". Such relative comparisons are key to understanding the relationship between different professional groupings, and should be used to help guide further studies, as well as more appropriate tool design. Table IV summarises the results of work practice trends for different groups.

[Insert Table IV here]

5.3.1 Impact of job title on performing day-to-day activities

The job titles of the survey respondents led to the creation of four groups (see Table IV). Fisher's exact test yields a statistically significant difference between these four groups (α=0.05) for the activities of *configuration and maintenance* (p<0.001), *monitoring* (p=0.007), *received notifications* (p=0.019), *incident containment* (p=0.033) and *training and awareness* (p=0.004), with no statistically significant difference for the remaining activities. Further pairwise comparisons with Bonferroni adjusted alpha (0.05/6 = 0.008) yields the following results:

- *Configuration and maintenance:* A statistically significantly larger proportion of "network professionals" (p=0.006) and "systems professionals" (p<0.001) perform this activity, compared to "security professionals".
- *Monitoring:* A statistically significantly larger proportion of "network professionals" perform this activity, compared to "security professionals" (p=0.003).
- *Received notifications:* A statistically significantly larger proportion of "network professionals" perform this activity, compared to "security professionals" (p=0.008).
- *Incident containment:* No statistically significant difference was found within any of the 6 pairwise comparisons.
- *Training and awareness:* A statistically significantly larger proportion of "security professionals" perform this activity, compared to "network professionals" (p=0.006).

The remaining pairwise comparisons for the aforementioned activities did not show any statistically significant difference.

5.3.2 Impact of daily exposure to network security on performing day-to-day activities

Four groups were created on the basis of daily time spent on performing security-related activities by the survey respondents (see Table IV). Fisher's exact test yields a statistically significant difference between these four groups (α=0.05) for the activity of *artefact handling* (p=0.023), with no statistically significant difference for the remaining activities. Pairwise comparisons with Bonferroni adjusted alpha (0.05/6 = 0.008) showed a statistically significantly larger proportion of network security professionals who spend "25% to 50%" of their daily time on security-related activities, performing the activity of *artefact handling,* compared to professionals who spend "less than 25%" of their daily time (p=0.008). The remaining 5 pairwise comparisons for this activity did not show any statistically significant difference.

5.3.3 Impact of organisation's sector on performing day-to-day activities

The survey received responses from 16 different organisational sectors. A logical grouping was performed to combine similar organisational sectors into the same category. In cases where an organisational sector did not provide a sufficient number of responses for statistically viable results, they were combined to form more general, larger groupings (e.g. "other"). Though, this did result in losing a logical theme for the group. This process led to the creation of three groups (see Table IV).

Fisher's exact test yields a statistically significant difference between these three groups (α=0.05) for the activity of *training and awareness* (p=0.037), with no statistically significant difference for the remaining activities. For *training and awareness*, none of 3 pairwise comparisons with Bonferroni adjusted alpha (0.05/3 = 0.017) yield any statistically significant difference.

5.3.4 Impact of organisation's size on performing day-to-day activities

Four groups were created on the basis of the organisation's size of the survey respondents (see Table IV). Fisher's exact test yields a statistically significant difference between these four groups (α=0.05) for the activities of *incident assessment* (p=0.016) and *external feedback* (p=0.002), with no statistically significant difference for the remaining activities. Further pairwise comparisons with Bonferroni adjusted alpha (0.05/6 = 0.008) yields the following results:

- *Incident assessment:* No statistically significant difference was found within any of the 6 pairwise comparisons.
- *External feedback:* A statistically significantly larger proportion of network security professionals working within organisations having "50 to 249" employees perform this activity, compared to organisations employing "less than 50" people (p=0.002) or organisations employing "250 to 1000" people (p<0.001). The remaining 4 pairwise comparisons did not show any statistically significant difference.

5.3.5 Impact of different SMMs on performing day-to-day activities

The data about the SMMs employed by the organisations of the survey respondents also led to the creation of four groups (see Table IV). The SSMs and their descriptions were adopted from Killcrece *et al.* (2003b) and Hawkey *et al.* (2008).

Fisher's exact test yields a statistically significant difference between these four groups (α=0.05) for the activities of *network security assessment* (p<0.001), *data correlation* (p=0.001), *triage* (p=0.041) and *incident assessment* (p=0.023), with no statistically significant difference for the remaining activities. Further pairwise comparisons with Bonferroni adjusted alpha (0.05/6 = 0.008) yields the following results:

- *Network security assessment:* A statistically significantly larger proportion of network security professionals working within organisations that employ a centralised SSM model (p=0.005) or hybrid SMM model (p<0.001) perform this activity, compared to professionals who work within organisations that do not employ any SMM model. The remaining 4 pairwise comparisons did not show any statistically significant difference.
- *Data correlation:* A statistically significantly larger proportion of network security professionals working within organisations that employ a hybrid SMM model (p=0.004) perform this activity, compared to professionals who work within organisations that do not employ any SMM model. The remaining 5 pairwise comparisons did not show any statistically significant difference.

- *Triage* and *Incident assessment:* No statistically significant difference was found within any of the 12 pairwise comparisons for these two activities.

6. Discussion and implications

The results of our study provide two key contributions toward a more complete understanding of network security professionals. Firstly, we propose a robust work practices model of network security professionals, which is created by utilising the existing empirical evidence and validated by gathering new empirical evidence through an online survey of 125 network security professionals. This model provides a relatively deep and broad understanding about the day-to-day activities performed by network security professionals, which could vastly benefit tool developers in designing and developing effective and efficient tools for network security management. The activities and their descriptions within the proposed model provide an outline of the functionalities for a usable tool, targeting one or a few specific activities. For example, if a tool developer intends to build a tool to support the activity of *incident analysis*, the proposed model would inform him/her that the process of *incident analysis* involves *incident verification, artefact handling* and *incident assessment.* Therefore, a usable tool targeted for *incident analysis* needs to provide sufficient functionality to perform the aforementioned sub-activities. This may include the support for analysing data collected from a diverse set of sources (e.g. packet captures, network flows and system logs), collection and analysis of artefacts (e.g. computer viruses, exploits and toolkits), and examination of the nature and scope of the incident, the extent of damage caused and available response strategies. In the absence of our proposed model, security management tool developers would not be able to acquire this level of details regarding the required functionalities of a particular tool, due to the numerous gaps and inconsistencies in the existing work practices models of network security professionals (see Table I).

Secondly, we identify some interesting work practice trends for different groups of network security professionals, which are summarised in Table IV. For example, a common perception about "network professionals" is that they are mainly concerned with the configuration and maintenance of network-related devices (e.g. switches, routers and network health/performance monitoring tools), and not with the *configuration and maintenance* of security-related devices (e.g. firewalls, IDSs/IPSs and anti-viruses) or the process of incident detection (i.e. *monitoring* and *received notifications*). However, this study highlights that a statistically significantly larger proportion of "network professionals" perform the security-related activities of *configuration and maintenance*, *monitoring* and *received notifications,* as compared to "security professionals". This is an interesting finding for which there could be several possible explanations. For example, in many organisations no dedicated security staff exists and the existing IT staff also perform security-related activities (Killcrece *et al.,* 2003b; Hawkey *et al.,* 2008). This was also confirmed in our online survey of network security professionals, in which around 31 percent respondents replied to be working within the organisations that do not have dedicated security staff. Also, *configuration and maintenance*, *monitoring* and *received notifications* are just three of seventeen security-related activities of network security professionals. Considering the scope and criticality of the remaining fourteen security-related activities, we think that even in organisations with dedicated security staff, it is highly likely that relatively less complex activities (e.g. *configuration and maintenance* and *monitoring*) are assigned to generic IT staff (e.g. network and systems professionals) while the dedicated security professionals are delegated to relatively complex and critical tasks (e.g. *network security assessment, incident analysis* and *incident response*). Both of the above reasons could potentially have led to the performance of the activities of *configuration and maintenance*, *monitoring* and *received notifications* by statistically significantly larger proportion of “network professionals”, as compared to “security professionals”.

7. Limitations and future work

While our approach allowed us to investigate in detail the work practices of network security professionals, this approach was not without limitations. An online questionnaire enabled us to gather a relatively large number of responses from a wide geographical spread of professionals, which was imperative to build a robust work practices model. However, this restricted us from gathering rich qualitative data, which could have been used to explore in detail different interesting trends highlighted in Section 6 of the paper. Also, while we have a reasonable spread of survey responses (see Table II) in terms of respondents’ daily time spent on security-related activities, a slightly higher participation of professionals who spend more than 50% of their time on security-related activities could have created a better mix, potentially enhancing the robustness of the proposed work practices model.

A relatively broad understanding of the work practices of network security professionals also highlights some apparent dependencies between the day-to-day activities of network security professionals. For example, incident detection initiates incident analysis, which then triggers the incident response. However, further empirical research is needed to explore these links and dependencies in greater detail. Further studies might also investigate the tools used by network security professionals to perform different security-related activities, in an effort to identify particular features that need to be added or require improvements, e.g. flexible reporting, support for collaboration and information sharing, and support for task prioritisation.

8. Conclusion

This work reviews several existing empirical studies and highlights numerous gaps and inconsistencies in the description of the work practices of network security professionals. It also merges existing empirical evidence to create a new and more consistent work practices model of network security professionals. The robustness of the proposed model is confirmed by conducting an online survey of 125 network security professionals with a wide demographic spread. The model itself should be a useful aid to tool developers, thus better meeting the needs of network security professionals. The findings of the survey also highlight interesting trends for different groups of network security professionals, with respect to performing different activities, which should help to better meet the needs of these groups.

Acknowledgments

The authors would like to thank the participants that responded to the survey. The research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Union's 7th Framework Programme (FP7/2007-2013) under REA grant agreement PIIF-GA-2011-301536.

Notes

1. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
2. http://ico.org.uk
3. Job title and daily exposure to network security are traits that are linked with individuals, and not with organisations. Therefore, only a “performed by me” response can equate to an activity being performed by an individual. In this case, there remains no difference between the responses of “performed by a colleague” and “never performed”.

4. Organisational sector, organisational size and SMM employed by an organisation are traits that are linked with organisations, and not with individuals. Therefore, both the "performed by me" and "performed by a colleague" responses equate to an activity being performed within an organisation.
5. In statistical hypothesis testing, a type I error is an incorrect rejection of a true null hypothesis. More simply, a type I error is detecting an effect that is not present.
6. In statistical hypothesis testing, a type II error is a failure to reject a false null hypothesis. More simply, a type II error is failing to detect an effect that is present.

References

Armstrong, R. A. (2014), "When to use the Bonferroni correction", *Ophthalmic and Physiological Optics*, Vol. 34, No. 5, pp. 502-508.

Biros, D.P. and Eppich, T. (2001), "Human element key to intrusion detection", available at: http://www.afcea.org/content/?q=node/516 (accessed 7 January 2014).

Botta, D., Werlinger, R., Gagne, A., Beznosov, B., Iverson, L., Fels, S. and Fisher, B. (2007), "Towards understanding IT security professionals and their tools", in *Proceedings of Symposium on Usable Privacy and Security (SOUPS),* ACM, pp. 100-11.

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012), "Computer security incident handling guide", available at: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf (accessed 10 February 2014).

D'Amico, A. and Whitley, K. (2008), "Real Work of Computer Network Defense Analysts", in in *Proceedings of VizSEC 2007*, Springer, Heidelberg, pp. 19-37.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B. and Roth, E. (2005), "Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts", in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 49, No. 3, pp. 229-233.

Dlamini, M. T., Eloff, J. H. and Eloff, M. M. (2009), Information security: The moving target, *Computers & Security*, Vol. 28 No. 3, pp. 189-198.

Goel, S., and Shawky, H. A. (2009), Estimating the market impact of security breach announcements on firm values, *Information & Management*, Vol. 46, No. 7, pp. 404-410.

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2004b), "The work of intrusion detection: rethinking the role of security analysts", in *Proceedings of 10th Americas Conference on Information Systems (AMCIS), New York, NY,* pp. 1421-1427.

Goodall, J. R., Lutters, W. J. and Komlodi, A. (2009), "Supporting intrusion detection work practice", *Journal of Information System Security*, Vol. 5, No. 2, pp. 42-73.

Hawkey, K., Muldner, K. and Beznosov, K. (2008), "Searching for the right fit: balancing IT security management model trade-offs". *Internet Computing, IEEE*, Vol. 12, No. 3, pp. 22-30.

Komlodi, A., Goodall, J. R. and Lutters, W. G. (2004), "An information visualization framework for intrusion detection", in *CHI'04 extended abstracts,* ACM, pp. 1743-1746.

Kandogan, E. and Haber, E.M. (2005), “Security administration tools and practices”, in *Security and Usability: Designing Secure Systems that People Can Use*, O’Reilly, Sebastopol, CA, pp. 357-78.

Killcrece, G., Kossakowski, K., Ruefle, R. and Zajicek, M. (2003a), “State of the practice of computer security incident response teams (CSIRTs)”, available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf (accessed 12 January 2014).

Killcrece, G., Kossakowski, K.P., Ruefle, R. and Zajicek, M. (2003b), “Organizational models for computer security incident response teams (CSIRTs)”, available at: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf (accessed 20 January 2014).

Perneger, T. V. (1998), “What's wrong with Bonferroni adjustments”, *BMJ*, Vol. 316, No. 7139, pp. 1236-1238.

Posey, C., Roberts, T. L., Lowry, P. B. and Hightower, R. T. (2014), “Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders”, *Information & Management*, Vol. 51, No. 5, pp. 551-567.

Shiravi, H., Shiravi, A., and Ghorbani, A. A. (2012), “A Survey of Visualisation Systems for Network Security”, *IEEE Transactions on Visualization and Computer Graphics*, Vol. 18, No. 8, pp. 1313-1329.

Stolze, M., Pawlitzek, R. and Hild, S. (2003a), “Task support for network security monitoring”, in *Proceedings of the SIGCHI Workshop on System Administrators Are Users, Too: Designing Workspaces for Managing Internet-Scale Systems,* ACM.

Stolze, M., Pawlitzek, R. and Wespi, A. (2003b), “Visual problem-solving support for new event triage in centralized network security monitoring: challenges, tools and benefits”, in *Proceedings of the international conference on IT-Incident Management & IT-Forensics (IMF),* pp. 67-76.

Thompson, R.S., Rantanen, E. and Yurcik, W. (2006), “Network intrusion detection cognitive task analysis: textual and visual tool usage and recommendations”, in *Proceedings of Human Factors and Ergonomics Society Annual Meeting (HFES),* Vol. 50, No 5, pp. 669-673.

Werlinger, R., Hawkey, K., Botta, D. and Beznosov, K. (2009), “Security practitioners in context: their activities and interactions with other stakeholders within organizations”, *International Journal of Human Computer Studies*, Vol. 67, No. 7, pp. 584-606.

Werlinger, R., Muldner, K., Hawkey, K. and Beznosov, K. (2010), “Preparation, detection, and analysis the diagnostic work of IT security incident response”, *Information Management & Computer Security*, Vol. 18, No. 1, pp. 26-42.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G. and Ruefle, R. (2003), “Handbook for computer security incident response teams”, available at: http://www.sei.cmu.edu/reports/03hb002.pdf (accessed 22 January 2014)

Table I:

Proposed work practices model of network security professionals		eConfiguration and	Threat analysis	ntNetwork security	Incident detection				Incident analysis			Incident response		Feedback		nentSecurity policy	olsDevelopment of	renessTraining and
					Monitoring	cationsReceived	correlationData	Triage	ficationIncident	andlingArtefact	essmentIncident	ainmentIncident	nalysisForensic	eedbackInternal	edbackExternal			
Activities identified by reviewed empirical studies [● = fully described; ○ = named only (without a description); empty cell = not mentioned]																		
a)	Biros and Eppich (2001)							○	○		○							
b)	Komlodi *et al.* (2004)				●				●	●	●	●		●		●		
c)	Thompson *et al.* (2006)	●			●		●	●	●			●					●	
d)	Goodall *et al.* (2004; 2009)		●		●			●	●		●	●		●	●		●	
e)	Killcrece *et al.* (2003a) *	○		○	○	○	○	○	○	○	○	○	○		○	○	○	○
f)	Werlinger *et al.* (2010)	●		●	●	●			●		●	●					●	
g)	Stolze *et al.* (2003a, 2003b)				●			●				●		●				
h)	Kandogan and Haber (2005)	●	●	●	●			●	●	●	●	●	●		●			
i)	Botta *et al.* (2007) ** and Werlinger *et al.* (2009)	●		●	●	●	●		●			●				●		●
j)	D'Amico *et al.* (2005; 2008)		●			●	●	●			●	●	●		●			

* Killcrece *et al.* (2003) do not explicitly name the activities of 'data correlation', 'triage', 'incident verification', 'incident assessment' and 'incident containment'. However, they identify the activity of 'incident handling', which is a relatively broad term and encompasses the aforementioned activities.

** Botta *et al.* (2007) do not provide formal descriptions of the activities, though they do present examples of how different tools are used to perform these activities. Therefore, the activities identified by them are considered as "fully described" within the table.

Table I: Proposed work practices model and mapping of activities identified by reviewed empirical studies

Table II:

Job title	
Security professionals	46.4 %
Network professionals	24.0 %
Systems professionals	20.8 %
Other (e.g. technology strategist and consultant)	8.8 %
Daily time spent on security-related activities	
Less than 25%	28.8 %
25% to 50%	26.4 %
51% to 75%	17.6 %
More than 75%	27.2 %
Organisation sector	
Information technology	46.4 %
Educational	24.0 %
Other (e.g. energy, healthcare and military)	29.6 %
Organisation size (No. of employees)	
Less than 50	18.4 %
50 to 249	21.6 %
250 to 1000	17.6 %
Over 1000	42.4 %
Organisation security management model (SMM)	
None	31.2 %
Decentralised model	9.6 %
Centralised model	34.4 %
Hybrid model	24.8 %

Table II: Spread of responses from answers to questions 1-5 as collected from the online survey

Table III:

Time spent on security-related activities (daily)	Security professionals		Network Professionals		Systems professionals		Other	
	Count	%	Count	%	Count	%	Count	%
Less than 25%	4	6.90	15	50.00	14	53.85	3	27.27
25% to 50%	10	17.24	11	36.67	8	30.77	4	36.36
51% to 75%	12	20.69	3	10.00	4	15.38	3	27.27
More than 75%	32	55.17	1	3.33	0	0.00	1	9.09

Table III: Correlation between job titles and their daily exposure to network security

Figure 1:

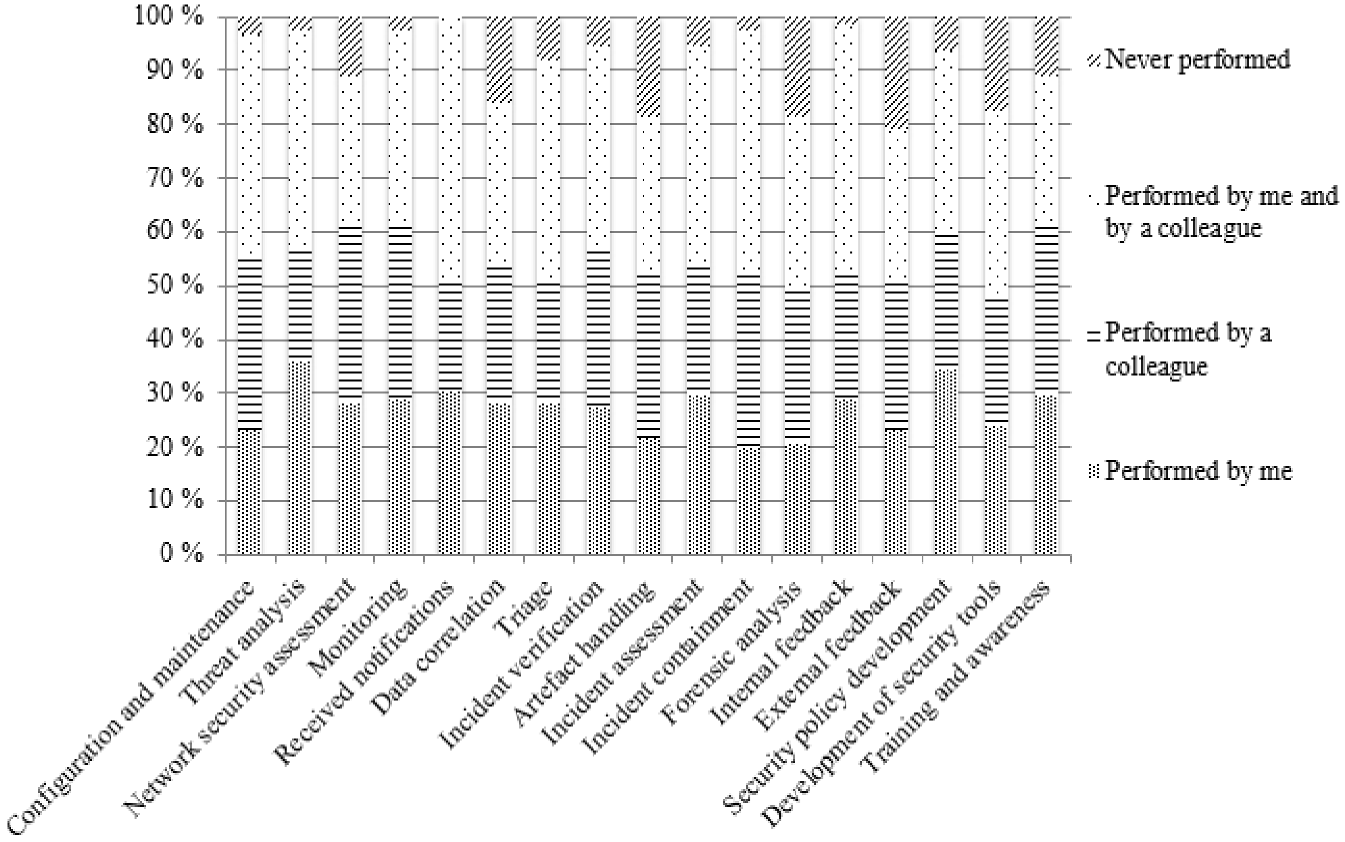

Figure 1: Validation results of the proposed work practices model

Table IV:

Demographic groups	Activities with statistically significant performance differences	Pairwise comparisons with Bonferroni adjusted alpha
Job titles of the respondents: 1. Security professionals 2. Network professionals 3. Systems professionals 4. Other	Configuration and maintenance (p<0.001)	Network professionals* vs. Security professionals (p=0.006)
		Systems professionals* vs. Security professionals (p<0.001)
	Monitoring (p=0.007)	Network professionals* vs. Security professionals (p=0.003)
	Received notifications (p=0.019)	Network professionals* vs. Security professionals (p=0.008)
	Incident containment (p=0.033)	No statistically significant difference found
	Training and awareness (p=0.004)	Security professionals* vs. Network professionals (p=0.006)
Daily exposure to network security: 1. Less than 25% 2. 25% to 50% 3. 51% to 75% 4. More than 75%	Artefact handling (p=0.023)	25% to 50%* vs. Less than 25% (p=0.008)
Sector of organisation: 1. Information technology 2. Educational 3. Other	Training and awareness (p=0.037)	No statistically significant difference found
Size of organisation: 1. Less than 50 2. 50 to 249 3. 250 to 1000 4. Over 1000	Incident assessment (p=0.016)	No statistically significant difference found
	External feedback (p=0.002)	50 to 249* vs. Less than 50 (p=0.002)
		50 to 249* vs. 250 to 1000 (p<0.001)
SMM employed by organisation: 1. None 2. Decentralised model 3. Centralised model 4. Hybrid model	Network security assessment (p<0.001)	Centralised model * vs. None (p=0.005)
		Hybrid model* vs. None (p<0.001)
	Data correlation (p=0.001)	Hybrid model* vs. None (p=0.004)
	Triage (p=0.041)	No statistically significant difference found
	Incident assessment (p=0.023)	No statistically significant difference found

* Indicates the groups with a larger proportion of members performing a particular activity.

Table IV: Summary of results of work practice trends for different groups