A Human Capital Model for Mitigating Security Analyst Burnout

Sathya Chandran Sundaramurthy
Kansas State University
sathya@ksu.edu

Alexandru G. Bardas
Kansas State University
bardasag@ksu.edu

Jacob Case
Kansas State University
jacobcase94@ksu.edu

Xinming Ou
Kansas State University
xou@ksu.edu

Michael Wesch
Kansas State University
mwesch@ksu.edu

John McHugh
RedJack, LLC.
john.mchugh@redjack.com

S. Raj Rajagopalan
Honeywell ACS Labs
siva.rajagopalan@honeywell.com

ABSTRACT

Security Operation Centers (SOCs) are being operated by universities, government agencies, and corporations to defend their enterprise networks in general and in particular to identify malicious behaviors in both networks and hosts. The success of a SOC depends on having the right tools, processes and, most importantly, efficient and effective analysts. One of the worrying issues in recent times has been the consistently high burnout rates of security analysts in SOCs. Burnout results in analysts making poor judgments when analyzing security events as well as frequent personnel turnovers. In spite of high awareness of this problem, little has been known so far about the factors leading to burnout. Various coping strategies employed by SOC management such as career progression do not seem to address the problem but rather deal only with the symptoms. In short, burnout is a manifestation of one or more underlying issues in SOCs that are as of yet unknown. In this work we performed an anthropological study of a corporate SOC over a period of six months and identified concrete factors contributing to the burnout phenomenon. We use *Grounded Theory* to analyze our fieldwork data and propose a model that explains the burnout phenomenon. Our model indicates that burnout is a human capital management problem resulting from the cyclic interaction of a number of human, technical, and managerial factors. Specifically, we identified multiple vicious cycles connecting the factors affecting the morale of the analysts. In this paper we provide detailed descriptions of the various vicious cycles and suggest ways to turn these cycles into virtuous ones. We further validated our results on the fieldnotes from a SOC at a higher education institution. The proposed model is able to successfully capture and explain the burnout symptoms in this other SOC as well.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

1. INTRODUCTION

With an increase in cyber threats, corporations and government agencies alike are establishing dedicated monitoring stations called security operation centers (SOCs). An organization can decide to build its own SOC or outsource the monitoring to managed operational service providers. The key component of any SOC, in-house or managed, is training and staffing of security analysts. Although tools and processes improve the efficiency of operations, it is the security analysts who make the final decision when analyzing a threat. Hence it is imperative for a SOC to spend adequate resources in developing and maintaining an effective team of security analysts.

In our work we wanted to find answer to an important question — How to maintain a capable and enthusiastic analyst workforce? The problem bears considerable similarity to the human capital model in economics. The Human Capital theory [13], first postulated by Adam Smith, holds that the investment made in education and training of individuals in a society is a resource in itself, more important than capital and natural resources. Security analysts are the human capital of a SOC and proper investment in their continuous improvement is key for efficient operation.

Unfortunately SOCs have been plagued by high analyst turnover due to burnout [10]. Burnout refers to diminished interest in work and is characterized by exhaustion, cynicism and inefficacy [9]. Burnout in SOCs usually results in a high analyst turnover leading to frequent hiring and training of new analysts. A white paper from Hewlett-Packard (HP) [7] points out that the life-time of a security analyst is between 1-3 years. Moreover, the volatile nature also makes it hard for analysts to know each other well, thus affecting team camaraderie, which eventually affects how the entire team responds to security incidents.

In spite of the burnout problem being well recognized, little to nothing is known about the concrete factors that cause the burnout. If the real reasons behind this issue are not identified, we will be only addressing the symptoms and not the actual problem. In order to understand challenges in a SOC environment we first had to find a way to interact with the SOC analysts. SOC analysts typically work under high stress; culturally SOCs are sensitive about talking to outsiders – such as security researchers – about operational issues. To get visibility into operational issues affecting the analysts, the research has to satisfy two requirements: (1) cause minimum interruption (and only when necessary) to the analysts; (2) gain the trust of the entire SOC so that the *real* reasons for burnout are explored.

With the above set of goals we adopted an anthropological approach to study SOC environments. Using an anthropological approach helps us attain the perspective of the analyst on exhaustion and burnout. Security analysts are typically consumed by the routines of their job that they have no time to reflect on the social issues in the SOC. Anthropology also allows the researcher to step in and out of the shoes of an analyst which helps in understanding the complex interactions not attended to by the participants.

A computer science graduate student trained in fieldwork methods by an anthropologist took up a job as a security analyst for six months in a corporate SOC. The corporation is a major information technology (IT) products and services provider headquartered in the United States. The SOC is monitoring the enterprise's network 24x7x365 for security threats. The fieldworker went through the whole new-analyst training process and at the end of it, he was able to do a junior analyst's job. Through the embedding process he earned the trust of the analysts (specific instances that led to building the trust are discussed in further sections) and also was able to simultaneously perform the research with minimum to no interruption to operations.

Daily observations of SOC activities were written down in a digital document for six months. The fieldnotes were analyzed after the fieldwork using a Grounded Theory approach. Through our analysis we found that to mitigate analyst burnout, SOCs have to pay special attention to the interaction of *human capital* with three other factors—*automation, operational efficiency*, and *metrics*. Our analysis yielded a model for human capital management in the SOC and we suggest a number of ways to mitigate analyst burnout, which is the focus of this paper. To the best of our knowledge this is the first study of the burnout problem in a SOC environment using anthropological methods.

2. ANTHROPOLOGICAL APPROACH TO STUDYING SOCS

We started our research, two years ago, with the broader goal of understanding how security analysts do their job and what happens inside a SOC [15]. Before this, our attempts towards this goal were through focused interviews with system administrators and security analysts. This approach was very hard to pursue over time as system administrators and security analysts worked under high pressure and had limited time to talk to the researchers. The other major obstacle was the issue of trust. As security monitoring is considered a sensitive job there is always some hesitation in the minds of the analysts when talking to researchers who are considered "outsiders." After years of failed attempts to truly understand security operations, we discovered that methodologies from anthropology, specifically cultural anthropology, are very relevant to studying this problem.

Anthropology is a discipline where researchers used to spend extended period of time, typically one to three years with an indigenous population. The goal of an anthropologist is to document and make explicit the various cultural aspects of the population as objective as possible. They do this through a research method called *participant observation*, where the researcher becomes one among the members of the society under study. Participant observers go through the same or similar challenges as the members of the group being observed and try to gain an empathetic perspective on the views and practices in that society.

Gaining the trust of the members of the society is a critical aspect for anthropological study. Clifford Geertz in his book Deep Play [6] talks about the experiences of studying cockfights in Bali, Indonesia. He reports that he and his fieldwork partner, both researchers, remained invisible to the villagers until one day they had to run away along with a group of Balinese people from an illegal cockfight when the police arrived to stop the fight. After this specific incident, the researchers were considered as ones among them by the Balinese people. Thus for an outsider to get accepted into a community they have to perform the same activities as the rest of the members. The acceptance leads to establishment of the trust which facilitates knowledge sharing and thus cultural understanding by the researcher.

An anthropological approach to study SOCs means that researchers become analysts and gain the acceptance – hence the trust – of the SOC members, even if it implies spending significant amount of time in the SOC. Towards this goal, our research team consists of an anthropology professor who helped train a graduate student in Computer Science in participant observation methods. One of the key elements of training was about performing reflections on daily observations in the SOC. Without periodic reflections the observations will remain just incidents without their cultural significance being understood. The student also attended a course offered by our anthropologist. This training ensured the student learned the basics of anthropological methods before conducting the fieldwork.

One important aspect of anthropological research is that it helps identify problems that the researchers may not have been aware of. The burnout problem, which includes the phenomenon and the associated causes/effects described in this paper, is one of many problems we discovered in the SOC, *without knowing them or looking for them a priori.* The phenomenon itself was known to SOC operators, but the causes and effects were not clear and there had been no systematic study of this problem in the published literature. There are also other problems we have discovered and analyzed but we will not present those in this paper in order to maintain focus and present a cogent description.

3. ETHICS AND PARTICIPANT SAFETY

The fieldworkers and the SOC analysts who were observed can be considered human subjects. Prior to starting the formal fieldwork, we obtained the appropriate IRB approvals. All participants were asked to sign an "informed consent form" approving of their participation in our research. The consent form explained clearly to the participants the goal of our research, what we expected from them, and how the fieldwork data will be used.

We took efforts to protect the privacy of the participants such as by not using real names of analysts during research discussions and also by not revealing opinions of one analyst to another. We also followed the standard practice in anthropology where the fieldnotes are accessible only to the

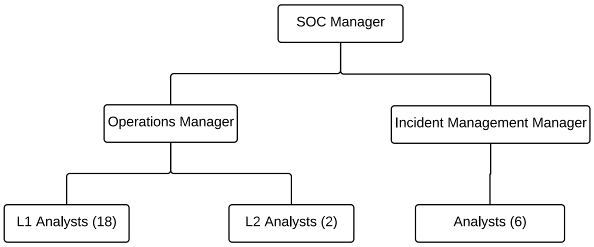

Figure 1: Organizational Chart for the corporate SOC

fieldworker who writes them. We can safely say that our research did not raise any ethical concerns for the participants.

4. FIELDWORK SETUP

Our fieldwork was conducted at a SOC run by and for a major IT products and services provider headquartered in the United States. The mission of the SOC was to monitor the network and hosts therein to identify and mitigate security threats. The network was spread all over the world and there were about 300,000 devices online on any given day. The SOC was the only monitoring station for cyber security for the corporate network spread across the globe.

The organizational layout of the SOC is shown in Figure 1. There were two different teams within the SOC: (1) operations; (2) incident management (IM). The operations team analysts were divided into two categories: Level 1 (L1) and Level 2 (L2). The L1 analysts work four days a week in 10 hour shifts while the L2 analysts work 5 days a week in 8 hour shifts. L1 analysts are the first line of defense monitoring the Security Information Event Management (SIEM) console for any possible (attempted) security breaches. The L2 analysts play more of a managerial and mentoring role for the L1 analysts. Their main job is to provide operational visibility for higher management through metrics and reports. At the time of our fieldwork there were 2 L2 and 18 L1 analysts in the operations team headed by an Operations Manager.

The IM team consisted of six analysts led by a manager. Of the six analysts two were off-site working remotely. The IM team handles incidents that are escalated from the operations team requiring in-depth analysis. The fieldworker spent three months as an L1 analyst in the operations team and the remaining three months as an incident responder in the IM team.

5. SOC DEMOGRAPHY

There were eighteen L1 and two L2 analysts in the operations team of the SOC. 15% (3 out of 20) of the analysts were female and 85% (17 out of 20) were male. 35% (7 out of 20) of the analysts had previously worked in a SOC and for 65% (13 out of 20) of them this was their first SOC experience. Among the analysts who were new to the role of SOC analyst 46% of them (6 out of 13) had worked in a job related to IT services. Of the six analysts in the IM team, one was female and five were male. Two worked previously as consultants performing forensic analysis and two had been system administrators in their previous jobs.

6. GAINING TRUST AND ACCEPTANCE

As described in Section 2 gaining acceptance of the SOC analysts and earning their trust was our initial goal. Trust of L1 analysts was gained by working alongside with them on the SIEM console processing alerts, similar to experiences of Geertz as described in Section 2. However, saturation occurred only after a few weeks of visibility into the SOC operations, as the fieldworker was just following the procedures. The procedures were very static and by following them he was consumed by the routines of an L1 analyst. He then started to identify high-severity threats that could have not been discovered by following the procedures. A number of teams were engaged in solving those high-severity cases through which he obtained the attention of senior analysts and SOC managers – he was not *invisible* anymore. At this stage everyone in the SOC – junior and senior analysts including managers – started to feel comfortable with the fieldworker.

7. DATA COLLECTION

The daily observations of SOC activity were documented in a digital document. The goal was to document every activity in the SOC without any premeditation on what to document. Often, a theme might emerge as the observations were being logged. In those situations, focused interviews were conducted with the analysts and managers to better understand the emerging concept. Taking notes while engaging in a conversation was avoided in order to focus more on the interaction. The details of the communication were transcribed into notes as soon as possible after the conversation. At the end of the six-month fieldwork, we had 85 pages of fieldnotes stored in a word-processor document.

8. GROUNDED THEORY APPROACH TO DATA ANALYSIS

Our goal in analyzing the fieldnotes was to uncover the different cultural aspects in an operational SOC environment. Grounded Theory Method (GT) [14] is a research methodology from the social sciences used to construct a theory from qualitative data such as interview transcripts, images, and video of participants. The outcome of GT-based analysis of data is a model or theory that explains the social connections represented by the data. Since we wanted to understand the burnout problem *through* fieldwork data, GT seemed to be the most appropriate analysis method.

GT analysis requires one to follow the steps of *open*, *axial*, and *selective* coding. In the open coding process labels are assigned to units of observed data. The researcher tries her best to assign codes that are not descriptive but analytical capturing the intent behind the observations. During axial coding the individual open codes are grouped into categories and sub-categories. The goal here is to understand the inter and intra categorical relationships. Finally, in the selective coding process the core category and the main concern of the participants is identified. There are a number of variations of the GT methodology and we used the one proposed by Strauss and Corbin due to its emphasis on theory development.

8.1 Open Coding

The goal of open coding was to assign short labels to fieldwork notes. Unlike other qualitative works where coding is performed by multiple people, the fieldnotes in our work were coded only by the fieldworker. In anthropological research one does not share the fieldnotes with anyone else due to privacy reasons; this is a standard practice in anthropology. Therefore, this was the rationale behind our decision to use the fieldworker as the only coder. The list of codes as they emerged were maintained in another document called the *code book*. When assigning a code to an observation, we first checked against the code book to see if any of the existing codes could be reused. If none of them were relevant to the observation at hand, a new code was generated and the process continued until we coded the entire document. The fieldwork notes made over a period of six months were 85 pages long. Below are a few examples of the codes that emerged through the open coding process.

An IM analyst expressed frustration about his current job:

> "I wanted to work in an environment where there will be continuous learning and I have started to feel that I am not learning anything new in my current job. In fact, I took the current job hoping to analyze malware every day and learn more in that process. I feel that the SOC currently is not doing any real threat detection which in turn is limiting my opportunities for learning. I have decided in my life, to spend a significant amount of time for the improvement of my career. Now I feel bad that my commitment is not paying off."

We assigned the code *lack of growth* to the observation above. This code captures the fact that the analyst felt a lack of intellectual growth, which is a major issue in maintaining a good morale.

The fieldworker and an L1 analyst were discussing an operational scenario:

> "I suggested to the analysts: why not we try to get access to the controller and lookup the data ourselves. One of the analysts said: access to the domain controller is too risky to be given to analysts."

We assigned two codes for this observation, *liability* and *restricted empowerment*. The SOC managers will be responsible if the analysts misuse the credentials and hence they chose to provide only limited privileges on the domain controller.

The open coding process was repeated multiple times. Sometimes there were too many codes which made it hard to proceed and other times the codes were not analytical enough.

8.2 Axial Coding

The goal of axial coding was to group the different codes obtained through the open coding process into categories. The categories emerged simultaneously as we were doing the open coding process. In the initial attempt of the axial coding process, where we coded around 50 percent of the fieldwork notes, we had around 10 categories. This initial attempt, which resulted in 10 categories, did not convey any useful information about the culture of the SOC. We then engaged in a few brainstorming sessions with our anthropologist. After that we repeated our coding process on the entire fieldwork notes that resulted in 4 categories at the end of axial coding. The most important result of the discussions was the identification of the various causal relationships between the four categories.

We followed the guidelines for axial coding proposed by Strauss and Corbin [14] who suggest to look for the following relationship between the codes:

- the phenomenon under study
- the conditions related to that phenomenon (context conditions, intervening structural conditions or causal conditions)
- the actions and interactional strategies directed at managing or handling the phenomenon
- the consequences of the actions/interactions related to the phenomenon

The description of codes and categories as they emerged during the early stage of axial coding process is shown in Table 1. In the end we identified *human capital, automation, operational efficiency, and metrics* as the major high-level categories.

8.3 Selective Coding

The goal of the selective coding process was to identify the *core category* and the *main concern*. The core category emerged out to be *human capital* and the main concern of the participants was the *development and maintenance of human capital*. In other words, the pressing issue in the SOC was to keep the analysts motivated at work. *Theoretical sampling* was performed when we looked for new data from the fieldnotes that supported the core category. The relationship framework between categories obtained as a result of the axial coding process was altered to focus more on the core category–the human capital.

As a result of selective coding we observed the existence of a number of *vicious cycles* connecting the core category with the rest. The final outcome was a model that explains the analyst burnout phenomenon. In the following section we explain the model in details by highlighting the effect of the vicious cycles on analyst morale and provide suggestions to turn them into virtuous ones.

9. A MODEL FOR SOC ANALYST BURNOUT

The grounded theory based analysis of our fieldwork data yielded us a model that explains the burnout of SOC analysts. In summary, the model shows that burnout occurs due to a cyclic interaction of Human Capital with the following three categories:

- Automation
- Operational Efficiency
- Management Metrics

We first describe the notion of Human Capital for the SOC – what it is and the ways it is developed. We then describe the influence of the above three categories on human capital management focusing on specific interactions that cause burnout.

Table 1: Categorization of codes at an early stage of axial coding process

Code	Meaning
Analyst Morale	
Inadequate compensation (perception)	Analyst perceives that she/he is not adequately compensated for their efforts.
Lack of growth	Analyst feels that she/he is not learning on their job.
Detailed procedures	Step by step procedures are too mundane.
Imposement	Analysts are given tasks to do without consultation.
Restricted empowerment	Inadequate privilege or access for an analyst to do their job.
Automation	
Increased workload	High event load is a good incentive for automation.
Lack of reflections	No review of procedures to look for possible automation.
Liability	Fear of responsibility hinders automation.
Operational Efficiency	
Restricted empowerment	Inadequate privilege or access for an analyst to do their job.
Poor intelligence	Incomplete information from sources outside the SOC.
Lack of cooperation	Lower efficiency due to inter-operation issue between teams.
Inadequate context	Low efficiency due to contextual information surrounding an alert.
Lack of clarity	Incomplete understanding of operational processes due to miscommunication.
Teams in silos	Inadequate communication between teams leading to inefficiencies.
Analyst Burnout	
Superficial briefings	Exhausted analysts stop providing detailed operational updates.
Cherry picking	Burned out analysts pick specific events to analyze.
Metrics	
Management visibility	Management uses metrics as a way to gain visibility into SOC operations.
Tools and workflow	Metrics influence the workflow and tools used in the SOC.
Perception	Metrics affect the perception the management has about the usefulness of the SOC.

9.1 Human capital

Human capital, in the context of a SOC, refers to the knowledge, talents, skills, experience, intelligence, training, judgment, and wisdom possessed by individual analysts and the team as a whole. Human capital can also be defined as the collective and individual intellectual stock of a SOC. Proper development and management of the human capital is crucial for the success of SOC operations. Mismanagement of human capital affects the morale of the analysts which in turn reduces operational efficiency. Our model indicates that there are four factors that influence the creation and maintenance of efficient human capital as shown in Figure 2.

- Skills
- Empowerment
- Creativity
- Growth

Next, we describe how the interaction between these factors might either lead to an effective team or an inefficient group of burned-out analysts.

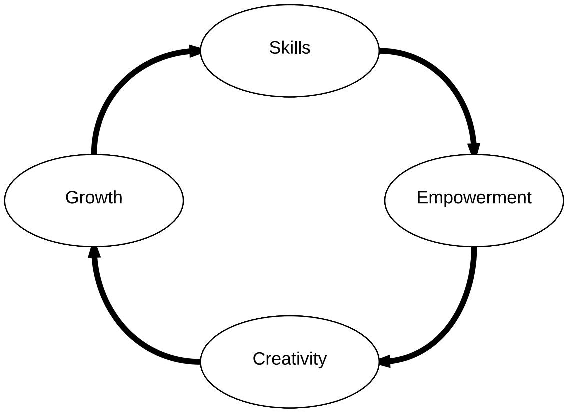

Figure 2: Human Capital Cycle

9.1.1 Skills

Security analysts need to possess the right skills to do their job. The skill set of analysts vary depending on a number of factors such as education and prior experience. The dynamic nature of security threats means the analysts have to undergo periodic training. SOCs send their analysts to paid training workshops such as those organized by SANS. The SOC also organized table top exercises for analysts to make sure they can respond to a crisis situation. Analysts were also encouraged to engage in peer training through presentations and hands-on exercises. For example, an L1 analyst who was a SOC analyst before was demonstrating a threat discovery tool. The tool took large volumes of alert information from a SIEM, summarized and provided a graphical interface to help analysts do threat discovery. The IM team also conducted training sessions on tools such as Volatility [5] and Cuckoo [4] for the operations analysts.

To summarize, development and continuous improvement of analysts' skill-set is an important aspect of human capital management. If the analysts are not adequately skilled it affects their confidence in dealing with the security alerts. Over time the lack of confidence will manifest itself as frustration, especially when their job demands them to do more than their skills level permits. SOC managers should make sure that analysts receive periodic and adequate training.

9.1.2 Empowerment

Analysts feel that they need to be adequately empowered to perform their job efficiently. An incident observed in the IM team sheds light on the importance of empowerment:

> An IM analyst expected that he be given privileged access on end user machines so that he can perform live monitoring for malicious activity on the suspicious hosts. The analyst was denied this access by the management. This led to frustration as the analyst felt that he was not able to perform his tasks efficiently.

We observed that analysts feel empowered when they were allowed to author new threat detection content or contribute to new tools development. Analysts feel enthusiastic when they see the impact of their effort in one form or the other. An L1 analyst expressed thus:

> "In my previous job as a SOC analyst, access was restricted to the alert console and what we could do was very limited. I like that in this SOC, analysts are asked to give periodic feedback on the tools and procedures. Also, I like the fact that we are encouraged to suggest new threat detection rules to the engineering team."

The skill level of the analysts influences the level of empowerment the management is willing to grant them as indicated by the causality between skills and empowerment in Figure 2. For example, only skilled analysts are trusted to be careful and are provided privileged access to user accounts. We also observed that even if analysts are highly skilled they may not always be empowered.

An IM analyst (highly skilled compared to L1 or L2 analysts) pointed out that his manager was reluctant to provide privileged access to his team due to *liability* reasons:

> "He is afraid that we, IM analysts, have accounts on social networking websites such as LinkedIn and might fall for phishing scams. He is worried that malicious entities might send us targeted emails. If one of us gets compromised, privileged credentials might be exposed and then the whole corporate network will be at risk. He does not want to give us administrator access on user accounts for this reason."

Empowerment plays a major role in boosting the morale of the analysts and SOC managers have to keep in mind this important factor. Highly skilled analysts might feel handicapped in their job when they are not adequately empowered by the management. More research is needed to understand how to provide the right amount of empowerment to the analysts while at the same time minimizing risk for the management.

9.1.3 Creativity

Creativity refers to the ability of analysts to handle an operational scenario that differs significantly from those they have encountered so far. The human capital model in Figure 2 indicates that empowerment directly affects analysts' creativity. If an analyst is adequately empowered, the analyst will be more willing to deviate from the operational norms. Usually, norms are written down procedures which severely inhibit creativity if analysts are not empowered. Lack of creativity will lead to analysts just executing the procedures failing to react appropriately to a novel operational scenario.

Another observation highlights the impact of "lack of creativity" on operations:

> "An analyst encountered an operational scenario where he had to email a member of a business unit to validate an alert but was very hesitant to proceed. After waiting for a while he contacted a senior analyst and asked him for advice on how to proceed. The junior analyst specifically said that he does not know how to proceed as this scenario was not covered by any of the procedures."

On the other hand, members of the IM team were more creative than L1 analysts. We observed that IM analysts were constantly trying to learn new technologies and this behavior was encouraged by their manager. The IM analysts were empowered as they were more skilled than the L1 analysts in the SOC. Thus one can see the causal influence between skills, empowerment, and creativity.

We also observed that the lack of variation in the operational tasks lead to lower creativity levels. The daily alerts received by the SOC are very much alike, which means an analyst has to take the same response steps for each of the received alerts. To summarize, creative development is an important aspect of human capital management. Empowerment plays an important role in ensuring creativity. The SOC management also must make sure that they find ways to engage their analysts in creative activities when the operational tasks get repetitive.

9.1.4 Growth

Growth in the context of the SOC refers to increase in the intellectual capacity of the analysts. Learning on-the-job is one of the dominant ways through which an analyst achieves growth. An analyst, by handling different types of security incidents, learns new skills and improves her knowledge on security analysis. This learning improves her morale as it gives a sense of purpose and accomplishment. As it can be observed in Figure 2, growth is directly influenced by creativity. Mundane daily activities will lead to lower creativity development. Lower creativity means the analyst will use the same set of skills everyday in the job which in turn inhibits intellectual growth. Growth also occurs through learning from role models – an analyst learns from a more experienced one.

We observed that highly empowered analysts sometimes were not satisfied with their growth because of lack of creativity in their job. During a conversation with an IM analyst, who had relatively higher empowerment than an L1 or L2 operational analyst, the analyst expressed his concerns over stagnation of growth:

> "I took this job as an IM analyst because I was excited about analyzing a *variety* of malware everyday but I am not able do it as the SOC is not doing real security monitoring. I also do not have anybody on the team to look up to and learn from. Everyone is less skilled than myself

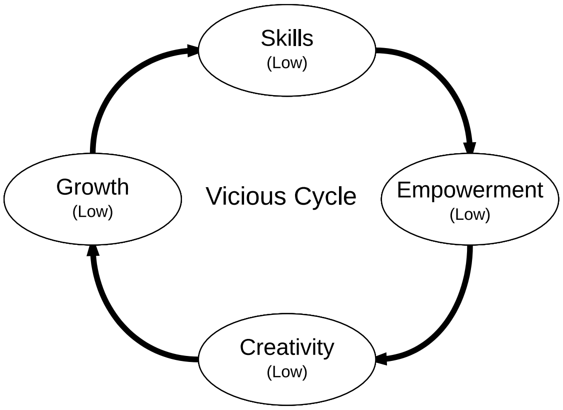

Figure 3: Human Capital Vicious Cycle

> and that means I have to teach them all the time. I love teaching new skills to other analysts but it affects me when I cannot learn from anybody else."

Another possibility through which growth occurs is through career progression.

> An L1 analyst in the SOC was planning to quit his job to pursue an analyst role at another SOC presumably requiring more skills. The managers realized this and offered him a job in the IM team team within the SOC. He accepted the job deciding to stay which was beneficial for the SOC management as they were able to retain an experienced analyst.

If an analyst has outgrown her current role – which may be because they stayed considerably long in the job and reached a saturation point in their learning process – then the manager can reassign her to another position that is more challenging. This will ensure that the learning process never stops ensuring growth and good morale. Unfortunately, this is not a solution that will work all the time since there are only a few positions available at any given time to reassign analysts.

Growth, through any of the suggested means, enhances the skill-set of the analysts.

9.1.5 Burnout trajectory and avoidance

As long as a positive causality among the factors – skills, empowerment, creativity, and growth – exists, the morale of the analysts will remain high. Burnout occurs when a SOC gets stuck in a vicious cycle connecting those factors. For instance, the SOC management hires entry level (not highly skilled) analysts due to budget constraints. These analysts will not be empowered enough as the managers do not trust the abilities of their analysts. This lower empowerment will lead to lower creativity, which will in turn lead to lower growth and skills. Since the skill level of analysts remains the same (very low) this will again lead to low empowerment, creativity, and growth. If this continues eventually the analysts will be burned out as they will start to feel that they are not accomplishing anything in their job–in other words, there is no growth, and the repetitiveness of the job exhausts the analysts. The vicious cycle is illustrated in Figure 3. We call it a vicious cycle because the management wants their analysts' skill set to progressively get better through on-the-job experience, but the negative causality among the four factors deteriorates the human capital of the SOC.

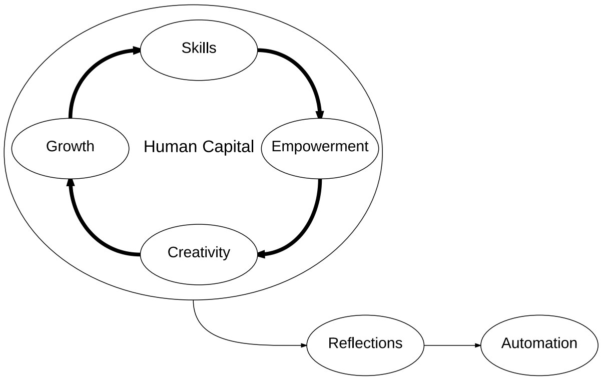

Figure 4: Automation

Although the analysts are less skilled, the management can take some risk and empower the analysts–perhaps gradually. After a few positive cycles in the human capital management cycle (Figure 2) the analysts will gain more skills. The SOC managers will now trust the skilled analysts and empower them with privileges. This will in turn encourage creativity and growth–turning the cycle into a virtuous one. It is possible that even after the cycle is taken in a positive direction the job of an analyst can become too repetitive. One way to deal with the repetitiveness is by providing new opportunities for analysts to stay creative. If the management finds that the analyst has completely outgrown her position, efforts should be taken to find a more challenging role for the person, ensuring positive growth. The bottom line is that to avoid analyst burnout SOC management must be careful not to get caught in the vicious cycle of human capital and be watchful for any signs leading to such trajectory.

9.2 Automation

Automation in a SOC refers to software tools that aid analysts' job and improve operational efficiency. Automation includes complex software such as Security Information Event Management (SIEM) to simple scripts written in Python or Ruby. Software tools are extremely efficient in performing repetitive tasks. Repetitiveness leads to lower creativity as we noted in the discussion on human capital. By automating repetitive tasks, skilled human analyst will have more freedom to engage in more sophisticated investigations.

During the fieldwork we discovered that effective automation takes place only if a process called *reflection* takes place within and among the analysts as shown in Figure 4. Reflection in a SOC is usually done by periodically reviewing the procedures with the goal of identifying operational bottlenecks that can benefit from automation.

Here is an example of reflection leading to automation from our fieldwork:

> Every time an end-user device is identified to be infected with certain classes of malware, the

> standard remediation measure in the SOC was to ask the user to reimage their device with a clean operating system (OS) image. The instructions were written down in an email template and the only data that varied from one user to another was the username and hostname of the device. Other than that, it was the same email and there were hundreds of such emails sent everyday manually. One day an L2 analyst *realized* that this process is cumbersome and wrote down a script that will automatically fetch the username, hostname, and email address of the infected device/user to send a mass mail.

Automation through reflection can only occur if the analysts are *empowered* and *incentivized* to do so. In the example mentioned above the analyst automated the repetitive process due to his own personal interest outside his working hours. He said that the management did not want him to consider automation at the same priority level as report generation.

Reflections are beneficial and practically easier if started earlier. An analyst pointed out the difficulty arising from delaying this process based on his experience:

> "At one point we had procedures written down for everything and analysts were starting to feel like robots performing the same tasks everyday. We did not have any reviews to refine the processes as at one point nobody was even documenting them properly."

To automate complex tasks the analysts have to work with software developers—another form of empowerment. By reflecting on the operational procedures the analysts provide requirements for tools to the developers. The developers develop the tool based on the requirements from the analysts through multiple development iterations. This is called the analyst-developer tool co-creation approach.

We are convinced that this actually works as the fieldworker engaged in a co-creation tool development process at the SOC. The research team of the company developed an algorithm to identify malware from DNS request and response traffic. An initial prototype of the tool was developed by the researchers through collaboration with software developers. The prototype was then deployed in the SOC and the fieldworker was asked to provide feedback on the usability and effectiveness of the tool. The fieldworker and other analysts observed a number of mismatches between the functionality of the tool and the workflow of the SOC. There were weekly meetings during when *actual* workflow requirements of the SOC were conveyed to the researchers. A new version of the tool would then be deployed with the feature requests implemented. Eventually the tool turned out to be very useful for the analysts in their investigations. This process continued even after our fieldwork as the workflow of a SOC is very dynamic. This experience showed that a better way to design tools for SOCs could be to engage the analysts and developers in a co-creation process.

It appears that automation serves two main purposes in enriching the human capital. First of all, analysts can engage in interesting and challenging investigation tasks if the repetitive tasks are automated. We also observe that the co-creation process, which results in automation, provides a platform for the analysts to express their creativity. SOC managers must pay attention to this important effect that automation has on human capital to mitigate burnout.

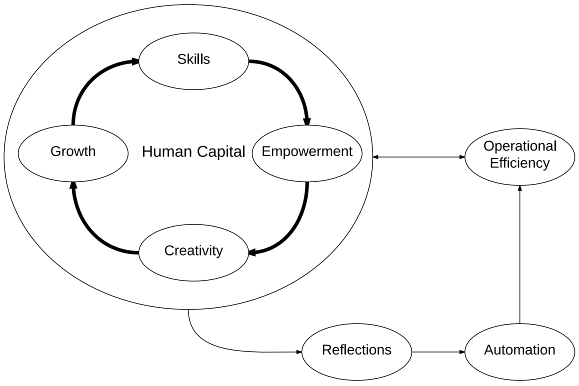

Figure 5: Operational Efficiency

9.3 Operational Efficiency

An efficient SOC will be able to leverage all its resources to detect and respond to threats in a timely manner. Since analysts make all the final decisions during operations, human capital has a direct influence on operational efficiency. We also observed that this relationship is bidirectional in that an efficient SOC positively influences the human capital. We see this two way relationship in Figure 5.

The direct causality from human capital to operational efficiency indicates the obvious fact the highly skilled and creative analysts make operations efficient. Human capital also affects efficiency in operations through automation via reflections. The resulting automation accelerates operations—especially in case of highly repetitive tasks. Here is an example for operational efficiency through automation from our fieldwork. An L1 analyst mentioned the following about creating incident tickets:

> "Case creation takes too much time. Filling in a ticket to locate hosts is the most demanding task. The fields are not fillable as you have to select the entry. There is a script written by an L2 analyst to automate this task. I need to give it a try."

On the other hand, the benefits resulting from operational efficiency in turn create a positive influence on the analysts. Most of the efficiency is achieved through automation by reflections. Reflections provide an opportunity for the analysts to exercise their creativity. This in turn helps in the growth of human capital. An inefficient SOC means reduced automation leading to analysts performing the repetitive tasks manually. This will lead to exhaustion and burnout of analysts eventually. In a vicious cycle, the SOC management could be spending resources on hiring highly skilled analysts who if not empowered to engage in reflections, will lead reduced automation. Operational efficiency suffers due to reduced automation. The inefficiency wears out the analysts as they have to manually perform tasks that could be effectively performed by software. The vicious cycle could be converted to a virtuous one by empowering analysts to facilitate automation through reflections.

9.4 Metrics

A SOC has to periodically measure its efficiency for a number of reasons:

- Measure employee efficiency for bonus considerations
- Measure and tune intrusion detection sensors
- Identify bottlenecks in operational procedures
- Most importantly, provide visibility into the SOC for the upper management

During the fieldwork we tried to understand the influence of metrics on the human capital. We observed that it is very challenging to come to light with good metrics for security operations. It is challenging because either the metrics are too technical making it hard for the management to measure their return-on-investment, or they are too managerial thereby failing to convey exactly the operational activities in the SOC. Some of the metrics that were automatically generated from the SIEM solution are shown in Table 2.

A SOC is an investment from a management perspective and SOC managers have to frequently communicate the benefit the company gets from such an investment. This is vital for the continued support from the upper management as one of the managers mentioned:

> "Corporations are very eager to start an operations center in-house and they fund SOC builders to establish one. After a while they stop seeing value in the SOC, shut it down and move it to managed services. A few years later they realize an in-house SOC is better for them and they redo the process all over. This is hard for guys like me as we spend more than a year establishing the SOC infrastructure and training analysts. A lot of effort goes into it. As SOC managers we need to keep communicating to the management how their investment in the SOC is justified."

Devising appropriate metrics is complicated by the fact that even the higher managers are not sure what shall be the right metrics. A senior manager once responded to an L1 analyst's question on what the higher management perceived as good metrics for SOC operations as thus:

> "I am not sure what the right metrics are and that is something I am working on. But I have some idea on what would be a good metric. If you tell me you processed some thousands of events over a month that does not tell anything interesting to me. But if you tell me a case where you engaged multiple teams–vulnerability management, red team, etc.–and how that resulted in the creation of new detection points–*e.g.* a new AV signature–or how it helped in creating new analytics that will be a good indication of what value I am getting from the SOC. Again, I do not know how you guys can give me the metrics but you have all the data and it is your job to come up with a good way to communicate your success stories."

The pressure for good metrics is relayed down to the SOC managers who in turn hand it down to the analysts. On one occasion, a SOC manager expressed frustration about the lack of good metrics for him to talk to his managers:

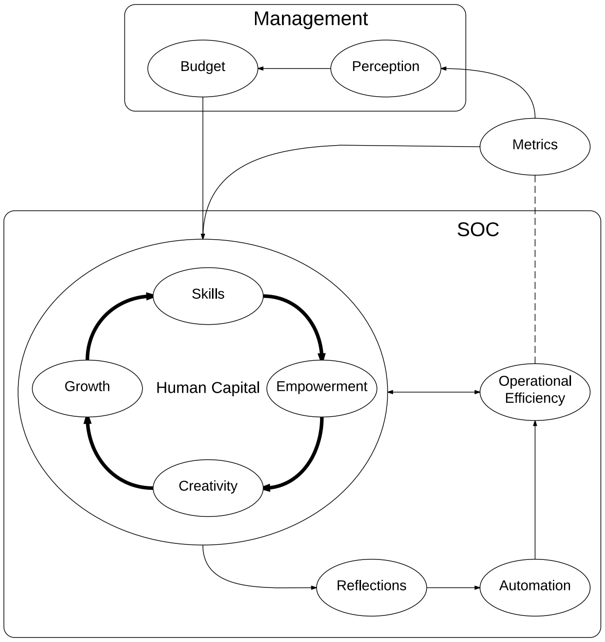

Figure 6: Metrics

> "I need stories to talk to my managers. You analysts are like snipers making a number of hits but I am not getting enough stories to tell my managers. You guys need to generate useful reports so that I can convey the usefulness of the SOC."

Figure 6 also shows that there is a direct causality between metrics and human capital. In the worst case, the metrics will decide the tasks an analyst can perform in the SOC–a form of restricted empowerment. An L1 analyst expressed frustration that supports our claim:

> "We feel that we are not doing security monitoring in the SOC. I think we are just working to generate numbers for higher management. We have raised some ethical concerns with the management regarding this."

The figure also shows the interlink between metrics and the rest of the categories. The dotted line between operational efficiency and metrics is to indicate the fact that metrics act as a communicating channel between SOC operations and the management. There is a possibility for the formation of a vicious cycle even in this context. The demand for metrics from the management might negatively affect the morale of the analysts, that in turn negatively affects operational efficiency. The management's perception of the usefulness of the SOC is driven by the metrics and the lack of good metrics communicating the value of the SOC will lead to reduced funds allocated for the SOC. A reduced budget is usually translated into less training opportunities which will drive the vicious cycle of human capital. More research has to be done on defining meaningful metrics to measure SOC efficiency benefiting the analysts and the management. The analysts benefit from good metrics as promotions and other perks are decided by the numbers conveyed

Table 2: SOC operations metrics

Metric	Measured Quantity	Purpose
Event volume graph	Number of events received per day	Used to anticipate how many analysts will be need to analyze new event sources.
Bulk processed count	Number of events that were bulk processed	Used to identify either improper analysis, or problem with a sensor generating too many events.
Duplicate comments graph	Number of events that were bulk processed	Used to identify either improper analysis, or problem with a sensor generating too many events.
Missed events	Number of events left unprocessed per day	Identify events falling through the cracks, taking more than a day to analyze, and if procedures are not followed.
Average processing time	Average time taken to analyze an event	Estimate how much time it takes for analysts to investigate an event.

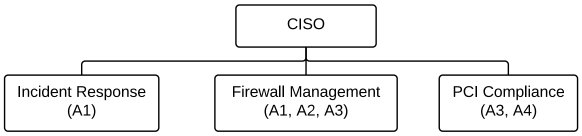

Figure 7: Organizational Chart for the University SOC

by the metrics. The management, on the other hand, will be able to measure better their return on investment on the SOC.

10. MODEL VALIDATION

We have been conducting anthropological fieldwork in a higher education University SOC for over 2 years now. The SOC is relatively smaller compared with the corporate SOC. There are 4 analysts headed by the Chief Information Security Officer (CISO). The SOC is the only security monitoring center for the three campuses of the University. There are 55,000 devices connecting to the network during business hours. The analysts performed operational tasks such as *incident management*, *firewall management*, and *payment card industry (PCI) compliance* as shown in Figure 7. The analysts in this SOC have diverse responsibilities compared to the corporate SOC. This is due to the smaller team size which also means analysts often have to multitask.

10.1 Fieldwork Setup

Five students in Computer Science, graduate and undergraduate, have worked as security analysts over a period of 2 years in the University SOC. They were trained by our anthropologist in participant observation methods and in note taking during fieldwork. The students were embedded as analysts and performed various tasks in the SOC such as incident handling, anti-virus management, host-based anti-virus maintenance, and firewall management. In addition to the operational tasks they also built useful tools to increase operational efficiency. As in the corporate SOC we recorded the observations made in a digital document.

10.2 Burnout Symptoms

We did observe signs of analysts burnout, but in the University SOC they exhibited different symptoms. The burnout manifested itself mostly in the form of *frustration*. However, there was not high analyst turnover contrary to the previous SOC. We postulate that this was due to the location of the University. The University is located in a small town and the analysts do not have too many options when switching jobs as was the case in the corporate SOC. In the following sections we present the results of validating our human capital model for analyst burnout on fieldnotes from the University SOC. Some of the factors actually helped improve the morale of the analysts, thus enriching the human capital. During the validation process we found examples for factors that enabled and also helped mitigate burnout.

10.3 Automation

Analysts of this SOC were stuck performing the repetitive tasks everyday. One analyst expressed his frustration:

> "I want to do some interesting analysis on the data we are collecting but I am stuck with processing the same tickets everyday."

Fortunately, the analysts in this SOC were empowered to engage in periodic reflection of operational procedures. The fieldworkers engaged in periodic reflections with the analyst as part of the co-creation process. The result was a tool that automated most of the ticket generation process enabling the analyst to focus on interesting investigations.

In another instance, the fieldworkers developed a tool that automated malware analysis. The University's email provider placed certain restrictions on the type of files that can be attached in an email. This was done to prevent the spread of malware through email. Any message that contained one of those restricted attachment types were forwarded to a special inbox monitored by the SOC. One of the analysts used to manually download the files in the inbox, conduct analysis to eliminate duplicates and false positives, and submit the list of unique file hashes to the anti-virus (AV) vendor. The AV vendor would then determine based on the submitted hashes if there were any new malware unknown to them. Signatures to detect new malware, if any, would then be pushed out to the University's AV subscribers.

All the steps in the above process were performed manually by one analyst. One day the analyst called one of the fieldworkers and asked for help in automating this process. He wrote down the steps he was undertaking in an email after a day of reflection. A tool was then written to automate most of the steps in the process. Later on, the tool was handed over to another team outside the SOC, presumably less skilled than the SOC analysts. The analyst was *very happy* that the task got offloaded to the other team as he now was able to focus on other sophisticated operational tasks.

Many such mundane operational tasks got automated this way, enabling the them to work on more creative tasks. These observations from our fieldnotes validated the causality between *operational efficiency* and *human capital* in Figure 6. Here we see a positive cycle between empowerment, automation, and operational efficiency leading to good morale of the analysts as suggested by our model.

10.4 Empowerment

The major factor that was affecting the human capital in this SOC was the cooperation issue with other information technology (IT) departments within the University. Often times the SOC has to work with other IT teams such as *networking* or *server management* to resolve a security incident. Since security might not be a high priority for other teams the remediation process gets delayed.

This often causes frustration for SOC analysts. For example, one analyst expressed dissatisfaction in ticket management process by stating this:

> "I cannot close my old tickets as we are waiting on these other departments."

In another instance, the university network was experiencing an unusual amount of traffic that was severely slowing down or disrupting vital services. Moreover, an uncommon behavior and load was noticed on several important networking devices. In order to troubleshoot the problem, the analysts needed to interact with the teams that manage the services and also the network equipment vendors. General reactions from the other entities:

> "Don't take my VLAN down. The problem is not here."

It was very challenging for the analysts to identify the source of the problem without temporarily disabling any services. Eventually, one of the analysts was able to pinpoint the misbehaving device. All these events happened during regular business hours and while the higher management was insisting on solving the problem as soon as possible.

During another instance an analyst had to wait on the department that managed servers for resources to deploy the developed tools. There were numerous issues with the *server management* department such as not enough staff and inadequate hardware resources that delayed the tool deployment.

On another occasion, one of the analysts came up with a *creative* way to distribute logs across machines to improve efficiency of log collection. Unfortunately, they were kept waiting for 11 months by the server management department. In this case the lack of inter-departmental support (cooperation) affected the use of the analyst's *creativity.*

In a nutshell, one can classify facilitating support of other departments as a form of empowerment called *cooperation.* The SOC management is in the most capable position to facilitate this. In the examples cited above the analysts required support from other departments in order to perform their jobs effectively. The analysts got *frustrated* due to the lack of support from other departments. This frustration has often led to analysts losing their temper, thus one can see that the causality between empowerment and creativity indicated by the model in Figure 2 is validated.

10.5 Metrics

Similar to the corporate SOC there were metrics in use to measure analysts performance and the usefulness of various tools used in the SOC. We observed that metrics influenced the analysts' view on the perception of their performance. In other words, the more reflective the metrics of the analysts' achievements were, the more confident they were in the management's evaluation.

Defining good operational metrics was again a challenging task for the management, similar to the corporate SOC. For example, the SOC manager wanted the analysts to spend a fixed amount of time on *operational tasks* and the rest on *projects*—tasks that lead to improvement of the SOC infrastructure. The manager also asked each of the analysts to enter the time they spend on each of the two tasks every week. The senior management wanted to know the amount of time the SOC analysts were spending on operations, hence the CISO devised this metric. The rationale behind this, from the management's perspective, was that the purpose of the SOC was to provide services to the users of the University's network. The management wanted the analysts to spend more time on operations for that reason.

The problem though was that there was a difference of opinion between the management and analysts on what constituted an operational task. Analysts were concerned that the metric did not account for the time spent on meetings and other tasks that were neither operational nor project work. The view among the analysts was that one cannot bin the tasks performed by analysts into discrete categories.

There were also attempts to measure the time each analyst spent on creating tickets. This feature was implemented in the ticketing system to track the time taken by an analyst to resolve an incident. The SOC management wanted to use this feature as a way to measure their return on investment on the analysts. The analysts raised *concerns* that this may not be reflective of the actual effort spent in resolving incidents:

> "I sometimes spend a few good hours on an alert and find out that it is a false positive. Does that mean I am not productive? It is just the way incident handling works and this metric does not capture that."

These observations validate the direct causality between metrics and human capital in Figure 6. The metrics did not reflect the effort of the analysts which in turn led to dissatisfaction, driving down their morale.

Another observation we made indicated the effect of metrics on human capital through management perception. As we described earlier this SOC has only 4 analysts but often have too many operational tasks to handle. The CISO mentioned a while ago, a few good times, about hiring a new analyst but that never happened. Meanwhile, we also observed that the analysts were not content with the financial compensation they were receiving. The perception was that they were given more tasks with no perceived increase in their compensation. The continued existence of this concern among the analysts highlighted the fact that the metrics were not reflective of the operational situation. Right metrics could have indicated to the management that the SOC was understaffed and could benefit from recruitment of another analyst. We thus see a validation for the causality between the metrics affecting the morale of the human capital via the management perception and budgeting.

11. LIMITATIONS

Our work has a few limitations. Firstly, the proposed burnout model was validated only on one more SOC thus far. Validating our model requires access to analysts at a number of different SOCs. We were fortunate so far to have been able to conduct our fieldwork at two different locations, a corporate SOC and a University SOC. Our next step in this direction is to try and obtain access to a few more SOCs (industry and government sectors) to validate our findings.

The second limitation of our work is that we cannot conclude that our model is exhaustive. The model is based on our fieldwork at a SOC for 6 months. Although we started to see repetitions in the observations we were making after a few months, one cannot say for sure if new events will or will not occur after we concluded our fieldwork. Despite this limitation the model was able to explain the burnout symptoms in the University SOC without any contradicting observations.

Lastly, the observations were documented and analyzed by the individual fieldworkers at the University SOC, as is the case with any anthropological fieldwork. We tried our best to be objective when documenting the observations. In spite of this we acknowledge the fact that there is a chance that the documented observations might have been affected by the subjectivity of the fieldworkers.

12. RELATED WORK

There have been a number of prior research efforts focused on tool development for analysts [2, 8, 16]. Werlinger et al. [18, 17] studied the effect of human, organizational, and technological factors on analysts through interviews of practitioners besides identifying activities that require communication in IT security management (ITSM). Botta et al. [1] examined the use of cues and norms in ITSM and discussed challenges that undermine their usage. Furthermore, Werlinger et al. [19] studied security analysts engagement in diagnostic work during incident response. In another work, a team of psychologists from George Mason University have been studying computer security incident response teams (CSIRTs) using organizational psychology [3].

Shropshire et al. [11] talks about various factors leading to information technology (IT) employees leaving the field of IT. First, they conduct a survey of studies in the nursing and accounting disciplines. Based on this initial study and survey of other articles on career exodus they identify stress, job insecurity, and burnout as most likely causes for IT analysts leaving the field. To validate their hypothesis, they conduct a survey of IT professionals in a public service organization in the southeastern area of the United States. Their results indicate a strong correlation between intention to leave the IT field and the mentioned three factors. Shuey et al. [12] conducted qualitative semi-structured interviews of 343 IT professionals in 40 small and medium sized companies in four countries to understand worker well-being in the modern economy. Their data was supplemented with quantitative data obtained from 403 employees in those 40 firms. They identify organizational structure, peer pressure, and individual constraints as reasons leading to burnout of IT employees. They found employees to be stressed out either due to working long hours as they thought that was their organization's culture, fear of losing their job when jobs were scarce, or due to transitions in personal life such as starting a new family. While these two papers are closer to our work there are significant distinctions. We study SOCs, a specific type of IT organization with very specific goals compared with IT in general. Moreover, we focus specifically on the burnout problem which is a main precursor to a security analyst leaving his/her job.

13. CONCLUSIONS AND FUTURE WORK

Human security analysts are the most critical components of a SOC followed by tools and procedures. Unfortunately, SOCs have been suffering from the high turnover rates of their analysts resulting form burnout. Frequent turnover leads to increased spending on hiring and training by the management. In this work we try to understand the concrete factors leading to burnout of security analysts. To understand the problem we performed an anthropological study in a corporate SOC for a period of six months. We worked with an anthropologist to train the students in participant observation methods and also in analyzing our fieldwork notes. The fieldnotes were analyzed using a Grounded Theory based approach and the result was a model describing the burnout problem.

To the best of our knowledge this is the first study of the burnout phenomenon in a SOC environment using anthropological methods. We believe that the burnout in SOCs is a human capital management problem. Specifically, burnout is caused due to cyclic interaction of human, technical, and managerial factors. We also note that there exist a number of vicious cycles between those factors leading to burnout. To validate the model, we used the fieldwork notes from a higher education institution SOC. The model was able to successfully explain the reasons for burnout in this other SOC. Throughout the paper we also provide guidelines for SOC management to maintain a high morale among the analysts. To further evaluate the model we are planning to conduct focused interviews of analysts in a few other SOCs.

14. ACKNOWLEDGMENTS

We would like to thank Dr. Jeff Yan of Newcastle University for his useful comments and suggestions.

This research is supported by the National Science Foundation under Grant No. 1314925 and by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, Cyber Security Division (DHS S&T/HSARPA/CSD), BAA 11-02 and the Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0258. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

15. REFERENCES

[1] 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.

[2] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher. Towards understanding it security professionals and their tools. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 100–111. ACM, 2007.

[3] T. R. Chen, D. B. Shore, S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, and A. K. Gorab. An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy*, (5):61–67, 2014.

[4] Cuckoo. Cuckoo sandbox. `http://www.cuckoosandbox.org/`.

[5] V. Foundation. Volatility. `http://www.volatilityfoundation.org/`.

[6] C. Geertz. Deep play: Notes on the Balinese cockfight. *Daedalus*, 101(1):1–37, 1972.

[7] Hewlett-Packard. Building a successful security operations center. `http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf`, 2011.

[8] P. Jaferian, D. Botta, F. Raja, K. Hawkey, and K. Beznosov. Guidelines for designing it security management tools. In *Proceedings of the 2nd ACM Symposium on Computer Human interaction For Management of information Technology*, page 7. ACM, 2008.

[9] C. Maslach, W. B. Schaufeli, and M. P. Leiter. *Job Burnout*. Annual Review of Psychology, Vol. 52: 397-422, 2001.

[10] B. Rothke. Building a security operations center. `http://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf`, 2012.

[11] J. Shropshire and C. Kadlec. I'm leaving the IT field: The impact of stress, job insecurity, and burnout on it professionals. *International Journal of Information and Communication Technology Research*, 2(1), 2012.

[12] K. M. Shuey, H. Spiegel, J. McMullin, and V. Marshall. The structure of it work and its effect on worker health: job stress and burnout across the life course. *Aging and working in the new economy: changing career structures in small IT firms. Northampton, MA: Edward Elgar Publishing*, pages 163–194, 2010.

[13] A. Smith and J. S. Nicholson. *An Inquiry Into the Nature and Causes of the Wealth of Nations*. T. Nelson and Sons, 1887.

[14] A. Strauss and J. M. Corbin. *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications, Inc, 1990.

[15] S. C. Sundaramurthy, J. McHugh, X. S. Ou, S. R. Rajagopalan, and M. Wesch. An anthropological approach to studying csirts. *IEEE Security & Privacy*, (5):52–60, 2014.

[16] N. F. Velasquez and S. P. Weisband. Work practices of system administrators: implications for tool design. In *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology*, page 1. ACM, 2008.

[17] 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.

[18] R. Werlinger, K. Hawkey, and K. Beznosov. An integrated view of human, organizational, and technological challenges of it security management. *Information Management & Computer Security*, 17(1):4–19, 2009.

[19] 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.