An Empirical Study of Root-Cause Analysis in Information Security Management

Gaute Wangen, Niclas Hellesen, Henrik Torres, and Erlend Brækken
NTNU Gjøvik
Teknologiveien 22,
2802 Gjøvik, Norway
Email: gaute.wangen@ntnu.no, niclashellesenl@gmail.com,
henrik.torres@gmail.com, erlendlbr@gmail.com

***Abstract*—This paper studies the application of Root-cause analysis (RCA) methodology to a complex socio-technical information security (InfoSec) management problem. InfoSec risk assessment (ISRA) is the common approach for dealing with problems is InfoSec, where the main purpose is to manage risk and maintain an acceptable risk level. In comparison, the RCA tools are designed to identify and eliminate the root-cause of a reoccurring problem. Our case study is a complex issue regarding multiple breaches of the security policy primarily through access control violations. By running a full-scale RCA, this study finds that the benefits of the RCA tools are a better understanding of the social aspects of the risk; RCA highlighted previously unknown social and administrative causes for the problem which in turn provided an improved decision-basis. The problem treatments recommended by the ISRA and the RCA differed in that the ISRA results recommended technical controls, while the RCA suggested more administrative treatments. Furthermore, we found that the ISRA and RCA can complement each other in administrative and technical issues. The main drawback was that our cost-benefit analysis regarding hours spent on RCA was on the borderline of being justifiable. As future work, we propose to develop a leaner version of the RCA scoped for information security problems.**

Keywords*—*Information Security; Root cause analysis; Risk Management; Case study.

I. Introduction

Judging by the available literature on standards and methods, the common approach to dealing with problems in information security (InfoSec) is risk assessments. Risk assessment aims to estimate the probability and consequence of an identified scenario or for reoccurring incidents, and propose risk treatments based on the results. By estimating the expected risk of repeating incidents or an identified scenario, risk assessment aims at proposing risk treatments based on the estimated results. The InfoSec risk assessment (ISRA) has been developed to analyze risks that occur when applying technology to information, and revolve around securing the confidentiality, integrity, and availability of information or other assets [1]. By focusing on assets and vulnerabilities, these assessments tend to have a technical scope [2] [3] with estimates of consequences and respective probabilities of events as key outputs. Although the InfoSec risk management (ISRM) approach is useful for maintaining acceptable risk levels, they are not developed to solve complex socio-technical problems. In comparison, the Root Cause Analysis (RCA) is *”a structured investigation that aims to identify the real cause of a problem and the actions necessary to eliminate it.”* [4] RCA incorporates a broad range of approaches, tools, and techniques to uncover causes of problems, ranging from standard problem-solving paradigms, business process improvement, benchmarking, and continuous improvement [4]. The ISRA and RCA approaches are different in that RCA investigates incidents that have occurred with some frequency aiming to understand and eliminate the problem from a socio-technical perspective. While ISRA attempts to estimate the risk and propose and implement risk treatments based on the results to achieve acceptable risk.

The case study presented in this paper extends the ISRA of a complex socio-technical problem with RCA and discusses the cost/benefit of the results. The objective of ISRM is to reduce risk to an acceptable level. A typical ISRA would be to estimate annual incident cost, compare it to risk appetite, and if found unacceptable: implement a treatment to address either probability, consequence, or both, to maintain the risk within acceptable levels, while RCA aims to remove the problem in its entirety. However, both approaches seek to treat the problem at hand, which makes the output comparable. The application of formal RCA tools is an area that has remained largely unexplored in InfoSec literature. Therefore, the problem we are addressing in this study is to determine the utility of RCA for InfoSec and if it provides useful input to the decision-making process beyond the ISRA. The problem is investigated using a case study, qualitative assessment of results, and cost-benefit analysis.

The case is of breaches to the access control (AC) security policy (SecPol), such as access card and Personal Identification Number (PIN) exchange between employees. This complex problem is located at the intersection of the social and technological aspects that many organizations may face. The Scandinavian organization in our case study had logged multiple occurrences of policy violations together with costly incidents as a consequence. This study investigates if RCA can be applied as a useful extension to the ISRM process for the AC SecPol problem. To investigate this issue, we qualitatively assess the results of a RCA conducted as an extension to a high-level ISRA of the problem. Further, we discuss if RCA can be justified for complex InfoSec problems through cost-benefit analysis. This paper applies the seven-step process RCA methodology [4] for comparison of results. The data collected for this study was primarily from historical observations and data in the target institution together with qualitative interviews of thirty-six representatives from six relevant stakeholder groups.

The remainder of the paper is structured as follows: The following section addresses previous work on RCA in InfoSec. Section III provides a description of the applied

ISRA method and the RCA tools methods including statistical analysis. Further, we present the results from the ISRA and the RCA. Lastly, we discuss the qualitative differences and discuss cost-benefit. Finally, we discuss the limitations, propose future work, and conclude the results.

II. Related Work

RCA was developed to solve practical problems in traditional safety, quality assurance, and production environments [4]. However, RCA has also been adopted in selected areas of InfoSec: Julisch [5] studied the effect of the RCA, by considering RCA for improvement of decision-making for handling alarms from intrusion detection systems. The study provides evidence towards the positive contribution of RCA, but it does not apply the RCA tools as they are proposed in the recent literature [4], [6], [7]. Julisch builds on the notion that there are root causes accounting for a percentage of the alarms, but proposes his tools for detecting and eliminating root causes outside of the problem-solving process, Fig. 1. A more recent study conducted by Collmann and Cooper [8] applied RCA for an InfoSec breach of confidentiality and integrity in the healthcare industry. Based on a qualitative approach, the authors find the root cause of an incident and propose remediation. Their results also show a clear benefit from applying RCA, although their RCA approach seems non-standardized, being primarily based on previously published complex problem-solving research articles. Wangen [9] utilizes RCA to analyze a peer review ring incident, where an author managed to game the peer review process and review his papers. This incident is analyzed by combining RCA tools and the Conflicting Incentives Risk Analysis (CIRA) to understand the underlying incentives and to choose countermeasures. Further, Abubakar et.al. [10] applied RCA as a preliminary tool to investigate the high-level causes identity theft. The study applies a structured RCA approach [7] and identifies multiple causes and effects for setbacks to the investigation of identity theft. The Abubakar et.al. study shows the utility of RCA for InfoSec by providing an insight into a complex problem such as identity theft. Hyunen and Lenzini [11] discuss RCA application in InfoSec by contrasting the traditional approaches to Safety and Security to highlight shortcomings of the latter. Furthermore, the authors propose an RCA-based tool for InfoSec management to address said shortcomings and demonstrate the tool on a use case. The tool is designed to reveal vulnerable socio-technical factors.

Some of the tools applied in an RCA are also recognizable in the risk assessment literature, for example, instruments such as Flowcharts and Tree diagrams model processes and events visually. Typical comparable examples from risk assessment are Event-tree and Fault-tree analysis, where the risk is modeled as a set of conditional events, however, these approaches are not specifically developed for InfoSec risk analysis. Schneier adapted the Fault-tree analysis mindset and created *Attack Trees* [12]. These tools resemble those of RCA. However, the frame for applying them is different in the sense that attack trees focus on the technical threat and vulnerability modeling, while RCA tools focus on problem-solving.

Although there are a couple of published studies on the application and utility of formal RCA methodologies, the previous work on RCA in InfoSec is scarce, and there is a research gap in experimenting with the RCA tools for solving re-occurring InfoSec problems. The studies we found provided positive results and motivation for further experiments with RCA for InfoSec problems.

III. Method

The primary research approach was a case study which was conducted in a Scandinavian R&D institution to investigate the complex problem of internal AC policy violations. The ISRA was conducted as a high-level risk assessment for the institution which revealed the need for deeper analysis of the problem. Three independent researchers conducted the RCA and gathered data from 36 scientific interviews and applied historical data on incidents caused by unauthorized access.

Further, we qualitatively compare the results where we analyze the differences in approaches, findings, and treatment recommendation. Additionally, we applied a cost-benefit analysis to measure resources regarding time spent on conducting RCA and benefits concerning additional knowledge about the problem.

The following section briefly describes the ISRA approach applied in this study, while the second section describes the RCA approach. The latter contains a description of the seven-step RCA process, the tools used, data collection method, and a brief overview of the statistical methods used for data analysis.

A. ISRA Method

The ISRA method applied for the case study is based on the standard ISO/IEC 27000-series [1]. Further substantiated with the Wangen et.al. [13] [14] approaches which centers on estimations of asset value, vulnerability, threat, and control efficiency, these are combined with available historical data to obtain both quantitative and qualitative risk estimations. The applied method identifies events together with adverse outcomes and uses conditional probability to estimate the risk of each identified outcome. The results section provides a summary of the initial ISRA results.

B. Approach to Root cause analysis

In choosing a RCA framework, we looked at comprehensiveness, academic citations, and availability. Based on the criteria, our study chose to follow the seven-step RCA process proposed by Andersen and Fagerhaug [4], as shown in Fig. 1. Each step consists of a set of tools to produce the results needed to complete the subsequent steps, whereas step 7 is out of scope. Each step consists of different tools to solve problems where one or more are required to complete the RCA and conclude the root cause(s). As recommended in the methodology, we chose tools per step based on our judgment of suitability. The RCA in this study was conducted by a three-person team supported by a mentor. We have anonymized information according to the employer's requests. The following subsections describe each step in the RCA process and our selected tools (see [4] for further description).

Step 1 - Problem understanding, Performance Matrices. The goal of this step is to understand the problem and rank the issues. Performance Matrices are used to illustrate the target system's current performance and importance. The performance matrix contributes towards establishing priority of the different problems, factors, or problems in the system [4]

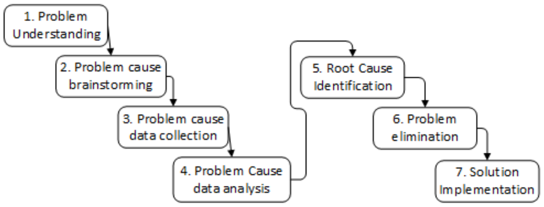
1. Problem Understanding
2. Problem cause brainstorming
3. Problem cause data collection
4. Problem Cause data analysis
5. Root Cause Identification
6. Problem elimination
7. Solution Implementation

Fig. 1: Seven step process for RCA [4].

(P.36-41): (i) which part of the problem is the most important to address, and (ii) which problem will reduce the highest amount of symptoms. The problems are qualitatively identified and ranked on a scale from 1 to 9, on performance (x-axis) and importance (y-axis).

Step 2 - Problem cause brainstorming. The main idea of this step is to cover other possible issues that may be causing the problem, not thought of in Step 1. For this purpose, we applied unstructured *Brainstorming*, which is a technique where the participants verbally suggested all possible causes they could think of, which was immediately noted on a whiteboard and summarized together at the end.

Step 3 - Problem Cause Data Collection - Interviews. RCA recommends several data collection techniques [4], this study chose scientific interviews as the main data collection approach as the study required an in-depth understanding of the motivations for AC SecPol violation problem. The interviews were conducted in a face-to-face setting, and was designed using category, ordinal, and continuous type questions together with open-ended interview questions for sharing knowledge about the problem. The interview subjects were primarily categorized as representatives of key stakeholder groups within the organization and one group of external contractors. Each interview had twenty-six questions with follow-up questions if deemed necessary to clarify the opinion or to extract valuable knowledge from particularly knowledgeable individuals.

Step 4 - Problem Cause Data Analysis - Statistics & Affinity diagram. We applied a variety of statistical data analysis methods specified in the results, and the IBM SPSS software for the statistical analysis. A summary of the statistical tests used in this research is as follows.

For *Descriptive analysis* on continuous type questions, we applied the median as the primary measure of central tendency. We also conducted *Univariate* analysis of individual issues and *Bivariate* analysis for pairs of questions, such as a group belonging and a continuous question, to see how they compare and interact. As the Likert-scale seldom will satisfy the requirements of normality and not have a defined scale of measurement between the alternatives, we restricted the use of mean and standard deviation. We analyzed the median together with an analysis of range, minimum and maximum values, and variance. This study also analyses the distributions of the answers, for example, if they are normal, uniform, bimodal, or similar. We used Pearson two-tailed *Correlation test* to reveal relationships between pairs of variables as this test does not assume normality in the sample.

The questionnaire had several open-ended questions which we treated by listing and categorizing the responses. Further, we counted the occurrence of each theme and summarized the responses. We also applied the *Affinity diagram* for analyzing our qualitative data, which is a RCA tool for grouping data and discovering underlying relationships.

Step 5 - Root Cause Identification - Cause-and-Effect Charts. The goal of this step is to identify the root cause(s) of the problem. For this task, we applied the Cause-and-Effect chart (Fishbone diagram) which is a tool for identifying the major causes of a problem, together with the secondary causes/factors influencing the problem. The results from this process should map to the undesired effect, the problem.

Step 6 - Problem elimination - Systematic Inventive Thinking (SIT). The goal of this step is to propose solutions to deal with the root causes of the problem, Andersen and Fagerhaug [4] describe primarily two types of tools for drafting treatments; one is designed to stimulate creativity for new solutions, while the other is designed for developing solutions.

IV. Case Study: Access Control Policy Violations

In this section, we first present a summary of the results from the ISRA, in terms of risk estimation and proposed treatment. Further, we present the results from our RCA for comparison.

The case data was collected from an institution whose IT-operations delivers services to about 3000 users. The organization is a high-availability academic organization providing a range of services to the users, mainly in research, development, and education. The IT Operations are the internal owners of the AC regimes and most of the lab equipment; they represent the principal in this study. The objectives of the IT-operations is to deliver reliable services with minimal downtime, together with information security solutions.

During the last years, the Institution has experienced multiple incidents of unauthorized access to its facilities. The recurring events primarily lead to theft and vandalism of equipment in a range of cost that is deemed unacceptable. Thus, the hypothesis is that this has partially been caused by employees and students being negligent of the SecPol regarding AC, providing unauthorized access to the facilities. While the SecPol explicitly states that both the token and the PIN are personal and shall not be shared, there has been registered multiple incidents of this occurring.

A. *The Risk of Access control policy violations*

The goal of the ISRA was to derive the annual risk of the incidents. This section summarizes the asset identification and evaluation, vulnerabilities assessment, threat assessment, control efficiency, and outcomes.

The Institution had two key asset groups: (i) hardware and (ii) physical sensitive information, both stored in access controlled facilities. The hardware's primary protection attribute was availability, and the value was estimated in the range of moderate according to the budget, with a low to medium importance in the day-to-day business processes.

The two controls in place are primarily (i) AC mechanisms - physical control in place to prevent unauthorized accesses and mitigate the risk of theft. (ii) The SecPol - administrative control, which is a written statement concerning the proper use of AC mechanisms.

For the vulnerability assessment, experience showed that illegitimate users were accessing the facilities on a daily basis. We identified two primary vulnerabilities; (i) lack of security training and awareness, whereas the stakeholders do not understand the risk exposure of the organization. (ii) Insufficient organizational security policies, whereas the SecPol itself lacks clear consequences for breaches, leaving the personnel complacent. The main attack for exploiting these two vulnerabilities was social engineering, where the attacker either manages to get a hold of a security token and PIN. Alternatively, the attacker manages to gain unauthorized access to the facilities by entering with others who have legitimate access (tailgating). With the number of stakeholders having access, both attacks are easy for a motivated threat actor. The exposure is summarized in Table I.

TABLE I. SUMMARY OF VULNERABILITY ASSESSMENT.

Scenario	**Vulnerability Description**	**Attack description**	**Attack Difficulty**	**Vulnerability Severity**	**Exposure Assessment**
A1	Lack of Security Training and Awareness, Insufficient InfoSec Policies	Social Engineering - Employee or Student Gives away Token and PIN (Likely)	Medium	Very High	High
A2	Lack of security training and awareness, Insufficient InfoSec Policies	Social Engineering-Employee or Student leaves doors opened for convenience	Easy	Medium	Medium

For the threat assessment, the experts identified one threat group motivated by a financial incentive with the intent of stealing either physical equipment or sensitive information, with two actors; (i) Actors who frequently steals small items, representing high frequency - low impact risk. (ii) Actors who conduct a few significant thefts, representing the low frequency - high impact risk.

B. Risk Analysis Results.

The ISRA results showed that the most severe risk facing the organization is theft of sensitive information, while physical theft of equipment is also a grave risk. According to past observations, the risk is greatest during holidays with few people on campus. The two primary risks were major equipment thefts during the holiday season and several minor equipment thefts that aggregated into an unacceptable amount.

C. Implemented Treatment - Camera Surveillance

As a result of the ISRA, the treatment implemented to reduce the two risks was camera surveillance of the main entry points of buildings. Firstly, this treatment has a preventive effect in the sense that it will heighten the attack threshold for threat actors. Besides, it will provide audit trails that will be useful in future investigations. Camera surveillance had also been proven to reduce the number of incidents as well as increasing the amount of solved crimes in similar institutions. This data indicates a high control efficiency; however, the measure also comes with some drawbacks, such as equipment cost together with the required resources to operate the system. Due to the data collection on employees surveillance brings, this risk treatment also subjects the organization to requirements from data privacy protection laws. Neither did it address the socio-technical problem with the SecPol, card swapping, and card lending.

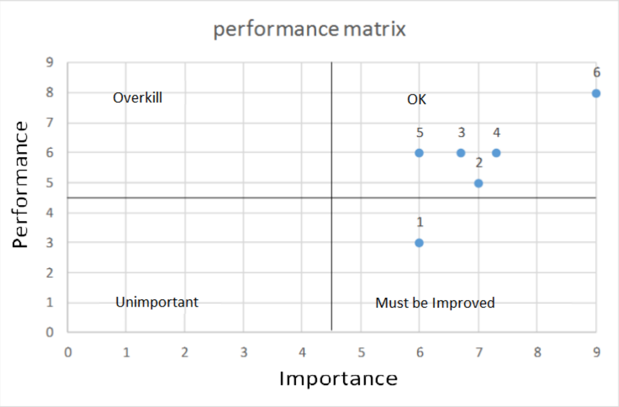

Fig. 2: Performance matrix.

V. Root Cause Analysis Results for a Socio-Technical problem

In this section, we present the results from conducting the RCA according to the method described in Section III-B. The results are derived from conducting RCA on the previously outlined problem and risk; we outline the hypothesized root causes and proposed treatments.

A. RCA Process, Step 1 & 2 - Problem Understanding and Cause Brainstorming

The goal of these steps is to scope the RCA and center on the preliminarily identified problem causes. The performance matrix, Fig. 2, is used to rank the identified causes on their *Importance* and *Performance*. With the help of resource persons, the team derived six topics from the preliminary *RCA steps 1 & 2*, Fig. 1): (i) Theoretical knowledge of the SecPol for AC, (ii) Practical implementation of the SecPol for AC, (iii) Consequences for policy breaches, (iv) Security Culture, (v) Backup solutions for forgotten and misplaced cards, and (vi) Card hand out for new employees. The RCA team and the expert ranked the issues and prioritized the data collection step accordingly, illustrated in Fig. 2.

B. RCA Process Step 3 - Data Collection

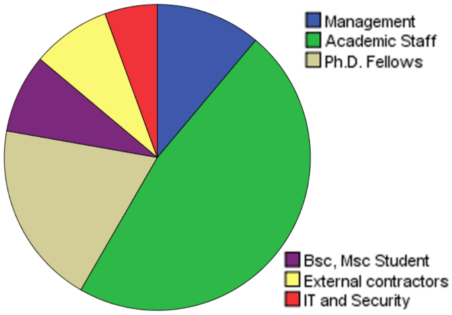

Fig. 3: Stakeholder groups included in the study

TABLE II. DEMOGRAPHICS INCLUDING AGE AND SEX DISTRIBUTIONS

	Age				Sex		
	Group	Freq.	Percent		Group	Freq.	Percent
Valid	20-29	8	22,2	Valid	Women	10	27,8
	30-39	7	19,4		Men	26	72,2
	40-49	10	27,8		Total	36	100,0
	50-59	8	22,2				
	60-69	3	8,3				
	Total	36	100,0				

For the categorical analysis, the team used age, gender, and stakeholder group as the primary categories, with the emphasis on the latter as our hypothesis was that parts of the root cause are found in conflicting interests between internal groups. The team interviewed thirty-six people located at the site, Fig. 3 displays age and gender distributions, with the six primary stakeholder groups. The interview subjects for the academic staff, Ph.D. Fellows, B.Sc. and M.Sc. students were chosen at random. The representatives of management and IT and security were key stakeholders in the organization, such as decision-makers and policy writers.

C. RCA Step 4 - Problem Cause data analysis

The Descriptive analysis showed that about half of the respondents had read the SecPol. All but two reported that it is was not allowed to lend away cards, whereas the remaining two did not know, indicating a high level of security awareness for the issue. Also, the study uncovered uncertainty among the respondents when we asked them about what the potential consequences for breaching the SecPol would bring for the employees. Whereas most of them assumed no consequence, and none perceived any severe consequences. We also uncovered that most people would be reluctant to admit to sharing cards. Further, we asked them *”How often do you think access cards are shared at the Institution?”* on a scale from 1 - 5 (1- Never, Yearly, Monthly, Weekly, 5 -Daily), to which the respondents thought that this is an issue that occurs on at least a weekly basis (Median 4). Using the same scale, the team asked how often the respondents had the need to borrow cards from others. Over half reported to not ever had the need, while twelve reported having had to lend cards on an annual basis, only two reported having the problem more than that. However, half of the respondents said to have been asked by others to borrow cards, which documented the frequency of the problem.

TABLE III. NOTABLE DIFFERENCES BETWEEN GROUPS ON ”HOW LONG DID IT TAKE FOR YOU TO GET ACCESS TO THE FACILITIES YOU NEEDED?” (BETWEEN 1 VERY LONG - 6 IMMEDIATE ACCESS)

Category	N	Range	Median	Minimum	Maximum	Variance
Management	3	0	6,00	6	6	0,000
Senior Academic Staff	17	4	6,00	2	6	1,654
Ph.D. Students	7	5	5,00	1	6	3,238
BSc. and MSc. Students	3	4	3,00	1	5	4,000
External Contractors	3	3	4,00	1	4	3,000
Total	33	5	5,00	1	6	2,729

1) Summary of categorical analysis: The statistical analysis showed differences between the responses of men and women; where the latter viewed incidents involving card borrowing among employees more severely than men. The women in our sample also believe that it is more likely that employees admit to borrowing cards. Another visible difference between the stakeholder groups was who had read the policy, where all the representatives of the Management and IT and Security groups had read it. The Ph.D. Fellows and the student groups scored the lowest on having read the policy. Another observable finding was that the waiting time varied between the groups, whereas the permanent employees perceived the shortest waiting times, Table III.

2) Qualitative analysis of differences between groups: **IT and Security.** The IT operations owned much of the hardware in the facilities and was in charge of both designing, implementing, and operating the AC policy. Both representatives had read the policy and considered it important that staff and students also know the policy. The IT operations believed that card lending is an increasing problem within the institution, especially in the modern facilities where AC mechanisms are more frequent. One also answered that since he had been involved in developing the policy, he felt more ownership of it and, therefore, experienced a greater responsibility to follow it than other departments. They also felt the legal responsibility not to break the policy due to owning the AC system.

Management. This group consists of middle and upper management, which had all read the SecPol. Half believed it was important to have those who will be subject to the policy involved in the policy development process. When we asked this group about what they saw as the worst scenario, this group had similar opinions: their main concerns was loss and compromise of information together with relevant legal aspects. Two members of this group reported that they did not get the service they expected from IT regarding forgotten cards. Three out of four said that they believed the security culture to be good, while the last one reported the security controls to be cumbersome.

Senior academic staff. Consists of different types of professors, researchers, and lecturers, and represents the majority of employees in the case. This group was the largest with the most widespread opinions. Regarding the SecPol, several expressed discontent and said that it was neither security department or IT service that should be responsible for it. The organization should provide the content of the policy to ensure that it was not an obstacle in the day to day work. Further, delivering on the aims and goals of the organizational assignment should be compared to the potential harm from card swapping incidents, meaning that the policy should be designed with a better understanding of risk. An example of this was that employees must have access to rooms to do their job where a too-strict policy would stand in the way. Regarding this, several mentioned that if the cards were not lent to other employees, it would be very problematic due to the lack of backup solutions. They missed good fallback solution if one had forgotten access card.

Ph.D. Fellows. Out of this group, only one had read the SecPol. Most assumed it was not allowed to lend out their access cards, but two said they did not know. One expressed discontent from not receiving his access card quick enough, which he hypothesized as one of the reasons for borrowing other people’s cards. Longer times to hand out access cards may force them to lend cards internally in an office. Another issue was that Ph.D. Fellows occasionally worked with students and that they often needed access to restricted facilities to be able to work. This issue required the Ph.D. fellow either to open the door physically for the students or to loan them their card. When we asked about the security culture, the responses were split: Two did not know, one thought that security was good, another one said that people trust each other, one said it was wrong, while one said that people knew that they should not lend it to others. The last one said that others could borrow it for practical reasons.

Students. Represents the main bulk of people with access to the main facilities, but with limited access to offices and employee areas. Only one of the students had read the policy, and none of the students who participated knew of any instances of card lending, although two out of three had been asked by someone if they could lend them their cards.

External contractors. Represents the contractors in charge of running the physical facilities, such as cleaning personnel and physical maintenance. In the External group, only one had read the policy. All believed that it was not allowed to borrow cards and that the school saw this as a serious offense. Only one of them reported having had the need to borrow a card.

D. RCA Step 5 - Identified Root causes

The interviews with the groups provided an insight into the many views on this problem and the complexity it entails, visualized with the Fishbone diagram in Fig. 4. Based on our RCA we found five possible root causes:

1. Uncertainty regarding fallback solutions. We found that there was uncertainty surrounding available backup solutions among all the stakeholder groups. Where 14 of the 31 respondents were undecided if there existed any fallback solution, and suggested to create better backup solutions. 17 said there existed backup solutions, but we uncovered different opinions regarding what these were and who was responsible for them. For example, six respondents thought they could summon the IT department, three thought the student help desk, while the remainder thought either management could help or ask a colleague to lend them access cards. Even from the two key stakeholders in IT the replies were contradictory.

2. Discomfort when using fallback solutions. Two of our respondents reported to have forgotten their cards and had contacted the on-campus card distributor to use the fallback solution. The respondents meant they had not been well-received and had not gotten the help they needed. Overall, they reported the situation to be discomforting, which was unfortunate, as this may lead to the employees using different methods for solving the problem.

3. Misaligned SecPol regarding authorization. Our interviews highlighted that being able to do their work is the most important goal for every employee. Thus, the SecPol should aim to facilitate this aim. Too strict AC will in some cases lead to obstruction in day-to-day tasks and lead to employees finding workarounds which may compromise security, such as asking trusted co-workers to borrow cards. Some of the respondents reported not having been included in the development of the SecPol and felt that it was misaligned.

4. Too much security. In especially one of the most modern buildings, there is a very strict AC regime in place, where low-level security rooms and facilities are regulated. Several of the respondents highlighted this as the main reason for card lending. These low-security rooms only required the card and not the PIN code, so the respondents did not consider this a serious breach of policy. Several of our respondents said that this was too much security and could not understand the reasoning underlying this decision.

5. Lack of risk awareness and consequences. 33 out of 36 defined possible negative consequences for the institution, so, the awareness around possible risks for the institution was high. However, we found that less than half of the respondents had read the overarching SecPol and that the respondents were unaware and uncertain about the organization's and their personal risk if their cards went astray. Everybody agreed that it was a bad thing, but nobody could say with certainty what the consequences would be, if any at all.

E. RCA Step 6 - Proposed root cause treatments

Based on our findings we conducted *Systematic Inventive Thinking* and came up with following root cause treatments:

Improve fallback solutions. Regarding root cause 1 and 2, the RCA team proposed to develop a solution for reserve access cards with adequate and tailored room access. The solution should provide basic access to low-security level facilities, with tailored room access according to stakeholder needs. This suggestion should be a public and low threshold offer for those who have forgotten or misplaced their cards.

Align SecPol with objectives. Regarding root causes 3 and 4, the RCA team proposed to risk assess the need for physical security and AC for the facilities based on the organizational goals, employee needs, and the assets stored in the room. Include key stakeholders in the process and focus on balancing productivity and security to revise the security baseline.

Improve the overarching SecPol. Regarding cause 5, the RCA team proposed to improve the overarching SecPol, the suggestions were: (i) clarify consequences for breaches of policy, (ii) assigning a responsible for sanctions per department, (iii) including the employees in the shaping of policy, and (iv) increase the accessibility of the policy.

Improving risk awareness. Regarding root cause 5, we also propose to improve risk awareness among the stakeholders, by running awareness campaigns including both the risks the organization and employees are facing. As a part of this, we proposed to create an information bank regarding risks, fallback solutions, and how to make use of them.

VI. Discussion

This section discusses the additional insight gained from the RCA; first qualitatively, and then through cost/benefit analysis.

A. Additional insight gained from RCA

Upon completing the RCA, we see that the results from the ISRA and RCA provide different models of the same problem. The information gathered from the ISRA process was scoped towards technical risks with solutions for reducing probability and consequence. Furthermore, we found the RCA

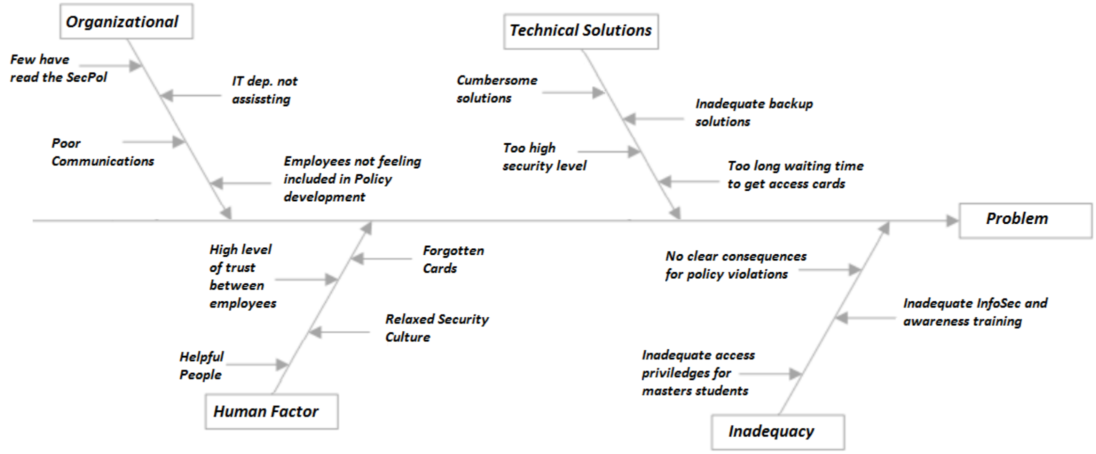
Organizational
Few have read the SecPol
IT dep. not assissting
Poor Communications
Employees not feeling included in Policy development
Technical Solutions
Cumbersome solutions
Inadequate backup solutions
Too high security level
Too long waiting time to get access cards
Problem
High level of trust between employees
Forgotten Cards
Relaxed Security Culture
Helpful People
Human Factor
No clear consequences for policy violations
Inadequate InfoSec and awareness training
Inadequate access priviledges for masters students
Inadequacy

Fig. 4: Fishbone diagram illustrating contributing causes to the main problem.

to work better to visualize complexity and providing insight into the human aspects of the problem. However, the RCA process was resource intensive and required extra training to complete. The RCA process also required the inclusion of more stakeholders than the ISRA.

The results show that the benefits of the RCA are a better understanding of the social dimensions of the problem, such as conflicts between users and the security organization. This insight provides an improved decision basis and an opportunity for reaching a compromise with the risk treatment. The risk assessment team were aware of two (cause 3. and 5.) out of the five identified root causes of the problem. Thus, in our case study, the RCA did provide a valuable extension to the risk assessment for solving the problem. The RCA results showed all root causes to be on the administrative and human side of the problem. Thus, the treatments produced from the two approaches were different; ISRA produced a technical treatment in camera surveillance, while RCA produced multiple administrative treatments, each for addressing separate root causes.

Although the ISRA did highlight the vulnerabilities related to the human factor and risk perception as one of the risk factors, in this case, the decision-makers did not opt for revision of the AC policy. To summarize, the ISRA findings viewed card lending as a technical security problem, while RCA extended the knowledge into the administrative problem.

B. Cost-benefit analysis

For cost-benefit analysis, we consider time spent on tasks and usefulness of the task. Table IV shows that the process of achieving desired results was time and resource consuming for our team. The reported hours are the total amount from start to end without having a budget constraint. The reported hours does contain resources spent beyond the three-man team, e.g. from interview attendance and supervision.
The most time consuming and crucial tasks were the steps 3 and 4, data collection and analysis. Further, the table shows that the resource demand for the Root cause identification and elimination phases as low, this is because the team primarily identified the root causes during the data analysis. While the main task of the root cause identification phase was to formalize the causes and effects, and the elimination was used to propose treatments.

TABLE IV. TOTAL HOURS SPENT CONDUCTING RCA FOR AN UNTRAINED THREE MAN TEAM (APPROXIMATELY 220 HOURS PER TEAM MEMBER)

Step	Phase	Tasks	Time spent
Preliminary	Preparations	Collecting available data	100 hours
Preliminary	Preparations	Testing and choosing tools	72 hours
1	Problem Understanding	Performance Matrix	3 hours
2	Problem cause brainstorming	Brainstorming	1 hours
3	Problem cause Data Collection	Planning interviews	150 hours
3	Problem cause Data collection	Conducting interviews	100 hours
4	Data analysis	Qualitative & Statistical	220 hours
5	Root cause identification	Fishbone	7 hours
6	Root cause elimination	SIT	7 hours
			Total 660 h.
		Only RCA Process	Total 488 h.

As the team gain experience with using RCA on cases, the time estimate should be significantly be reduced. For example, our study spent 172 hours in the preparation phases gathering data on the problem and testing tools. With more experience, the preliminary steps will be significantly shortened. Our team also estimated that the whole process itself would become leaner with practice.

To summarize, we derived the primary benefit from the problem cause data collection and analysis phases, which enabled the root cause identification. Furthermore, the group benefited from working on the performance matrix, which set the direction for the remainder of the project. Regarding the remaining tools, the benefits the problem cause brainstorming was that it helped to provide an overview of the problem space and invited creative thinking. The advantage of the Fishbone tool was to group and visualize the identified problems in the context. Further, the process step contributed to determine and analyze causes. The SIT tool has a series of five principles that attempts to discover how to solve the components of the root cause. This tool offers a well-structured way to traverse a problem situation but could be resource intensive when handling many problems with all their components.

Issues of minor importance should not be subject to such an extensive effort as RCA requires. During the preparations for this study, we ran RCA for minor issues and found it not worthwhile as it was unproductive to use a complicated problem-solving process to less costly problems. However, future projects should consider RCA when they perceive the issue as important and do not know its nature or cause. The problem should be expensive, complicated, and cannot be addressed sufficiently with less comprehensive methods. These properties make conducting an RCA on the project justifiable and a valuable addition to the decision-making process.

C. Limitations & Future Work

The case study presented in this article is specific to the organization and culture; thus our results have limited generalizability, but the RCA method and results provide an insight into what to expect from the process. Another aspect is that our RCA team was inexperienced and other more experienced teams will run the process more efficiently with a better cost-benefit. Another issue is if a similar insight could have been gained if we delegated a similar amount of resources into the ISRA to investigate the problem. It is possible that the results of the ISRA would have overlapped more with the RCA with more time and resources spent on the former. However, the ISRA process does not argue for such a deep dive into the problem as the RCA process and does not provide tools for doing so. It is therefore unlikely that a more thorough ISRA process would have produced a similar result. However, the incentive for such an investigation was not there, and we perceive the ISRA methodologies as immature in this area [14]. Instead of considering the RCA as an extension of the ISRA, a possible path for future work is to conduct case studies where the researchers invest a similar amount of resources into both the RCA and ISRA and then compare results.

An additional direction for future work is to apply RCA to more and diverse case studies to get a better understanding of the contributions and limitations of the approach for InfoSec. Recent work has also proposed a novel approach for conducting socio-technical security analysis [11], and a path for future work is to adapt, develop, and improve RCA tools for InfoSec. Furthermore, the future efforts could research RCA efficiency through automation of tasks and build knowledge repositories. Regarding the latter, a repository of tools for data collection would help streamline step 3 in the RCA process.

VII. CONCLUSION

This study has applied RCA tools to propose a solution to a complex socio-technical InfoSec problem and found the RCA method a valid but costly extension to the ISRA. Running a full-scale RCA requires a lot of time and resources and the problem should be expensive enough to justify the RCA. The results from the RCA overlapped slightly with the initial ISRA. The main differences were that the RCA team proposed administrative treatments aimed at solving problems in the social domain, while the ISRA produced a more technical analysis and treatment for the problem. We conclude that practitioners should look at these two approaches as complimentary for dealing with complex socio-technical risks and problems. The combination of the ISRA and RCA will also have utility when planning for defense-in-depth, where administrative and technical risk controls can work in coherence to mitigate threats. The main drawback was that our cost-benefit analysis of the time and resources invested in the project is on the borderline of being justifiable, and the cost of the problem should be considered before launching a RCA. Thus, the RCA provides a viable option when dealing with complex and costly InfoSec problems and should be a part of the InfoSec management toolbox.

ACKNOWLEDGEMENTS

The authors acknowledge the help and support from Professor Einar Snekkenes, Christoffer Hallstensen and Stian Husemoen. We also extend our gratitude to all the participants in our study and to the anonymous reviewers.

REFERENCES

[1] *Information technology, Security techniques, Information Security Risk Management*, International Organization for Standardization Std., ISO/IEC 27005:2011.

[2] G. Wangen and E. Snekkenes, “A taxonomy of challenges in information security risk management,” in *Proceeding of Norwegian Information Security Conference - NISK 2013 - Stavanger*, vol. 2013. Akademika forlag, 2013, pp. 76–87.

[3] P. Shedden, W. Smith, and A. Ahmad, “Information security risk assessment: towards a business practice perspective,” in *Australian Information Security Management Conference*. School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2010, pp. 119–130.

[4] B. Andersen and T. Fagerhaug, *Root cause analysis: simplified tools and techniques*. ASQ Quality Press, 2006.

[5] K. Julisch, “Clustering intrusion detection alarms to support root cause analysis,” *ACM transactions on information and system security (TISSEC)*, vol. 6, no. 4, pp. 443–471, 2003.

[6] P. F. Wilson, *Root cause analysis: A tool for total quality management*. ASQ Quality Press, 1993.

[7] A. M. Doggett, “Root cause analysis: a framework for tool selection,” *The Quality Management Journal*, vol. 12, no. 4, p. 34, 2005.

[8] J. Collmann and T. Cooper, “Breaching the security of the kaiser permanente internet patient portal: the organizational foundations of information security,” *Journal of the American Medical Informatics Association*, vol. 14, no. 2, pp. 239–243, 2007.

[9] G. Wangen, “Conflicting incentives risk analysis: A case study of the normative peer review process,” *Administrative Sciences*, vol. 5, no. 3, p. 125, 2015. [Online]. Available: http://www.mdpi.com/2076-3387/5/3/125

[10] A. Abubakar, P. B. Zadeh, H. Janicke, and R. Howley, “Root cause analysis (rca) as a preliminary tool into the investigation of identity theft,” in *Cyber Security And Protection Of Digital Services (Cyber Security), 2016 International Conference On*. IEEE, 2016, pp. 1–5.

[11] J.-L. Huynen and G. Lenzini, “From situation awareness to action: An information security management toolkit for socio-technical security retrospective and prospective analysis,” in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017, pp. 213 – 224.

[12] B. Schneier, “Attack trees,” *Dr. Dobbs journal*, vol. 24, no. 12, pp. 21–29, 1999.

[13] G. Wangen, A. Shalaginov, and C. Hallstensen, “Cyber security risk assessment of a ddos attack,” in *International Conference on Information Security*. Springer, 2016, pp. 183–202.

[14] G. Wangen, C. Hallstensen, and E. Snekkenes, “A framework for estimating information security risk assessment method completeness,” *International Journal of Information Security*, Jun 2017. [Online]. Available: http://dx.doi.org/10.1007/s10207-017-0382-0