Empirical Case Studies of the Root Cause Analysis Method in Information Security

Niclas Hellesen, Henrik Miguel Nacarino Torres, and Gaute Wangen
Norwegian University of Science and Technology
Gjøvik, Norway
Email: niclash@stud.ntnu.no, henrik.torres@gmail.com, gaute.wangen@ntnu.no

***Abstract*— Root cause analysis is a methodology that comes from the quality assurance and improvement fields. Root-cause analysis is a seven-step methodology that proposes multiple tools per step, which are designed to identify and eliminate the root cause of a reoccurring problem. Lately, the method has been adapted into the information security field, yet there is little empirical data regarding the efficiency of the Root cause analysis approach for solving information security management problems. This paper presents three empirical case studies of root cause analysis conducted under different premises to address this problem. Each case study is qualitatively evaluated with cost-benefit analysis. The primary case study is a comparison of information security risk assessment and root cause analysis results from an analysis of a complex issue regarding access control violations. The study finds that in comparison to the risk assessment, the benefits of the Root cause analysis tools are a better understanding of the social aspects of the risk, especially with regards to social and administrative causes for the problem. Furthermore, we found that the risk assessment and root cause analysis could complement each other in administrative and technical issues. The second case study tests root cause analysis as a tabletop tool by modeling an information security incident primarily through available technical documentation. The findings show that root cause analysis works with tabletop exercises for practice and learning, but we did not succeed in extracting any new knowledge under the restrictions of a tabletop exercise. In the third case study, the root cause analysis methodology was applied in a resource constrained setting to determine the root causes of a denial of service incident at small security awareness organization. In this case, the process revealed multiple previously undetected causes and had utility, especially for revealing socio-technical problems. As future work, we propose to develop a leaner version of the root cause analysis scoped for information security problems. Additionally, root cause analysis emphasizes the use of incident data and we suggest a novel research direction into conducting root cause analysis on cyber security incident data, define some of the obstacles, research paths, and utility of the direction. Our findings show that a problem needs to be costly to justify the cost-benefit of starting a full-scale root cause analysis project. Additionally, when strictly managed, root cause analysis performed well under time and resource constraints for a less complex problem. Thus, the full-scale Root cause analysis is a viable option when dealing with both complex and costly information security problems. For minor issues, a root cause analysis may be excessive or should at least be strictly time managed. Based on our findings we conclude that Root cause analysis should be a part of the information security management toolbox.**

Keywords*— *Information Security; Root cause analysis; Risk Management; Case study; Socio-technical; Empirical.

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 (ISRA). 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. Although the InfoSec risk management (ISRM) approach is useful for maintaining acceptable risk levels, they are not developed to solve complex socio-technical problems or improve the system performance beyond keeping risk acceptable. For example, given a malware infected network the aim of the ISRA is to identify and deal with unacceptable risk, not to identify and deal with the root cause(s) of the problem. To aid the InfoSec industry in problem elimination, this paper continues the study of applying Root cause analysis (RCA) methodologies in InfoSec [1]. RCA is *"a structured investigation that aims to identify the real cause of a problem and the actions necessary to eliminate it."* [2]. The current RCA is not a single technique, rather, it describes a structured process that comprises of a range of approaches, tools, and techniques to uncover causes of problems, ranging from standard problem-solving paradigms, business process improvement, bench-marking, and to continuous improvement methods [2], [3]. 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 the objective of ISRM is to manage the risk by keeping it at an acceptable level.

Our literature review found that the application of formal RCA tools in InfoSec is an area that has remained largely unexplored. 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 contribution of this research is knowledge regarding the application and performance of established RCA methods on InfoSec problems. Specifically, the paper addresses the following research questions:

1) How does the results from running a full-scale RCA extend the findings from the ISRA process?
2) Does the RCA approach have utility in tabletop exercises?
3) How well does the RCA approach work in a resource and time restricted setting?
4) Which RCA tools are suited for InfoSec analysis?

The problems are investigated mainly through case studies, qualitative assessment of results, and cost-benefit analysis.

This paper applies the seven-step process RCA methodology [2] for comparison of results, each step in the RCA method includes multiple tools for completing the step. The data collected for this study was primarily from technical re-

ports, historical observations and data in the target institutions. Together with qualitative interviews of stakeholders in two of the case studies. A key limitation of this study is that the applied RCA all come from the tool selection described in Andersen and Fagerhaug.

The structure of this paper is as follows: The following section addresses previous work on RCA in InfoSec. Section III provides a description of the applied ISRA method for case comparison and an in-depth description of the applied RCA method and the associated tools including statistical analysis. The primary 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. Firstly, we present the results from the ISRA application as a comparison basis followed by the results of a full scale RCA. The case study is of breaches to the access control (AC) security policy (SecPol) with consequent costly incidents, 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 ISRA and the RCA presents different tools and approaches, but both seeks to treat the problem at hand, which makes the output comparable. The primary case 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. The second case study is of RCA performed as a tabletop exercise constrained to technical documentations of the Carbanak incident, in which a group of cyber criminals managed to steal large amounts of money from multiple banks. For this case study we analyze whether the RCA provides a useful insight into the incident. The third case study investigates the root causes of a DDoS attack against a Norwegian security awareness organization. This case was conducted under resource and time restrictions to test RCA performance under these conditions. Furthermore, this paper qualitatively evaluates the performance of RCA tools for InfoSec cases together with cost/benefit analysis. The RCA method suggests incident data as a source of knowledge [2] and we have conducted some preliminary work in applying incident data for RCA. This paper presents insight into key issues together for applying incident data in RCA with a proposal for future work. Lastly, we conclude the results.

II. Related Work

The RCA results presented in this paper represents the summary of the work presented in the Thesis "Root cause analysis for information Security" [4] and is an extension of the conference version of the paper "An Empirical Empirical Study of Root-Cause Analysis in Information Security Management" [1].

RCA was developed to solve practical problems in traditional safety, quality assurance, and production environments [2]. 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 [2], [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.

According to Wangen et al. [12] one of the most developed InfoSec risk analysis methods is the Factor Analysis of Information Risk (FAIR) [13]. The authors of FAIR have recognized the need for RCA as an extension of the ISRA method to eliminate problems and they propose a short version of RCA based on flowcharts (p. 366-373). Yet, the book does not go in-depth regarding the RCA method and does not provide any data regarding application. 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* [14]. 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 research approach was case studies of problems occurring in a Scandinavian R&D institution (primary case study), multiple banks (tabletop exercise) and a small security

awareness company. The case studies were conducted to investigate the complex socio-technical security problems.

Each case study was conducted following the seven step RCA process, Fig. 1. Furthermore, we qualitatively assessed the results. For the primary case study, we also analyzed the differences in approaches between RCA and ISRA, 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, overview of the applied tools used, data collection methods, and a brief overview of the statistical methods used for data analysis.

A. ISRA Method for the primary case study

The ISRA was conducted as a high-level risk assessment for the institution, which revealed the need for deeper analysis of the problem. The 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 [15]. By focusing on assets and vulnerabilities, these assessments tend to have a technical scope [16], [17] with estimates of consequences and respective probabilities of events as key outputs.

The ISRA method applied for the case study is based on the standard ISO/IEC 27000-series [15]. It was further substantiated with the Wangen et al. [18], [12] approaches, which center 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. To illustrate the risk, we modeled it using the CORAS language [19].

B. Applied Root cause analysis method

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 [2], 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 was out of scope. Depending on the problem one or more tools are required to complete the RCA steps and conclude the root cause(s). As recommended in the methodology, we chose tools per step based on our judgment of suitability. All 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 starting with the tool applied for the primary case study (see [2] for further description).

1) Problem understanding: The goal of this step is to understand the problem and rank the issues. The tools for understanding the problem are meant to give a better understanding of the problem itself and what aspects in the case one should consider for further investigation. In order

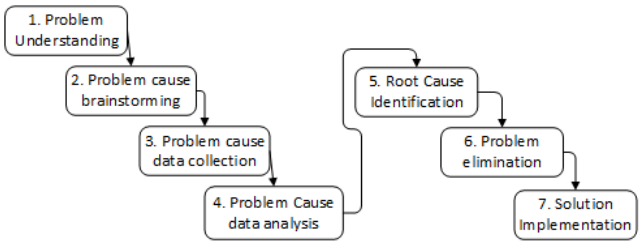

Fig. 1: Seven step process for RCA [2].

to know which tool to use on the problem and to handle the correct problem, it is important to first understand it. Below we will list some of the tools we tried out in our research.

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 [2] (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).

Critical Incident: The main purpose of the Critical Incident tool is to understand what are the most troublesome symptoms in a problematic situation. By using the Critical Incident, you will get a better understanding of the aspects of the problem that must be solved, as well as the nature of the problem and its consequences. As with most root cause analysis tools, they are best used by a team to determine the cause of the problem. To work it requires an atmosphere of trust, openness and honesty that encourages people to disclose important information without fear of the consequences. This applies to all tools but especially Critical Incident.

Swim Lane Flowchart: Swim Lane Flowchart shows the flow of events through a timeline and shows connections between events. The chart is divided into players where each player has his horizontal path.

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. Brainstorming 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. Brainstorming can take place in different ways, structured or unstructured brainstorming and brain writing. A structured brainstorming is based on the members coming back with suggestions to ensure that no person dominates the process. Unstructured brainstorming allows spontaneous responses from anyone in the group at any time. Brain Writing can be done in two ways. Group members write down their ideas on so-called ID cards, or on a blackboard. During brainstorming, it is important that ideas and suggestions are not criticized until all the ideas and suggestions will be reviewed.

3) Problem Cause Data Collection: The data collection phase helps to make searches for problems more accurate. Random problem solving tends to result in assumptions and guesswork while structured RCA is based on a systematic collection of valid and reliable data that is an important step in

root cause analysis. It is therefore important to plan carefully what tools one might think about using. RCA recommends several data collection techniques [2].

Interviews: For the primary case study, this study chose scientific interviews as the main data collection approach as this 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. More informal interviews were also applied as a data gathering method in case study 3.

Check Sheet: is used to systematize collected registered data. The main purpose is to ensure that all data collected complies with reality. Can be used to record the frequency of events that are believed to cause problems.

Incident data analysis: Andersen and Fagerhaug [2] proposes to analyze incident data as a part of the RCA. However, analysis of InfoSec incident data is quite complex and the future work section outlines some of the research problems encountered working with RCA and incident data. Additionally, we propose research directions for solving the problems.

4) Problem Cause Data Analysis: The purpose of this phase is to clarify possible causes before attempting to solve the problem in the final preparatory stage, for example, how are the possible causes related to the problem and what is the most harmful? The purpose of the data analysis phase in the final preparatory stage before attempting to solve the problem is to clarify possible causes. It is important to look at how different aspects of the problem are linked. In data analysis, the following tools can be used:

Statistical analysis: 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.

Affinity diagram: helps to correlate apparently unrelated ideas, conditions, meanings, and reasons so that they can collectively be explored further. When analyzing qualitative data, Affinity Diagram is useful as it groups data and findings of underlying relationships into groups.

Relationship Diagram: Relationship diagram is a tool used to identify logical relationships between different ideas or problems in a complex and confusing situation. In such cases, the strength of the relationship diagram is its ability to visualize such relationships. The main purpose of a relationship diagram is to help identify issues that are not easily recognizable.

5) Root Cause Identification: The goal of this step is to identify the root cause(s) of the problem. From the list of possible causes created and analyzed previously, this step is designed to identify the root cause. With root cause identification, the goal is to develop solutions that will eliminate the symptoms and thus eliminate the problem. In terms of duration and complexity, this stage is rarely the hardest or longest. With thorough preparation, you can usually go through this stage quickly.

Cause-and-Effect chart (Fishbone diagram): Fishbone is a tool that analyzes a relationship between a problem and its causes. It has aspects of brainstorming and systematic analysis to create an effective technique. The main purpose of the tool is to understand what causes a problem together with the secondary causes/factors influencing the problem. It can be used to develop as well as group reasons for a problem. The Fishbone diagram also evaluates systematic causes, finds the most likely root causes and should map to the undesired effect to the problem.

Five Whys is designed to identify a problem then ask why this is a problem. When you get an answer, ask why. This is usually repeated five times until you get to the root cause.

6) Problem elimination: The goal of this step is to propose solutions to deal with the root causes of the problem, Andersen and Fagerhaug [2] 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. This step is successful if you remove the correct root problem (s), the symptoms will disappear along with the problem and will not resume.

Systematic Inventive Thinking (SIT): It is based on investigating one or more components of the problem. All components should then be assessed using the five SIT principles [1]. These principles are as follows: Attribute dependency: Assess if a change in component will lead to improvement. Component control: examine how the component is connected to the environment around it. Replacement: Replace something in the component with something from the component's environment. Displacement: Assess if the component can increase performance by removing part of the component. Division: Assessing splitting of a component or product's attributes can provide improvement.

Countermeasures Matrix: It is a method to help you prioritize what actions to take. Priority is established by ranking based on the impact and feasibility of recommended measures.

7) Solution implementation: Solution implementation focuses on the implementation phase. This step includes how to organize the implementation of solution implementation and how to develop an implementation plan. We have not been able to implement solution implementations in our task, but we have made suggestions for the execution of the tools to which the book refers.

Tree Diagram: Implementation processes can be complicated, but in order to break down and organize the work, Tree Chart is used to structure the activities. It is a tool that is easy to use to break down major tasks in the business to manageable sizes. Tree Diagram is simply a way to represent a sequence of events.

IV. Primary Case Study: Risk Assessment of 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.

1) Risk Analysis Results.: The risk is modelled in Fig. 2 using the CORAS modelling language [19]. From the model, we have two likely conditional events where (i) the attacker obtains access token and PIN, or (ii) access to the facilities by piggybacking employees or students. 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 (not differentiated in the CORAS model). In addition, we have the low probability and high impact risk that sensitive information gets compromised through this attack.

2) 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

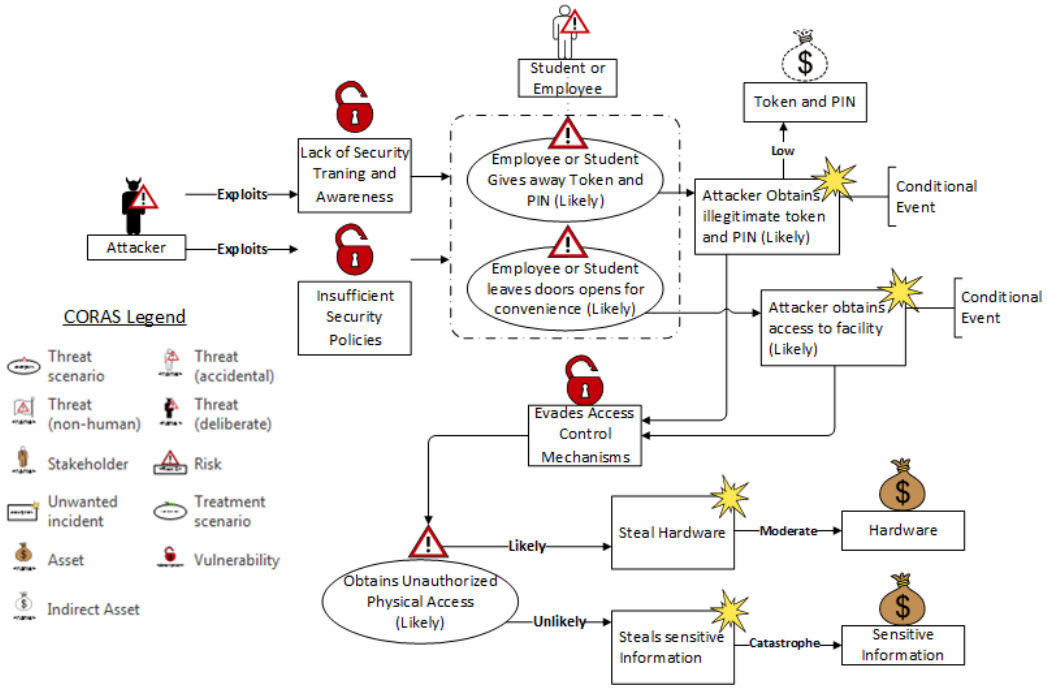

Fig. 2: Risk modelled with CORAS [19]

data privacy protection laws. Neither did it address the socio-technical problem with the SecPol, card swapping, and card lending.

V. Primary Case Study: RCA of Access Control Policy Violations

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 preliminary identified problem causes. The performance matrix, Fig. 3, 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. 3.

B. RCA Process Step 3 - Data Collection

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. 4 displays the distribution among the six primary

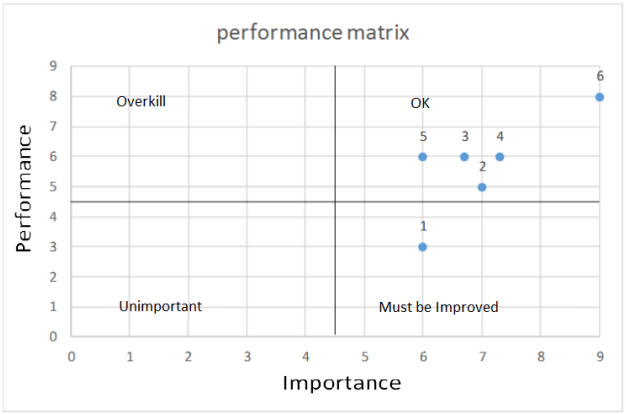

Fig. 3: Performance matrix.

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				

stakeholders. The interview subjects for the academic staff, Ph.D. Fellows, 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.

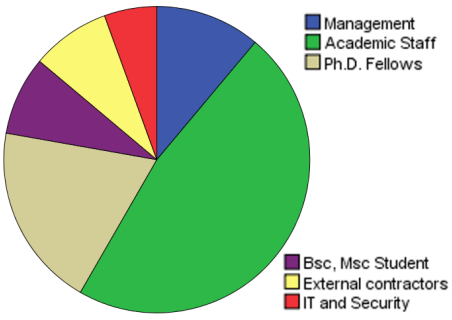

Fig. 4: Distributions of stakeholder groups included in the study

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. 5. 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.

F. Comparison of Risk Assessment and RCA Results

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 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

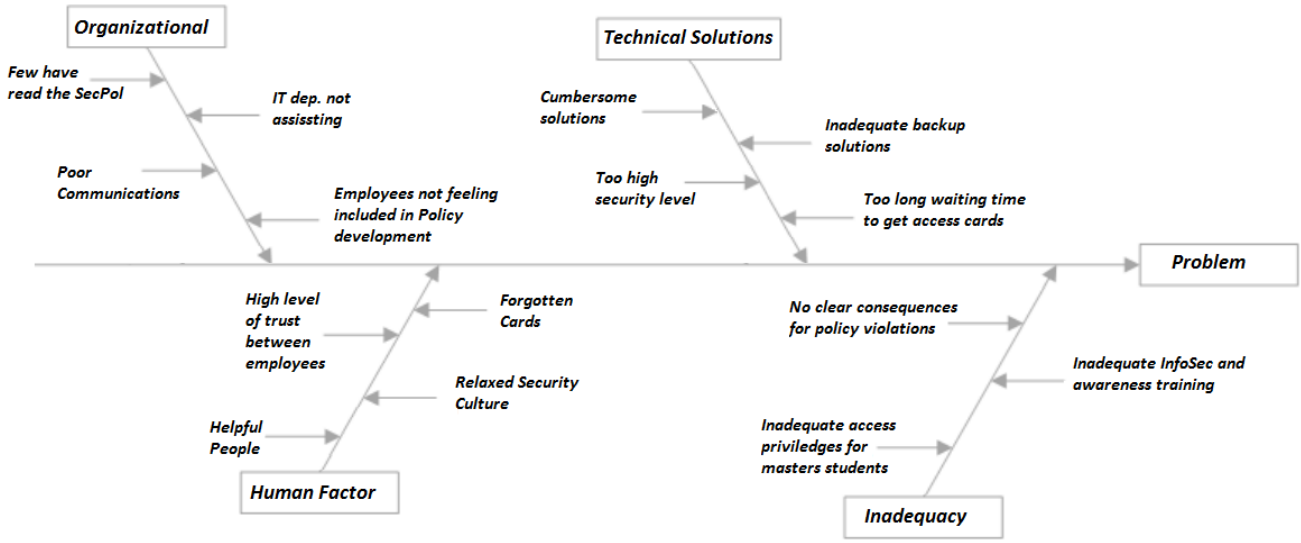

Fig. 5: Fishbone diagram illustrating contributing causes to the main problem.

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.

Moving on, the nest section presents the results and evaluation of RCA as a tool for tabletop exercises.

VI. Tabletop RCA case study: Carbanak

The RCA tabletop case was meant as an experiment on how well RCA worked on a case with only historical data and technical documentation available. A tabletop exercise is a discussion-based exercise where personnel meet in a classroom or simulated setting. The group got presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident. Which means that there was restrictions regarding access to new information. This case investigated how the RCA work on a tabletop case.

The case study concerned attacks on multiple banking institutions, where the attackers managed to steal large amounts of money. The attack was often referred to as Carbanak, but also Anunak [20], [21]. The tools used on each step during the analysis of the tabletop case is described in the following sections.

A. Problem understanding

Since we worked only with documentation of the attack we needed to gain an overview of information that was gathered. Based on the constraints we found swimlane flowchart to be the best suited tool for modelling the attack, Fig. 6. As noted in Section III-B this flowchart works by having a swimlane representing each actor on the y-axis, where the lanes progress following the x-axis, which represents the chronological order of actions or events in time. The flowchart had three lanes representing actions taken by either the attacker, the bank employees and administrator. This tool visualized the main events and how one lead to another. We found that the primary way the attackers got into the banks was by using phishing emails that was sent to employees, as documented at page 3 in a Kaspersky report [20]. Furthermore, the attackers exploited vulnerabilities in Microsoft Office and Word before installing the backdoor named Carbanak. In a video of a presentation by a Kaspersky employee, the employee said that the attackers escalated their privileges by sending an email from the infected computer to the IT help complaining that the computer ran slow [22]. The IT employee then logged in to the computer and had his or her credentials stolen by a keylogger. The attackers now escalated their privileges by obtaining access to more machines to spy on additional bank employees. The attackers then observed common working patterns and learned how to use the tools the employees was using. This knowledge allowed them to proceed with their attack and steal money from the bank. The swimlane chart helps to visualize the attack flow and allowed us to obtain an overview of the situation, steps taken, involved parties, and the timeline.

The second tool applied in the problem understanding was *Critical Incident*, which is a tool meant to aid in the process of uncovering symptoms of the most problematic root causes [2]. Critical Incident is a two column table where the left column is the name of a type of incident and the right column is the frequency occurrence. Due to the constraints of the tabletop exercise, we did not have the numerical data on the frequency of different incidents that we needed to complete

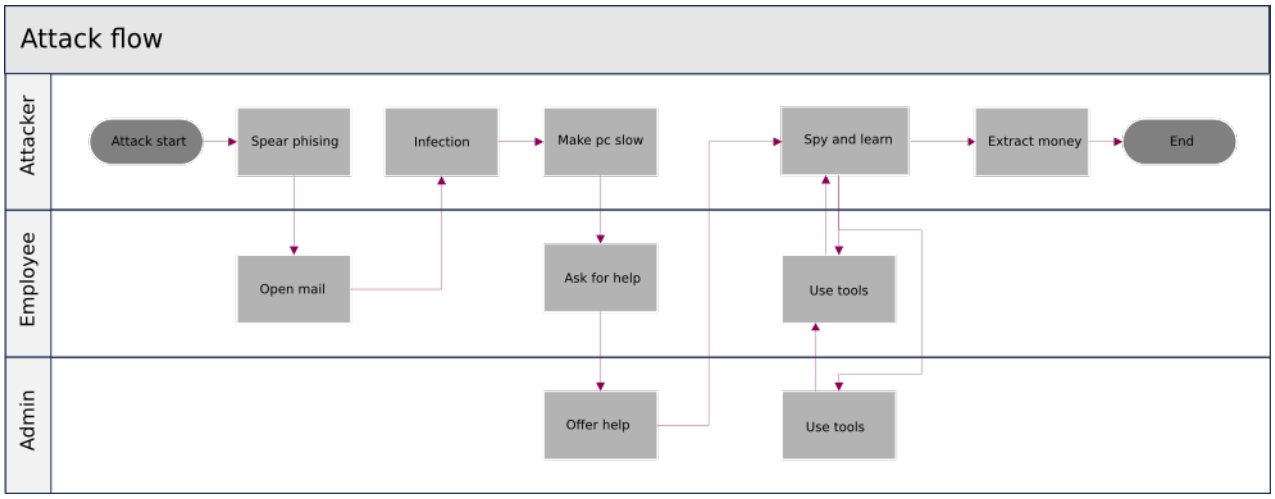

Fig. 6: Swimlane Flowchart illustrating attack flow, the timeline of the attack from left to right.

TABLE IV. CARBANAK CRITICAL INCIDENT TABLE FROM PAGE IN 88

Name	Frequency
Suspicious traffic	High
Monitoring of machines	High
Opening of e-mail attachments	Medium
Policy violations	Medium
Unfaithful employees	Low
Attackers has access to servers	Low
Undiscovered infections in IT systems	Low
Ignorance of spyware	Low
Low security awareness among coworkers	Low

the tabletop case. The solution was to use logical reasoning to estimate which incident most likely had the highest frequency based on the technical documentation. We estimated this using weights ranging from High - happens daily, Medium - weekly, to Low - monthly or less often.

Suspicious traffic has the highest frequency in the table. This traffic represents communication that goes from and between IT equipment inside the banks that are infected and the machines owned by the attackers. The frequency is set to high as we expected that this traffic could reasonably be argued as high. The attackers monitored machines owned by the banks in order to see how the employees operated them, page 21 [20], and this is also placed as high frequency. Since the collected documentation described that the attackers got into the bank through email attachments it may be possible that it is not too uncommon that employees opens and runs files received in mail attachments. An employee may break a policy without being purposefully unfaithful, but rather negligent. Thus it was ranked as with medium frequency. The amount of times it is believed that the attackers felt a need to enter the server infrastructure of the banks is deemed as low. This happens most likely when the attackers wants to place backdoors or start malicious processes.

B. Problem cause brainstorming

Unstructured brainstorming aims to brainstorm on possible causes and present them to the group members. The results were generated as a list of problems that can be improved. We also wanted to identify possible consequences that originated from the problem being analyzed.

The produced list from the brainstorming process is not sorted in any way, and may contain suggestions that more or less overlap. The following step is therefore to sort the list and merge suggestions that overlap and improve upon the suggestions. The list is then sorted according to what is deemed to be the most realistic cause of the problem by the RCA team.

Lastly, in the third step we categorized the proposed problem causes. A total of four categories were created, where the first category deals with the training of employees and the follow-up of the training. This category included the suggestion that there might be a lack of policies or a lack of training and exercise of said policies. The second category referred to weaknesses such as lack of updates and the failing to notice suspicious activity in their systems. The third category referred to monitoring of network and the fourth and last category was about corporate threats.

C. Problem cause data collection

It was not possible to do an active data gathering during the tabletop case since there is no access to personnel to interview or systems to look into.

D. Problem cause data analysis

In this phase we used Relation Diagram and Affinity Diagram III-B. The Relation Diagram, Fig. 7, illustrates the relation between different systems and computers, compared to the Swimlane Flowchart which showed the flow of actions over time. A large circle was drawn on a whiteboard and elements that was viewed as important and overarching was written around the circle. Arrows was then drawn between these items according to relations. In this case, we did not find any new relations that we did not expect already from the documentation and previous RCA steps.

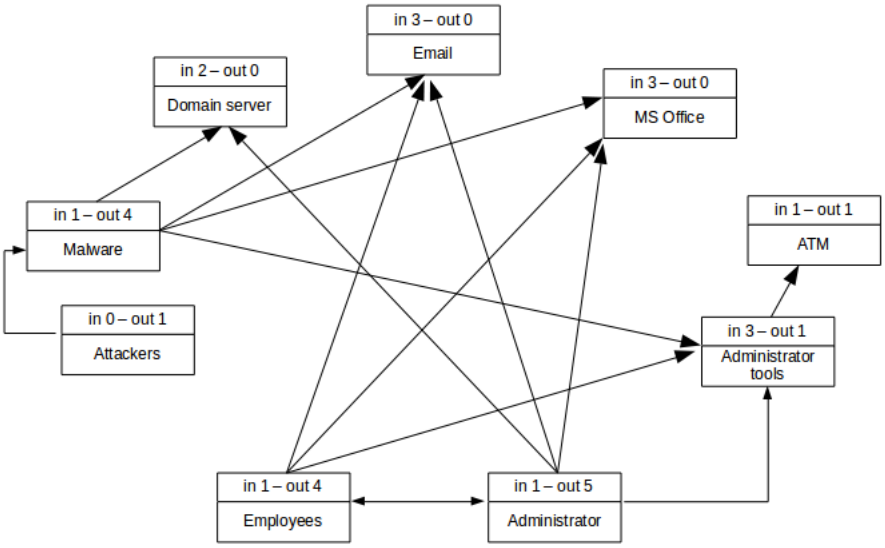

Fig. 7: Relation Diagram illustrating connections between employees and systems.

The Affinity Diagram is a tool for organizing ideas and data. Fig. 8 represents the affinity diagram for the case where we organized the problem situations under the groups malware, training, and environment.

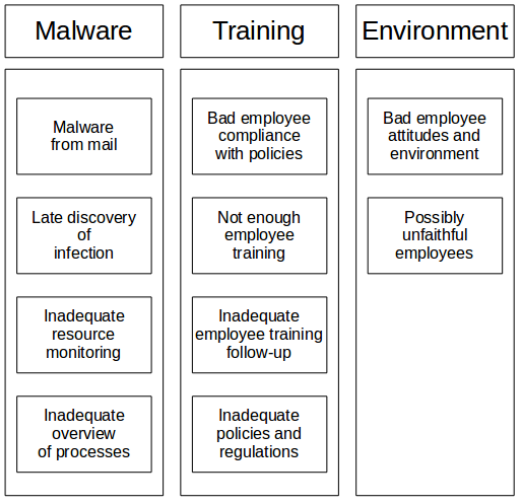

Fig. 8: Affinity Diagram illustrating ordering by context.

E. Root cause identification

The Five Whys approach was used to identify root cause, Table V. The tool was used on the question of why the ATM's gave away money to the criminals. The reasons that answers each of the five why questions was suggestions of what could be realistic, given that this was a tabletop case. The tool did uncover one root cause, however it is not visible if there exists more root causes. The tool appear to be able to isolate the users on one root cause unless it is run several times. The tool was very quick to complete.

TABLE V. CARBANAK TABLETOP CASE, FIVE WHYS

ATM giving away money	Reason
Why?	Because the system was compromised
Why?	Because the attackers exploited a vulnerability when employees opened mail
Why?	Because their software was not up to date
Why?	Because the bank had inadequate update routines
Why?	It was not considered to be critical enough

F. Problem elimination

The tool Countermeasure Matrix, Table VI, was used to suggest worthy countermeasures based on efficiency and feasibility. The way the group solved it was by rating efficiency and feasibility of a counter measure from 1 to 5. The two scales are then summarized, and if the number is ten or above, an action is suggested to be taken. However, for upgrading of legacy systems an action was set to not do anything because it could be unrealistic in many large organizations. We define updating as installing a newer version of a software while patching as installing security patches and bug fixes of a given version of the software. With baseline, it was meant as to have a hash of most files in a system that could be used to detect changes to these files.

G. Solution implementation

A Tree Diagram, displayed in Fig. 9, was used to show which solutions and problems was related to each others, sorted under categories that was linked together with branches that are rooted to the main problem.

H. Assessment of RCA as a tabletop exercise

We found that doing a tabletop case gave us experience on the choosing and execution of RCA tools, but it did not provide any new information about the case being analyzed.

We do see that doing a RCA requires allot of information

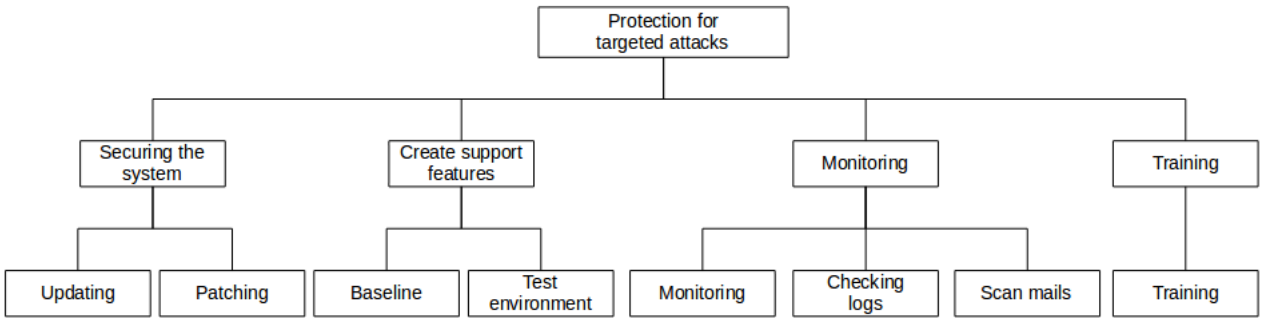

Fig. 9: Tree Diagram illustrating relations between problems and solutions.

TABLE VI. CARBANAK TABLETOP CASE, COUNTERMEASURES MATRIX

Countermeasures	Efficiency	x Feasibility	Sum	Action
Updating	4	5	20	Yes
Patching	4	5	20	Yes
Auto-updates	4	2	8	No
Training	2	5	10	Yes
Baseline	4	3	12	Yes
Monitoring	4	4	16	Yes
Temporarily close bank	2	1	2	No
Trace attack back to attacker	2	1	2	No
Upgrade legacy systems	5	2	10	No
Sandboxing	3	3	9	No
Test environment	4	3	12	Yes
Going through logs	3	5	15	Yes
Scan incoming emails	3	4	12	Yes

about the case. For practice reasons a tabletop case works with providing practice in selecting tools and applying them, but in order to do an actual RCA and discover root causes and implement solutions to them it is necessary to have access to key personnel, logs about what happened, and any other information that can be gathered.

As the tabletop case was dealing with protection versus an APT, we got the impression that completely eliminating a treat of attack from such an opponent is not completely possible. However, eliminating a root cause for an exploited vulnerability increases the organizations resistance towards attacks from the attacker.

VII. Case Study 3: Root cause of DDoS against small security awareness organization

In this case study, we analyzed a case we received from a small Norwegian security awareness organization of a DDoS attack that occurred in May 2015. At the time, the organization consisted of approximately ten employees with the primary objective of preventing and mitigating the consequences of identity theft. In this case we applied the RCA tools to investigate the root cause why their primary website became unavailable during the attack. We also studied whether the solution proposals implemented to date answer all the problems or if any problems remain.

The data sources we had available for the case study was primarily access to key personnel and the police report. Meetings with key stakeholders were conducted in connection with the problem understanding and data collection. An important limitation was that the organization told us that they wanted to largely ignore technical issues, like for example how to avoid DDoS and type of DDoS. The case study was also conducted under time and resource constraints and was conducted to see how the RCA method perform under these conditions. This case study was completed within approximately 150 hours.

A. Problem understanding - Multiple tools

The police report of the attack was an important contribution to the problem understanding and facilitated modelling the problem in a *Swimlane Flowchart*. The model is intended to show the flow through performances and events. The incident involved three stakeholders: The attacker, the website host, and the organization. The incident spanned over two days, following is a description of the timeline and elements in Fig. 10:

7th of May 2015

- 14:30 - Organization is notified via external service that Organization's web pages are unavailable.
- 15:45 - Organization contacts their service provider and is informed that they are working on the matter.
- 16:16 - Organization is contacted by its service provider, who informs that it is a denial of service attack (DDoS)
- 19:50 - Organization is contacted by their service provider explaining that Organization's web pages continuously receive between 40 and 60000 requests from foreign IP addresses and fails due to overload. There was an attempt to block foreign traffic, but due to the challenges of the service provider's network provider, this did not make it possible. It was then attempted to change the IP address of Organization 'web server and update the DNS of the domain Organization.no. This worked for 15-20 minutes. Afternoon/Evening - Organization informs National CERT (NorCERT) and the related security operations centre about the denial of service attack. NorCERT also gets the logs of the attack.

8th of May 2015

- 08:00 - All Organization websites are still unavailable.
- 08:10 - All web pages are available again
- 10:15 - The attack starts again, with the result that all the pages again becomes unavailable

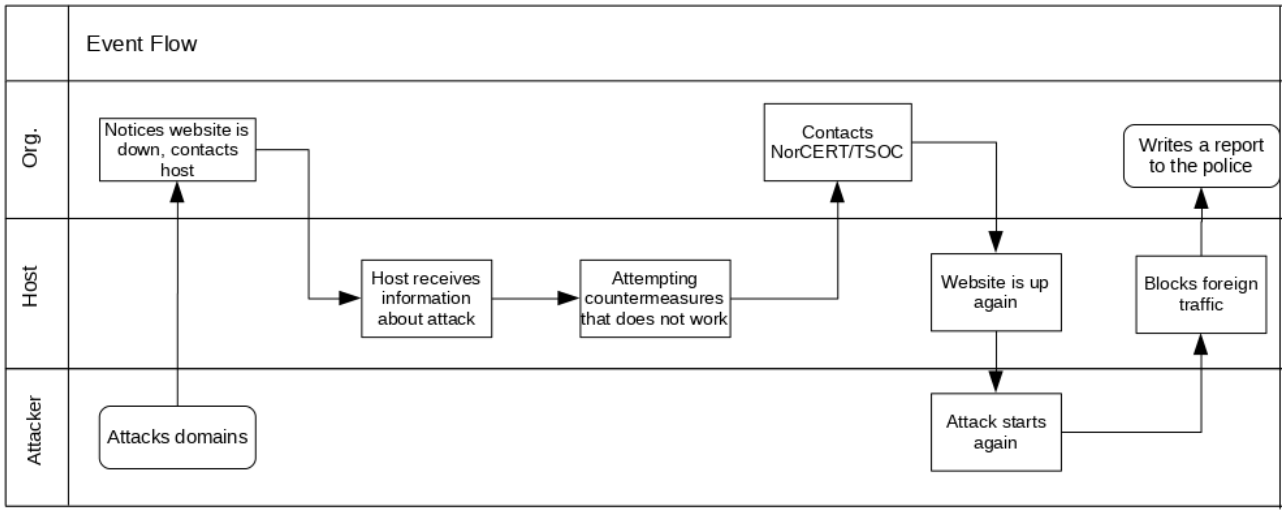

Fig. 10: Flowchart for DDoS case study.

- 12:24 - Service Provider informs that they are now blocking traffic from abroad, and web pages are gradually available for Norwegian and Scandinavian visitors. 12:30 - The local police is contacted for assistance in the case.

Performance Matrix

Performance Matrix was used to find out the most important priorities for the organization and the current performance within these areas. The priorities were identified in co-operation with key stakeholders. The stakeholders said that the most problematic about their site being down was that people could not access the self-help sites for identity theft mitigation. At the time, the organization had no sufficient countermeasure in place against DDoS. They could not quite answer how many times they were exposed to DDoS in a year, because they lacked the overview.

We were told that there was a high number of inquiries to the main website. Another problem was that it could also be difficult to respond to each inquiry within an acceptable time frame and provide sufficient help. Their self-help page and also website uptime were highly ranked within the performance matrix, as it is an organizational objective from them that the self-help site should serve and solve the majority of the inquiries. For the performance matrix we investigated the importance and performance of four areas: (i) Ability to help together with uptime and capacity for managing requests, (ii) Customer contact possibilities, (iii) Response Time, and (iv) Availability of the Self-help page. Fig. 11 shows the performance matrix for the four areas rated in co-operation with the expert.

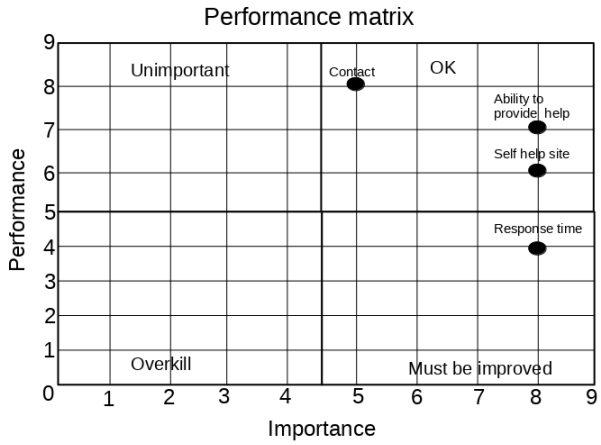

Fig. 11: Performance matrix for DDoS Case Study.

B. Problem cause brainstorming

Here we used unstructured brainstorming to obtain an overview of and consensus on what is being seen as problem causes. We developed a list of expected consequences and causes of the problem or the problems that build up the visible symptoms. The following list is grouped by importance, starting with identified possible consequences of the problem:

1) No accessibility for clients/users of the service.
2) Reduced reputation.
3) If the organization is unable to drive self-help, they will experience increased queues in other channels which they are not staffed to manage.
4) Possible financial problems.

Possible causes of the problem:

1) Service Provider had no tested plan for handling the situation.
2) Not enough knowledge and training in the organization for handling the incident.

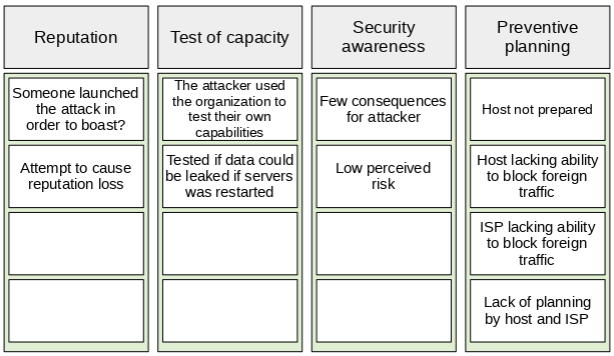

Fig. 12: Affinity diagram for the DDoS case study.

3) The organization is a target because it puts itself in a cross fire between individuals' problems and cyber crime attempting to make money.
4) The attackers can be outside Norway, which limits the jurisdiction and prosecution for domestic authorities.
5) No existing DDoS deterrence.
6) DDoS of the website was not a prioritized risk.
7) Missing/insufficient risk assessment.
8) Insufficient resources spent on server computing power, throughput, and bandwidth.

C. Problem cause data collection

Due to the case constraints and since we already had collected data on the problem, we chose to apply the check sheet approach for systematizing the problem cause data. With the Check Sheet tool we examined how the situation was while under attack and how the situation was afterwards. The desired dividend is to achieve a priority or a ranking of the items to be analyzed.

The points generated in the brainstorming phase were discussed with our contact person at the organization. Each item in the causes and consequences list were discussed and ranked. No graphical models of the check sheet was produced for the case.

D. Problem cause data analysis

Very few of the available RCA tools suited the case study. On the other hand, it was feasible to look for hidden contexts in the data collected. An Affinity Diagram 12 was attempted even though the data was not numeric.

The desire is to look for hidden contexts in the data collected. Following is qualitative assessment of the causes from the data collection phase:

The police did not look at the evidence: The organization collected the available evidence in the form of logs, and these were encrypted and password protected. The organization then reported the attack to the police and sent the encrypted evidence file and wrote that the police could contact them to receive the password for the file. The police never contacted them to obtain the password and dropped the case. Which means that there is a low probability of the attacker experiencing any consequences.

Contact with service provider: The website provider had no procedures on how to handle the situation, and contacted its network provider who could not immediately assist. The time it took to establish contact was relatively short. Slettmeg.no experiences it as an important aspect of this situation that contact time is short and that they themselves know that there are problems with the services they are delivering.

Ad-hoc situation handling: The provider of the web services was not trained in such situations and could not handle it when the attack occurred. Therefore, they contacted their network provider and suggested that they block the traffic from foreign addresses when they discovered that the attack did not originate from Norway. The network provider was also unable to immediately respond to this request. The organization itself had not completed any exercises on DDoS situations, so the incident was handled ad-hoc.

Host unable to block foreign traffic immediately: The website host did not have any mechanisms in place to shutdown network traffic from abroad. Thus, they had to contact the ISP they used, which also had no solution in place. Thus, it took unnecessary time for network traffic from abroad to be closed.

Wide-spanning vulnerability: The crash was aimed at the domain and not the IP address, however, the traffic took down all web services provided by the organization.

Unnecessary resources spent on handling the incident: The attack also led to people having to prioritizing to handle the situation leading to production loss. This situation occurred both at the web host and the ISP.

E. Root cause identification

Due to the restrictions of the case study, no visualization tools were applied to this phase. For this case, we identified 5 primary root causes

1. The attacker's motivation and intention: The attacker is motivated to perform an attack for several different reasons. Some of the reasons may occur from the work on mitigating the consequences of identity theft. There may also exist motivations that are not due to the organization's primary objectives but may be motivated by the attacker attempting to gain recognition. Bragging also deal with hacktivists that is motivated by publicity and fame. There may be a prestige in taking down a website that is managed by a security organization. DDoS is an easy to implement attack and with the right measures it is difficult to reveal the attacker.

2. Low perceived risk: It is costly to track down a moderately skilled attacker on the Internet. This may contribute towards the attacker thinking that there is a low probability of detection and therefore, there are no effective deterrents.

3. Easy to implement: A DDoS attack is easy to conduct. Even with little knowledge, there are standardized tools available for the task, some for free and others for sale. Amplification attacks also contribute contribute to an uneven distribution of power between attacker and defender, as the vulnerable protocols are easy to exploit.

4. Lack of preparation: Neither the organization, website host, or the ISP was prepared to manage the DDoS incident.

5. Lack of security management: The situation was poorly managed and the organization delegated responsibility for the situation without verifying that the host was able to handle such situations.

F. Problem elimination

Systematic inventive thinking is an approach to eliminate the problem. Since the case study had time constraints, the root cause we proposed to address was primarily Lack of security management. Furthermore, we listed components for the problem and according to tool description we took suggestions on components even though they could seem irrelevant. The areas we proposed to improve was:

1) Responsibility and chain of command
2) Security procedures for handling the problem
3) The contract and service level agreement
4) Incident handling cooperation and communication with the supplier
5) Knowledge and experience building of the provider.

These problem-solving components were chosen according to the 5 SIT principles. However, several of the principles turned out to be unworkable on the component, and in our case we chose to leave them blank. During the implementation of an SIT principle, we have described a proposal for improvement based on the purpose of the principle. Following are SIT analysis examples of the three first countermeasures:

No. 1 Responsibility and chain of command.
Component control: Ensure that the responsible person is linked to environments with professional knowledge.

No. 2 is Security procedures:
Attribute dependency: Impose greater control on the purchased services.
Component control: Compare own procedures with best practices.
Procedure: If one compares their procedures with similar organizations and best practices, one can discover weaknesses in their own and get new ideas on how problems can be solved. By carefully examining the service provider, an attempt can be made to reduce possible problem situations in the future.

No. 3 is Contract:
Attribute dependency: The contract should clearly describe the supplier's responsibilities.
Component control: Make sure the contract is equivalent to the environment.
Procedure: If the contract had held the service provider responsible, it could have been possible for the organisation to receive compensation for lost working hours caused by reorganization of work tasks during and after the attack. Contracts can also specify that the provider must have knowledge of how such situations should be treated.

G. Solution implementation

We have presented suggestions for improvement on procedure and contract. Furthermore, it is necessary to determine how the implementation is to be organized. The solution implementation tools available to help explain how the organization should be. Then there is the question of whether a tool is needed to guide, organize and structure the implementation. If the implementation is large or unintentional, it is recommended to use a Tree Diagram. We see from previous analyzes that the three chart has a structured review, as shown in the access card case for access cards and DDoS case. When it is appropriate to make comparisons with other organizations, a Spider Chart can be used.

TABLE VII. TOTAL HOURS SPENT CONDUCTING THE PRIMARY 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.

H. Assessment of RCA in situations with limited resources and time

Having a limited amount of time and resources on the analysis of the DDoS attack was very demanding. Two analysts completed the case within two weeks ($\sim$ 150 hours of effective work). In this case, the project team would have benefited from more contributors, for example, by identifying more potential problems during the brainstorming phase. Additionally, more project members would have provided a stronger quality control of the RCA process in the early phases. Due to time constraints, the tool selection and model development had less emphasis as the pressure was to deliver results within the time frame. However, going through the RCA process did produce results and insight into the problem. The RCA tools do force a structure onto a complex issue, which makes it more comprehensible. Our results shows that carrying out a RCA can provide a better understanding of the situation even with limited resources. We came up with suggestions for changes that the organization had not considered following the incident, providing evidence that the RCA process does have utility for InfoSec issues in more time constrained environments as well. However, the results would have improved with more time and resources, and more of both would be needed to complete a case with increased complexity and scope of the problem.

VIII. Discussion

This section discusses the cost/benefit of RCA, then evaluates the RCA tools for InfoSec application, and lastly, outlines the limitations and proposals for future work within the field.

A. Cost-benefit analysis

For cost-benefit analysis, we consider time spent on tasks and usefulness of the task. Table VII shows cost in time for

our team from conducting the primary case study. 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. Case studies 2 and 3 were conducted within approximately 150 hours per assessment, but without a concrete distribution of hours per task. Because of this, they are left out of the cost benefit discussion.

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.

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.

B. Evaluation of the applied RCA tools

In this section, we evaluate the tools regarding expectation, application, and outcome. The cases are numbered as follows; the case about the access control for the Scandinavian R&D institution is *case one*, the tabletop exercise is *case two*, and the DDoS on the Security awareness website is *case three*. Table VIII shows an overview of the RCA tools applied on each case.

1) Performance Matrix: The performance matrix was applied in two cases. The purpose of this tool is to achieve a better understanding of the problem, prioritization of problem components, and to identify which part of the problem will reduce the largest amount of symptoms if removed. In the primary case study, we interviewed key personnel from the IT department at the institution based on the tool. The difference between what we estimated the answers to be and the responses we got was quite different, which shows how important it is to have key personnel partaking in the process of applying a Performance Matrix. Overall, this tool helped the group to gain a better understanding of the problem.

TABLE VIII. OVERVIEW OF RCA TOOLS USED IN THE CASE STUDIES.

RCA Phase	Tool name	Case 1	Case 2	Case 3
		Card Swap	Carbanak	DDoS incident
Problem Understanding	Performance Matrices	X		X
	Critical Incident		X	(X)
	Swimlane Flowchart		X	X
Problem Cause Brainstorming		X	X	X
Problem Cause Data Collection	Interviews	X		X
	Check Sheet			(X)
	Incident Data Analysis			
Problem Cause Data Analysis	Affinity Diagram	X	X	X
	Relationship Diagram		X	
Root Cause Identification	Fishbone Diagram	X		
	Five Whys		X	
Problem Elimination	Systematic Inventive Thinking	X		X
	Countermeasures Matrix		X	
Solution Implementation	Tree Diagram	X	X	

X = Applied
(X) = Tested, but experienced restrictions

In the DDoS case, it was essential for us to determine what was important for the website owner and how they felt that the functions they offer were working. We did experience that communication was critical, such as our ability to communicate what we were looking for. A note here is that more planning on how to teach the workings of performance matrices to the stakeholders would have made the process easier and quicker than we experienced it to be.

In both cases, we found that performance matrices were worth the effort as they are not time-consuming and they provide valuable insight into the problem.

2) Critical Incident: This tool was used in case two and three. Our expectations of the tool in these cases were that it would give a canonical and graphical display of the most frequent incidents. In both cases, we realized that it was not possible to generate actual numerical frequency labels. However, our experience in case two shows that it was possible to substitute these numerical frequencies with variables such as ”low, medium, and high,” as long as a description of what these ranges are. In case three, this issue was solved by creating questions that we gave them, and they ranked them according to what they found the most problematic. Our experience shows that it was difficult to acquire numerical frequencies of InfoSec incidents or other events, which rendered the critical incident tool having low utility. We managed a workaround using subjective values but quantified numbers are less prone to biases, and an approach for quantifying InfoSec incidents is proposed in the future work section.

Under the premises for the case studies the critical incident tool still provided information regarding problem causes without numerical data. However, frequencies of incidents should be in place before using the tool.

3) Swimlane Flowchart: This tool was first used in the tabletop exercise and then in case three regarding the DDoS incident. When using swimlanes, we wanted to investigate the flow of actions and get a visual representation of the incident. The goal was to obtain a better understanding of the incident details and detect connections between elements, which otherwise would not be easy to spot. The tool resulted in a graphical representation of the links and relationships between events and summarizes the events and their occurrence. We found this tool useful for visualizing the problem flow, involved stakeholders and actions taken. Flowcharts have a low cost to produce and a high utility.

4) Problem cause Brainstorming: This tool was applied in all cases with the aim to generate a list of probable causes and unify the project members views as a foundation for the next steps. Further, we also wanted the brainstorming process to help us identify possible consequences from the problems brainstormed. The tool worked well in categorizing the issues as well as bringing forth information about how some problems may relate to others. The brainstorming together with the problem understanding sets the scope for the remainder of the RCA and is therefore crucial step in the process.

5) Interview: Interviews were used in the case 1 and 2, and we experienced it as a good way to obtain contact with stakeholders, establish a network, and collect useful data for the RCA process. The interviews had to be planned with due care and tailored for the interview subject. With case one from the R&D organization we experienced that doing interviews revealed the attitude on card lending between the employees. Additionally, interviewing the primary stakeholder in case 3 provided invaluable information and insight into the problem space. Interviews were very time consuming, but did also provide the most reward through insight into the problem.

6) Check Sheet: By using Check Sheet in case three we wanted to achieve a ranking on either a prioritization or ranking of problems that has occurred. We also wanted to gain experience on the usage of the tool and evaluate how the tool worked in the given situation. It was not possible to obtain the frequencies of the events, which we then had to solve by asking questions concerning the problems that we had listed. The check sheet also partly relies on incident or problem frequencies as some tools rely on them to work as intended.

The check sheet tool did not provide the information needed to continue the case study and had to be exchanged with interviews.

7) Incident data analysis: This tool was not applied in the case studies but is discussed under future work.

8) Affinity Diagram: In case one, the goal of the Affinity Diagram was to categorize the suggested solutions to the problem, and then research which category the interview objects was the most interested in. We addressed this task by using a number on each proposed solution and summarized the numbers in the top of each column.

The affinity diagram worked well in our case studies to categorize and sort the identified elements. For each case study, we identified multiple elements rendering a high problem complexity. The affinity diagram aided in categorizing these elements and reducing them to a manageable problem. In case three our goal using Affinity Diagram was to discover hidden relationships in the data. However, no hidden relationships were found.

We experienced that the tool was useful for categorizing elements and reducing complexity. But it did not reveal or correlate any hidden relationships between the causes of the problem. For overview purposes, the tool has high utility and low cost. However, the utility is more uncertain when it comes to revealing hidden relationships.

9) Relationship Diagram: We applied the Relationship Diagram in case two where we aimed to see relationships between elements in the diagram and how they affect each other. We did not find any previously undiscovered relationships, and the tool did not have utility for advancing the RCA. However, the tool might be helpful in communication settings and is has a low cost time-wise to implement.

10) Fishbone Diagram: Fishbone Diagram was used on solving case one in the root cause identification stage. The diagram displays the causes leading up to the card lending problem for then to use this information to uncover the root causes. We experienced that it was difficult to generate the categories and the elements in the diagram. However, as Fig. 5 shows, this is one of the highest utility tools in the RCA toolbox. It visualizes the problem space and the contributing causes in a comprehensive way, which also aids in stakeholder communication. The time spent using the tool and making the diagram was worth the time, and the cost will diminish with more practice.

11) Five Whys: The RCA tool Five Whys was used in case two in the root cause identification phase. The tool itself has a low cost. However, the completeness of the process is questionable as there might be more causes than five. It would have been preferable that the tool opens up for more possibilities. A modification could be to run it in more than one iteration to see if more possible causes to the problem could be generated. The tool is easy to understand and to implement, with a time-wise low cost.

12) Systematic Inventive Thinking (SIT): SIT is designed to find the problem-causes where solutions could be applied to eliminate the occurrence of the problems overall. We experienced that the tool worked well for its purpose, but the cost was high to complete the process, and it was time-consuming to deal with all the small components as well as it was error-prone. We expect the amount of work needed to apply this tool will vary depending on the task size. Designate enough time to this tool and try to have as much overview of the problem and its environment before embarking on it. In case three, the SIT helped us discover components we earlier did not notice, so, it has the tool has utility.

With smaller problems SIT can be useful, however, the amount the work grows proportionally with the size of the problem. The utility of running this tool is high as it provides insight into the problem and strategies to eliminate it.

13) Countermeasure Matrix: Countermeasure Matrix was used in case two to determine which countermeasures would best solve the problem. The tool takes into account risks and

costs associated with applying the solutions. We found that one of the tool's limitations was that it was not able to take into consideration the consequence a countermeasure could present. Meaning that implementing a control can solve the problem, but also likely introduces a new risk or problem into the system. The countermeasures matrix is a useful tool for sorting problem treatments and ranking them according to estimated efficiency and feasibility. However, the tool could also benefit from estimating treatment cost.

14)Tree Diagram: In case one, the Tree Diagram was used to present a structured plan for implementation of solutions found while using SIT to the card lending problem. The tool was able to display the order of the steps to be taken as well as what category the action belongs. While applying this tool, key personnel should be actively partaking in the process. In case two, the goal with the tool was to generate a structure of the solution implementation tasks and to visualize the links between these tasks and their respective activity. Tasks are represented by leaves and activities are represented by the root and the branches. Since all the cases were limited to proposing solutions and not implementations, we do no estimate the utility of the tool.

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.

An important limitation for this study was that we limited the tool selection to the method proposed by Andersen and Fagerhaug [2]. We did this to limit the complexity of the process and tool selection. Future studies may wish to include tools from other RCA methodologies and frameworks. We found interviews have the highest value in the data collection process. Similarly, questionnaires were not included in our cases, but they have the potential for reaching a broader audience and can also contribute to the RCA process.

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 [12]. 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.

D. A proposal for RCA of InfoSec incidents

Andersen and Fagerhaug [2] proposes the use of incident data analysis for use in RCA. An InfoSec incident is in short a violation of the integrity, availability, or confidentiality of information assets or resources that fall under the security constituency. If logged properly, incident data documents a security incident from its detection until it is solved, including measures taken by the incident handler to solve it. Thus, incident data is a reliable and important source both for RCA and risk analysis. However, we have conducted preliminary research into utilizing RCA for InfoSec incident data and encountered several challenges that must be solved for the data to readily lend itself to RCA:

1) *No two incidents are the same.* Both incident frequencies and risk quantification requires incidents to be counted. So, to determine whether an incident is re-occurring or not, we need to be able to quantify incidents. However, in our preliminary work we found that no two incidents are identical. For example, we might be facing two incidents that are caused by compromised accounts, but the incidents do not involve the same account, and the initial compromise and malicious actions are likely different. The root-cause might be vulnerable account security, but we need a framework to classify and quantify to determine the frequencies of re-occurring incidents. There are already taxonomies of computer security incidents [23], [24] that provide a nice starting point, but as the threat landscape changes an update to these are needed and a higher granularity is also desirable for incident analysis.
2) *A security incident has at least one cause and one malicious action.* Trying to analyze a security incident one quickly reaches the conclusion that there are at least two parts of the incident that must be quantified. There is both an observable cause and an observable outcome of an incident, where the latter is often what is detected and triggers the incident. An example of a typical incident:
   "Incident topic: Compromised user
   User XX is sending spam email internally to employees. The email contains a suspicious link to a foreign IP address."
   In this case, the cause of the incident would classify as a compromised user account, while the observable outcome and malicious action is sending spam email. Typically, the paper trail of an incident consists of the original incident report or trigger, which varies quite a lot depending on how the incident was detected. Further, the incident handler logs each step he takes to solve the incident and all correspondence with affected parties. In short, all correspondence, analysis, follow ups, and treatments are present in the logs. Both the cause and the outcome of the incidents should be observable from the incident data, so, a

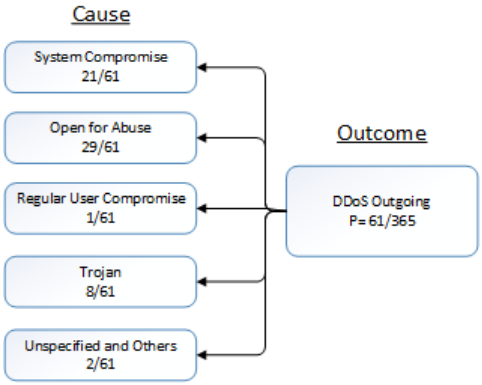

Fig. 13: Distributions of causes for DDoS Outgoing

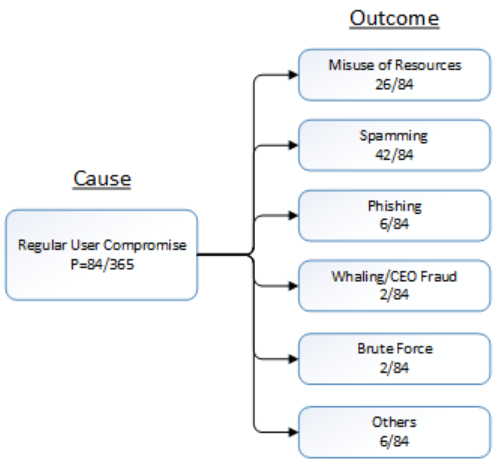

Fig. 14: Distributions of User Compromise outcomes

comprehensive classification scheme should aim to classify both. However, our research into state-of-the-art frameworks suggests that no such classification scheme exists.

3) *Organization maturity.* The organization must be sufficiently mature to have a developed and repeatable process for handling and documenting incidents. A non-standard process will generate a large variety of incident logs, which will not easily lend itself to incident quantification.

In our preliminary analysis, we have tried to determine the root causes of outgoing DDoS attacks for an organization, where an attacker abuses vulnerable systems through for example amplification attacks. In Fig. 13, we have applied a preliminary incident classification framework and attempted to classify all the the causes leading to the 61 security incidents.

Further, by classifying both the cause and the outcome we can also analyze the outcomes of a particular incident cause. This approach is useful for determining attacker motivation once he has exploited a vulnerability and gotten a foot-hold inside the network. In Fig. 14, we have classified 84 incidents as ”Regular User Compromise” and mapped the malicious actions of each incident with frequency distributions.

The incident data does show great promise as an addition to the InfoSec management and resource allocation. From a management perspective, the causes can be addressed by likelihood reducing measures, while the outcomes can be addressed with consequence reducing measures. However, there are some challenges that need to be overcome in order to adapt RCA into incident analysis. We have conducted some preliminary research into the topic, but more research is needed particularly into framework development.

IX. 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 of 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.

This study found that the RCA process does lend itself to the constrictions of a tabletop exercise for training purposes. RCA did not reveal any additional root causes. The group has to manage the limitations of not having access new information for solving the case. So, RCA has utility for exercise and experimenting with the tools on different types of data, but it is unlikely to provide any additional knowledge.

Applying the RCA under the time and resource-restricted setting did generate valuable insight into the root causes of the problem. For the case study of the DDoS attack, the process revealed multiple causes that were previously undetected by the principal. Several of these causes were in the socio-technical domain, and are not likely to be found using typical InfoSec analysis approaches. Therefore, we conclude the RCA process worked well under resource and time restricted setting.

Several RCA tools proved useful for addressing til InfoSec problems, with an overarching process tailored for problem-solving. Examples of tools that worked well for our case-studies for problem understanding was performance matrices and swimlane flowcharts. For data collection, interviews had the highest utility. We found the affinity diagram to have the highest cost-benefit in the problem cause data analysis phase. One of the best tools in the RCA process for visualizing several existing causes in the problem and communicating was the fishbone diagram. Although SIT has some drawbacks regarding problem scaling, it worked well to provide solutions to identified root causes.

The main drawback of RCA was that our cost-benefit analysis of the time and resources invested in case one is on the borderline of being justifiable, and the cost of the problem should be considered before launching a RCA. However, RCA performed well under time and resource constraints for a less

complex problem. Thus, the full-scale RCA is a viable option when dealing with both complex and costly InfoSec problems. For minor issues, a RCA may be excessive or should at least be strictly time managed. Based on our findings we conclude that RCA should be a part of the InfoSec management toolbox.

ACKNOWLEDGEMENTS

The authors acknowledge the help and support from Erlend Brækken, 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] G. Wangen, N. Hellesen, H. M. N. Torres, and E. L. Brækken, "An empirical study of root-cause analysis in information security management," in *SECURWARE*, vol. 2017. IARIA, 2017, pp. 26–33.

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

[3] M. F. Peerally, S. Carr, J. Waring, and M. Dixon-Woods, "The problem with root cause analysis," *BMJ Qual Saf*, vol. 26, no. 5, pp. 417–422, 2017.

[4] H. M. N. Torres, N. Hellesen, and E. L. Brækken, "Bruk av rotårsaksanalyse i informasjonssikkerhet," B.S. thesis, NTNU in Gjøvik, 2016.

[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] 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

[13] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, 2014.

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

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

[16] 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.

[17] 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.

[18] 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.

[19] F. den Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen, "Model-based security analysis in seven steps - a guided tour to the coras method," *BT Technology Journal*, vol. 25, no. 1, pp. 101–117, 2007.

[20] Kaspersky, "Carbanak apt the great bank robbery," 2015. [Online]. Available: https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

[21] "Anunak: Apt against financial institutions," Group-Ib, Fox-It. [Online]. Available: https://www.group-ib.com/resources/threat-research/Anunak_APT_against_financial_institutions.pdf

[22] J. van der Wiel, "How did the carbanak cybergang steal $1 billion from banks? (1/3)," accessed 22-Feb-2016. [Online]. Available: https://www.youtube.com/watch?v=csc9VDuHBNU

[23] M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors," *Computers & Security*, vol. 25, no. 7, pp. 522–538, 2006.

[24] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security*, vol. 24, no. 1, pp. 31 – 43, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404804001804