Fault Tree Analysis of Accidental Insider Security Events

Pallavi Patil, Pavol Zavarsky, Dale Lindskog, Ron Ruhl
Information Systems Security, Concordia University College of Alberta
7128 Ada Boulevard, Edmonton T5B 4E4, Canada
pallavipatil@hotmail.com, {pavol.zavarsky, dale.lindskog, ron.ruhl}@concordia.ab.ca

Abstract— **Insider threats have been categorized as unintentional and malicious. The frameworks and models which are used to detect malicious behavior of employees would likely fail to detect unintentional insider as there is no malicious intent. This paper accentuates the limitation of MERIT (Management and Education of Risks of Insider Threat) in its scope for accidental insider threats and proposes Fault Tree Analysis (FTA) of the security events caused by accidental insiders. We perform FTA on two cases involving accidental insiders which help understand human side behind the user errors. The first case involves data loss via outbound email due to employee error while the second case involves accidental disclosure of sensitive information by insiders. The countermeasures are thus better interpreted and communicated as the causes of a threat are well understood which is essential for human fault avoidance.**

Keywords—Accidental insider event; Fault Tree Analysis (FTA); Minimal Cut Set (MCS); root event; basic event

I. INTRODUCTION

An organization's information (systems) may not always result in a compromise due to an accidental insider threat, but can still be damaging. Depending on the severity of the human error, it has a potential to cause financial uncertainty, disruption to communication, harm to organizational reputation or corporate instability. We start the paper by reviewing related literature in Section II. While studying the related literature we found that the major cause of data leakage in organizations has been due to user errors or negligence [1]. If a serious error occurs accidently, it may leave the system vulnerable to malicious insiders, anticipating any vulnerability. Apart from being a threat in itself, accidental errors can elevate the level of risk if exploited as vulnerability. To protect confidentiality, integrity and security of information systems, organizations need to understand the behavior of employees that increases the risk of accidental insider security incidents. In Section III we evaluate one such case published by CERT (Computer Emergency Response Team) in the book "The CERT Guide to Insider Threats" to understand human factors responsible for the occurrence of accidental insider incident. The evaluation was helpful to understand if the accidental errors are being exploited by malicious insiders to commit and/or hide the malicious activity. This provided an insight on the human behavior resulting in those errors.

CERT's MERIT (Management and Education of Risks of Insider Threat) project employs system dynamics modeling and simulation to convey the complexity of insider threats and produce interactive learning environment [2]. The CERT Insider Threat Center has been doing research on "Insider Threats" since 2001 [3]. However, their work is noticeably focused on intentional or malicious insider attacks. CERT has a database of more than 700 insider threat cases, but they have analyzed those cases mainly from the view of a malicious insider. We reviewed MERIT insider threat model and found that it was created with the same view and hence shows some limitations in its scope for accidental insider security threats. In Section IV we review MERIT for accidental insider threats.

Methods to analyze risk fall under either deductive (i.e. top-down) or inductive (i.e. bottom-up) approach. With the top-down approach the reasoning works from general to more specific. While, in bottom-up approach the reasoning moves from specific to general or broader observations. FTA is deductive or is based on a top-down approach. It is a graphical representation evaluating the pathways from a root event or a failure, leading to the root causes. A fault tree identifies all the possible scenarios that can make the root event occur. FTA is a widely used and accepted technique for analyzing system safety and is based on the concept: The failure of a system or sub-system can be caused by the failure of lower level system or sub-systems. Similar to the concept of FTA, failure to detect accidental errors by employees may result in an accidental insider security incident or a root event to occur. Hence, a FTA based on top-down approach would be more effective to analyze accidental errors. In Section V we perform FTA on two cases involving data loss due to accidental errors by employees. The fault tree gave us an inverted tree like structure with the root event or the failure at the top and root causes or the basic events at the bottom. The tree thus created was analyzed by evaluating Minimal Cut Sets (MCS). MCS list threat agent(s) or the basic event(s) in each set whose existence would increase the likelihood of the occurrence of the main event. The MCS decipher the failure event and provide an ease for interpreting countermeasures on the threat agents it encapsulates. In Section VI we implement a qualitative risk assessment for accidental insider threats and end the paper with a conclusion and future work in Section VII.

II. RELATED RESEARCH

Many research papers are proposing solutions on malicious insiders and some are acknowledging unintentional insiders in the definition of "insider threat" [4]. One of the research papers identified unintentional insider as "Oblivious Insider" and suggested measures to complement the existing controls for

978-0-7695-5014-5/12 $26.00 © 2012 IEEE
DOI 10.1109/CyberSecurity.2012.21

malicious insiders to overcome the threat [5]. According to the research by International Data Corporation (IDC), commissioned by RSA; accidental security incidents caused by employees are more frequent and could potentially have a greater impact on information security than malicious insider attacks [6]. Cisco performed few surveys on "Data Leakage Worldwide". The findings of one survey revealed that employee behavior is the major cause of data leakage [1]. To better understand employee behaviors that put corporate assets at risk, Cisco commissioned a second survey to examine data leakage in ten countries around the world [7]. The results start with the revelation that one out of four companies does not even have a security policy for the appropriate access and use of corporate information. The results also revealed reasons why employees knowingly ignore or bypass security policies and put personal & corporate data at risk. FTA technique is successfully used in many areas including software engineering. One research study proposed a human factors analysis by applying FTA method to seek the human factors causing software accidents [8]. In this paper FTA was applied to the event in which cancer patients were overdosed by Therac-25 radiation therapy machines. Software errors in the machine were a significant factor that caused overdose and was analyzed using fault tree. The human factors fault event tree was created and analyzed by evaluating MCS using Fussell-Vesely algorithm. The analysis technique proposed in the paper is qualitative and provides insight on the human factors that affect a failure of the system.

III. A Case Study Involving Accidental Insider Errors

The book "The CERT Guide to Insider Threats" by CERT discusses insider incidents and categorizes them into IT sabotage, theft of intellectual property (IP) and fraud [9]. Our study of this book identified cases involving exploitation of user errors to create and/or hide fraud. We reviewed and analyzed the following case:

"A supervisor in a department handling disability claims used her own account to modify claims and direct monthly disability payments to her fiancé over almost two years. The negligence to update her access rights when she changed position enabled her to modify data and also approve the changes. Both positions used the same application but different roles for entering, approving, and authorizing payments for medical and disability claims. When she was promoted, she was authorized for her new access level, but administrators neglected to rescind her prior access level. As a result, she ended up having full access to the application, with no one else required to authorize transactions (payments) from the system. She also recruited a co-worker to increase the disability rating on her fiancé's claim, which increased the amount of the monthly checks. The co-worker detected the incident when she recognized the insider's fiancé's name and reported that he was not disabled [9]". We analyzed this case on three distinct factors:

- Negligence by the administrators;
- Understanding the relation between employee reliability and security; and
- Cascade of errors.

In this case, the negligence or lapse by administrators to update access rights proved to be a vulnerability which was exploited by the malicious insider to commit fraud. It also highlights the importance of drawing a fine line between employee reliability and security. Did the vulnerability inspired employee to create fraud, who was otherwise reliable? Or is it a case of malicious insider anticipating any vulnerability to be exploited to create fraud? The result can also be viewed as a cascade of errors such that; the lack of information security policy itself or the absence of its enforcement, led to the negligence by administrators. The negligence by administrators led to the malicious insider having excessive access controls which finally resulted in fraud. The lessons from this brainstorming would be:

- The controls to monitor malicious behavior of an insider would fail to detect accidental insiders.
- To mitigate the vulnerability in a system, produced by the user errors; it would be necessary to perform root cause analysis to understand the cause-event relationship resulting from the human errors.

There is a constant uncertainty and variability surrounding user errors. The risk from unintentional errors is difficult to mitigate completely as it includes a fundamental aspect of security, i.e., People. Organizations need to review their security risk assessment models or methodologies to incorporate risks from accidental insiders. The publication "Guide for Conducting Risk Assessments" by the National Institute of Standards and Technology (NIST), states that the end result of the risk assessment is a determination of risk, i.e., the degree and likelihood of harm occurring [10]. Hence, risk assessment should be an integral part in the mitigation of an accidental insider threat.

IV. Review of the MERIT Model for Accidental Insider Threats

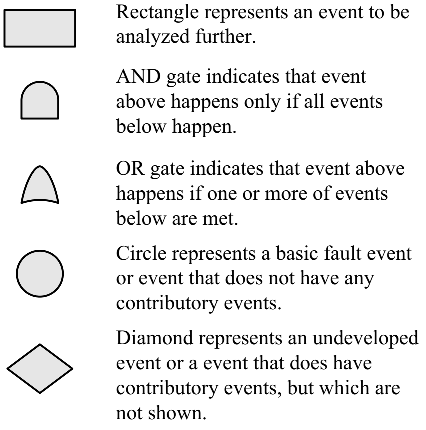
The MERIT model on insider threats, developed by CERT was based on the cases from Insider Threat Study (ITS). Our examination of the MERIT model shows that it primarily assumes "Insider" as malicious. It does not consider the accidental or negligent aspect of an "Insider". Moreover model's behavioral aspects, technical attack aspects and defense aspects are derived on this primary assumption and hence are limited to the malicious view of an insider. The MERIT model focuses on administrative and technical controls to mitigate risk of insider threat [2]. It does not incorporate operational controls which would be significant to mitigate insider risk. The model's assumption of organizational defenses for technical controls to detect malicious activity would likely work for accidental errors too. But, some of the assumptions for administrative controls that were meant to positively affect human behavior of a malicious insider would be ineffective on unintentional insiders. The Table I below shows the ineffectiveness of some administrative controls of the MERIT [2] on accidental insiders.

TABLE I. INEFFECTIVENESS OF CONTROLS ON ACCIDENTAL INSIDERS

Policy lever	Description	Ineffectiveness on unintentional insiders
Employee intervention	Positive interventions like employee assistance or counseling that attempt to lower disgruntlement directly, to reduce inappropriate behavioral or technical actions by insider.	If there is no inappropriate behavior or disgruntlement then there would be no employee intervention.
Sanctioning	Punitive measures that attempt to motivate the insider to reduce his inappropriate behavioral or technical actions to avoid additional sanctioning.	If sanctioning is imposed on unintentional insiders, it may lower employee morale and result in reduced productivity.
Training	Currently limited to education of employees on appropriate usage of computer and network systems and the consequences if misused.	Would be effective only to a certain extent if not trained from the aspect of unintentional errors or social engineering, for e.g. An employee may have a misperception that his/her actions are correct, but in reality they might be unintentional errors.

V. FAULT TREE ANALYSIS METHOD

Fault Tree Analysis technique was developed by H.R. Watson of Bell Telephone Laboratories in 1962 and was further developed and refined by Boeing Company [11] to analyze system reliability. A fault tree starts with a top or root event(s) that is the end result of a failure and represents the problem to be solved for which predicted reliability and availability data is required. This technique determines the probability of the system failure qualitatively or quantitatively. For this paper, we propose qualitative analysis to help improve the process by identifying the root causes for the top event and suggesting countermeasures to mitigate them. The advantage of using FTA for accidental insider security incident is that it displays all potential event combinations for the root event in a structured, graphic way. This structure would break down to basic events or root causes and would make it easy to interpret or communicate the countermeasures.


Rectangle represents an event to be analyzed further.

AND gate indicates that event above happens only if all events below happen.

OR gate indicates that event above happens if one or more of events below are met.

Circle represents a basic fault event or event that does not have any contributory events.

Diamond represents an undeveloped event or a event that does have contributory events, but which are not shown.

Figure 1. Basic fault tree symbols

The basic events at the bottom of the fault tree are connected to the root event at the top, as shown in Figure 2; using logic symbols called gates as shown in Figure 1. In Figure 2 the secondary events are indicated by C and the basic events are indicated with B. The root event shown in the figure has a logic relationship with the secondary events C1 & C2, such that the occurrence of either of the event will cause the root event to occur.

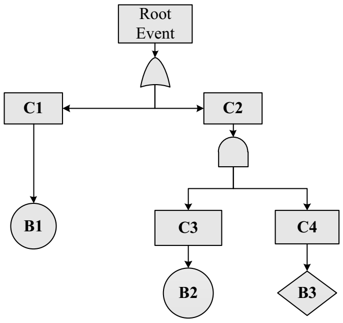


Figure 2. An example of a fault tree analysis

Applying the rules of Boolean algebra, we can evaluate the MCS for the fault tree in Figure 2. The root event is expressed as C1⋃C2. Similarly, events C3 and C4 are required to occur for the event C2 to occur. So the logic relationship between C2 and C3 & C4 can be expressed as C2= C3⋂C4 [2]. Thus, the root event will be expressed as C1⋃C2= B1⋃ (B2⋂B3). Once the tree is created, it is analyzed using minimal cut sets. A cut set is a set of events that together cause the root event to occur. The MCS is a cut set with the minimum number of events that can still cause the root event to occur. In Figure 2 a cut set is {B1, B2, B3} and MCS are {B1} and {B2, B3}.

Next, we perform the FTA on two cases involving accidental insider events. The first case involves data loss via outbound email while the second case involves accidental disclosure of sensitive information by insiders.

A. *FTA of an Accidental Data Leakage via Outbound Email*

Data leakage from the outbound emails has been a concern for information security across all sectors of the economy. Although the leakage is more often accidental than intentional, the repercussions could be severe for any organization. On September 3, 2009 Scarborough and Associates released a notification regarding a possible private information security breach. The situation was concerned with one of their client, who was a resident of Maryland. The notification quotes:

"On September 1, 2009 one of our employees accidentally sent private information attached to an email to an incorrect email address including name, phone numbers, and related insurance policy numbers, date of birth and Social

Security number. It did not include a specific address. On September 2, 2009 we recognized the error and contacted the email provider to ascertain whether or not the account was active at the time email was sent. Our firm received emails bouncing back on September 2, 2009 that the account was disabled but the original email in question did not bounce back. We are requesting from the email provider they let us know if account was active from August 31, 2009 to date [12]". To create fault tree we formally analyze errors made by the employee. From the data available it is clear that employee accidently sent email to an incorrect email address. This means that the employee failed to verify recipient of the email due to lack of due diligence. The incidence also shows lack of policy and procedures which would control the content in the files attached with the outbound emails. Insufficient technical controls such as email encryption or attachment password protection or software to monitor outbound emails could also be the reason of the data leakage. We created a fault tree as shown in Figure 3 where:

Root Event: Accidental data leakage from the outbound email

C1: Incorrect entry of the email recipient
B1: Failure to verify email recipient
B2: Lack of policy & procedures to monitor outbound emails
B3: Lack of technical controls to monitor outbound emails
B4: Lack of due diligence

Evaluation of MCS for the fault tree below is as follows:

Root Event = C1= B1 ∩ (B2 ∪ B3)
Since B1=B4, Root Event = B4 ∩ (B2 ∪ B3)
= (B4 ∩ B2) ∪ (B4 ∩ B3)
MCS = {B2, B4}, {B3, B4}

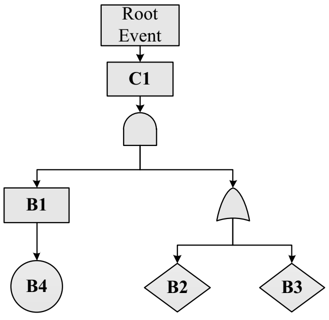


Figure 3. An example of a fault tree analysis of an accidental data leakage via outbound email

MCS implies that if the basic event(s) enclosed in either of the cut sets occur, then the root event will likely occur. For example, consider the MCS {B2, B4}; if an organization lacks policy and procedures to control the content in the files attached with the outbound emails and an employee shows lack of due diligence, then it is likely that the data would leak accidently from an outbound email. Therefore, as a countermeasure it would be essential for an organization to have an appropriate policy to control the sensitive information sent in the emails and increase awareness & understanding of policy amongst employees to avoid occurrence of the root event. Thus performing FTA on the root event gives an ease of interpretation and communication of corrective measures behind the user errors, which otherwise would be ambiguous.

B. FTA of an Accidental Disclosure of Sensitive Information by Insiders

We reviewed the following case published by 'The Department of Veterans Affairs (VA)' to analyze the resulting accidental data leakage using fault tree. The Department of Veterans Affairs announced:

"It accidentally handed over the data of living veterans when complying with a Freedom of Information request from Ancestry.com. The request was for data from a database of deceased veterans; however the data of 2,257 living veterans had also been identified in the database, and that the number could potentially grow to more than 4,000. The data included names, Social Security numbers, dates of birth and military assignments [13]". VA announced the mistake on January 20, 2012 and officials began contacting affected veterans on January 18, 2012 as they identified which veterans are living. A Fault Tree is created for the data leakage event to provide scientific approach for predicting human behavior that caused the event to occur and determine the countermeasures for the root causes behind it. Since there is no data available on the investigation of this event, we will make a hypothetical analysis about the causes that made the event to occur. As the data was accidentally handed over, there could be two potential causes:

- Employee negligence, and
- Mistaken action.

Analyzing the cause of negligence, we found that it can be the result of excessive privilege and lack of due diligence. Similarly, lack of concentration, misperception, mistaken priorities or miscommunication can result in employee taking a wrong action. We analyzed what could be the cause for an employee having excessive privilege or access control rights and found that it could be due to non-compliance of current access control procedures or failure to maintain minimum privileges. The cause of non-compliance of access control could be either due to absence of an information security policy or non-compliance of the existing policy. Lack of awareness or understanding of the policy, disregard for the policy or trying to work around the policy can result in the non-compliance of the policy. Failure to maintain minimum privilege could be either due to ineffective implementation of audit findings or lack of segregation of duties. Poor (information) management could result in ineffective implementation of audit findings. Finally, lack of segregation of duties can be caused due to insufficient business knowledge of security administrators or permission creep. The fault tree is shown in the Figure 4 where:

Root Event: Accidental data leakage
C1: Employee negligence
C2: Mistaken/Incorrect action
C3: Excessive privilege or access control rights
C4: Lack of due diligence
C5: Non-compliance with access control procedures
C6: Failure to maintain minimum privileges

C7: Non-compliance of the information security policy
C8: Ineffective implementation of audit findings
C9: Lack of segregation of duties
B1: Lack of concentration
B2: Misperception
B3: Mistaken priorities
B4: Miscommunication
B5: Absence/Inadequate quality control procedures/ supervision

B6: Absence of information security policy
B7: Poor (information) management
B8: Lack of awareness or understanding of information security policy
B9: Disregard for the information security policy
B10: Working around the information security policy
B11: Insufficient business knowledge of security administrators
B12: Permission creep

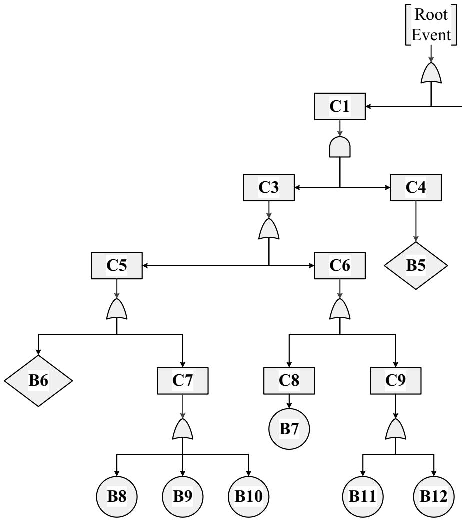


Figure 4. An example of a fault tree analysis of an accidental data leakage by the Department of Veterans Affairs

Evaluation of MCS is as follows:

$\text{Root Event} = C1 \cup C2$
$C1 = C3 \cap C4$
$C2 = B1 \cup B2 \cup B3 \cup B4$
$C3 = C5 \cup C6$
$C4 = B5$
$C5 = B6 \cup C7$
$C6 = C8 \cup C9$
$C7 = B8 \cup B9 \cup B10$
$C8 = B7$
$C9 = B11 \cup B12$

Substituting the values we get:

$$\text{Root Event} = (B6 \cap B5) \cup (B7 \cap B5) \cup (B8 \cap B5) \cup (B9 \cap B5) \cup (B10 \cap B5) \cup (B11 \cap B5) \cup (B12 \cap B5) \cup (B1 \cup B2 \cup B3 \cup B4)$$

$$MCS = \{B5, B6\}, \{B5, B7\}, \{B5, B8\}, \{B5, B9\}, \{B5, B10\}, \{B5, B11\}, \{B5, B12\}, \{B1, B2, B3, B4\}$$

MCS represents unique combinations of basic events to understand the structural vulnerabilities in a system. Consider the MCS {B5, B8}; if an organization has an inadequate quality control procedures and employees lack awareness or understanding of the information security policy, then it is likely that the data would leak accidently. Therefore, as a countermeasure it would be essential for an organization to have sufficient quality control procedures and increase awareness & understanding of policy amongst employees to avoid occurrence of the root event. For a very large fault tree it may be difficult to evaluate a complete list of MCS. In such case, it would be reasonable to evaluate only those MCS that significantly contribute to system failure [14].

VI. Qualitative Risk Assessment

Measures against accidental insider threats should be proactive as compared to reactive. FTA can be a means of identifying, capturing, assessing and managing implications of unintentional threats. Technical and administrative controls meant for malicious insiders may prove to be reactive rather than proactive for accidental insiders. Information derived from the past incidents can be used to recognize existing vulnerabilities in current environment. The analogies can be used to create a fault tree to predict known or unknown human threats resulting in an accidental insider incident. The structured cause-event relationship developed by a tree explores paths in which the causes and events may interact. This exploration predicts the behavior of risk agents through logical relationships in the tree. MCS forms a principal part and structurally important to FTA. As the name suggests it contains only minimal failures necessary for the incident to occur. A fault tree can be evaluated qualitatively on the basis of MCS. The criticality of a cut set is inversely proportional to the number of basic events in the set. For example, if a cut set is long it is less vulnerable and vice versa. Likewise, a set containing one event indicates single point of failure (SPOF) and is of high vulnerability [15]. An organization can be secured only to a level where the risk is acceptable, creating a balance between security and productivity. National Institute of Standards and Technology (NIST) SP 800-30 defines risk as "a function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" [16]. In other words, where a threat intersects with vulnerability, risk is present [17]. If we consider basic events as threat agents and MCS as vulnerability then existence of MCS in an environment, indicates the presence of risk.

Human Fault Tolerance and Single Point of Failure (SPOF)

A SPOF represents high risk elements which can compromise the entire system if not planned for redundancy. To survive component failures the system should be designed for fault tolerance. But if the component failure is due to user errors, the system needs to be designed for human fault tolerance. In systems designed for human fault tolerance a single type of control such as technical or administrative can be a SPOF. To avoid SPOF and incorporate redundancy a layered approach would be more effective towards human fault tolerance. Human errors are not only difficult to recover but also difficult to detect. To design a system for human fault tolerance, the recovery time from an error must be short. Hence error detection becomes primarily important to confine the effects of damage. In a fault tree analyzing accidental insider event, a MCS is a set of basic human errors leading to a system failure. If all the basic errors in a set occur at the same time, a MCS fails and there is high probability of the occurrence of the root event. MCS encapsulating single basic error indicates a SPOF. This implies that for a system to be redundant MCS enclosing single error should be dealt with a layered defense controls including technical, administrative and operational. The layered defense approach would be more effective against SPOF and ensure human fault tolerance in the system.

VII. Conclusion and Future Work

Accidental insider security incidents are difficult to detect and mitigate as it involves human errors. The frameworks and models which are used to detect malicious behavior of employees would likely fail to detect unintentional insider as there is no malicious intent. The best solution would be to understand human behavior behind the errors. By performing FTA, we can analyze all the possible scenarios causing security incidents caused by human errors. Also, evaluation of the root event for causes that leads to basic events maps different behavior patterns as every individual is different. The solution that exists to detect malicious insider activity cannot be replaced but requires separate or a complimentary mitigation strategy for unintentional insiders. FTA performed on accident insider security incidents considerably explores human factors to help understand and interpret effective countermeasures. This research would convey organizations and researchers that accidental insider threats also demand equal attention as the malicious threats because the consequences of a human error can be severe.

The publication "Security and Privacy Controls for Federal Information Systems and Organizations" by National Institute of Standards and Technology (NIST), provides guidelines for selecting and specifying security controls for organization and information systems [18]. The document contains the security control baselines that represent the starting point in determining the security controls for low-impact, moderate-impact and high-impact information systems. As a future work, the fault trees created to analyze accidental insider security events can be standardized using the set of controls provided by the NIST.

References

[1] Cisco, "Data leakage worldwide: Common risks and mistakes employees make", 2008. Available: http://www.cisco.com/en/US/solutions/collateral/ ns170/ns896/ns895/white_paper_c11-499060.pdf

[2] D. Capelli et al., "Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage", 2007. Available: http://www.cert.org/insider_threat/modeling.html

[3] The CERT Insider Threat Center: http://www.cert.org/insider_threat/

[4] M. Alawneh, I. Abbadi, "Defining and Analyzing Insiders and their Threats in Organizations", 2011.

[5] S. Colson, "Insider Threats 2.0: The Oblivious Insider, A Case Study", 2009. Available: http://shaycolson.com/wp-content/uploads/2009/04/case-study-1-insider-threats.pdf

[6] B. Burke, C. Christiansen, "Insider Risk Management: A Framework Approach to Internal Security", 2009. Available: http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf

[7] Cisco, "Data leakage worldwide: The effectiveness of security policies", 2008. Available: http://www.cisco.com/en/US/solutions/collateral/ns170 /ns896/ns895/white_paper_c11-503131.pdf

[8] Y. Zheng, R. Xu, "A Human Factors Fault Tree Analysis Method for Software Engineering", 2008.

[9] D. Capelli, A. Moore, R. Trzeciak, "The CERT Guide to Insider Threats", 2012.

[10] NIST, "NIST SP 800-30 Rev.1 Guide for Conducting Risk Assessments", 2011. Available: http://csrc.nist.gov/publications/drafts/800-30-rev1/sp800-30-Rev1-ipd.pdf

[11] Fault Tree Analysis (FTA). Available: http://www.hcrq.com/fta.html

[12] Scarborough & Associates Security Breach Notification, 2009. Available: http://www.oag.state.md.us/idtheft/Breach%20Notices/ITU 181679.pdf

[13] N.B. Johnson, "A Veterans Affairs Department data breach" 2012. Available:http://www.federaltimes.com/article/20120125/departments04/201250304/

[14] J. Andrews, "Tutorial Fault Tree Analysis", 1998. Available: http://www.fault-tree.net/papers/andrews-fta-tutor.pdf

[15] P. Clemens, "Fault Tree Analysis", 1993. Available: http://www.fault-tree.net/papers/clemens-fta-tutorial.pdf

[16] G. Stonebumer, A. Goguen, A. Feringa, "Risk Management Guide for Information Technology Systems" Recommendations of the National Institute of Standards and Technology, 2002. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[17] P. Bowen, J. Hash, M. Wilson, "Information Security Handbook: A Guide for Manager" Recommendations of the National Institute of Standards and Technology, 2006. Available: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[18] NIST," NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations" National Institute of Standards and Technology, 2012. Available: http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf