ISSN: 2473-3857
v3 n4307

The Need to Teach Root Cause Analysis in an Information Security course

Garry L. White
gw06@txstate.edu

Jaymeen Shah
js62@txstate.edu

Department of Computer Information Systems & Quantities Methods
Texas State University
San Marcos, TX 78666 USA

Abstract

Even with laws and technology, corporations still have computer/information security incidents. Not only do corporations need to protect, but also be able to detect and respond to security incidents. But, what happens after that? It is essential to understand the cause to take corrective actions. This is where Root Cause Analysis (RCA) comes in. It is used in many fields. However, it is not taught in higher education information/computer security classes. There is very little literature on applying RCA when there is an information/computer security incident. The purpose of this paper is to show the need to teach RCA in an information security course and to lay the foundation for further research to assess student benefits. The paper discusses the benefits of RCA and how it could avoid future mistakes. In other words, learn from analyzing mistakes.

Keywords: Security, Root Cause Analysis, Education, Training

1. INTRODUCTION: SITUATION/PROBLEM

Information security has been changing over the past decades. In addition, information security has received increased attention, due to the increase in cybercrimes and vulnerabilities during the past decades (Gerber and von Solms, 2008; Rasmussen, 2003). Even with the passage of the HIPPA law, over 1,950 HIPPA breaches affecting 500 or more people occurred between 2009 and 2017. (USDHHS, 2017). "On Friday, May 12, 2017, a global ransomware campaign began targeting computers around the world with a ransomware variant called WannaCrypt malware (alternatively known as WCry, WannaCry or WanaCrypt0r), hitting dozens of organizations across the globe. Among the victims are universities in China, Russia's Ministry of Internal Affairs, National Health Service in the UK, and enterprises including Federal Express, the Spanish telecommunication company Telefonica, French car manufacturer" (Radware, May 15, 2017). Today, there is no perimeter to protect, and it is difficult to know where the hacker is (White, 2010). What makes things worst is that the development of security technology moves slower than criminals (Luo & Liao, 2007). Hence, even with laws and technology to protect us, we still are hacked.

We will be hit no matter how well educated the user is and protected (White, 2012; White, 2015). What is needed is to detect and respond to attacks and breaches (White & Hewitt, 2017). The next step in this sequence of security actions is to learn from mistakes, which could avoid future occurrence of similar security incidents. New corrective measures must be developed from such mistakes. This is where Root Cause Analysis (RCA) comes in. "RCA is a structured investigation of the problem to identify which underlying causes need to be fixed" (Lehtinen,

Mäntylä, & Vanhanen, 2011). Focus is not on symptoms, which at times is taken as causes. RCA is used in other fields (manufacturing, software development, industrial) for identify root causes and undertaking performance analysis. Examples of areas using RCA are: healthcare (Bowie et.al, 2013), occupational safety and health (OSH) (Black & Vernetti, 2015), electronics manufacturing (Huertas-Quintero et. al, 2011), and industrial systems in order to plan maintenance strategies (Sharma & Sharma, 2010).

There was no literature showing corporations using RCA in the aftermath of computer/information breaches to identify the root cause(s). This does not necessarily mean corporations do not use RCA for computer/information breaches. Making public RCA findings can aid the hacker. Hence, a reluctance by corporations to publicize their RCA findings is the likely reason.

What is Root Cause Analysis (RCA)?

RCA is a problem solving method to find the main cause(s) of a problem. The focus of RCA is on the cause of the problem, not the symptoms. Often computer professionals confuse symptoms with the causes (Nailen, 2015; Spencer, 2015). By eliminating the cause, you eliminate the problem. Hence, the need for RCA. For example, the symptom is getting large volumes of spam e-mails. The focus is on "what" is happening. To deal with what is happening, delete the spam e-mails. Now, "why" is it happening? The cause is a poor e-mail spam filter on the e-mail server. By fixing the poor e-mail spam filter, you eliminate spam e-mails; no more deleting spam e-mails.

The three types of causes defined by MindTools (2017) can be found within security breaches and incidents. They are:

1. Physical – hardware/software failure.
2. Human – computer users either deliberately do harm or make an honest mistake.
3. Organizational – errors in a process, system, or policy.

Purpose of Security Incident and Root Cause Analysis

The purpose of security incident analysis is to identify what actually happened and to determine who within the organization is responsible for taking necessary actions to ensure the incident does not reoccur (Black and Vernetti, 2015). This requires analysis of security incident from different perspectives before moving on to identifying the factors that may have contributed to the security incident. The key to preventing future reoccurrence of a security incident is to identify the primary causes of the security incident (Lehtinen et al., 2011). The intent of RCA is to dig deeper into the security incident to pinpoint the main cause(s), which necessitates tracing back from the point of security incident across the interconnected IT systems to discover where the problem started and how it led to causing the incident (MindTools Editorial Team, 2017). Thus, RCA requires deeper analysis by asking 'Why' and 'Why not' several times to find the main cause(s) of the incident. This process ensures looking into all possible cause(s) of the security incident instead of simply focusing on the most obvious ones.

Identifying root causes of a security incident and fixing these issues protects the organization against similar security incidents in the future. RCA requires a thorough analysis of the IT systems and processes, which enables the organization to develop and implement solutions to address the security incident. Before implementation of the proposed solution, RCA process also involves exploring the impact of the solution on the capability of the IT systems. This additional step ensures the solution deployed to fix the root cause(s) of the security incident does not negatively affect organizational IT systems and processes.

Thus, the main purpose of performing RCA for a security incident is to identify what happened, why it happened (i.e., discovering hidden defects in the organizational IT systems and processes), and to determine what needs to be done to fix the root cause(s) of the security incident. This enables an organization to develop and implement effective solution to fix issues in the IT systems, policies and procedures that caused the security incident. Protecting organizations against future security incidents is critical to maintain positive image of the company and prevent significant liability due to the security breach.

2. NEEDS

Corporate Needs

To make adjustments to improve security and prevent security incidents from happening again, what corporations want is to understand why a breach or incident occurred. The ultimate goal is to have fewer security incidents. These needs vary with management levels as explained below.

RCA and Management Levels Needs

"Strategic management answers the question 'why do security enterprise problems exist?' This question of security leads to developing security policies that deal with people issues, and evaluates internal/external risks" (White, 2009). Often security breaches are a result of poor policies, not the technology used (White, 2013). Hence, strategic management must address the why's of the security incidents. RCA provides this information, which leads to better security policies.

RCA leads to corrective actions needed by top management to change programs, policies and procedures.

"Tactical management answers the question 'how are security problems mitigated?' It involves how the security systems are developed and implemented to satisfy policies" (White, 2009). RCA provides this information, which leads to better security implementation.

"Operational management answers the question 'what security procedures and practices are to be utilized?' Use of analysis tools, auditing tools, physical controls, scanners, and packet sniffers are utilized (White, 2009). RCA provides this information, which leads to better security operations (Chadha, 2016).

Need for RCA Training and Education

Bowie, et al. (2013) concluded to a potential organizational learning need to provide RCA-trained staff with continuous development opportunities and performance feedback. Unfortunately, RCA is not taught in information security classes. Of the ten security textbooks for higher education that were reviewed, none contained RCA exercises (See Appendix A).

What are corporations looking for in an employee? Corporations need employees who are team players, problem solvers, and knowledgeable in dealing with corporate data and information security breaches and incidents. Experience with working world projects is important for corporations. Using RCA exercises in a security course can prepare a student as an employee corporations desire. Such RCA exercises can introduce Risk Management content to undergraduate and graduate students.

3. RCA COURSE CONTENT

The best method to incorporate RCA in a security course is via a team project to do a RCA for an incident that is publicly well documented, such as the Target Breach in 2013. The students can follow the RCA method by MindTools at www.mindtools.com/pages/article/newTMC_80.htm. This site offers a RCA template that students can use with their project (see Appendix B). Instead of a report, a presentation can be required. *Different cases can be assigned for variety, if the instructor wishes for the students to present their project to the class.* This furthers student presentation skills and ability to communicate with management.

RCA Process

MindTools (2017) has five steps for a RCA process.

Step #1: Define the Problem.
This Step has two questions; 1) "What" is happening. 2) "What" are the symptoms?

Step #2: Collect Data.
This Step has three questions; 1) "What" proof do you have that the problem exists? 2) "How" long has the problem existed? 3) "What" is the impact of the problem? This Step also involves meetings with people who are familiar and understand the situation. The situation needs to be viewed from different perspectives of those involved.

Step #3: Identify Possible Causal Factors.
Three specific questions for this Step are: 1) "What" sequence of events leads to the problem? 2) "What" conditions allow the problem to occur? 3) "What" other problems surround the occurrence of the central problem? This Step also involves identifying causal factors. Four methods to use are:
1) ask "so what?" of all the facts. This determines possible consequences of a fact.
2) ask "why?" five times to get to the root of the problem. This moves from symptoms to causes (Chadha, 2016).
3) "drill down," break down a problem into small and detailed parts.
4) there is "cause and effect diagrams." It is a chart showing where the trouble possibly began, leading to possible causal factors.

Step #4: Identify the Root Cause(s).
This Step has two questions: 1) "Why" does the causal factor exist? 2) "What" is the real reason for the problem? The same methods used in Step #3 are used. However, the stress is on the "why" question. Cause and effect are further analyzed.

ISSN: 2473-3857
v3 n4307

Step #3 and Step #4 addresses Strategic management question 'why do security enterprise problems exist?'

Step #5: Recommend and Implement Solutions.
This Step has four questions: 1) What can be done to prevent the problem from happening again? 2) How will the solution be implemented? 3) Who will be responsible for it? 4) What are the risks of implementing the solutions? This is when you analyze cause-and-effect processes. With that, you can identify the system changes needed. These changes will then have analyses of risk and impact.

Step #5 addresses the Tactical management question 'how are security problems mitigated?' and the Operational management question 'what security procedures and practices are to be utilized?'

"As an analytical tool, RCA is an essential way to perform a comprehensive, system-wide review of significant problems as well as the events and factors leading to them" (MindTools, 2017).

Expected Outcomes/Benefits for RCA Content Course

Students will be better able to document and analyze security breaches and incidents and practice with brainstorming ideas regarding the whys. They will learn how to be a team player and problem solver. Analysis of an actual security breach ensures student understand the need to carefully analyze security alerts and not to ignore them. It also helps students realize that in real world consequences of sloppiness and errors in security management can cause significant damage in terms of dollars and image of an organization. Often, students do not understand the need for being detail-oriented in security management as on assignments and projects they only feel the pain of points deducted; but, when undergraduate students read a detailed description of an actual breach they realize that careless mistakes can lead to significant loss to an organization and they may lose their job. Thus, performing RCA of a well-documented security incident afford students an opportunity to learn how to perform a deep analysis of a security incident, understand the importance of being detail-oriented in security management, and consequence of oversight and errors in responding to security alerts. Thus, RCA should be an integral part of an undergraduate and graduate security course.

4. CONCLUSION

With more security students learning RCA as a class project, corporations will have employees with analytic and problem solving skills along with communication and team member skills. As more information security professionals have knowledge of RCA, actual causes of security incidents can be found which can lead to corrective actions in organizational policies, processes, and procedures. These actions can prevent similar security incidents from occurring in the future.

5. REFERENCES

Black, N. H., & Vernetti, B. J. (2015). Root-cause analysis: Creating & utilizing a functional database. *Professional Safety, 60*(2), 60-62. Retrieved from http://libproxy.txstate.edu/login?url=http://search.proquest.com/docview/1659754982?accountid=5683

Bowie, P., Skinner, J., & de Wet, C. (2013). Training health care professionals in root cause analysis: A cross-sectional study of post-training experiences, benefits and attitudes. *BMC Health Services Research, 13*, 50. doi:http://dx.doi.org/10.1186/1472-6963-13-50

Chadha, R. (2016). Why ask why? *Quality Progress, 49*(1), 49. Retrieved from http://libproxy.txstate.edu/login?url=http://search.proquest.com/docview/1762043642?accountid=5683

Gerber, M. and von Solms, R. (2008), Information security requirements – Interpreting the legal aspects. Computers & Security, 27(5-6), 124-135.

Huertas-Quintero, L.A.M., Conway, P. P., Segura-Velandia, D., & West, A. A. (2011). Root cause analysis support for quality improvement in electronics manufacturing. *Assembly Automation, 31*(1), 38-46. doi:http://dx.doi.org/10.1108/01445151111104155

Lehtinen, T. O. A., Mäntylä, M.,V., & Vanhanen, J. (2011). Development and evaluation of a lightweight root cause analysis method (ARCA method) - field studies at four software companies. *Information and Software Technology, 53*(10), 1045. Retrieved from

ISSN: 2473-3857
v3 n4307

http://libproxy.txstate.edu/login?url=http://search.proquest.com/docview/880377816?accountid=5683

Luo, X. & Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. Information Security Journal, 16(4), 195-202.

MindTools, Editorial Team (2017). "Root Cause Analysis – Tracing a Problem to its Origins." Accessed from htpps://www.mindtools.com/pages/article/newTMC_80.htm on March 29, 2017.

Nailen, R. L., P.E. (2015). Root cause analysis: Methodology or mythology? *Electrical Apparatus, 68*(1), 19-24. Retrieved from http://libproxy.txstate.edu/login?url=http://search.proquest.com/docview/1645885058?accountid=5683

Radware, Inc. (May 15, 2017). Threat Alert: WannaCry Ransomware. White paper. Radware, Mahwah, NJ 07430. Accessed May 21, 2017: https://security.radware.com/ddos-threats-attacks/ddos-attack-types/wannacry-ransomware/

Rasmussen, M, (2003) Analyst Report: IT Trends 2003 – Information Security Standards, Regulations and Legislation – Giga Information Group® 2003. Retrieved May 21, 2005 from CSOonline.com site: http://www.csoonline.com/analyst/report721.html.

Sharma, R. K., & Sharma, P. (2010). System failure behavior and maintenance decision making using, RCA, FMEA and FM. *Journal of Quality in Maintenance Engineering, 16*(1), 64-88. doi:http://dx.doi.org/10.1108/13552511011030336

Spencer, K. (2015). Getting to the root cause. *Quality, 54*(8), 42-45. Retrieved from http://libproxy.txstate.edu/login?url=http://search.proquest.com/docview/1704359845?accountid=5683

White, G. (Spring, 2009). "Strategic, Tactical, & Operational Management Security Model." *Journal of Computer Information Systems, 49(3), 71-75.*

White, G. (2010). "The Evolution and Implementation of Global Assurance." Issues in Information Systems, 11(1), 35-40. (Also appears in PROCEEDINGS of the International Association for Computer Information Systems, Las Vegas, NV, October 6-9, 2010).

White, G. (2012.). *Information Security Education Relationships on Incidents and Preventions: Cyber Assurance Literacy Needs.* Paper presented at the Proceedings of the Information Systems Educators Conference, Nov. 1-4, 2012, New Orleans, LA.

White, G. (2013). "A New Value for Information Security Policy Education." PROCEEDINGS of the 2013 Annual Information Systems Educators Conference (ISECON), San Antonio, Texas, November 7-10, 2013.

White, G. (2015). Education and Prevention Relationships on Security Incidents for Home Computers. *Journal of Computer Information Systems, 55*(3), 29-37. Retrieved from http://www.tandfonline.com/doi/full/10.1080/08874417.2016.1232991

White, G., & Hewitt, B. (2017). More Security Education, More Security Incidents on Home Computers! Why? *International Journal of Information Security and Privacy (Submitted for Initial Review)*.

USDHHS (2017). U.S. Department of Health and Human Services, Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf accessed May 24, 2017.

ISSN: 2473-3857
v3 n4307

APPENDIX A
Academic Text Books lacking RCA

Greene, S. (2006). Security Policies and Procedures: Principles and Practices, Prentice Hall, Upper Saddle River, NJ.

Johnson, R. (2011). Security Policies and Implementation Issues, Jones & Bartlett Learning, Sudbury, MA.

Kim, K. & Solomon. M (2018). Fundamentals of Information Systems Security, 3nd Ed; Jones & Barlett Learning publishers; Burlington, MA.

Merkow & Breithaupt, 2006; Information Security: Principles and Practices, Prentice Hall, Upper Saddle River, NJ.

Panko, R. R., 2004; Corporate Computer and Network Security. Prentice Hall, Upper Saddle River, NJ.

Vacca, R. (2016), Cloud Computing Security: Foundations and Challenges. CRC Press – Taylor & Francis Group, Boca Baton, Fl.

Whitman, M. & Mattord, H. (2017). Management of Information Security, 5th Ed; Cengage Learning; Boston, MA.*

Winkler, J.R., (2011), Securing the Cloud: Cloud Computer Security Techniques and Tactics 1st Ed. Elsevier Publisher, New York, NY.

* Whitman & Mattord (2017) contains one brief paragraph that explains what RCA is.

APPENDIX B
Root Cause Analysis Template

MindTools
Essential skills for an excellent career

Template

Root Cause Analysis Template

- For information about Root Cause Analysis, visit www.mindtools.com/rs/RCA.

Issue				Likely Root Cause			Possible Solutions					
Description	Source	Criticality		Description	Likelihood	Information	Description	Risks			Measure of Success	
		Level (High/ Medium/ Low)	Rationale		High/ Medium/ Low	Tests to Clarify		Description	Likelihood	Mitigation	Test	Results
Client not aware of project status	Client	Medium	Doesn't affect delivery but damaging to account	Status reports not being issued weekly because of lack of info from Project Mgr	High	Check with Program Office	Simplify info required for report so less time-consuming for PM to supply	Client feels report lacks detail	Medium	Agree detail-level required for new report with client	Check with client after four weeks	TBA