https://doi.org/10.48009/3_iis_2015_209-218

Issues in Information Systems
Volume 16, Issue III, pp. 209-218, 2015

EFFECTIVE NETWORK SECURITY AUDIT TRAIL MANAGEMENT PRACTICES: AN EXPLORATORY STUDY

Daniel O'Kelley, JKL Technologies, Inc., dkokelley@gmail.com
Richard L. Ye, California State University, Northridge, richard.ye@csun.edu
Christopher G. Jones, California State University, Northridge, christopher.jones@csun.edu
David W. Miller, California State University, Northridge, dwm3265@csun.edu

ABSTRACT

Modern organizations face an increasingly difficult task of protecting their information system networks from intruders. The process by which network security audit trails are managed varies considerably among organizations. Little research has been done to identify a set of well-researched best practices for Information Systems network security managers to follow. This paper presents the results of graduate student research exploring current industry practices and management policies used in audit trail management. The thesis research formulated several conjectures regarding factors that may lead to faster malware detection times. A research plan, a modified audit trail management model, and a survey instrument were developed to test these conjectures. Although the pilot study response rate was insufficient for statistical analysis, respondent feedback helped refine the instrument and clarify future research direction. Using a thematic approach, the graduate researcher shares insights gleaned from respondents and summarizes literature on effective network security audit trail management.

Keywords: Malware detection, Information security, Network Security, Audit Trail Management, IPS/IDS, Intrusion Prevention System, Intrusion Detection System

INTRODUCTION

According to a recent study, the average cost of a data breach is over $7 million, or $214 per compromised record [8]. Effective audit trail management could potentially improve the effectiveness of information system security controls and reduce the occurrence of such breaches. Organizations of significant size face the increasingly difficult task of protecting their information system networks from intruders or malicious actors. Meanwhile, network protection must also be balanced against accessibility and convenience for authorized users.

In order to achieve this balance of security and usability, organizations generate considerable amounts of data relating to network traffic and security logs. This information is generated automatically, and technologies such as Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are employed to assist information systems and network security personnel in identifying and stopping network intrusions [7]. However, while organizations rely heavily on utilities such as IDS and IPS to sort through the volume of data generated from internal logging, human management of this information can also be an important factor in effectively monitoring network traffic.

The process by which network security audit trails are managed varies considerably among organizations, and there does not exist currently a set of well-researched best practices for IS network security managers to follow. Organizations invest heavily in information systems. Keeping these systems secure against unauthorized access and breaches is critical to maintaining business operations and protecting proprietary and confidential information.

This paper analyzes current industry practices and management policies used in audit trail management and provides an overview of management practices and policies believed to be effective for network protection. The research formulates several conjectures regarding factors that may lead to faster malware detection times, and describes a research plan and survey instrument to test these conjectures.

According to a study by the Verizon RISK team into network data breaches for year 2011, external attackers committed the vast majority of strikes. Of those security incidents, 69% of breaches used malware to perpetrate the

attacks [9]. The audit trail's purpose is to provide a resource for detection, though not necessarily prevention. This study focuses on the detection of malware that has infected a networked device. The research measures the amount of time malware goes undetected as an indicator of effectiveness, such that shorter detection times would indicate greater effectiveness.

This research aimed to identify management practices that might lead to quicker discoveries of malware infections, specifically those practices that relate to the implementation of IDSs. The first step in my investigation was to identify what the key success factors of audit trail management were. These "success factors" were specifically management policies and organizational conditions that allowed for quick detection of malware infections on networked computers.

In order to determine the key success factors of an organization's audit trail management, a survey was developed to collect responses from managers who had access to policy data and breach information. This survey asked respondents questions related to their company's policies over practices within the network and information security group. In addition, public information regarding information security breaches was referenced to provide a more complete picture of security effectiveness in the organizations surveyed. For purposes of this research "effectiveness" was defined as the time between an adverse event occurring and its discovery in the audit trail.

The research plan called for the survey results to be analyzed to identify any correlation between information system policies and data security effectiveness. Although the pilot study response rate was insufficient to provide enough data for statistical analysis, respondent feedback helped refine the survey instrument and clarify the direction of future research. Using a thematic approach to the survey responses, this graduate research offers insights gleaned from respondents as well as a summary of recommendations drawn from the literature for effective network security audit trail management.

RESEARCH PROGRAM AND METHODOLOGY

There is much that is unknown regarding effective network security audit trail and intrusion detection system management. This research investigated a model of current practices in place in organizations today. As part of the research, I attempted to formalize and expand upon a model provided by The National Institute of Standards and Technology (NIST) for audit trail management.

Audit Trail Management Theoretical Model

The foundation for the theoretical model of audit trail management came from recommendations by NIST [6] regarding certain factors that are believed to have a significant impact on the effectiveness of audit trail management. The NIST report listed a record of "audit events," review of audit trails, reviewer's relationship to the audit trail data, and tools for audit trail analysis as important audit trail considerations. The components identified by NIST for effective audit trail management, therefore, were (a) log extensiveness, (b) log review, (c) reviewer's role, and (d) audit trail tools.

Using these factors, an initial theoretical model was constructed. This research sets the time (in hours) from event to discovery as the dependent variable, with shorter times indicating greater effectiveness.

The nature of an adverse event can vary significantly, which could lead to mixed or unreliable results. This research plan attempted to mitigate this by limiting the scope of such events to malware present on a device in the network.

In addition to the variables presented by the NIST for a theoretical model of audit trail effectiveness, other researchers and industry publications have identified other variables that may be relevant to maintaining an effective intrusion detection system [1, 3]. This literature suggested that using IDS effectively relies on proper initial installation, configuration and tuning, and proper operational procedures such as established incident response policies, IDS update frequency, and adequate staffing. The theoretical model was expanded based on the research

presented in these publications. The formal expanded theoretical model for this paper was as follows where $T(AE_d)$ is time to adverse event detection:

$$T(AE_d) = f(\text{detail}, \text{review}_{(\text{frequency, depth})}, \text{role}_{(\text{analyst familiarity, training})}, \text{tools}_{(\text{reduction, analysis, signatures})}, \text{installation}_{(\text{configuration, tuning})}, \text{operations}_{(\text{incident response, staffing, updates})})$$

This revised model added to the NIST model by including *installation* and *operations* to the function, as well as expanding the *role* variable.

While the expanded theoretical model was now more comprehensive, it was infeasible to test each component within the scope of a single study. The emphasis of this study was on the human management of IDS/IPS (i.e., installation, operations, role), and therefore, to make the scope of the study more manageable, it did not measure the technical components (i.e., detail and tools). For the purposes of this research, I extracted a subsetted model from the expanded theoretical model and proposed tests for each variable of this modified theoretical model. The final subsetted audit trail theoretical model was as follows where $T(M_d)$ is time to malware detection:

$$T(M_d) = f(\text{installation, operations, role})$$

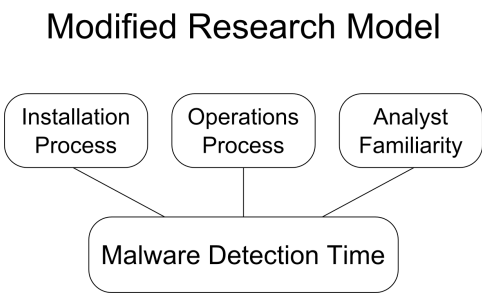

Figure 1. Subsetted Theoretical Model

Adverse Events

The dependent variable in the research model was interpreted as the detection of some adverse event. An adverse event in this context is considered a breach or security incident related to the organization's information systems. An effective audit trail management process should be able to rapidly identify such events and notify the appropriate security personnel of the event. This research used time to discovery as a quantifiable metric to assess audit trail effectiveness.

Given the high incidence of malware in breaches of all kinds [9] and the ability of the intrusion detection system to identify malicious traffic caused by such malware [5], this research focused on the presence of malware as the adverse event necessary for the dependent variable. The research asked the respondents to provide detection times for their three most recent breaches, and used the mean time among the three events as the dependent variable for the respondent.

Intrusion Detection System Testing

This research focused on various aspects of Intrusion Detection System (IDS) policies and procedures to see what relationship these policies had to the rapid detection of malware on the system. Formally, the IDS policies served as the independent variables that were tested in the research.

In selecting specific variables to test, I attempted to align them with the variable categories from the modified research model above.

Summary of Proposed Variables to Study

- Independent variables
  - Installation: Strategies for implementation
    - In-house, vendor assisted, or third-party assisted
  - Operations: Policies and procedures
    - Incident response policy in place (yes or no)
    - Number of weekly man-hours dedicated to IDS operations
    - Number of employees primarily dedicated to IDS analysis
    - IDS signature updates (yes or no)
      - Frequency of updates
      - Days since last update
  - Role: Analyst's familiarity with the environment
    - Number of years employed at the organization
    - Number of years in current position
    - Self-evaluated familiarity (1 to 10 scale)
- Dependent variable
  - Average time-to-detection for the three most recent malware incidents

Survey Instrument

I created a survey to collect data regarding IDS management practices and malware detection time. Variables measured by this survey are outlined in ***Summary of Proposed Variables to Study*** above. Most questions yielded interval or ratio-type data. The research plan called for the use of the Pearson correlation test for this data, as well as the point-biserial and Kendall correlation tests for the data that could not be evaluated via the Pearson correlation. However, insufficient data were collected in the pilot survey to apply the statistical tests.

Survey administration can be accomplished through a number of channels. I elected that the survey be administered via a web application, with responses automatically recorded in a spreadsheet. The Google Form tool was used to accomplish this. Responses to the Google Form were automatically recorded in a corresponding Google Sheet. The complete survey instrument is available in Appendix 1 to this paper.

Respondents

Because this study's objective was to better understand the inner workings of audit trail management, the survey targeted individuals who could provide unique and valuable insight into their firm's information system management. The ideal respondent would be an active member in the organization's information systems department, who had formal or informal responsibilities with network monitoring or security.

The respondent's tenure with the firm or position and responsibilities would be recorded, but these were not necessary selectors for respondent inclusion. Insights from a wide variety of employees by responsibilities and years of experience in the information systems department were valuable for the purposes of this study.

The difficulty of acquiring a sufficient number of acceptable respondents was largely unknown. I, along with my thesis committee, suspected that potential respondents would be hesitant to volunteer much information, given the proprietary and sensitive nature of information security practices. In order to encourage participation, it was emphasized to potential respondents that their individual responses would be held strictly confidential, and that all published results would be anonymized and presented in aggregated form only.

All respondents had some form of "network or information security" in their title. Additionally, respondents were responsible for IDS management, maintaining and enforcing information security policies, and responding to information security incidents.

The survey was administered from September 2013 through February 2014, and was reviewed and approved through the university's Human Subjects Committee. As a preliminary research trial, I solicited responses from professional organizations such as ISACA (Information Systems Audit and Control Association) and ISSA (Information Systems Security Association). Combined, these organizations have well over 100,000 members worldwide, many of whom qualify as target respondents for the survey [2, 4]. Responses were gathered through an online survey distributed to members of ISACA and professional contacts.

FINDINGS: PRELIMINARY RESEARCH TRIAL

There were four qualified respondents from this trial. Due to the limited response rate, no statistically significant inferences could be made from the survey data. However, the response data provided some basic insight into procedures in practice today and hint at their effectiveness. This may be of value to future researchers. Evaluating the survey responses from a qualitative standpoint suggested the following:

- Network security managers are generally confident in their familiarity with the network environment.
- IDS/IPS installation often relies on vendors or other 3rd parties.
- IDS/IPS are updated frequently (often weekly or sooner).
- Robust incident response policies are common in both medium and large organizations.
- IDS/IPS teams are small (1-3 people) relative to the number of end-user devices in the organization (400-30,000 devices in the case of this study).
- There was little observed difference in network security management practices from 400 to 30,000 end-user devices.

The following averages were collected from the survey responses:

- The average malware detection time was 12 hours.
- An average of 2.25 employees work 24.75 hours per week on IDS management.
- There is an average of 10,225 computer devices on the respondents' networks.

There were several instances in the survey responses that indicated some respondents did not fully understand some questions, and therefore were unable to provide a usable response. This finding was used to make survey revision recommendations for future studies.

Survey Revision Recommendations

Based on the observations above, I recommend that certain survey questions and response format be revised so that future researchers can avoid the issues discovered with the pilot survey. Specifically, the survey should limit the response format for quantitative responses, and the following questions should be reworded as follows:

Original Survey Question	Revised Survey Question
How many man-hours per week do you estimate are dedicated to managing and administering the intrusion detection system?	How many man-hours per week do you estimate are dedicated to analyzing and responding to alerts generated by the intrusion detection system?

How frequent are the signature updates for the intrusion detection system?	How many days are there typically between signature updates for the intrusion detection system? (Limit responses to numerical values only) Alternatively, keep original question and limit responses to specific date ranges (daily, weekly, every two weeks, monthly)
In the past please recall the three most recent malware infection incidents. For each incident, how long did it take before the incident was responded to and the infected device(s) quarantined?	In the past please recall the three most recent malware infection incidents. For each incident, how long did it take before your network or information security team detected the incident?

Expanding the survey tool to accept comments on each question would provide additional qualitative data for researchers. The comments should be optional to prevent respondents from exiting the survey due to the survey length.

LIMITATIONS OF THIS STUDY

The extent of this research has certain limitations. First, many factors from the theoretical model were excluded from the scope of the study. The subsetted theoretical model omits factors that might have a significant impact on malware detection times. Factors such as analyst training or which specific IDS tools are used may play an important role in quickly detecting malware, but these factors were not considered in this study. By limiting the number of factors studied, it was hoped the sample size necessary for statistical analysis could be reduced. Additionally, certain omitted variables were not conducive to measurement via a survey.

Second, responses to the preliminary survey were limited, so there may be issues that become apparent when analyzing survey data from a larger response pool. This limitation largely stems from the limited access to qualified respondents. A larger pool of qualified responses would provide more statistical confidence in the survey responses, but identifying and collecting more respondents would require more time than allotted for this study.

Third, this study limited adverse event consideration to malware infections. Limiting the scope of adverse events to malware infections makes quantitative analysis of the theoretical model simpler, but does so at the risk of ignoring the impact of other adverse events, such as internal data theft or destruction, fraud, or malicious network interruption (e.g. Denial of Service attacks).

RECOMMENDATIONS: IDS MANAGEMENT

At the conclusion of this research, certain preliminary recommendations can be made to network security managers to help effectively detect malware on their network. These recommendations are based on qualitative analysis of survey responses and review of prior literature on the subject of network security and intrusion detection, keeping in mind the pilot survey response rate was insufficient for deriving statistically significant conclusions about IDS management.

Ensure Analysts are Familiar with Network Environment

Based on research interviews conducted by Goodall, Lutters and Komlodi [1], IDS managers strongly agreed that the analyst's familiarity with the environment contributed to their effectiveness. Senior management should work to retain longstanding analysts within the company.

Establish a Training Program for Analysts

A strong training program for junior analysts would ensure that internal knowledge regarding the environment is passed to all analysts. Ensuring that senior talent is available to monitor the organization's network is not always possible. A training program should help ensure all analysts meet a minimum level of network familiarity.

Encourage Knowledge Sharing

To ensure knowledge and experience is not being inadvertently hoarded, fostering a culture of knowledge sharing is suggested. This should ensure that compartmentalized knowledge about the organization's network becomes distributed to all IDS analysts and network/information security personnel.

Consult with IDS/IPS Vendors and Consultants when Installing New Systems

IDS vendors and external consultants can ensure that a new IDS/IPS is set up properly and trained to monitor traffic patterns [3]. Organizations that are installing a new IDS/IPS should work closely with the vendor and/or external consultants. If a system is already in place, the organization may choose to have the vendor or a consultant review the system's configuration to ensure the IDS/IPS is installed correctly and is utilizing all available internal tools.

CONCLUSIONS AND FURTHER RESEARCH

Given the limited response rate from the pilot study, it is unlikely that a distinct contribution to network security theory can be extracted from quantitative analysis of the survey results. Review of prior literature provided some insight into practices that could be effective in quickly identifying malware on networked devices. Qualitative analysis of the limited number of survey responses received during the pilot study does yield some interesting observations, though their effect on theory contribution is dubious, as they do little to explain relationships between the factors from the audit trail theoretical model. Even so, these observations provide some comfort that the audit trail theoretical model factors (installation, operations, role) are worthy of further research. Further research could investigate the effectiveness of one or several of the factors outlined in this paper, and qualitative analysis and case studies may yield other factors that play a significant role in identifying malware on networked devices.

The following is a research plan outline that may be followed in order to further the preliminary research on the subsetted audit trail model provided in this paper. I recommend the following hypotheses be tested:

1. Analysts who are more familiar with the organization's network will identify malware-infected devices faster than analysts with less familiarity.
2. Intrusion detection systems installed with the assistance of the IDS vendor will lead to faster malware detection on the network.
3. Organizations with a formal incident response process will discover malware infections faster than organizations without a formal incident response policy.
4. More IDS analysts will lead to faster malware detection times.
5. More IDS analyst-hours dedicated to analyzing security alerts will lead to faster malware detection times.
6. Intrusion detection systems that are updated frequently will lead to faster malware detection than systems that are updated less frequently.

A survey research methodology should be used to test these research hypotheses. In order for future research to be effective, the survey response rate must be increased. For future research, I recommend that the survey links be distributed via a more direct approach. Methods such as direct email from a list of qualified respondents could yield many more responses, provided the researcher can gain access to such a distribution list. It may be valuable to partner with a security-focused organization or a group that represents (and has access to) network security professionals, so that the group's members may be specifically targeted for survey distribution.

REFERENCES

1. Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People*, 92-108.
2. Information Systems Security Association. (2012). *About ISSA*. Retrieved June 27, 2015, from Information Systems Security Association: http://www.issa.org/?page=AboutISSA
3. Innella, P., McMillan, O., & Trout, D. (2002, April 4). *Managing Intrusion Detection Systems in Large Organizations.* Retrieved June 27, 2015, from Symantec Connect: http://www.symantec.com/connect/articles/managing-intrusion-detection-systems-large-organizations-part-one
4. ISACA. (2013). *2013 ISACA Fact Sheet*. Retrieved May 8, 2013, from ISACA: http://www.isaca.org/About-ISACA/Press-room/Pages/ISACA-Fact-Sheet.aspx
5. Meyer, R. (2008). *Challenges of IDS in the Enterprise.* SANS Institute.
6. National Institute of Standards and Technology. (1995). An Introduction to Computer Security: The NIST Handbook. In *Special Publication 800-12* (pp. 213-223).
7. Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, 277-290.
8. Ponemon Institute, LLC. (2011). *2010 Annual Study: U.S. Cost of a Data Breach.* Traverse City: Ponemon Institute.
9. Verizon. (2012 April). *Thought Leadership - Verizon Enterprise Solutions.* Retrieved June 27, 2015 from Verizon Business: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

APPENDIX 1

Original Survey Instrument

1. What is your current title or position at your organization?

2. Briefly describe your responsibilities as they relate to Information Security.

3. How many years have you been employed with your organization in an IT-related role? (Please enter a number, rounded up to the nearest year.)

4. How many years have you been in your CURRENT position with your organization? (Please enter a number, rounded up to the nearest year.)

5. On a scale of 1 to 10, how familiar are you with your network environment and topology? (1 is not at all familiar, and 10 is completely familiar)

Not familiar	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	Completely familiar

6. During the installation of your organization's intrusion detection system, were external consultants utilized?

- ☐ Yes, the IDS vendor assisted with the installation
- ☐ Yes, a third-party consultant assisted with the installation
- ☐ No, the IDS was installed using only in-house resources
- ☐ Other:

7. When your organization's intrusion detection system identifies a potential security incident, is there a formal incident response procedure in place?

- ☐ Yes
- ☐ No

8. Briefly outline your organization's incident response policy.

9. How many man-hours per week do you estimate are dedicated to managing and administering the intrusion detection system? (Please enter a number, rounded up to the nearest hour.)

10. How many individuals are employed whose job duties are primarily to analyze and respond to alerts generated by the intrusion detection system? (Please enter a number.)

11. Does your organization's intrusion detection system receive regular signature updates?

- ☐ Yes
- ☐ No

12. How frequent are the signature updates for the intrusion detection system? (e.g. monthly, weekly, annually)

13. How many days has it been since the most recent update to the IDS signatures? (Please enter a number rounded up to the nearest day.)

14. How many personal computers (laptops and desktops) are in your organization's network? (Please enter a numeric estimate.)

15. How many unique devices were infected with a virus or malware in the past 30 days?

16. Please recall the three most recent malware infection incidents. For each incident, how long did it take before the incident was responded to and the infected device(s) quarantined? (Please enter a number rounded up to the nearest minute.)

- **Incident 1** Detection time in minutes
- **Incident 2** Detection time in minutes
- **Incident 3** Detection time in minutes