Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Industry Based Information Assurance: a new role for user awareness training?

Steven Fulton, *United States Air Force Academy,* Stella Porto, *University of Maryland University College*

Abstract –

As networked computers become more accepted in businesses and homes, so has the recognition for a need to improve and simplify computer security, increase access to information, and ensure that data is not compromised. Leading the way in this effort is the U.S. Government, which focuses its efforts on what it defines as information assurance. One aspect of information assurance programs in both public and private organizations is workforce awareness training. The U.S. Government's Department of Defense mandates such awareness training annually to all employees and contractors who use their information technology systems. Many corporations follow this methodology as well. This study empirically examines such information assurance programs in industry using a two phased explanatory mixed method research design to identify quantitatively a candidate industry which recognizes and responds well to computer security issues and qualitatively examine that industry to understand how it accomplishes information assurance.

Based on these findings, awareness programs must change from the difficult goal of attempting to bring about an employee's prescriptive recognition and response through continued education and training of the original information assurance model to a more reasonable expectation of attempting to influence an employee's understanding of corporate policy regarding a computer's usage and data ownership. This paper proposes an industry based information assurance model, based upon technology while focusing employees on the understanding of corporate computer usage and data ownership policies.

I. Introduction

Today's technology has revolutionized many aspects of life. Computers have become ubiquitous in both workplace and home environments. Where once networked computers were restricted to high tech workplace environments, today networks can be found in small businesses and many homes. Along with these changes in the use of computers has come recognition for a need to improve and simplify computer security, increase access to information, and ensure that data is not compromised. Leading the way in this effort is the U.S. Government, which focuses its efforts on what it defines as *information assurance*.

One aspect of information assurance programs in both public and private organizations is a need for workforce awareness of issues which relate directly to the security of information. So important is this subject, the United States Government's Department of Defense has mandated training in *information assurance awareness* to all employees or contractors prior to being permitted access to government owned computing devices This training mandate requires not only initial training prior to system usage but annual individual refresher training as well. Such training efforts are monitored and reported as "an element of mission readiness" [1]. The tracking requirement of these training efforts focuses not on a successful completion of the course as measured by an assessment tool but on the physical attendance (computer based or face to face) of the individual in the class.

II. Background

Information assurance is focused on measures that protect and defend computer systems by ensuring their "availability, integrity, authentication, confidentiality and non-repudiation" [2]. Often confused with computer security, information assurance includes computer security yet goes beyond typical security concerns to include access and control of information on a given computer system.

Information Assurance is often viewed as multi-leveled environment in which organizations wishing to focus on improving their information assurance posture look at three fundamental categories of countermeasures: technology, operations policy & practices, and user awareness training & education [3]. Note that this view takes the responsibility of information assurance away from a solely technical solution and instead views it as a combined technology, organization policy and user responsibility. This countermeasure theory is referred to as the information assurance *defense in-depth* model and is viewed graphically as a pyramid where the role of awareness training and education are seen as the pyramid foundation, operations policy and procedures seen as the next step on the pyramid and technology seen at the top. This is visually displayed in *Figure 1: Defense in-Depth Pyramid*. The placement of "awareness training and education" on the bottom of the pyramid signifies that the other categories (operations policy and practice, and

ISBN 1-933510-99-4

technology) are built upon a successful education and awareness program.

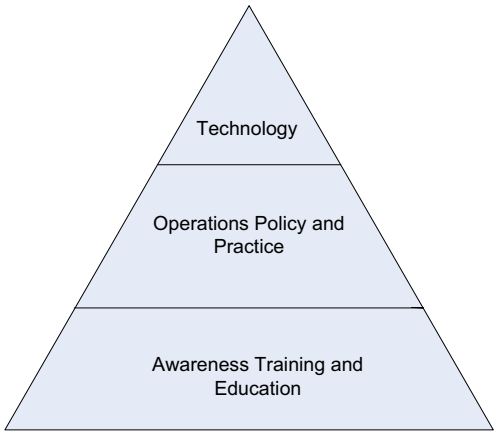


Figure 1- Defense in-Depth Pyramid from Schou & Trimmer (2004)

Until recently, formal programs focusing on awareness training were limited primarily to financial and governmental organizations; however, with the introduction of new regulations both nationally and internationally (Sarbanes-Oxley, UK Data Protection Act, Canadian Data Privacy Act, etc.), the literature suggests that such programs have become more widespread in industry as well [4].

While Department of Defense regulations [1, 5, 6] allow organizations the ability to tailor training to individual job duties, costs of developing individual training based on job duties and the need to ensure requirements are properly reported make it difficult to create individualized training. In fact, it is easier for Defense Department organizations to mandate all employees participate in the same training.

III. Research Design

This study was driven by three research questions:

> *Is IA training a factor of success for those industry sectors identified as responding successfully to information assurance/computer security issues?*
>
> *Is organizational support of IA resources (as measured by organizational resourcing, employee recognition for reporting IA issues, etc.) a factor in industry sectors which respond well to IA/CS issues?*
>
> *What role does organizational support at the department level (as measured by formal or informal processes, management recognition and support, etc.) play in identifying and reporting IA/CS issues among those sectors, which respond well to IA/CS issues?*

The approach used to examine these questions is defined by Creswell and Plano Clark [7] as *a two- phased explanatory mixed methods research design*. The design uses qualitative data to build upon information previously identified through a quantitative approach. In such an approach, it is the expectation that the first phase (or the quantitative phase) *will lead to purposeful sampling* for the qualitative phase [7]. This process is outlined graphically in *Figure 2: Explanatory Design*. Creswell points out that as this design starts quantitatively, emphasis is often placed on the quantitative phase to ensure that the sample identified for the qualitative phase will bring about an understanding of statistically significant differences and anomalous results. In this study, the quantitative phase was used to identify a candidate industry which to be examined in detail during the qualitative phase. The qualitative phase was used to explore industry-wide IA related processes and procedures in an attempt to answer the proposed hypotheses. Findings are drawn from an interpretation of what is found in both the quantitative and qualitative phases.

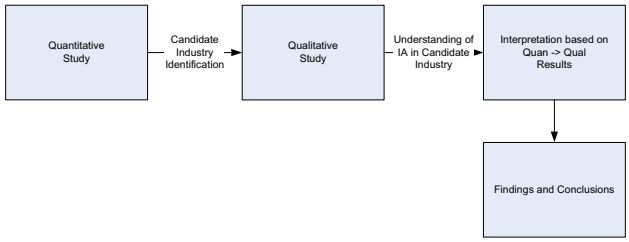


Figure 2- Explanatory Design–Adapted from Creswell (2007)

The quantitative data is based on an archival survey of businesses gathered and released by the Rand Corporation for the Bureau of Justice Statistics and the Department of Homeland Security. This data is grouped into business sectors based on their North American Industry Classification System (NAICS) code [8]. This classification system was originally created in 1997 and is maintained by the Office of Management and Budget to allow for comparability in business statistics within North American countries [9]. Specific industries excluded from the survey included public sector entities, education related entities and private households [8]. Corporations were chosen using the Dunn and Bradstreet Strategic Marketing Records Database and consisted of all companies operating in the United States, which had 10 or more employees. Sampling was done by industry and a stratified random sample was used. The sampling frame consisted of three types of companies: companies with a single location, companies with multiple establishments

but one company headquarters, and companies that were part of a large conglomerate. The stratified sampling was created using business sector and company size as the variables with the United States economy divided into 36 industries. Furthermore, nine other strata were added, one for each employment size class to create a total of 333 strata. However, 81 of the strata were empty most likely due to the use of certainty companies or companies which were already included due to their importance to the United States economy [8].

The qualitative data collection piece of this study consisted of a series of interviews performed based on the outcome of the findings mentioned previously as well as a review of specific industry-wide procedures relating to computer security. The interviews focused primarily on two areas: the role of organizational training related to computer security and the role of organizational support when focusing on computer security. *Table 1: Qualitative Interview Themes* outlines interview themes. *Table 1* also aligns the themes and provides an explanation of the rationale behind the theme choice.

Table 1: Qualitative Interview Themes

Theme	Rationale
Does your organization have a policy which requires all users of computers to complete information assurance/computer security training prior to using a computer system? Are any such policies driven at the industry level or the corporate level?	This question will probe an individual firm's policies regarding information assurance training. Specifically, it will focus on the defense in depth requirement of workforce awareness training.
If you organization does require computer security training, what assessment is performed to ensure that training has taken place?	This question focuses on the measurement aspect of computer security training. Effective training would ensure that the measurement of behavior and results takes place (Kirkpatrick's evaluation of training program) instead of knowledge alone.
Does your organization have policies and procedures that support employees who identify and act upon computer security incidents? Is this focused primarily in the IT department or across the organization?	This question focuses on the role that organizational support plays in causing an individual to recognize and respond to a computer security event.
How does your organization make computer security policies and procedures known to the workforce? Do you feel that the workforce recognizes and follows such policies?	This question looks at two aspects of the organization– how it goes about making policies and procedures known and how well it is perceived that the workforce recognizes and follows such policies.

a) Quantitative Research Findings

The quantitative phase of this study looked specifically at those individual industries having a high level of cyber attacks, yet lower monetary loss and system down time, in the attempt to identify an industry sector which not only recognizes higher cyber attacks but experiences overall lower total monetary loss and system downtime.

Looking at the overall incidents of cyber attacks by individual businesses within industries some interesting trends can be observed. Those which are at the upper end of the scale with 60% or more of the individual businesses identifying cyber attacks include Internet service providers, architecture, non-durable manufacturing, scientific research, construction, motion picture, business/technical schools, publications/broadcasting, chemical drugs, durable goods manufacturing, computer systems design and telecommunications. The range is from a low of 60% (Internet service providers and architecture) to a high of 74% (telecommunications).

In the case of the evaluation of the data in this study, the goal was to identify an ideal candidate industry using four key data points:

- percentage of businesses within a given industry identifying cyber attacks
- percentage of businesses within a given industry detecting 10 or more attacks
- percentage of businesses limiting loss to under $9,999
- percentage of businesses limiting system down time due to cyber crimes to under four hours.

Based on this scenario, four sectors are considered a good candidate possibilities for the study. These four are outlined in *Table 2: Possible Candidate Sectors*

Table 2: Possible Candidate Sectors

Industry Sector	Candidate Possibility	Comments
Publications and Broadcasting	High	Not only high recognition of incidents and reports of multiple incidents, monetary loss and system downtime also kept to a minimum.
Construction	High	While incident recognition is low, recognition of multiple incidents is also low. Monetary loss and system downtime is also kept to a minimum.
Scientific Research and Development	High	Recognition of multiple incidents is medium and monetary loss is medium, the reduction of system downtime makes this a possible incident.
Manufacturing: Non-durable Goods	High	Recognition of high number of incidents, limited monetary loss and system downtime make this a strong candidate.

The final decision of which industry to use in the qualitative evaluation was based not only on the ability of the industry to recognize and respond to cyber incidents,

but on the responsiveness of the industry to the questionnaire and the detailed analysis of the information provided. Four possible candidate industry sectors (publishing and broadcasting, construction, scientific research and development, and non-durable manufacturing) were identified based on their ability to recognize and respond to incidents.

The key difference in the remaining candidates, however, is in the percentage of system downtime noted. Publishing and broadcasting and non-durable manufacturing report 22% of their businesses have experienced 1-4 hours downtime with 88% reporting greater than four hours of system downtime due to cyber attack. The scientific research and development industry sector, however, reports 31% of businesses reporting system downtime to be 1-4 hours total with 69% of the firms reporting greater than four hours of system downtime. This suggests that, while the three remaining possible candidates are similar, the scientific research and development industry may be a good candidate for the second phase of the study. However, one overriding concern regarding the scientific research and development industry sector is that they are often funded through government sponsored research programs or grants. These support programs may come with requirements on how the sector protects the data systems that may cause the industry to match closely the models that the government uses. As this study is focusing on studying an *industry*-based model of information assurance, the scientific research and development industry sector will not be used for the qualitative analysis section of this report.

While both the publishing and broadcasting and the non-durable manufacturing industry sectors may be ideal candidates for the qualitative portion of this study, the lower number of firms reporting monetary loss, coupled with the fact that 100% of the companies report computer system usage, suggests that overall the publishing and broadcasting industry sector would be of more value to the qualitative portion of the study, and therefore, the qualitative study will be performed using firms in this industry sector.

b) Qualitative Research Findings

The trend toward consolidation and multiple outlet ownership in the publishing and broadcast industries presents an opportunity to study large numbers of broadcast stations (radio and television) and newspapers and magazine outlets with relatively few interviews. The focus on the interview choice is based on the following:

- Large corporations with multiple broadcast and/or publishing outlets
- Media content providers generating content for the broadcast and print environments
- Not-for-profit broadcasters providing unique services to areas across the country
- Single station broadcast outlets and single journal publishing environments to understand their role in the computer security environment
- Electronic publishers providing limited print media

By choosing these interview subjects carefully, not only were trends be examined to understand what this industry has done to position itself as a candidate industry, but also relationships (formal and informal) between these organizations will be studied to understand how this industry as a whole focuses on computer security and understand related trends toward computer security/information assurance. All together, the interviews included the strategic planners for 145 newspapers, more than 1,000 magazines, 900 radio stations, 59 broadcast television stations and six cable stations.

The goal of the interview process was to speak with the corporate strategic information technology resource (typically the corporate Chief Information Officer or similar position) to gain insight to the related computer security practices and to understand the origin of such practices. The expectation was that such insight will allow a better understanding of how this industry compares with the model set for information assurance in the literature.

IV. Findings

The findings of this study suggest that current information assurance models which are grounded in the expectation that increased education and training would bring about increased employee recognition and response to information assurance events are false. The publishing and broadcasting industry as a whole no longer trains their employees in the recognition or identification of such information assurance events, instead focusing on the use of other methods (specifically technology-based methods) for recognition and response to computer security events. In fact, none of those interviewed acknowledged that such training at the user level was being performed any longer in their organizations. Only one company reported the existence of information assurance or computer security training and that training was restricted to their information technology workers.

An unexpected finding of this study was the overarching industry move from a more traditional information assurance model to a technology-based IA program. One would expect, at a minimum, a gradual implementation of

new information assurance models and the reflection of these new models in the literature. While certainly much of this could be blamed on industry consolidation through mergers and acquisitions, which bring different media organizations under larger corporate strategic planning umbrellas [10, 11], it appears that in this candidate industry, other reasons exist for this phenomenon as well. When queried about the fact that there was such commonality between the different media organizations, one interviewee described the existence of a "Newspaper Systems Group" for the past 30 years which meets up to twice a year to "exchange technology information, successes and failures, and have discussions about strategies or emerging technologies." As they do not compete in similar markets, this was not seen as a conflict of interest, as long as they do not "discuss contract pricing or try to steal staff from each other." A similar relationship was described during an interview with a strategic planner at an independent broadcast radio station, which stated that the large corporate broadcast organizations publish their solutions to information technology problems (as well as other broadcast solutions) in journals that target radio station engineers. These industry based technical organizations helped to explain why the industry wide response to information assurance was drastically different from the literature.

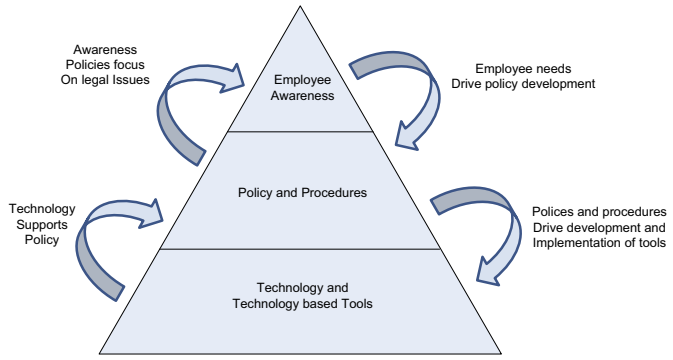
V. Conclusions

This study found that the publishing and broadcasting industry performs information assurance quite differently than literature recommendations. The original multi-tiered defense in depth model builds upon an environment in which employees play a strong role in the recognition and response to IA issues suggesting that organizations focus on extensive and repetitive training in an attempt to modify employee reactions to such events.

This education and training model brings to mind Kirkpatrick's [12] work on outcomes of training. Kirkpatrick theories suggest that for the defense in depth model to be successful, employees must have training in which *measurable results* are seen in an increased ability of employees to recognize and respond to information assurance issues. Such outcome-based training is also thought of as *deep learning* in which training brings about a result change beyond the end of the formal training effort [13]. Siponen [14], specifically looking at the role of education and training in information assurance, agreed with the need of deep learning in such instances suggesting that to be truly effective, the goal of such information assurance related training efforts must bring about a prescriptive response of users in line with organizational expectations.

This study provides strong evidence for a change in existing management theories regarding information assurance. The IA defense in-depth model must be re-examined to understand how an information assurance program, which focuses on technology for the recognition and response of information assurance issues, can provide a successful industry-based information assurance program. One recommendation, based on the findings in this study, is outlined visually in *Figure 3: Industry-Based Information Assurance Model*. This model, which closely matches what was seen empirically in the study, focuses upon technology as the building block of an information assurance program. In *Figure 3*, the series of arrows on the left demonstrates how technology supports organizational policy and procedures. The organizational policies and procedures, in turn, are where limited awareness resources in an organization are placed. Awareness programs are focused on what employees are permitted to do legally on their computers and expectations of the organization in response to the usage of computer systems focusing on legal system usage and data ownership issues. According to this study, awareness programs must change from the difficult goal of attempting to bring about an employee's prescriptive recognition and response of the original information assurance model to a more reasonable expectation of attempting to influence an employee's understanding of corporate policy regarding a computer's usage and data ownership. The information assurance defense in-depth pyramid's employee awareness training foundation has been replaced by specific technology based awareness, which recognizes and responds to threats. This technology supports the development of policies and procedures which are then brought to the awareness of employees through non-training methods. The publishing and broadcasting industry has accomplished policy awareness through e-mail or *push technology* in which messages are delivered to user's terminals and users must respond.

Figure3: Industry Based Information Assurance Model



The arrows on the right side of the model refer to the way policies are created supporting the user's need for data. In the case of the publishing and broadcasting

industry, this means that users are continually finding the need to access sites which would be restricted in other industries as they research information for their stories. This need has driven policies which, while respecting the fact that some of these sites may be dangerous to the corporate enterprise, still allow users to access these sites. These corporate policies, in turn, have driven a stronger technology-based response in recognition and reacting to computer threats driving the development of technology-based solutions to recognition and response to information assurance issues.

VI. Repercussion to Government and Industry

For years, information assurance has been grounded in the theory that user awareness training is the cornerstone upon which government and industry must build their foundation. This study of empirical data suggests that as technology has changed, the focus on awareness training may need to be re-addressed. The publishing and broadcasting industry, through use of technology, was able to reduce monetary loss and system down time due to cyber incidents and yet was able to recognize and respond such incidents when they did occur. This suggests that a change in the Information Assurance literature may be forthcoming. As technology becomes capable of recognizing and responding to cyber incidents, the need to focus employees on awareness training and education may not be as much as important as it was in the past In fact, it appears that any training efforts should focus on awareness of company policies and procedures as they relate to information assurance as opposed to the recognition and response to cyber incidents. Those corporations in publishing and broadcasting which do so often limit such training to new employee orientation and occasional email updates to changes to such policies.

This study suggests a better solution to extensive information assurance awareness training efforts would be to redirect funding which is spent on such training programs to the acquisition of hardware and software tools to recognize and respond to such cyber incidents. Asking a workforce which is not technology savvy to recognize and respond to an incident, as has been done in the past, may not be a valid solution.

Based on this study, any workforce training should be focused on policies and procedures which define the expectation of employees would be a better use of such funding efforts. Employees who understand what is permitted in their organizations would be better way for corporate and government organizations to work with limited information assurance funding.

VII. Future Research

In the findings of this study, it was noted that IT professionals (or those who recognize the need to secure systems) were more likely to recognize and respond to an information assurance incident. It was also mentioned that those who recognized the value of securing data (such as those working in finance and accounting organizations) were also likely to identify a computer security issue. It would be interesting to study this phenomenon in more detail to understand what role such a recognition of the value of the data plays in the identification and response to computer security issues.

The design of this study focuses primarily on industry as opposed to governmental or non-profit organizations. Future studies should look at the implementation of such programs in governmental environments whose business cost basis is different than industry. Such a study must address issues, which include the value of governmental data (especially in areas as national defense or critical infrastructure) in which the loss of data can be harmful to the nation as a whole as opposed to a loss of profit as seen in the for profit environment.

VIII. References

[1] U.S. Department of Defense, “Information assurance training, certification and workforce management,” 2004. http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf.

[2] Committee on National Security Systems, “National information assurance (IA) glossary CNSS instruction number 4009,” 2006.

[3] Schou, C.D. and Trimmer, K.J., Information assurance and security. *Journal of Organizational and End User Computing*, 2004. **16(3)**

[4] Curran, T., “Information assurance awareness programs in multinational manufacturing organzations,” in *Managing an information security and privacy awareness and training program*, R. Herold, Editor 2005, Auerbach. Boca Raton, FL. pp. 322-329.

[5] U.S. Department of Defense, “DoD Directive 8500.01E: Information assurance,” 2002.

[6] U.S. Department of Defense, “DoD 8570.01-M: Information assurance workforce improvement program incorporating change,” 2005.

[7] Creswell, J.W. and Plano Clark, V.L., *Designing and conducting mixed methods research.* 2007, Thousand Oaks, Calif.: SAGE Publications. xviii, 275 p.

[8] Davis, L.M., Golinelli, D., Beckman, R., Cotton, S., Anderson, R., Barnezai, A., Corey, C., Zander-Cotugno, M., Adams, J., Euller, R., and Steinberg, P., *The national computer security survey (NCSS): Final methodology.* RAND Corporation: Safety and Justice, 2008. Retrieved on October 18, 2008. From http://www.rand.org/pubs/technical_reports/2008/RAND_TR544.pdf.

[9] U.S. Census Bureau, "North American industry classification system (NAICS)," 2002. http://www.census.gov/eos/www/naics/2002NAICS/2002_Definition_File.pdf.

[10] Amobi, T. and Kolb, E., "Industry surveys - Broadcasting, cable and satellite," in *Standard and Poor's Industry Survey*2009.

[11] Peters, J., "Industry surveys: Publishing," in *Standard and Poor's Industry Survey*2008.

[12] Kirkpatrick, D., Great ideas revisited. *Training & Development*, 1996. **50**(1): 54.

[13] Marton, F. and Saljo, R., On qualitative differences in learning: 1--Outcome and process. *British Journal of Educational Psychology*, 1976. **46**(1): 4-6.

[14] Siponen, M.T., A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 2000. **8**(1): 31.