Examining the Level of Educational Factors on Reducing Data Security Breaches

Oscar Ukpere / Oscar@Ukpere.com

Steven Brown / Steven.Brown@Capellauniversity.edu

Capella University
225 South 6th Street, Floor 9
Minneapolis, MN 55402

Abstract - The purpose of this quantitative correlational research study was to examine the relationship between the levels of educational factors possessed by information security managers (ISMs) and the number data security breaches in their organizations. Previous research reported that levels of educational factors have an increasing impact on the reduction of organizations' data breaches, leading researchers to conclude that various levels of educational factors are effective in implementing appropriate controls to address data breaches. A quantitative correlational study was used to determine the relationship between data security breaches and ISMs' levels of educational factors (level of completed formal education, number of professional certifications, number of training programs, and years of work experience) to provide quantifiable data on data security breaches. Data analysis revealed a significant, positive correlational relationship between the reduction of organizations' data breaches (dependent variable) and each of the four independent variables (levels of formal education, completed data security certifications, on-the-job training, and hands-on experience).

Keywords

Data Breaches, Educational Factors, Certifications, Education. Training, Work Experience

1 INTRODUCTION

The increasing use of the Internet by organizations to perform transactions has attracted malicious users who perpetrate attacks to cause data security breaches. Using the Internet creates exposures to security threats and requires security enforcement and risk-management mechanisms [1]. The level of organizational dependency on the Internet has been increasing data security breaches that present threats to our way of life and our national security [2,3]. As a result, researchers have argued that information security managers' levels of educational factors can help minimized threats [4]. To better inform the need for the levels of educational factors among information security managers in organizations, there have been analytic attempts to quantify and understand its effects on data security breaches [4,5,6]. Previous researchers have suggested that these data security breaches occur since those responsible for protecting organizational networks do not have the necessary levels of educational factors to thwart these attacks [1,4].

2 DATA BREACH IMPACT

Hackers continue to be responsible for a significant number of data breaches, making up 40 percent of all cases [7]. Data security breach is the most significant challenge in the use of information systems, and the evolution of data security breach changed the way organizations manage and secure information with the Internet [1,8]. The ultimate intention of data security breach by an attacker is to steal data for personal gains and sometimes for competition as these are mostly personally identifiable and financial information, and a huge issue is protecting these data [9,10,3]. Organizations that store, process, and transmit data of this kind for business purposes are at higher risk for attack. Data security requires protecting sensitive data and avoiding the root-causes of data security breaches [11]. There are still a lot of unknowns on how the levels of educational factors of information security managers are affecting the decisions made by ISMS on protecting against data security breaches [4]. The increased number of data security breaches over the past decade has affected millions of customers worldwide costing billions of dollars.

2.1 Education and Data Security Breaches

Although data security breach is on the increase, the issue is not the data breaches themselves. The increasing data breach is due to the lack of the right level of educational factors among information security managers to make security focused decisions [4,5]. Certain levels of information security managers' educational factor are beneficial to organizations in producing a favorable degree of data security to combat hackers that take advantage of new technologies [5]. Education, training, and employees' experience are the main factors for influencing information security decisions and awareness amongst information security managers [4,5]. Training and education of information security managers provide valuable information for protecting assets, maintaining the integrity of information, and responding to security threats [4]. Information Security Managers are often responsible for assuring the secure use and operation of information assets by using the right knowledge acquired from various levels of educational factors [4,5,11]. Information security managers must implement defensive strategies to protect against the growing vulnerabilities by addressing human threats from the lack of knowledge; as training, education, and management decisions can reduce data security occurring from human errors [13,14]

3 THEORETICAL BOUNDARIES

Knowledge theory, leadership theory, and rational choice theory provide frameworks for research in ISMs levels of educational factors and data security breaches [4,12]. While each of the theoretical frameworks in isolation can inform further academic inquiry across all levels of educational factors and data security breach studies, consideration of all three theoretical frameworks intertwined aligned with the current body of research in ISMs' levels of educational factors and data security breaches. Research through the lens of these theories combined informs the influence of ISMs' levels of educational factors and data security breaches in organizations [4].

3.1 Knowledge Theory

Knowledge theory that informs data security breaches did not have a lot of journals before 1960 [4]. The earliest scholarly journal published in the database of Business Source Complete was on American Economic. Also, the search for the theories of knowledge and data security in the database of Business Source Complete provided very narrow results. To trace the origins of the theory of knowledge to its original date and place as evidence indicates, is impossible, as it has its links to various Eastern and Western civilizations, cultures, and notions [15]. The limited existence of journals on knowledge theory and data security breaches led researchers to suggest that only very few studies exist that incorporated the knowledge theory in the field of data security [4,5,9,11]. Several theories recognized knowledge as an essential and crucial organizational asset that should be applied intelligently and managed more efficiently [11,15,16]. Since knowledge is considered a strategic asset in organizations, it is crucial to for organizations to improve and protect information security managers' expertise to stay competitive and secure in a vulnerable environment. It is vital to the success of any organization that information security managers maintain a level of educational factors and current working knowledge in the areas of data security [5]. Developing organizational capabilities and improving performance are an integral part of the system in an organization resulting from knowledge. The knowledge of employees including information security managers is a valuable asset, an indispensable tool for businesses, a sustainable competitive advantage to a firm, and has become a significant economic asset and the most important and perhaps the only source of competitive advantage [17,18].

3.2 Leadership Theory

For centuries, leadership reflects behaviors, traits, role relationships, interaction patterns, and occupations of someone in an administrative position [12]. Search for theories on leadership reveals that much of recent work on leadership is on leadership as it relates to management. A significant number of management studies and some Leadership related studies exist in organizations and a broad management

context, and, often, are not applicable to data security or breach mitigations. The leadership theory does not seem to have constant attributes that are measurable and dissectible. Personality traits theory is the oldest on the study of leadership since its origins date back to the 1920s [1]. This theory is one of the earliest theoretical concepts of leadership because researchers are interested in the need for, or importance of, successful leaders, especially leaders that demonstrate unique skills or attributes that create uniqueness for them among their subordinates or followers [1,19]. It is an ongoing mindset that leaders have unique expertise or surpassing abilities that give them control and influence over their subordinates or followers. In leadership, higher self-efficacy scores indicated higher levels of leadership efficacy, and people were more positive about their leadership ability when they did not compare themselves to others [1].

3.3 Rational Choice Theory

The rational choice theory is about rationalizing the decisions made to solve a problem or to enhance a situation. Based on behavioral psychology and extended to other fields; rational choice theory suggests that individuals premeditate their actions to their most significant advantage [20]. The basic premise is that humans will make the choice that offers the most benefits for the least costs or overhead, which implies costs and benefits are the considered in that decisions [4,20,21]. The decision maker thus can quantify the anticipated merits or benefits, evaluate them against the potential losses of deciding, and, if the expected gains are higher than the perceived failures, the individual is more likely to proceed. Decisions based on cost and benefit aligns with the classical theory of the economic man, in that the rational choice for a leader with economics in mind leans towards that which tends to maximize gains and minimize costs, as is right to the premise of the decision [22].

4 EDUCATION AND DATA SECURITY

Levels of educational factors (formal education, certifications, training programs, and hands-on experience) provide security knowledge to information security managers. Educational programs must be developed to adequately train and educate

a sustainable cybersecurity employee pipeline to build a competitive data security workforce that meets both current and future demands [11]. Using information security management officers in small businesses in the state of Texas as a target audience, Spear's applied a quantitative correlational research methodology to investigate and answer the research questions. Results of Spear's analysis indicated that all levels of educational factors have positive influences in reducing data security breaches in organizations. Knowledge of data security is essential in helping practitioners, and research communities find ways to identify and prevent data security flaws effectively [4,23,24]. The authors' suggestion is in line with the theory of knowledge as it embraces seeking the relationship between an information security managers' level of educational factors and their organization's data security breaches. In general, gaining the necessary expert knowledge in any trade including information security may be a matter of investing in current employees. Expert knowledge in data security encompasses support for information security managers to attain academic credentials and industry certifications, and structuring work assignments to build employees' security experiences [25]. Also, mentoring and apprenticeships are possible ways for formally nurturing employees' skills in any job function.

4.1 Hands-on Experience and Data Security

Changes in technology and security threats require aspiring information security managers to set a goal of 10,000 hours of relevant, hands-on skill development over a long-term career [6]. Providing hands-on experience, even if only in a simulated lab environment, instills in scholars and practitioners not just the ability to understand what must be done to secure systems, but also how to go about doing it [4,5]. Hands-on experience helps to address the concerns of employers that formal education, training, and certifications alone do not guarantee the needed competence to protect data.

4.2 Professional Certification and Data Security

Certifying bodies are rolling out programs geared towards demonstrating skills through hands-on experience to promote the use of practical experience in combating data security breaches. Advanced professional certifications such as Licensed Penetration Tester and Offensive Security Certified Professional require a hands-on penetration test demonstration in a cyber-range. While select few certifications require that information security managers demonstrate skills to be certified, nearly all discuss the use of tools and techniques within the field of cybersecurity like the Certified Ethical Hacker (CEH) credential [6]. Different professional security certifications will have different foci. The Global Information Assurance Certification (GIAC) offers some security-focused certifications aimed to ensure an individual has the skills necessary as a practitioner. Professional certifying organizations such as Information System Security Certification Consortium (ISC)2, Information Systems Audit and Control Association (ISACA), International Council of Electronic Commerce Consultants (EC-Council) respond to industry forces such as standards and best practices to develop certification exams. Over the past decade, numerous industry standards and guidelines have emerged worldwide, such as International Organization for Standardization (ISO) standards, National Institute of Standards and Technology (NIST) security frameworks, and the Payment Card Industry Data Security Standard (PCI-DSS). The International Organization for Standardization (ISO) 27000-series is a prominent international standard providing both authoritative statements on information security management as well as procedures to be adopted by organizations to ensure information security [6].

4.3 Leadership and Data Security

The leadership of the information security manager encourages compliances with data security standards and presents an environment with established data security controls [12]. The role of information security managers has received attention considering the trend data security breaches and these managers responsible for encouraging and motivating data security-aware culture in

organizations. Transformational leadership by information security managers improves the efficacy of organizations' data security posture [12]. Informed information security managers possess the leadership skills to deal with the dynamic, unpredictable, and constantly changing data security environment [4]. The new problem facing the twenty-first-century businesses is understanding how well-educated their leaders are in the methods and practices that are required to protect the companies from cyber intrusions and criminal activities [5]. Information security managers with the right skills, education, and training can safeguard businesses and society from Internet crime, thereby encouraging the safe exchange and containment of data [5,14]. Most senior security leaders in today's global corporations may not have proper education on electronic cyber-criminal activities and how to handle them. Years back, formal education and training programs geared toward data security were not available in academic institutions of learning. Most managers in today's global companies got their education before this electronic cyber-criminal activity had advanced to the stage it is in currently [5].

4.4 Information Security Education and Training

Multiple studies exist on the impact of training and education on data security. These studies often focus on security awareness training for end users and how they impact organizations' data security. While very few studies exist on the effect of information security managers or decision makers education (formal education, certifications, formal training, on the job training) on data security breaches, [3] conducted a case study to determine the effect of information technology managers training on data security in educational institutions. Stark's case study research explored the cyber-security systems and training and education of IT professionals at a member college of the Florida College System using thematic analysis to analyze interview transcripts of respondents. Levels of educational factors of information security managers do not end upon graduation from a degree program and more often occurs outside the bounds of formal education, primarily by way of company culture and through the context of specific industries or technologies [3]. The leaders of the organization show they value the continuous education of

cybersecurity professionals after graduation and have large training budgets, use online training companies to meet the training requirement for the information security managers [12,26]. The return on investment for providing adequate security training and education is enormous if it prevents even one data breach and a good training plan is essential in providing appropriate data security for the organization [3,24].

5 METHODOLOGY

The researchers performed a quantitative correlational study to examine the relationship between Information Security Managers (ISMs) levels of educational factors and the data security breaches in their organizations. This research further informs ongoing knowledge on information security managers' level of educational factors and the data security breaches recorded by their organizations to inform investment on the appropriate educational requirements for effective data security [4,5]. The researcher employed a quantitative correlational research design to examine the relationship between an information security manager's (ISM's) level of educational factors and the number of data security breaches in an organization. Using this research design determined the level of significant relationship that exists between the research variables and if the relationship correlations are positive. The variables correlated include ISM's levels of completed formal education, the number of information security certifications completed, years of on-the-job experience and number of completed training as independent variables (IVs), and the number of data security breaches, as a dependent variable (DV). The researcher employed a quantitative correlational and bivariate research design to examine the research questions and test the hypotheses for the significant relationship between ISMs levels of educational factors and the number of data security breaches. The intent of the correlational and bivariate analysis portion of the study was to determine if a relationship exists between the ISMs various levels of educational factors and the number of data security breaches that occurred in their organizations. This process supported the correlational methodology as the researcher attempted to determine if a relationship exists. The Pearson's product-moment correlation coefficient was

used to achieve this analysis. This study's population consisted of small, medium, large organizations in the state of Illinois. Illinois represents a fair amount of businesses in the United States. CareerBuilder and Economic Modeling Specialists International found Illinois to be among the top three states with the fastest growth of business establishments in the US [27]. Additionally, Verizon's 2013 Data Breach Investigations Report confirms that the business sector has the highest incidence of data breaches [28]. The population of firms that have suffered data security breaches in the state of Illinois was not easy to quantify, due to the sensitive nature of data security breach data [29]. However, through the outsourcing data collection process to QuestionPro and the use of QuestionPro's audience, the target population was reached, and the recruitment was successful. The target participants were a section of QuestionPro's audience who are information security managers directly involved in making information security decisions regarding the practices of securing their organizations' information assets and may have had access to company breach data in the state of Illinois. Due to the large population size in some studies, time, and financial constraints, researchers often cannot test every individual in the population. Therefore, a sample possesses the same characteristics as the population it is sliced out from [24]. To ensure the recruitment of the right individuals and avoid bias, the researcher used stratified random probability sampling to provide a representation of the population [30]. Acharya et al. posited that stratified random probability sampling allows the investigator to generalize the findings of the sample to the target population. G*Power was used to compute an approximate sample size of 134 completed responses. However, if construct validity is high, a sample size of 100 is adequate [4]. Therefore, to achieve a suitable sample size of close to 100 and acknowledging a return rate of close to 25%, 434 ISMs in small, medium, and large organizations in the state of Illinois received a consent form, and the study questionnaire launched by QuestionPro, requesting their participation. Of the 434 ISMs who received the survey through QuestionPro, 101 ISMs responded. The response rate of 101 ISMs met the approximate sample size as computed with G*Power.

5.1 Hypotheses

The following hypotheses were addressed in this study

- H1a. Information security managers' level of formal education has a significant correlation to their organizations' number of data security breaches.
- H2a. Information security managers' professional certification has a significant correlation to their organizations' number of data security breaches.
- H3a. Information security managers' years of experience has a significant correlation to their organizations' number of data security breaches.
- H4a. Information security managers' number of training programs attended has a significant correlation to their organizations' number of data security breaches

6 RESULTS

These results were to determine the level of significant relationship that existed between ISMs' levels of educational factors (formal education, number of professional certifications, years of hands-on experience, number of attended security training programs (IVs), and the number of data security breaches (DV) in their organizations in the past five years (2012 to 2017), see (Figure 1).

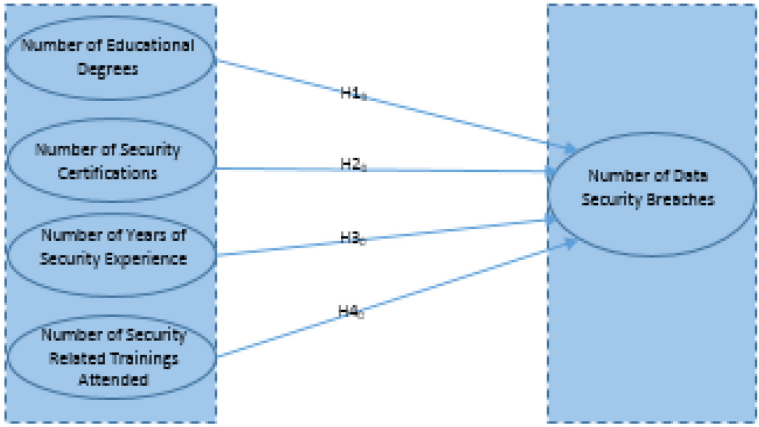

Figure 1. Result overview showing the dependent variables (ISMs' levels of educational factors) and independent variable (number of data security breaches).

The test of $H1_0$ showed a positive correlation that formal education does influence the reduction in the number of data security breaches. Being informed translates to having the needed knowledge or education, and having the necessary education, yielded encouragingly positive data security outcomes [14]. Also, the null hypothesis $H2_0$ was accepted indicating that the number of professional security certifications does influence the reduction in the number of data security breaches. Information security professional certifications are currently an essential measure that the industry has for regulating professional competency in managing data security [6,32]. Additionally, the null hypothesis $H3_0$ was also accepted, which signified that years of professional information security management experience does influence the reduction in the number of data security breaches. Hands-on experience proved to be an important predictor of how people respond to security or show security behavior [4]. Finally, the null hypothesis $H4_0$ was also accepted, and that security training of ISMs does influence the reduction in the number of data security breaches. In support of Spears, the present study generated support substantiating the need for organizations and most especially ISMs to acquire new

knowledge through training. With the analysis of ANOVA linear regression, when the value of $p < .001$, which indicates that the correlation has a statistically significant relationship between the independent variables of this study and the reduction in the number of data breaches. The researcher used ANOVA to calculate the deviation to find out if significant differences existed between the independent variable (ISMs education, certifications, training programs and experience) and reduction in the number of data security breaches.

7 DISCUSSION

The findings from Pearson' correlation analysis revealed the null hypotheses $H1_0$, $H2_0$, $H3_0$, and $H4_0$ were accepted while the alternate hypotheses $H1_a$, $H2_a$, $H3_a$, and $H4_a$ rejected, as significant relationships exist between the independent variable and the reduction in the number of data security breaches. See (Table 1).

Independent Variables	Dependent Variable	Hypotheses	Pearson Correlation Coefficients (r)
Highest education level achieved	Number of data security breaches	$H1_0$, $H1_a$	.384
Completed IT security certification	Number of data security breaches	$H2_0$, $H2_a$	.315
Years of IT security experience	Number of data security breaches	$H3_0$, $H3_a$	.115
Attended training programs	Number of data security breaches	$H4_0$, $H4_a$	.376

Table 1. Results of Pearson Correlation Coefficients (r) for ISMs levels of educational factors and number of data security breaches.

The results revealed the Pearson's correlation coefficient for $H1_0$ with a value of .384 had a positive correlational relationship between ISMs level of education and the reduction in the number of data security breaches ($r = .384$, $n = 101$, and $p < .001$). With the analysis conducted for each of the other hypotheses, the Pearson's product-moment correlation analysis revealed a positive correction value of .315 between an ISMs number of certifications and reduction in data breaches ($r = .315$, $n = 101$, $p < .000$). Also, the analysis showed a positive correction value of .115 between ISMs' years of IT and security experience, and the reduction in the number of data security breaches ($r = .115$, $n = 101$, $p < .255$). Pearson correlation coefficient value of .315 between ISMs number of IT security related security training on secured data practices and the reduction in the number of data breaches ($r = .376$, $n = 101$, $p < .000$). This implies that all educational factors are critical for implementing security mitigations to curtail data security breaches. Correlation quantifies the strength of the linear relationship between paired variables, expressing this as a correlation coefficient [33].

REFERENCES

[1] Martinez, F. E. A correlational study of leadership styles and employees' behavior toward information security and awareness, 2015.

[2] Caudle, D. Improving cyber warfare decision-making by incorporating leadership styles and situational context into poliheuristic decision theory. Proceedings of the International Conference On Information Warfare & Security, 2013, 240-247.

[3] Stark, A. An examination of information security training and education for IT professionals in a community college: A case study, 2017.

[4] Spears, P. D. Education and the degree of data security. (Doctoral dissertation) Retrieved from ProQuest Dissertations and Theses, 2013.

[5] Pitcock, R. W. Evaluating the cybersecurity capabilities of senior managers employed by companies located in the United States. Available from ProQuest Dissertations & Theses Global, 2015.

[6] Knapp, K. J., Maurer, C., & Plachkinova, M. Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. Journal of Information Systems Education, 2017, 28, 101-113.

[7] Kuei-Hu, C. Security threat assessment of an internet security system using attack tree and vague sets, 2014.

[8] Drtil, J. Impact of information security incidents - theory and reality. Journal of Systems Integration, 2013, 4, 44-52.

[9] [Knott, C. L., & Steube, G. Encryption and portable data storage. Journal of Service Science, 2011, 4, 21-30.

[10] Galbraith, M. L. Identity Crisis: Seeking A unified Approach to Plaintiff Standing For Data Security Breaches pf Sensitive Personal Information. American University Law Review, 2013, 62, 1365-1397.

[11] Mangold, L. V. An analysis of knowledge gain in youth cybersecurity education programs. Available from ProQuest Dissertations & Theses Global, 2016.

[12] Choi, M. Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing, 2016 8, 638

[13] Selamat, M. H., & Babatunde, D. A. Mediating effect of information security culture on the relationship between information security activities and organizational performance in the Nigerian banking setting. International Journal of Business and Management, 2014, 9, 7, 33–38.

[14] Smith, T. T. Examining data privacy breaches in healthcare, 2016.

[15] Wiig, K. Knowledge Management: An emerging discipline rooted in a long history. In D. Chauvel, & C. Despres (Eds.). Knowledge Horizons Woburn, MA: Butterworth-Heinemann, 2012.

[16] Cyr, S. The effect of personality differences, knowledge types, and sharing targets on the psychological costs and benefits perceived in knowledge sharing decision situations. Available from ABI/INFORM Global; ProQuest Dissertations & Theses Global, 2009.

[17] Anzano, C. G., & Khanser, M. A. Towards an integrated approach in knowledge management in the creative industry. International Journal of Information and Education Technology, 2013, 3, 4, 424-432.

[18] Ghiorghita, E., & Grzegorczyk, A. Knowledge management as a strategic business resource. Journal of Economic Development, Environment and People, 2017, 6, 2, 63-72.

[19] Gehring, D. R. Applying traits theory of leadership to project management. Project Management Journal, 2007, 38, 1, 44-54.

[20] Krull, S. School selection patterns through the lenses of rational choice theory and behavioral economics theory, 2016.

[21] Paternoster, R., & Pogarsky, G. Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. Journal of Quantitative Criminology, 2009, 25, 2, 103-127.

[22] Pope, M. B. Time orientation, rational choice and deterrence -- an information systems perspective (Order No. 3590232). Available from ProQuest Dissertations & Theses Global, 2013.

[23] Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. A survey of cyber crimes. Security & Communication Networks, 2012, 5, 4, 422-437.

[24] Sardaryzadeh, A. Identifying effective cybersecurity team behaviors in-order to transform cybersecurity. Available from ProQuest Dissertations & Theses Global, 2017.

[25] [Patton, M. Batting data breaches. Community College Journal, 2015, 86, 1, 20-24.

[26] Westphal, J.D., & Clement, M.B. Sociopolitical Dynamics in Relations between Top Managers and Security Analysts: Favor Rendering, Reciprocity, and Analyst Stock Recommendations. Acad. Manag. J. 2008, 51, 1, 873–897.

[27] EMSI. CareerBuilder & Economic Modeling Specialists Report: Which Job is Most Unique to Your State, 2014.

[28] Verizon. Data Breach Investigation Report, 2013.

[29] Pelletier, J. M. Effects of data breaches on sector-wide systematic risk in financial, technology, healthcare and services sectors. Available from Dissertations & Theses @ Capella University; ProQuest Dissertations & Theses Global. 2017.

[30] Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. Sampling: Why and how of it? Indian Journal of Medical Specialties, 2013, 4, 2, 330-333.

[31] McCrohan, K. F., Engel, K., & Harvey, J. W. Influence of awareness and training on cyber security. Journal of Internet Commerce, 2010, 9, 1, 23-41.

[32] Fulton, E., Lawrence, C., & Clouse, S. White Hats Chasing Black Hats: Careers in IT and the Skills Required to Get There. Journal of Information Systems Education, 2014, 24, 1, 75-80.

[33] Hazra, A., & Gogtay, N. Biostatistics series module 6: Correlation and linear regression. Indian Journal of Dermatology, 2016, 61, 6, 8Euy6A5luEI