Modeling and Analysis of Key Management Security Factors for Organizational Data Protection: A Multi-Source Approach

Nattakan Yahattaa[1], Usa Humphries[2]
[1,2]King Mongkut's University of Technology Thonburi, Thailand.

Article Info

Article history:

Received Mar 15, 2025
Revised Apr 20, 2025
Accepted May 16, 2025

Keywords:

Management security factors
Data security
Information security governance
Risk management
Confidentiality-integrity-availability (CIA)

ABSTRACT

Despite a wealth of technically advanced outcomes and strategic efforts, managing information security continues to be a persistent and complex challenge for organizations. The dynamic nature of hierarchical data security is heavily dependent on a range of interrelated factors that must be aligned effectively. For data security administrators, it is crucial not only to identify relevant data but also to understand and manage the interdependencies among various security factors. The primary objective of this study is to develop a comprehensive model of key Management Security Factors (MSFs) essential for ensuring hierarchical data safety. Initially, an extensive literature review was conducted, involving a systematic and open-coding analysis of 136 academic and industry papers. This process led to the identification of critical variables influencing data security. These variables were organized into 12 major categories: physical security, system vulnerabilities, technical infrastructure, awareness, access control, risk management, organizational resources, internal organizational dynamics, confidentiality-integrity-availability (CIA), business continuity, security governance, compliance, and policy frameworks. Subsequently, interviews with 19 industry experts were conducted to validate the practical significance of these components and to explore how they interact with one another in real-world environments. The result was a detailed visual representation that highlights both direct and indirect key-security indicators. Direct indicators have a measurable impact on the security posture of an organization, while indirect indicators influence security through interconnected pathways. This model serves as a valuable decision-making tool, enabling data security leaders to address core and peripheral factors more effectively and ensure a robust and adaptive security management strategy.

Corresponding Author:

Nattakan Yahattaa,
King Mongkut's University of Technology Thonburi, Thailand.

1. INTRODUCTION

Previously, data security was absolutely a specialized concern and along these lines, specialized representatives were liable for data safety problems inside an association (Willison and Back-house, 2006). The view bombs with regards to a comprehensive and all-encompassing perspective and the general security procedure. Therefore, in the previous days, there was a move from the official innovation master to an administration duty and a more business-centered view ensuring data. These days, safety supervisors are completely mindful to believe and react to data safety problems. Different situations similar to the "Equifax break" had demonstrated the ramifications for the top administration if there should be an occurrence of data security dismisses. There, more than 146 million individual data were taken given an unpatched framework, which was a specialized deficiency. This causes, the organization to dispose of its CEO, CIO, and CSO by the "retirement" of them directly following the penetrate. The technical individual was not influenced.

Further, this goes in showing the administration duty inside acts similar to the German Stock Corporation Act (§91 Section 2) which likewise needs a functioning danger the board inside organizations.

Considering the move from a particular to an organization for each spective, the investigation concentrates moreover altered from packs in a practical setting to examining the organization's work. Executives must have the choice to acknowledge specific threats similarly as various segments like humans lead into a record to take the benefit and reasonable exercises to lighten perils (Coronado et al., 2009).

The study focus shifted from studies in a technical environment to examining the management function as a result of the transition from a technical to management point of view. To take the appropriate and efficient steps to reduce risks, managers need to be able to consider both technical dangers and other elements, such as human behavior. Information security managers must comprehend the intricacy of security of data and have a broad perspective on the subject in order to supply the required funding, make wise decisions, and persuade the organization. There is still a research vacuum in this thorough perspective with particular components and connections between them together with their bearing on an organization's security status. In order to ultimately produce a comprehensive model to comprehend the complexity of information security and, consequently, provide sound information security management decisions, this study aims to identify the important variables, assess them, and investigate mutual dependence.

The remainder of the investigation article is sorted out as given. In segment 2, past work on the board performance and regulatement accomplishment factors in data security is portrayed and the necessity for an expansive data security representation with current insufficiencies is showed up. In Section 3, the three-advance way of thinking which contains the composing study, the literature assessment, and the ace talk with the game plan is shown. In part 4, the surveyed MSFs are given. The MSFs in con-crossing point with beliefs are introduced as a thorough representation in Segment 5. In Segment 6, an essential argument of the outcome and districts for potential assessment is included. An end is specified in Segment7.

2. LITERATURE REVIEW

Dhillon et al. [64] proposed Value-focused assessment of information system security in organizations. For professionals and executives, information system (IS) security remains a concern. The majority of IS vulnerability investigation is technical in nature, giving little thought to organizational and human factors. The research provided in this paper takes a more comprehensive approach and offers an organizational view of IS cybersecurity in terms of people's values. It identifies the "fundamental" goals for IS security and the "means" by which a company might achieve them using the value-focused thinking approach. 103 managers were interviewed in-depth regarding their values in managing IS security in order to gather data for the study. The findings of the interviews point to 86 goals that are crucial for IS security management. Twenty-five clusters comprising nine fundamental and sixteen methods categories comprise the 86 objectives. The study's goals are socio-organizationally based and offer guidance for future IS security measure development. This is a noteworthy addition since earlier studies have acknowledged the need of organizationally grounded principles but have not offered concrete solutions. The results of this study also call into question the generalization of the availability, confidentiality, and integrity principles as the only pillars of security architecture. Organizations place confidentiality, integrity, and availability in the larger context of things. Lastly, the report suggests ways that the results given here could be expanded upon in future studies.

Mishra [65] introduced Organizational objectives for information security governance: a value focused assessment. Developing theoretically supported and empirically developed organizational security governance (OSG) goals is the aim of this work. Given the growing vulnerability resulting from improper or nonexistent controls, businesses have considerable problems when formulating organizational security governance (OSG) objectives. In recent years, there have been numerous reports of businesses incurring massive losses due to inadequate security governance procedures. Cross-comparison and simple interpretation are made possible by the compilation and presentation of the data gathered in Step 1. Step 3: categorize the goals as essential and means for the context of the decision. After grouping the objectives, they are categorized into essential and means. The OSG objectives in this study are developed using a value-focused methodology. It would be easier to connect corporate and individual ideals about OSG if individual values were taken into consideration while creating governance objectives. This study suggests 17 means and 6 key OSG objectives. Based on the values of an organization's stakeholders, the study offers a thorough list of OSG.

3. METHODOLOGY

Developing a detailed representation of considerations for managers on security of data. The above framework of functions is made up of a pair stages. Figure1 sets out the processes. The initial stage is to disco ver the correct composition with the aid of a composing search method defined in Section 3.1. The resulting advance is to look at the overwhelming composition of variables that contain an impact on the results of security of data.

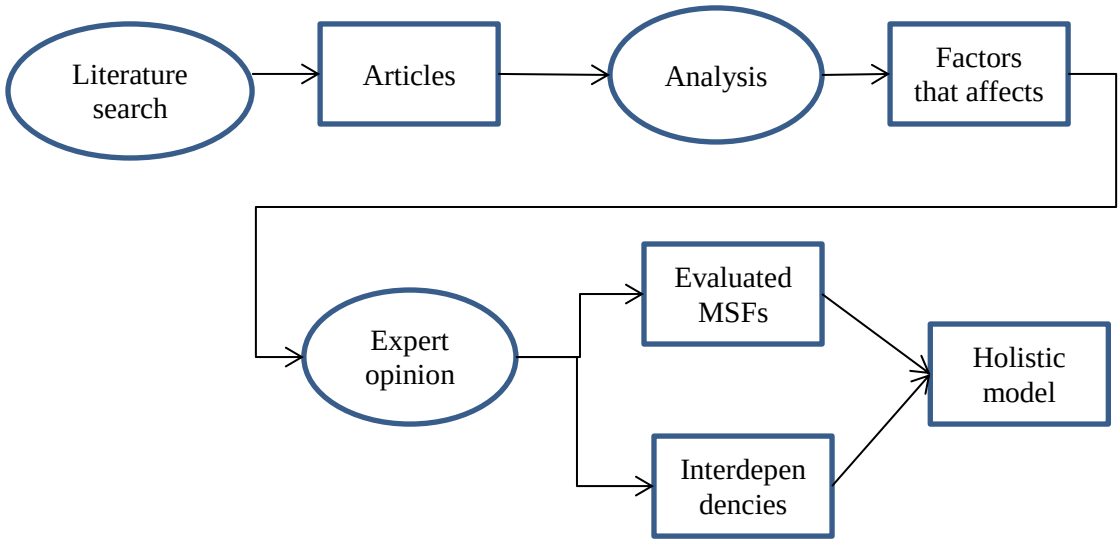

Figure 1. Development of Proposed system

Figure 1 describes the development process of proposed system. Executive executives, who were interviewed individually, selected interviewees who had participated in a certain decision. Since everyone was informed in advance of the topics to be covered, the majority had prepared minutes, memos, and other materials, and many had been in touch with colleagues to confirm points during the interview. 18 broad qualitative questions about the significance of the choice, the primary timeline, the participants, and the advantages or drawbacks resulted were covered in the one maximum of two and a half-hour interviews. Additionally, each interviewee received a questionnaire consisting of 40 items, the majority of which were fixed-choice and derived from previous theory. The responses were previously tested on a small group of MBA learners with work experience, and their language was periodically significantly modified to make them understandable in certain contexts. 53 cases were analyzed after 53 questionnaires and the basic interview were satisfactorily completed. The information provided was not attitudinal or personal. In 24 cases, a second informant also provided the whole data, either to elaborate on certain areas or to allow the most knowledgeable of both participants to be used for the final analysis. Any discrepancies were in the breadth of the information provided, not it's content.

The findings are organized and the influencing elements of the degree made are derivated from the composition. The third phase involves a semi-composed ace discussion to explore the importance of long-term effect factors and the interdependencies of research between them. Results are surveyed and meaningful MSFs are, at the end of the day, identical to those between conditions that achieve the overall MSF model for the pioneers. The definition of the ace talk with the theory. Figure 2 describes the factors model that affects the data safety.

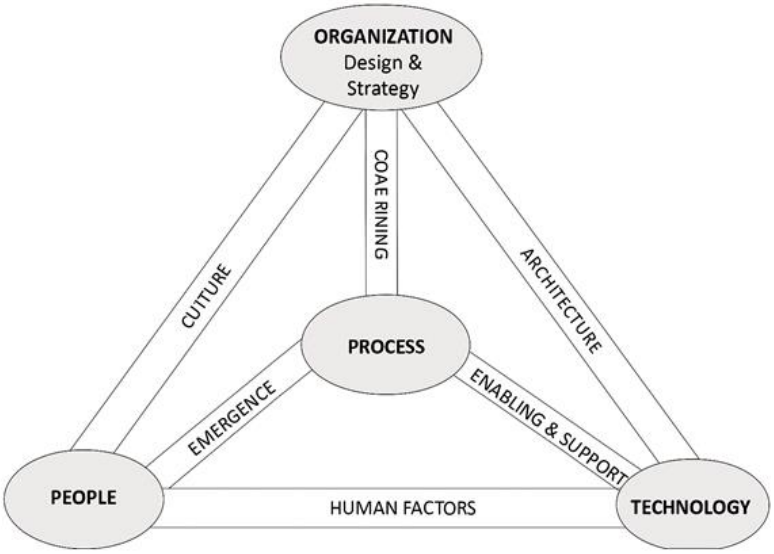

Figure 2. A complete model of the factors that affect data safety

3.1. Literature search

Since the administration writing isn't data In terms of safety, the series of questions found in those diaries were changed in accordance with the first two sections: "(it OR data OR cyber) AND (strength OR security)". Another change was finished via looking only for the title and unique inside data safety particular origins due to the fundamental different point. The choice of pertinent items Depending on the subtitle and concept, a watchword search was conducted out of the previous ones. The counting criterion was that there were references or depictions of elements affecting data security decisions. The investigation was conducted both ahead and backward. enforced to every single chosen article while the forward pursuit depended on the "referred to by" capacity of Google Scholar. The writing recognition strategy brings about a total of 136 pieces.

4. FINDINGS OF MANAGEMENT SUCCESS ASPECTS

The essential MSFs are assessed for a comprehensive model, which influences data security choices. In part 4.1, the aftereffects of the writing examination appear. These are the aspects that have consequences on data security choices from the writing point of view. From that point forward, the components must be assessed and demonstrated for their significance in performs which outcomes in assessed MSFs. These outcomes appear in Section 4.2.

4.1 Factors got from the writing

Approximately 188 first-request identifiers were found after 136 significant papers from the hunt approach were examined. The tuple "factor in writing"-"writer" is a code. Therefore, the unique effect components for each artist were inferred. These codes show up in the accompanying circumstances:

(1) They show up straightforwardly inside the writing. A model is the accompanying "increase the edge effort in other linked metrics, such as people property, organization buildings, international management, regulation structures, awareness initiatives and along these lines give an increasingly point by point outline work". This outcome straightforwardly in the relating rundown of first request codes. The greater part of these immediate codes show up in enumerations inside the presentation or future work segments of them broke down writing and are not additionally clarified. (2) The initial question codes are a part of the hypothesis. The initial question codes are a piece of intuition focused on a hidden suggestion and are used in quantitative or subjective studies. The model research is Kankanhalli et al. (2003), which de-copy the impact of authoritative scale, top management support, and business form on data structure security viability. This model outcomes in comparing first-request codes.

(3) Ultimately within the papers or due to their key value. These manifestations are derivated from the general analysis of the papers or from a few portraits within the material which are not identified by the first request code although the denotation of the name was selected. The article entitled "Structure and acceptance of the data protectionculture system" (AlHogail, 2015) is referred to as "information culture" as a first-request document.

The paradigm for circuit alerts is those companies that possess an asset system for a long time to use these evaluation techniques to authorize the implications of various strategies. And Cross-checking that any major vulnerabilities have not been ignored "(Wood, 1987) which is the" weakness evaluation "as the first request code. Identifying factors of organizational is management is expressed in Table 1.

Table 1. Identifying Factors of Organizational IS Management

MSF	not imp	rather not imp	rather imp	imp
Vulnerability	0	0	6	11
Resources	0	0	6	11
Awareness	1	0	5	11
Access Control	0	1	7	9
Physical Security	1	0	10	6
Infrastructure	0	1	11	5
Risk	0	1	11	5
Continuity	1	1	12	3
Security Management	3	1	7	6
Organizational	3	4	10	1
CIA Triad	7	1	7	2
Compliance & Policy	6	3	6	2

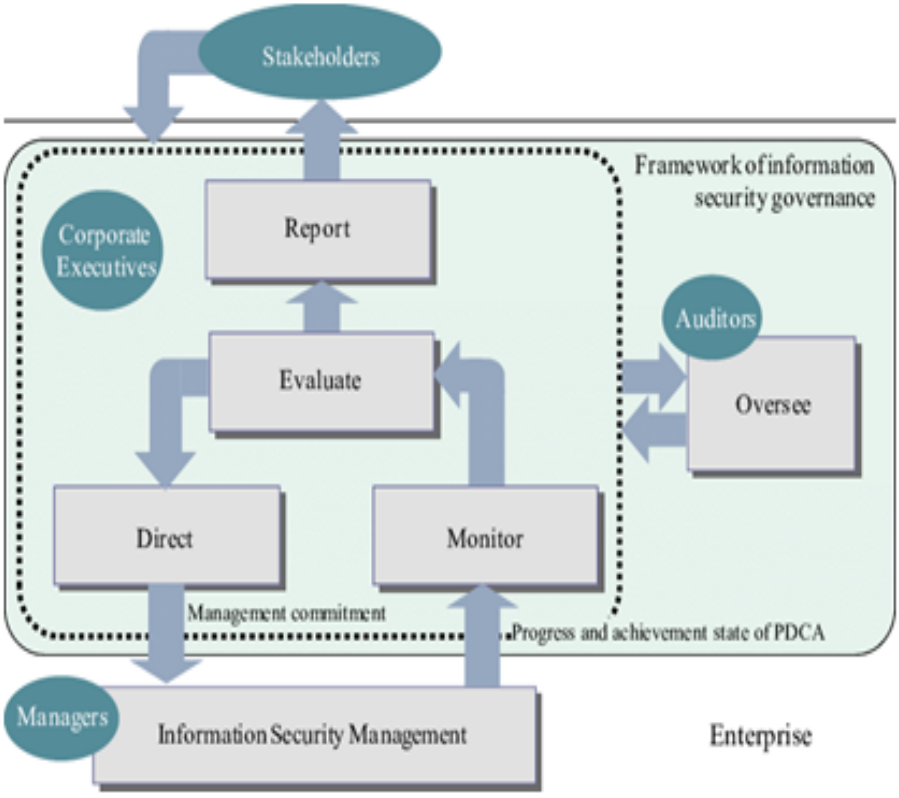

Figure 3. Framework of Information Security Governance

Incomplete parts of individual elements are not secured by the writing or are not considered by information security governance which is represented in Figure 3. Notwithstanding, the substance and the comprehension of the variables from the writing investigation concur with those of the specialists. The difficulties are not upheld by the entirety of the specialists, since this was no unequivocal inquiry. In this

way, they were simply included, if there are multiple notices of a similar test. The difficulties further demonstrate that a thorough representation of them could help in developing the comprehension of in-arrangement protection inside associations and to assist, developing particular factors.

Relevance approval of MSFs

The "valence or force investigation" (Part 3.3) was utilized to approve the components about their substance as well as to stop mine from their significance practically speaking to the data security of an association. Subsequently, the extent of the examination was additionally set to the entire meeting records yet the primary inquiry aiding this approval is Q1.2. The feature's importance for the association's data security is assessed using a 4-point Likert scale. The scale is coded from substantial (devil) to not significant (not demon). Table 2 displays various perspectives on the outcome. The assertion depends on the total of the codings for "not significant" and "rather not significant" related to the aggregate of the code "instead of significant" and "significant", diving by the significance of the MSFs.

Table 2. Categorization of MSFs based on nature

Category	MSFs Included	Description
Technical	Infrastructure, Access Control, Risk	Tangible, system-based security measures
Human-centric	Awareness, Resources, Management Support	Soft factors impacting human behavior and involvement
Organizational	Continuity, Compliance & Policy, CIA	Structural or procedural elements impacting decision-making

This outcome assistance, that's all components are significant practically speaking. "Consistency and Policy," "CIA," and "Authoritative components" are the final three components. Each of them has an explanation from the experts as to why it is less important than other variables. In order to comply with the legislation, "consistency and strategy" are crucial, but they have no bearing on the association's data security, uphold defensive measures, as well as to modify the association's top management. The "CIA" element is an objective characteristic that is useful for communicating and elucidating different threats or attacks and their consequences. "Regulatory elements" are less important because, while they can be important in some situations, they can also be insignificant in other attack circumstances. To make wise decisions, the administration must take into account every factor. The suggested elements are legitimate in their set just as applicable by and by for chiefs and hence are currently called administration achievement factors (MSFs).

4.2 Control inquiries

Most specialists (12) don't have a factor, which is extremely irrelevant. The main notices of variables were the "Consistency and Policy" just as "CIA" which concur with the positioning on the past outcome. The topic of missing elements brings about a comparative circumstance like previously. 10 specialists don't refer to missing components. Different variables missing are "the executives support", "outer interfaces", "danger scene" and "system" which are a piece of the coding and therefore remembered for the total of the writing investigation.

5. DISCUSSION AND FUTURE WORK

The results of this analysis offer data security chiefs a comprehensive model of MSFs and how they interact. Assumed to be reliant on the writing, the MSFs are evaluated by trained specialists. Additionally, these gatherings strengthen the MSFs' interconnections. The combination of these results progresses the full MSFs concept. Professionals, just as the writing, expressed the requirement for an extensive perspective on the data security of associations.

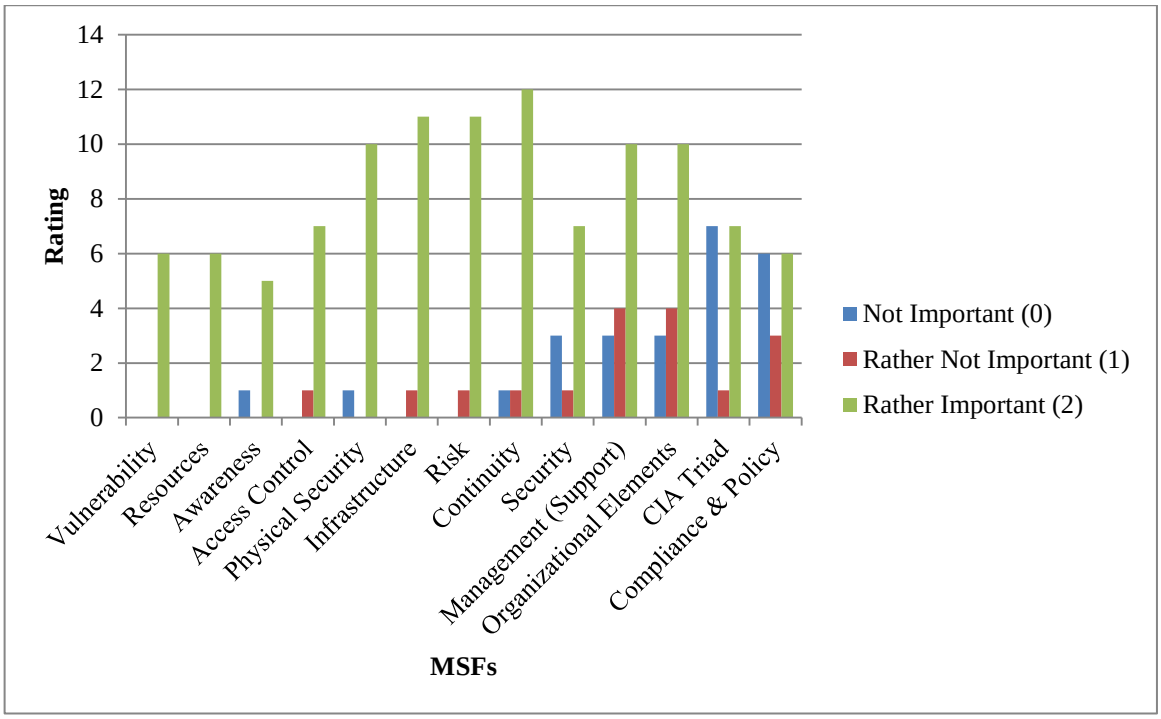

Figure 4. Importance Ratings of each MSF

Figure 4 visualizes how experts evaluated the importance of each Management Success Factor (MSF) using a 4-point Likert scale. The graph is based on data collected from 19 industry experts during interviews and follow-up surveys. It shows that Vulnerability, Resources, Awareness, Access Control, and Physical Security received the highest ratings in terms of practical importance for data security decision-making.The suggested model supports a broad and theoretical viewpoint on the complex topic of security of data from an administrative perspective. Although the many MSFs are not explained in great length, this analysis does provide information on their interdependencies as well as the general dynamic procedure. The concept provides leaders with a foundation that helps them decide whether specific countermeasures are necessary or even beneficial when it comes to data security. It is not just a cause for security managers, but also for executives and other professional representatives of the company. This model might help them comprehend the issues and better recall specific decisions. A superior seeing likewise prompts better arrangement and mindfulness.

The findings include a range of open doors for potential analysis. The proposed model relies on the interdependencies discussed in a subjective study. Also, interdependencies will be discussed in quantitative ways to guarantee their effectiveness. Table 3 gives summary of interview insight.

Table 3. Summary of interview insight

Expert ID	Most Critical MSF	Least Relevant MSF	Notable Quotes/Summary Notes
Expert 01	Awareness	CIA	“Without awareness, no control is effective.”
Expert 05	Vulnerability	Compliance & Policy	“Policies help but don’t stop insider threats.”
Expert 12	Access Control	Management Support	“We lack tools to enforce what the leadership asks.”

Such MSFs have been grouped into square shapes. There may be interdependencies between those having MSFs at a deeper stage, which is not discussed in this study. Similarly, looking deeper into any of the proposed MSFs would be an opportunity for potential analysis. The accessible review of past writing may be approached with an increasingly concentrated approach centered on these outcomes.

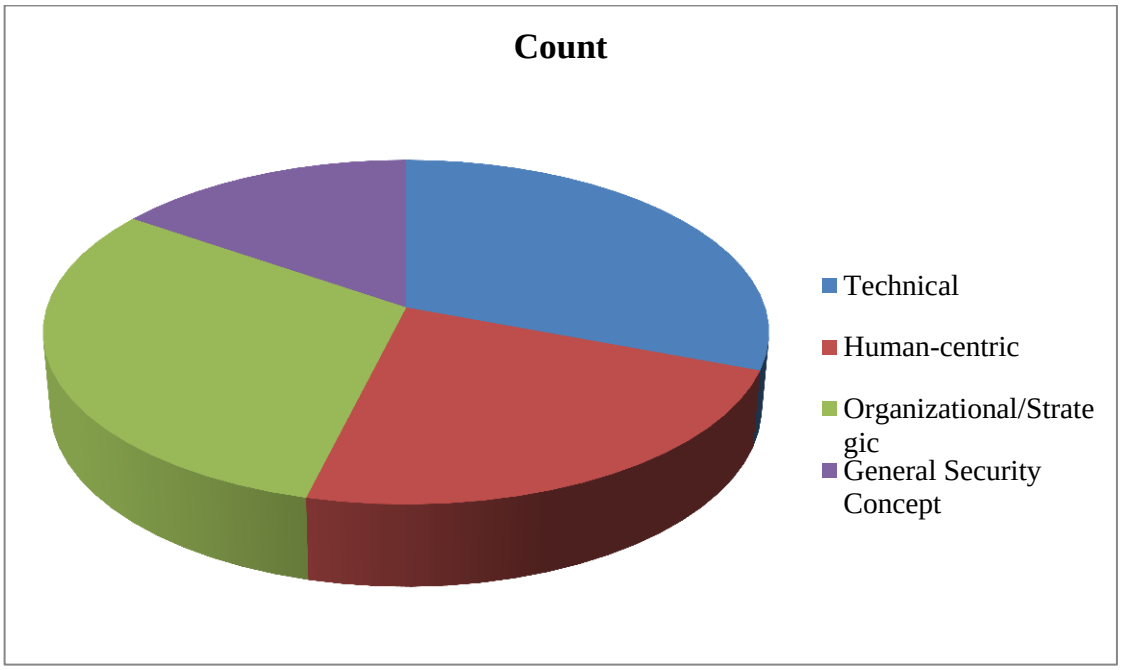

Figure 5. Categorization of MSFs by type

Figure 5 demonstrate the interdisciplinary nature of IS decision-making and the need for holistic consideration across technical, human, and structural dimensions. Data security supervisors ought to think the entire investigated MSFs by considering choices. The values and procedures ought not exclusively to be embraced as a result of the shape in best practices and recommendations, but they should be appropriate for the situation at hand. Another common technique is the default to chance recognition (Bayuk, 2013), which is not only challenging to implement but also does not raise the security grade in any way. The results of this investigation promote comprehension of the astounding topic of data security and enable more individuals to settle on fitting choices and take the correct activities inside their present circumstances.

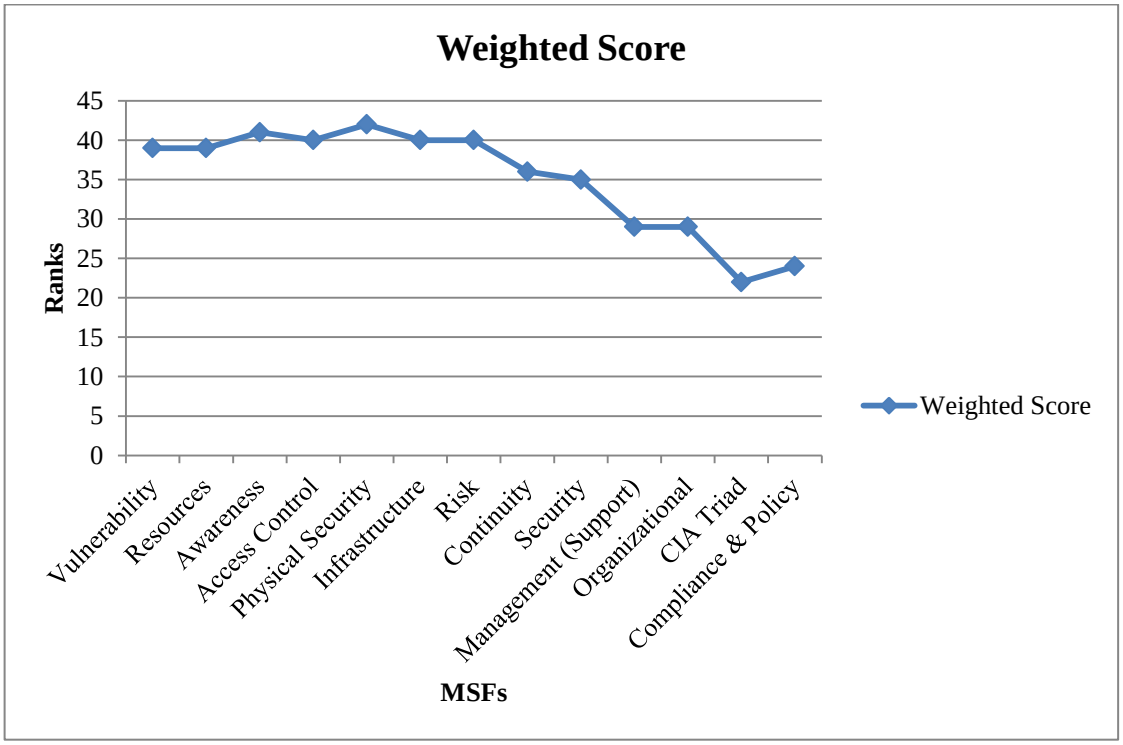

Figure 6. MSFs Ranked by Total Perceived Importance Score

Figure 6 assigns scores to each MSF based on expert feedback using weighted values (0 = Not Important, 3 = Important). It provides a ranked order of MSFs by total weighted scores, reflecting which factors should be prioritized in policy and planning. The comprehensive evaluation and triangulation of literature findings, expert interviews, and factor validation have culminated in a set of twelve Management Success Factors (MSFs) that critically influence data security decision-making. The categorized MSFs span across technical (Infrastructure, Access Control, Risk), human-centric (Awareness, Resources, Management Support), and organizational (Continuity, Compliance & Policy, CIA) dimensions, demonstrating the multidimensional nature of information security management.

The importance of each MSF was validated through qualitative and quantitative measures using Likert-scale analysis and expert consensus. This reinforces the practical relevance of the identified MSFs and their capacity to guide security governance strategies. While some factors like "CIA" and "Compliance & Policy" were deemed relatively less impactful in isolation, their strategic role within broader organizational frameworks remains vital.

Overall, the results emphasize the necessity for a holistic, integrative model that not only identifies but also explains the interdependence of these success factors. This model equips security managers and decision-makers with actionable insights for developing adaptive and context-sensitive information security policies.

6. CONCLUSION

This examination is proposing a complete model of the executive's achievement factors (MSFs) for data security leaders. Consequently, a writing examination with an open-pivotal particular methodology of 136 publications are used to identify the elements that impact chiefs' decisions on data security. These features were approved, and their significance was confirmed by organizing a meeting with 19 training specialists resulting in 12 MSFs. The purpose of the sessions is to examine the connections among the MSFs in order to ultimately construct the comprehensive model. In order to determine the elements that impact managers' judgments on information security, 136 articles are analyzed using an open-axial-selective methodology. A series of interviews with 19 practice-based specialists was conducted to validate these parameters and assess their applicability. There are 12 MSFs as a result. The interviews serve as the foundation for examining the interdependencies among the MSFs in order to ultimately construct the comprehensive model. This exploration offers an elevated level perspective on the mind-boggling subject of data security dynamic from security the board specialists. The thorough model of MSFs causes them and different workers just as the business the executives to all the more likely comprehend the security requirements and unique decisions in this particular circumstance, and so enhance their awareness. Future developments in objectively organized metrics and methods to assess the state of data security, as well as methods to sum them up based on the most important security guidelines, are both intriguing to researchers and professionals.

REFERENCES

[1] Abu-Musa, A., 2010. Information security governance in Saudi organizations: an empirical study. Inf. Manag. Comput. Secure. 18(4), 226–276. DOI:10.1108/09685221011079180.

[2] AIS Members, 2011. Senior scholars' basket of journals. URL: https://aisnet.org/page/ SeniorScholarBasket Last checked: 04.12.2018.

[3] Alavi, R., Islam, S., Mouratidis, H., 2016. An information security risk-driven investment model for analyzing human factors. Inf. Comput. Secure. 24(2), 205–227. doi:10.1108/ICS-01-2016-0006.

[4] AlHogail, A., 2015. Design and validation of information security culture framework. Comput. Human Behav. 49, 567–575. doi:10.1016/j.chb.2015.03.054.

[5] Alqahtani, A., 2015. Towards a framework for the potential cyber-terrorist threat to critical national infrastructure. Inf. Comput. Secur. 23(5), 532–569. doi:10.1108/ICS-09-2014-0060.

[6] Anderson, R., Moore, T., 2006. The economics of information security. Science (New York, N.Y.) 314, 610–613. doi:10.1126/science.1130992.

[7] Arora, A., Krishnan, R., Telang, R., Yang, Y., 2010. An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. Inf. Syst. Res. 21(1), 115–132. doi:10.1287/isre.1080.0226.

[8] Ashenden, D., 2008. Information security management: a human challenge? Inf. Se- cur. Tech. Rep. 13(4), 195–201. doi:10.1016/j.istr.2008.10.006.

[9] Atoum, I., Otoom, A., Abu Ali, A., 2014. A holistic cyber security implemen- tation framework. Inf. Manag. Comput. Secur. 22(3), 251–264. doi:10.1108/IMCS-02-2013-0014.
[10] Azuwa, M.P., Sahib, S., Shamsuddin, S., 2017. Technical security metrics model in compliance with iso/iec 27001 standard. Int. J. Cyber- Secur. Digital Forens. (IJCSDF) 1(4), 280–288.
[11] Bayuk, J., Mostashari, A., 2013. Measuring systems security. Syst. Eng. 16(1), 1–14. doi:10.1002/sys.21211.
[12] Bayuk, J.L., 2013. Security as a theoretical attribute construct. Comput. Secur. 37, 155–175. doi:10.1016/j.cose.2013.03.006.
[13] Ben-Aissa, A., Abercrombie, R.K., Sheldon, F.T., Mili, A., 2012. Defining and comput- ing a value based cyber-security measure. Inf. Syst. e-Business Manag. 10(4), 433–453. doi:10.1007/s10257-011-0177-1.
[14] Beresnevichiene, Y., Pym, D., Shiu, S., 2010. Decision support for systems security in- vestment. In: 2010 IEEE/IFIP Network Operations and Management Symposium workshops, pp. 118–125. doi:10.1109/NOMSW.2010.5486590.
[15] Bernard, T. S., Cowley, S., 2017. Equifax breach caused by lone employee's er- ror, former c.e.o. says. URL: https://www.nytimes.com/2017/10/03/business/ equifax-congress-data-breach:html, Last checked: 01.12.2018.
[16] Björck, F., Henkel, M., Stirna, J., Zdravkovic, J., 2015. Cyber resilience – fundamentals for a definition. In: Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P. (Eds.), New Contributions in Information Systems and Technologies. In: Advances in Intel-ligent Systems and Computing, 353. Springer International Publishing, Cham, pp. 311–316. doi:10.1007/978-3-319-16486-1_31.
[17] Boehm, J., Merrath, P., Poppensieker, T., Riemenschnitter, R., Stähle, T., 2017. Cyber risk measurement and the holistic cybersecurity approach. URL: https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk- measurement-and-the-holistic-cybersecurity- approach Last checked: 03.12.2018.
[18] Bogner, A., Littig, B., Menz, W., 2014. Interviews mit Experten: Eine praxisorientierte Einführung. Qualitative Sozialforschung. Springer Fachmedien Wiesbaden.
[19] Bortz, J., Döring, N., 1995. Forschungsmethoden und Evaluation. Springer-Lehrbuch, Springer Berlin Heidelberg.
[20] Boyer, W., McQueen, M., 2007. Ideal based cyber security technical metrics for control systems. In: Critical information infrastructures security, pp. 246–260. doi:10.1007/978-3-540- 89173-421.
[21] Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. A model for evaluating it security investments. Commun. ACM, 47(7), 87–92. doi:10.1145/1005817.1005828.
[22] Chai, S., Kim, M., Rao, H.R., 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. Decis. Support Syst. 50 (4), 651– 661. doi:10.1016/j.dss.2010.08.017.
[23] Cisco Systems Inc., 2018. Cisco 2018: annual cybersecurity report. Technical Report. Cisco Systems Inc.
[24] Collier, Z.A., Panwar, M., Ganin, A.A., Kott, A., Linkov, I., 2016. Security metrics in industrial control systems. In: Colbert, E.J.M., Kott, A. (Eds.), Cyber-Security of SCADA and Other Industrial Control Systems. In: Advances in Information Secu- rity. Springer, Switzerland, pp. 167–185. doi:10.1007/978-3- 319-32125-7_9.
[25] Corbin, J., Strauss, A., 1990. Grounded theory research: procedures, canons and evaluative criteria. Zeitschrift für Soziologie 19(6), 418–427 doi:10.1515/zfsoz-1990-0602.
[26] Coronado, A.S., Mahmood, M.A., Pahnila, S., Luciano, E.M., 2009. Measuring effec- tiveness of information systems security: an empirical research. In: 15th Amer- icas Conference on Information Systems, pp. 282–290.
[27] Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101. doi:10.1016/j.cose.2012.09.010.
[28] DeLone, W.H., McLean, E.R., 1992. Information systems success: the quest for the dependent variable. Inf. Syst. Res. 3(1), 60–95. doi:10.1287/isre.3.1.60.
[29] Dhillon, G., Torkzadeh, G., 2006. Value- focused assessment of information system security in organizations. Inf. Syst. J. 16(3), 293–314. doi:10.1111/j.1365-2575. 2006.00219.x.
[30] Diesch, R., Pfaff, M., Krcmar, H., 2018. Prerequisite to measure information secu- rity: a state of the art literature review. In: 4th International Conference on Information Systems Security and Privacy (ICISSP), pp. 207–215. doi:10.5220/ 0006545602070215.
[31] Dinev, T., Goo, J., Hu, Q., Nam, K., 2009. User behaviour towards protective infor- mation technologies: the role of national cultural differences. Inf. Syst. J. 19(4), 391–412. doi:10.1111/j.1365-2575.2007.00289.x.

[32] Dinev, T., Hu, Q., 2007. The centrality of awareness in the formation of user behav- ioral intention toward protective information technologies. J. Assoc. Inf. Syst. 8(7), 386–408.
[33] Dogaheh, M.A., 2010. Introducing a framework for security measurements. In: IEEE International Conference on Information Theory and Information Security, pp. 638–641. doi:10.1109/ICITIS.2010.5689505.
[34] Dzazali, S., Sulaiman, A., Zolait, A.H., 2009. Information security landscape and ma- turity level: case study of malaysian public service (mps) organizations. Gov. Inf. Q. 26(4), 584–593. doi:10.1016/j.giq.2009.04.004.
[35] Ernest Chang, S., Ho, C.B., 2006. Organizational factors to the effectiveness of im- plementing information security management. Indus. Manag. Data Syst. 106(3), 345–361. doi:10.1108/02635570610653498.
[36] Fenz, S., Heurix, J., Neubauer, T., Pechstein, F., 2014. Current challenges in information security risk management. Inf. Manag. Comput. Secur. 22(5), 410–430. doi:10.1108/IMCS-07- 2013-0053.
[37] Fenz, S., Neubauer, T., Accorsi, R., Koslowski, T., 2013. Forisk: formalizing information security risk and compliance management. In: 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop, pp. 1–4. doi:10.1109/DSNW. 2013.6615533.
[38] Gao, X., Zhong, W., 2015. Information security investment for competitive firms with hacker behavior and security requirements. Annal. Oper. Res. 235(1), 277–300. doi:10.1007/s10479-015-1925-2.
[39] Geer, D., Hoo, K.S., Jaquith, A., 2003. Information security: why the future belongs to the quants. IEEE Secur. Privacy Mag. 1(4), 24–32. doi:10.1109/MSECP.2003.1219053.
[40] Glaser, B.G., Strauss, A.L., 1967. The discovery of grounded theory: strategies for qualitative research. AldineTransaction, New Brunswick.
[41] Goel, S., Chengalur-Smith, I.N., 2010. Metrics for characterizing the form of security policies.J. Strategic Inf. Syst. 19(4), 281–295. doi:10.1016/j.jsis.2010.10.002.
[42] Goldstein, J., Chernobai, A., Benaroch, M., 2011. An event study analysis of the eco- nomic impact of it operational risk and its subcategories. J. Assoc. Inf. Syst. 11(9), 606–631.
[43] Gonzalez, J.J., Sawicka, A., 2002. A framework for human factors in information se- curity. In: 2002 WSEAS International Conference on Information Security, Hard- ware/Software Codesign, E-Commerce and Computer Networks, pp. 1871–1877.
[44] Gosavi, H.R., Bagade, A.M., 2015. A review on zero day attack safety using different scenarios. Eur. J. Adv. Eng. Technol. 2(1), 30–34.
[45] Gupta, A., Hammond, R., 2005. Information systems security issues and decisions for small businesses. Inf. Manag. Comput. Secur. 13(4), 297–310. doi:10.1108/09685220510614425.
[46] Hajdarevic, K., Allen, P., 2013. A new method for the identification of proactive in- formation security management system metrics. In: 36th International Conven- tion on Information & Communication Technology, Electronics & Microelectron- ics, pp. 1121–1126.
[47] Hajdarevic, K., Pattinson, C., Kozaric, K., Hadzic, A., 2012. Information security mea- surement infrastructure for kpi visualization. In: Proceedings of the 35th Inter- national Convention MIPRO, pp. 1543–1548.
[48] Hall, J.H., Sarkani, S., Mazzuchi, T.A., 2011. Impacts of organizational capabilities in information security. Inf. Manag. Comput. Secur. 19(3), 155–176. doi:10.1108/09685221111153546.
[49] Hayden, L., 2010. IT security metrics: a practical framework for measuring security & protecting data. McGraw Hill, New York.
[50] Hedström, K., Kolkowska, E., Karlsson, F., Allen, J.P., 2011. Value conflicts for infor- mation security management. J. Strateg. Inf. Syst. 20(4), 373–384. doi:10.1016/ j.jsis.2011.06.001.
[51] Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, H.R., 2014. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Inf. Syst. J. 24(1), 61–84. doi:10.1111/j.1365-2575.2012. 00420.x.
[52] Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125. doi:10.1057/ejis.2009.6.
[53] Herrera, S., 2005. Information security management metrics development. In: 39th Annual 2005 International Carnahan Conference on Security Technology, pp. 51–56. doi:10.1109/CCST.2005.1594818.
[54] Herzog, A., Shahmehri, N., Duma, C., 2007. An ontology of information security. Int.J. Inf. Secur. Privacy 1(4), 1–23. doi:10.4018/jisp.2007100101.
[55] Holm, H., Afridi, K.K., 2015. An expert-based investigation of the common vulnera- bility scoring system. Comput. Secur. 53, 18–30. doi:10.1016/j.cose.2015.04.012.

[56] Höne, K., Eloff, J., 2002. Information security policy — what do international in- formation security standards say? Comput. Secur. 21(5), 402–409. doi:10.1016/ S0167-4048(02)00504-7.
[57] Hong, K.-S., Chi, Y.-P., Chao, L.R., Tang, J.- H., 2003. An integrated system theory of information security management. Inf. Manag. Comput. Secur. 11(5), 243–248. doi:10.1108/09685220310500153.
[58] Horne, C.A., Maynard, S.B., Ahmad, A., 2017. Information security strategy in organi- sations: review, discussion and future research. Aust. J. Inf. Syst. 21. doi:10.3127/ ajis.v21i0.1427.
[59] Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.
[60] Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. Information & Computer Security, 23(2), 122-144.