Making ROSI More Human

An Alternative Theoretical Model for Calculating Returns on Security Investments

By

Fabian Muhly[1,2]

[1]Leo & Muhly Cyber Advisory, Wettswil, Switzerland
[2]School of Criminal Sciences, University of Lausanne, Batochime, Lausanne, Switzerland

Abstract

Purpose – The purpose of this paper is to derive an alternative theoretical model for calculating return on security investments (ROSI) from a more generalist perspective. Effective information security (IS) measures are becoming increasingly vital for the security of an organization, but they are also reflecting liabilities in the financial statements. Senior decision makers should therefore be able to evaluate expected returns as complete as possible to secure the health of the organization. The researcher believes that current ROSI frameworks are incomplete to do so.

Approach – An idealistic approach is used to derive an alternative theoretical ROSI model that puts security as the most important return of security investments in the center of the discussion.

Findings – ROSI is not a one time, and one size fits all indicator, but is a function of technical and human aspects of IS that need to be addressed separately and continuously.

Orginality/value – The author presents a novel approach to calculate ROSI and demonstrates in a theoretical model the importance of the human factor for the calculation of an effective security investment decision-support tool.

Keywords: Return on Security Investment (ROSI), Human Factor, Information Security, Theoretical Model, Decision-Making, Financial Indicator

1. Introduction

Financial indicators guide senior management and accountable personnel in their future decisions. From performance indicators to forecast and planning indicators, they are key tools to help leaders defining and executing the strategic goals of the organization. Return on security investment (ROSI) calculations support senior management in information security (IS) investment decisions (Sonnenreich, 2006). Proper information security (IS) policies and procedures in an organizational setting are vital to guarantee the confidentiality, integrity and availability of a company's data and information no matter its degree of criticalness (von Solms, 2001; Posthumus and von Solms, 2004). Different industry reports illustrate the importance of IS systems and the associated threats for organizations without intact and sufficient procedures. In a report by IBM (2020) it is said that the average cost per data breach for companies was $3.86 million and that the average lifecycle of a breach took 280 days from identification to containment. Not only do these numbers show that breaches are costly in pure direct financial terms, they also claim company resources for a significant period. Time, that would have been otherwise available for engagements that are more profitable. Even worse, data breaches increased by 67% since 2014 and by 11% since 2018, according to Accenture (2019).

Although IS threats are dependent on specific conditions and differ in type or extent, they are independent from geographical location or the industry you find yourself in (Yeh, and Chang, 2007; Kam *et al.*, 2020; Srivastava *et al.*, 2020). Research argues that appropriate IS management and strategies have to be as holistic as possible (Soomro *et al.*, 2016), so should be security investments. Investments in technical security measures are highly important, necessary but not sufficient. A critical mass of threats specifically targets the human dimension (Proofpoint, 2019). Incidents like the 2020 Twitter hack or spear phishing campaigns specifically required humans to interact with the malevolent attacker (Thompson & Barrett, 2020; Kwak *et al.*, 2020). However, the increase in ransomware attacks and corresponding malware campaigns show that IS needs both, technical security appliances, as well as knowledgeable and alert end users. Breaches like the ones mentioned before may otherwise become rather the rule than the more favored exception.

The impact of such IS breaches on companies is manifold. Besides directly suffering the loss of even critical or confidential data and information, with sometimes long data recovery times or no recovery at all, organizations face financial losses (Garg *et al.*, 2003; Arcuri *et al.*, 2017) and reputational damage (Sinanaj & Muntermann, 2013; Sinanaj *et al.*, 2015; Confente *et al.*, 2019). There is even evidence that suffering IS breaches will have negative impacts on the organization's market share and leads to competition effects with market power being moved to competitors of breached firms (Jeong *et al.*, 2019). It goes therefore without saying that investments in IS are a reasonable and logical step taken by IS practitioners to retain not only the confidentiality, integrity and availability of corporate information, but also to safeguard the organization's tangible and intangible value.

The investments in solutions that prevent information from unauthorized access or getting lost is therefore an important task pursued by security professionals in a countless amount of organizations. However, security professionals often have to engage with superior stakeholders that eventually take the investment decision. Approaches that make returns in security investments tangible are therefore a thankful tool for security professionals to engage with their strategic risk decision-making counterparts.

The concept of measuring ROSI has been introduced almost two decades ago (Al-Humaigani & Dunn, 2003; Sonnenreich, 2006) in a quantitative model, which is similar in its purpose to the return on investment (ROI) indicator in Finance. In the following sections, we will present its concept and relevant academic contributions before providing a theoretical model that tries to address the lack of the human factor as a critical variable to be respected whenever security investments shall lead to effective returns.

2. The ROSI model

Decisions about the reasonableness of future investments are typically supported by (ROI) calculations. The reasonableness of investment decisions that center around outpayments with the intention to generate information security are more frequently measured by the ROSI indicator. It is a strategic and leadership metric that helps to bring IS issues to the attention of senior management and boards (Anu, 2021) and, moreover, guides as a decision-making tool. Since its formal introduction at the beginning of the century (Al-Humaigani and Dunn, 2003; Sonnenreich, 2006), the concept has gained more and more traction in organizations as a helpful tool to guide security investment decisions, and among scholars in discussing the appropriateness of the indicator effectively measuring the returns of security investments.

Brocke *et al.* (2007) argue, similar like this article does, that existing approaches to calculate the ROSI figure do lack a proficient methodological basis to reasonably support the respective responsible persons in their decision-making process. The authors say that current methodological approaches are only taking into account direct costs of security breaches and investments. Moreover, such approaches present an isolated view of only one period, which is a misleading indicator. Security investment decisions rather induce long-term consequences that sometimes do not materialize when, for instance, specific security solutions have to be developed first. Additionally, they mitigate costs of greater extent than the pure loss of data or information. Security investments also safeguard intangible organizational assets. Brocke *et al.* (2007) argue that ROSI should be based on capital budgeting instead to provide sufficient decision support.

In a rather recent study, Yaqoob *et al.* (2019) screened the literature for different frameworks calculating the return on security investments and analyzed the used methodologies before presenting yet another framework themselves. Previous ROSI frameworks use risk assessments (ENISA, 2018), cost-benefit analysis (Butler, 2002; Sonnenreich, 2006), return on attack (Cremonini *et al.*, 2005), game theory (Don, 2007; Fielder *et al.*, 2016), Fibonacci sequence (Pontes, 2011), attack trees (Bistarelli, 2012), countermeasure impact analysis (Gonzalez-Granadillo *et al.*, 2014) or classical economic analysis (Huang *et al.*, 2014). Yaqoob et al. (2019) however try to improve the ROSI indicator by proposing a six stages ROSI framework based on cost-benefit analysis.

The vast amount of available frameworks for calculating ROSI that has evolved over time shows that there is neither a single, *one size fits all*, concept that universally operates under the same methodological umbrella, nor is it a simplistic approach to look for such an umbrella that safely guides senior management personnel through security investment decision processes. This article is not an approach to solve the issue, but rather a thought-provoking theoretical attempt to look at ROSI from a more general perspective and probably initiate a discussion around the concept of ROSI beyond the choice of the methodologically most promising approach. Interestingly, the criticism of Brocke *et al.* (2007) seems not to have received large attention in the different frameworks proposed since then. Especially the fact that ROSI frameworks should respect more than only direct costs seems not yet to be addressed. However, Yaqoob *et al.* (2019) respected periodic security investment decisions in their proposed framework. Moreover, they reflect that ROSI is rather defined by the sum of various security investments. Thus, they account for a conclusion that was already mentioned by Lockstep Consulting (2004). In their ROSI calculation guide for government agencies they highlight that ROSI models usually did not separate among different security investments that however all contribute to the overall cost-benefit of information security approaches.

3. An alternative theoretical model

Security and vulnerability

The previous section has provided a brief introduction into the various approaches in calculating an indicator that measures the likely reasonableness of investments in IS. Approaches using risk assessments, cost-benefit analyses of the like are all valid in their existence. In this section, the author will however, take on a stance that rather focuses on a more general perspective on how returns on security investments can and probably should be expressed in order to provide a set-up as holistic as possible and thus leave senior manager best informed in their decision-making process.

Returns on security investments can be expressed in terms of a mitigated likely loss in a cost-benefit approach (Butler, 2002; Sonnenreich, 2006) or on a capital budgeting basis (Brocke *et al,* 2007), amongst others. On a more theoretical basis, however, IS investments should and have to return *security* at first place, independent from how security is translated into business figures. Security practitioners and accountable management would probably agree with such a statement. It is reasonable to materialize security in terms of money not lost, or capital not lost, or risk mitigated. However, from a general point of view, security investments should return security independent of how it will be measured on a more specific level. When we take on this idealistic approach, we can write this consideration the following:

$$ROSI = Security \tag{1}$$

In case security investments do not return the envisaged security, the organization will remain with the specific vulnerability that was meant to be patched. Thus, the invers of security is vulnerability, such that investments that do not patch vulnerabilities will not return security. Equations (2) – (4) account for this theoretical consideration:

$$Security \neq Vulnerability \tag{2}$$

with the invers being

$$Security = 1 - Vulnerability \tag{3}$$

leading to

$$ROSI = 1 - Vulnerability \tag{4}$$

Any return on security investments can therefore be seen as patching vulnerabilities to achieve a desired maximum level of security, with diminishing returns on security, the farther away a security investment is from completely patching a vulnerability. Thus, the question that comes to mind is: What does it take to completely patch a vulnerability and achieve a maximum level of return on the respective security investment? The answer to this question may be manifold and dependent on the specific vulnerability on a detailed level. However, once this consideration is abstracted on a more general level, we see that for a security investment leading to a maximum return on security, namely complete security, vulnerability needs to be 0 in the equation. To further define how this can be possible, we first need to know what defines vulnerability. In this regard, we define an IS vulnerability as a *risk exposure* (Sonnenreich, 2006) to the organization. IS vulnerabilities present a specific risk to the organization. The risk exposure for the organization, which refers to the materialization of the vulnerability (Vul) is defined by the impact (I) it would have on the organization multiplied by the probability of occurrence (P), such that (5) and (6) read:

$$Risk\ Exposure = I * P \tag{5}$$

implying that vulnerability (Vul) is a function of I and P

$$Vul\ (I,P) = I * P \tag{6}$$

From (6) we see that a maximum return on security investments is given when either the possible impact has been mitigated to 0 or the probability of a risk event taking place has been mitigated to 0. Then, and only then, a security investment returns full level security against the respective vulnerability. Thus, any investment in a security solution (S) should eliminate either the impact or the probability of occurrence of a vulnerability, such that for ultimate return on security:

$$Vul\ (I,P) - S\ (I,P) = 0 \tag{7}$$

implying that

$$(I - S(I)) * (P - S(P)) = 0 \tag{8}$$

and eventually leading to

$$ROSI(I,P) = 1 - [(I - S(I)) * (P - S(P))] \tag{9}$$

Hence, the indicator that illustrates the rate of return of security investments is defined by the degree of security investments, S(I) and S(P), reducing the degree of vulnerability and simultaneously increasing the degree of security, whereas for ineffective security investments

$$ROSI = 0 \tag{10}$$

and for effective security investments, leading to ultimate security

$$ROSI = 1 \tag{11}$$

Any figure in between 0 and 1 indicates incomplete security with investments closer to 1 to be favored over those closer to 0. In other words, *ROSI* is increasing in the effectiveness of security investments that patch vulnerabilities, with the highest rate of return, when security is as high as possible and vulnerability as low as possible.

Finally, these theoretical considerations of an alternative model for ROSI should also integrate the findings and applications from previous studies. IS investments are neither a once in a lifetime nor a one size fits all investment. It is, on the contrary, necessary to place security solutions on every single IS vulnerability with the specific investments involved. Further, vulnerabilities are changing and evolving continuously over time. Thus, periodic investment in

security solutions is imperative. An indicator that tries to illustrate the rate of return of those IS investments therefore has to take this into account as well, such that for an organization wide ROSI indicator the equation would read the following:

$$\sum_{i,j=1}^{n} ROSI_{i,j}(I,P) = 1 - [(I_{i,j} - S_{i,j}(I)) * (P_{i,j} - S_{i,j}(P))] \quad (12)$$

whereas different periods of security investments are respected by

$$i = 1 \rightarrow n \quad (13)$$

and different types of vulnerability solutions

$$j = 1 \rightarrow n \quad (14)$$

Equation (12) illustrates an indicator that is rather focused on the effectiveness of specific information security investments with the rate of return representing the level of security induced by specific investments. This model rather takes on a more generalized and idealistic approach. It rather follows a similar vein as introduced by Gonzalez-Granadillo *et al.* (2014), than other ROSI models that have been discussed in the literature presented in section 2. Equation (12) already illustrates that IS as derived by any investment in it is not a stable unidimensional construct. IS has many different facets instead and is in the need of continuous periodically improvement. IS has to be subject to a manifold, holistic agenda of security solutions that patches as many vulnerabilities as possible. The following subsection takes these considerations a step further.

The human factor

IS vulnerabilities and solutions are diverse and continuously changing. An indicator for measuring the return of the investments in these solutions has to be as complete as possible to account for these conditions. Both, vulnerabilities and IS solutions underly those conditions, which are more or less stable in their occurrence and application. Kraemer *et al.* (2009), for example, show that besides technical, IS vulnerabilities are also caused by the human and organizational dimension. IS solutions need to account for those categories as well when it is intended to effectively eliminate either vulnerability. One can argue that (12) already accounts for different types of vulnerabilities with *j = 1 to n.* The article, however, proposes to separate the categories in the equation, whereas it is hypothesized that the technical part is a rather fix component and the human part a more variable one. Hence, *ROSI* is a function of technical and human vulnerabilities and the respective IS solutions to it:

$$\sum_{i,j=1}^{n} ROSI(t,h)_{i,j} = 1 - [(\left(I(t)_{i,j} - S(t)_{i,j}(I)\right) * \left(P(t)_{i,j} - S(t)_{i,j}(P)\right)) * ((I(h)_{i,j} - S(h)_{i,j}(I)) * (P(h)_{i,j} - S(h)_{i,j}(P)))] \quad (15)$$

The researcher argues that technical vulnerabilities and the respective patches are more stable over time and more specific than human vulnerabilities are. Therefore, it should be separated in the equation, respectively. Technical vulnerabilities, which can be hardware or software related, are by production and point of installation reflecting specific vulnerabilities that need to be patched. Zero-day vulnerabilities, different quality, capability and security levels are rather specific, stable and tangible, though quite often not discovered at first place. Moreover, they are to a certain degree quantifiable, like in the example of Sonnenreich (2006; p. 46). Misconfiguration of hard- and software does, however, present some incalculability, but supports our argument, as it is mainly based on human failure. This leads us to the human dimension of vulnerability. Investments in security solutions that patch the human factor are not only desirable, but still tremendously important. According to Proofpoint (2019) the human factor is exploited in 99% of cyber-attacks to initiate fraudulent activities or to steal data. Even for advocates of the human security dimension this seems to be somewhat propagandistically high. However, in a study that lasted for five years, researchers were physically penetrating security systems of 1,000 banks, using human psychology to steal confidential data about customers. They were successful in 96.3% of the cases (Robinson, 2008). However, solutions that try to patch the human factor heavily underly greater fluctuations than technical solutions do. Security solutions for human vulnerabilities are less tangible and more difficult to quantify and more flexible over time. One (security) solution fits all (vulnerabilities) does not hold for individuals. Character, experiences, motivations, skills or the personal attachment to the organization are just a few examples for individual and highly variable drivers of human IS vulnerability. Hiring and firing processes induce different levels of security awareness in the organization. The level is subject to continuous fluctuations. Whereas specific software applications are applied company wide and security patches can be induced to the whole system, humans are individuals that require specific patches that are not that easy to quantify. Individual resilience against malicious attacks is a key driver to build a cyber-resilient organization and to decrease IS risk eventually (van der Kleij and Leukfeldt, 2019). Organizations are in the need of capable and motivated employees that have psychological and physical abilities to demonstrate resilient IS risk behaviour (van der Kleij and Leukfeldt, 2019). The fact that employees are individuals shows that IS solutions to patch human vulnerabilities have to be as diverse as is the workforce or address the average human vulnerability, otherwise. On the other hand, differentiating technical and human dimensions in the equations also leaves room to account for unused potential of human IS. Unused human IS potential can be an effective leverage to the overall ROSI by, for instance, promoting a security aware corporate culture (Muhly *et al.*, 2021), which can be pursued in a very cost-effective way when managers incorporate it in their daily corporate communication. Another example of complementing IS investments is a multilevel defense approach against social engineering threats that consists of human and technological layers (Gragg, 2003).

4. Conclusion

This article has presented an alternative rather general theoretical approach to define return on security investments. Senior managers rely on decision supporting tools for approving investment requests, especially on topics they are not fully acquainted with. ROSI acts as such an indicator for investment decisions centered around IS investments. In this article we tried, however, to derive a theoretical model that demonstrates the incompleteness of current ROSI frameworks. In contrast, our theory has derived a model that is based on an idealistic approach, putting security as the primary return of IS investment in the spotlight. Moreover, IS investments are not one time and one size fits all investments, but are subject to various needs in terms of application and continuous improvement. Implying an overall effectiveness of IS investments through the act of approving investment requests is as misleading as thinking that IS investments do not differ in their scope, extent or purpose. It is not reasonable to approve any investment that leads to a return expressed in figures which do not reflect the essence of IS investments, namely providing security. Moreover, IS investment can have a positive short-term return in terms of mitigated potential economic loss, but can at the same time be ineffective, if implemented insufficiently. An approach that rather focuses on the effectiveness of IS investments seems to better fit this purpose. Corporate wide security of information requires the interplay of different components and dimensions of investments in security to patch vulnerabilities and eventually return security. The article argues that one has to separate among vulnerabilities and security solutions that are rather related to the technical dimension of IS and among those referring to the human dimension of IS. Technical vulnerabilities underly less flexibility and can be easier measured compared to individual human vulnerabilities.

One can criticize that this paper does not present an ultimate formula to precisely calculate a ROSI indicator, and the researcher would not reject this criticism. What this article nevertheless tries to communicate is that for security investment decisions the human factor is relevant, should be accounted for separately, can be a critical measure to leverage IS and that senior manager should question whether any specific presented number of probable returns is reason to feel safe. We also would like to encourage scholars to address the content of this article in future research and broaden the discussion on alternative approaches to better calculate returns on security investments, which finally helps organizations to become safer.

5. Disclosure Statement

No potential conflict of interest was reported by the authors.

6. Notes

7. References

ACCENTURE (2019). The Cost Of Cybercrime. Ninth annual Cost of Cybercrime Study – Unlocking the Value of Improved Cybersecurity Protection. Research Report.

Al-Humaigani, M., & Dunn, D. (2003). A model of return on investment for information systems security. In *2003 46th Midwest Symposium on Circuits and Systems* (Vol. 1, pp. 483-485). IEEE.

Anu, V. (2021). Information security governance metrics: a survey and taxonomy. *Information Security Journal: A Global Perspective*, 1-13.

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns. In *ITASEC* (pp. 175-193).

Bistarelli, S., Fioravanti, F., Peretti, P., & Santini, F. (2012). Evaluation of complex security scenarios using defense trees and economic indexes. *Journal of Experimental & Theoretical Artificial Intelligence*, 24(2), 161-192.

Brocke, J., Buddendick, C., & Strauch, G., (2007). Return on Security Investments - Design Principles of Measurement Systems Based on Capital Budgeting. AMCIS 2007 Proceedings. 94.

Butler, A. (2002). Security attributes evaluation method: a cost-benefit approach. Proceedings of the 24th international conference on Software engineering, *ACM (2002)*, pp. 232-240.

Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal*, *37*(4), 492-504.

Cremonini, M., & Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). *WEIS*.

Don, O. (2007) Calculating Security Return on Investment. Software Engineering Carnegie. *Mellon University Institute and US Department of Homeland Security*.

ENISA (2018). Investing in Security for ROI. *Enisa.europe.ea*, 2018, [Online]. Available at: https://www.enisa.europa.eu/news/enisa-news/investing-in-security-for-roi. (Accessed on 16.10.2021).

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision Support Approaches for Cyber Security Investment, *Decision Support Systems* (2016), doi: 10.1016/j.dss.2016.02.012.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*.

Gonzalez-Granadillo, G., Ponchel, C., Blanc, G., & Debar, H. (2014). Combining technical and financial impacts for countermeasure selection. *arXiv preprint arXiv:1411.0654*.

Gragg, D. (2003). A multi-level defense against social engineering. *SANS Reading Room*, *13*, 15.

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, *61*, 1-11.

IBM (2020). Cost of a Data Breach Report 2020. IBM Security & Ponemon Institute.

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681-695.

Kam, H. J., Mattson, T., & Goel, S. (2020). A cross industry study of institutional pressures on organizational effort to raise information security awareness. *Information Systems Frontiers*, *22*(5), 1241-1264.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28, 7, 509-520.

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails?. *Telematics and Informatics*, *48*, 101343.

Lockstep Consulting (2004). A Guide for Government Agencies Calculating Return on Security Investment, [Online]. Available at: http://lockstep.com.au/library/return_on_investment, (2004). (Accessed on 16.10.2021).

Muhly, F., Jordan, J., Cialdini, R.B. (2021). Your Employees Are Your Best Defense Against Cyberattacks. *Harvard Business Review*, [Online]. Available at: https://hbr.org/2021/08/your-employees-are-your-best-defense-against-cyberattacks. (Accessed on 31.08.2021).

Pontes, E., Guelfi, A. E., Silva A.A.A., & Kofuji, S.T. (2011). A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI), *Risk Management in Environment, Production and Economy*, Matteo Savino, IntechOpen, DOI: 10.5772/25911.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646.

Robinson, J. (2008, September 9). Researchers dupe banks with heists without holdups. Arizona Republic, p. D5.

Sinanaj, G., & Muntermann, J. (2013). Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis. In *Bled eConference* (p. 29).

Sinanaj, G., Muntermann, J., & Cziesla, T. (2015). How Data Breaches Ruin Firm Reputation on Social Media!-Insights from a Sentiment-based Event Study. *Wirtschaftsinformatik*, *2015*, 902-916.

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), 45-56.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a nation: A cross-country study. *Journal of Global Information Technology Management*, *23*(2), 112-137.

Thompson, N., & Barrett, B. (2020). How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One. WIRED, 24 September 2020. [Online]. Available: https://www.wired.com/story/inside-twitter-hack-election-plan/. [Accessed 24 August 2021].

van der Kleij, R., & Leukfeldt, R. (2019, July). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In *International conference on applied human factors and ergonomics* (pp. 16-27). Springer, Cham.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215-218.

Yaqoob, T., Arshad, A., Abbas, H., Amjad, M. F., & Shafqat, N. (2019). Framework for calculating return on security investment (ROSI) for security-oriented organizations. *Future Generation Computer Systems*, *95*, 754-763.

Yeh, Q. J., & Chang, A. J. T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, *44*(5), 480-491.