Winter 12-11-2022

Factors influencing the organizational decision to outsource IT security

Antra Arshad
The University of Melbourne

Atif Ahmad
The University of Melbourne, atif@unimelb.edu.au

Sean B. Maynard
The University of Melbourne

Factors Influencing the Organizational Decision to Outsource IT Security

Antra Arshad
School of Computing and Information Systems, The University of Melbourne
Melbourne, Victoria, Australia

Atif Ahmad[1]
School of Computing and Information Systems, The University of Melbourne
Melbourne, Victoria, Australia

Sean B. Maynard
School of Computing and Information Systems
The University of Melbourne
Melbourne, Victoria, Australia

ABSTRACT

IT security outsourcing is the process of contracting a third-party security service provider to perform, the full or partial IT security functions of an organization. Little is known about the factors influencing organizational decisions in outsourcing such a critical function. Our review of the research and practice literature identified several managerial factors (e.g., cost-benefit, inability to cope with the threat environment) and legal factors (e.g., regulatory/legal compliance). We found research in IT security outsourcing to be immature and the focus areas not addressing the critical issues facing industry practice. We, therefore, present a research agenda consisting of fifteen questions to address five key gaps relating to knowledge of IT security outsourcing – i.e., the effectiveness of the outcome, lived experience of the practice, the temporal dimension, multi-stakeholder perspectives, and the impact on IT security practices, particularly agility in incident response.

Keywords: IT security outsourcing, organizational decisions, managerial factors, legal factors, IT security outsourcing effectiveness

---

[1] Corresponding author. atif@unimelb.edu.au

INTRODUCTION

The cyber-threat landscape has shifted, with the emergence of organized and sophisticated actors who use increasingly sophisticated tools and techniques to compromise organizations (Kotsias et al., 2022; Ahmad et al., 2019). As a result of the increasing IT security risk and the exorbitant cost of managing an IT security function, many firms choose to outsource IT security. IT security outsourcing is increasing and has the largest growth rate of all outsourced functions in terms of the percentage of work outsourced (Computer Economics 2021).

In this paper, we examine a particular form of IT security outsourcing, i.e., the process of contracting a third-party security service provider to perform, the full or partial IT security functions of an organization (Sung and Kang 2017). The practice of IT security outsourcing can be divided into three phases, namely: the pre-outsourcing phase, the actual-outsourcing phase, and the post-outsourcing phase. The IT security outsourcing ecosystem involves six major stakeholders namely: the outsourcing organization (client), the managed security service provider (MSSP), the regulatory/governing bodies, the attacker/hacker, the insurance companies, and the organization's employees (Cezar et al. 2010; Naicker and Mafaiti 2018; Wu et al. 2021).

The reasons that organisations outsource IT security and the inherent risks involved make the outsourcing decision critical and challenging. Our review of the literature shows the precise factors considered by organizations in making such a decision have not been identified. Therefore, this literature review poses the following question: *What factors influence the organizational decision to outsource IT security?* By identifying said factors, the paper guides organizational decision-makers around the critical decision of IT security outsourcing.

This paper is structured as follows. First, the methodology adopted for searching the relevant literature is presented followed by a thematic review of the literature. We categorize IT

security outsourcing factors into two: managerial factors and legal factors. Then an analysis of the literature review is presented followed by a discussion of the gaps derived from the systematic analysis along with recommendations for future work.

RESEARCH METHOD

Our literature review approach is based on Mathiassen et al. (2007) and looks at two sets of research on IT security outsourcing: the researcher perspective (using Google Scholar), and the practitioner perspective (using Google to identify grey literature and white papers). A four-step approach to the review was undertaken (see Table 1).

Selection Step	Research literature (Google Scholar)	Practitioner literature (Google)
Step 1: Apply the search string to the search engine	**Search String:** "IT Security Outsourcing" | "Information Security Outsourcing" – The search produced 297 results.	**Search String:** "IT Security Outsourcing" 8500 results plus "Information Security Outsourcing" 9200 results report. The search produced 17,700 results in total.
Step 2: Select authoritative venue publications	Criteria 1: Peer-reviewed articles Result: 184	Criteria 1: Most recent publications (last 5 years). Result: 2780+1320 (total 4100)
Step 3: Select the most relevant articles.	These articles were reviewed. **Criteria 1:** The main focus is outsourcing IT/information security. Review for relevancy is determined by reviewing: the abstract, introduction, and conclusion of the article. Results: 20 remaining articles	Initial 100 articles from each search. **Criteria 1**: Remove duplicates (129 articles remain). **Criteria 2**: Result illustrates practitioner perspective only (27 remain). **Criteria 3:** The main focus is outsourcing IT/information security. **Review for relevancy determined by reviewing:** the title, executive summary, and collected data. Result: 6 remaining articles
Step 4: Combining Results	Researcher stream + practitioner stream = number of reviewed articles - 20+ 6 = 26	

Table 1: *Literature Search Process*

Step 1 identifies and applies the search terms to both of our literature streams which identified 297 IT outsourcing research papers and over 17,000 hits on google looking for practitioner literature. Step 2 was to limit the publications to peer-reviewed academic publications & practitioner articles limited by age (last 5 years) so that we had the latest industry practice whilst still having a large sample. This resulted in 184 research and 4100 practitioner

articles. Step 3 limits our search for research articles by reviewing each article (reading the abstracts, introductions, and conclusions) for relevance to the subject area (resulting in 20 articles). Similarly, we limited the practitioner articles using 3 steps – removing duplicates from the set of 200 papers, reviewing these remaining 129 pages to ensure a practitioner perspective on the area (27 papers) and then reviewing for relevancy (title, executive summary, and collected data) – resulting in 6 papers. In our review of both sets of papers, we looked to ensure that the focus was on IT security outsourcing. Step 4 combined the results of the search resulting in 26 articles that we then carefully read and analyzed using the open, axial, and selective thematic coding steps (Neuman 2014).

LITERATURE REVIEW

This section provides the outcomes of our analysis of the literature on IT Security Outsourcing. The literature shows that as a result of organizations relying on internet connectivity to conduct business along with increasing regulatory requirements that IT security is a critical business function with complexities and challenges (Cezar et al. 2010). However, many organizations lack the expertise or do not possess adequate resources to perform this critical security function internally (Karyda et al. 2006). Therefore, outsourcing the IT security function is appealing to many organizations wishing to achieve a higher level of security maturity (Oladapo, et al. 2009). IT security outsourcing is the establishment of a contractual relationship between organizations and sources that are external to the organization, for undertaking the responsibility of one or more IT security functions (Wilde, et al. 2006). Our review of the literature reveals that there are two categories of factors that influence an organization's decision to outsource IT security - managerial and legal. These are discussed in detail below.

Managerial Factors

Eight main managerial factors influence IT security outsourcing.

The need for state-of-the-art expertise and resources to provide IT security

Lack of expertise and resources drives organizations toward IT security outsourcing. Effective security management requires knowledge and skills to address the diversity of security threats and escalating rates of security incidents (Karyda et al. 2006). Effective security management requires highly skilled employees, which are difficult to acquire and retain. This discourages in-house management of IT security functions and directs firms toward outsourcing their IT security. Furthermore, MSSPs tend to specialize in providing IT security services for specific industries (Cezar et al. 2017). As a result, MSSPs are better equipped with resources and expertise than their client organizations. Hence, the constraints of time, resources, and expertise drive organizations to outsource their IT security (Cezar et al. 2017).

Industry literature reflects the trend toward outsourcing IT security. Deloitte's (2019) survey found the primary reasons for IT security outsourcing were: difficulty in attracting and retaining IT security experts in the competitive market, and the lack of in-house technical resources required to do cyber security right. PwC (2017) estimates that the unfilled cybersecurity positions worldwide would be an astounding 3.5 million, which will drive more organizations to outsource their IT security function.

Cost savings

Literature advocates that there are cost savings associated with the outsourcing of IT security for the client organization. Therefore, the advantage of cost-saving favors outsourcing IT security. Research studies infer that many firms decide to outsource security operations

because the cost is the principal concern and there are benefits in the form of cost savings or security improvements per dollar of investment (Naicker and Mafaiti 2019). A critical factor in outsourcing decisions is the relative cost efficiency of MSSPs (Hui, et al. 2012; Lee, et al. 2013; Wu et al. 2020). However, our review of these studies shows that the risk associated with outsourcing to a third party was not adequately considered.

Internal security culture

Outsourcing IT security has negative consequences for the security culture of the organization (Dhillon et al. 2017; Sung and Kang 2017, Oladapo et al. 2009). Further, removing internal security may send a message that security is not important. Outsourcing IT security diminishes security awareness and a sense of responsibility among the employees of the client organization (Karyda et al. 2006).

Deloitte (2019) also reports that "in this age of digital transformation, perception leads reality when it comes to an organization's ability to create a cyber-secure culture". Executives will need to frequently reconsider their organizations' security strategies for a stronger internal security culture, through close monitoring of the evolving ecosystem of specialized contractors and outsourcing providers available to help manage cyber risk (Deloitte 2019).

Threat environment

Recent surveys conclude that besides hacker's behavior, high rates of cyber-attacks and constant high-profile security threats compel organizations to outsource IT security (Avasant 2020; Syntax 2021) as there is a feeling that they are unable to cope with the constant attack pressure from the threat environment. However, the research literature presents contrasting arguments. A cyber-threat actor's behavior and frequency of attack should be considered by

organizations before making an outsourcing decision (Hui et al. 2012; Syntax 2021; Wu, et al. 2020). Wu et al. (2020) point out that "a strategic hacker always has a higher incentive to attack firms that manage security in-house, which reveals the advantages of outsourcing the security service to an MSSP". Whereas other studies argue that cyber-attacks may be more massive and pervasive when hackers can breach MSSP's adopted security technologies, as multiple clients adopt similar security technologies provided by the MSSP (e.g., Hui et al. 2012).

Characteristics of MSSP

The literature discusses the characteristics of MSSPs (cost efficiency, technical advantage, and how compatible they are legally with the client) as the merits that organizations should identify while finalizing the security outsourcing agreement (Hui et al. 2012; Karyda et al. 2006; Lee et al. 2013; Wu et al. 2017). "Competence of the vendor to ensure information security" and "compliance of the vendor with client requirements and external regulations" were two important MSSP characteristics identified (Dhillon et al. 2017). The prospects of IT security outsourcing increase if the MSSP has a partnership with a technology vendor, as muti-sourcing IT security contracts that involve both service providers and technology vendors, benefit the client organization (Naicker and Mafaiti 2019). "For the client, access to the service provider brought access to the technical skills from the vendor as well" (Naicker and Mafaiti 2019).

IT value proposition

Researchers believe that organizations should consider their IT value proposition before outsourcing their IT security functions (Fenn et al. 2002; Feng et al. 2019; Karyda et al. 2006). The literature argues that organizations that regard IS/IT security as a commodity asset are more likely to outsource their security functions to concentrate their resources on core competencies

(Fenn et al. 2002; Karyda et al. 2006). The literature also argues that in those firms where IT provides a strategic advantage (IT is closely connected to their core competencies), their IT security function is kept in-house (Feng et al. 2019). However, the practice literature shows that most organizations undergoing digital transformation tend to outsource their IT security functions (Syntax 2021).

Outsourcing contract structure

The structure of an IT outsourcing contract can mitigate client organizations' concerns with outsourcing IT security. For example, a multilateral contract structure can solve issues of the double moral hazard, regardless of the externality (Cezar et al. 2014; Lee et al. 2013). Researchers advocate penalty-based contracts consisting of fixed service fees and penalties for degraded services (Cezar et al. 2010; Feng et al. 2019; Hui et al. 2012). Moreover, the inclusion of contractual warranties that ensures MSSP compliance with the client's policy favorably affects an organization's decision to outsource. For example, IBM's Internet Security System SLA contains a $50,000 money-back warranty for each breach offered to win security outsourcing clients (Fenn et al. 2002; Lee et al. 2013). PwC (2017) illustrates that the inclusion of threat intelligence sharing in outsourcing contracts results in better prospects of outsourcing IT security to managed service providers.

Outsourcing an organization's IT governance structure

IT governance structures should be considered by organizations before making IT outsourcing decisions, as affects the results of outsourcing decisions (Liu et al. 2017). Their study illustrated that educational institutions with centralized IT governance structures benefit more from outsourcing their IT security as compared to institutions with decentralized IT

governance. Centralized IT governance impacts the regulatory compliance of an organization which ultimately impacts the occurrence of cybersecurity breaches. Due to this better compliance and system integration, these institutions have coordinated responses to security events and can utilize security outsourcing to further lower the probability of encountering cybersecurity breaches (Liu et al. 2017). PwC (2017) also shows that organizations with a centralized governance model tended to benefit more from outsourcing IT security as they can have centralized threat management and response to sharing of threat intelligence.

Legal Factors

Three key legal factors influence IT security outsourcing. These are discussed below.

Regulatory / legislative compliance

Researchers suggest that evolving regulatory requirements trigger security outsourcing practices (Cezar et al. 2014; Naicker and Mafaiti 2019). New regulations are devised as technology evolves. Since compliance with regulatory requirements demands resources and expertise, firms outsource to transfer the burden of this ever-changing mandate. Literature categorizes compliance with legislation in the very high impact category as "when the trigger to outsourcing security services is required by legislation; outsourcing is highly likely" (Oladapo et al. 2009). In industry practice, regulatory compliance is one of the reasons CISOs prefer to outsource IT security (Bissell et al. 2020). Due to the increase in indirect attacks, organizations also need to secure their third parties and partners. However, regulatory compliance is a major challenge in managing third-party cyber risks due to third-party organizations being in different legal jurisdictions (and countries). Therefore, organizations tackle this wider scope and scale of IT security by outsourcing it to managed security service providers (Bissell et al. 2020).

Data protection requirements

While deciding to outsource IT security, organizations should ensure that they don't violate data protection laws, especially if the outsourced function includes personal data (Cezar et al. 2017; Fenn et al. 2002; Hui et al. 2012; Karyda et al. 2006). Breaches of data privacy and protection are also reported as one of the main risks associated with IT security outsourcing (Bissell et al. 2020; Ernst & Young Global 2019). Interestingly, "fines excess of US$100 million resulting due to violations of general data protection regulations (GDPR), may match, or even exceed, the overall cost of cybercrime for an organization" (Bissell et al. 2020). Therefore, organizations are skeptical about outsourcing IT security due to data protection requirements.

Protection of intellectual property

Although there is little discussion about legal implications involving intellectual property (IP) in security outsourcing, it is critical that organizations consider IP while making outsourcing decisions. The protection of IP generates the need to acquire licenses to retain rights while entering into a security outsourcing contract (Fenn et al. 2002). The involvement of IP in security outsourcing can offset the financial viability of the outsourcing decision (Dhillon et al. 2017). Moreover, a lack of compatibility between the applicable law of the client and the MSSP, under which the IP is protected may result in loss, misuse, and damage to IP (Karyda et al. 2006). Therefore, the protection of IP becomes critical when considering IT security outsourcing.

Summary

There are eight managerial and three legal factors that affect an organizational decision to outsource IT security. An organization can make an informed decision regarding its IT security

outsourcing by carefully considering the factors to achieve IT security goals through outsourcing. The next section discusses the findings from the literature review.

DISCUSSION

There is limited research literature on IT security outsourcing despite its industry-wide adoption. Conversation in the literature is dominated by discussion on the pre-outsourcing phase, from the outsourcing organization's perspective. The literature emphasizes the conditions in which organizations choose to outsource IT security; complete or partial IT security outsourcing practices; the features or characteristics of MSSP that are desirable in terms of outsourcing IT security; and IT security contract finalization. Research in IT security outsourcing is immature and doesn't address the major areas of potential opportunity and issues which results in research gaps. As mentioned previously, IT security outsourcing is the process of contracting a third-party security service provider to perform the full or partial IT security functions of an organization. It has three temporal phases (pre-outsourcing, actual outsourcing, and post-outsourcing) and has six major stakeholders. Based on the review and given the definition of IT security outsourcing, we present a research agenda based on four gaps in knowledge.

Gap 1: Effectiveness of IT Security Outsourcing is Not Addressed

There is no discussion in the literature about the success of IT security outsourcing. Therefore, how can the success of IT security outsourcing be measured? This potential area of opportunity could be addressed through studies of success factors, maturity models, cost-benefit tools, and strategic evaluations of IT security outsourcing decisions. The effectiveness of IT security outsourcing is a key area of interest for practitioners which could be addressed through studies of the post-outsourcing phase. Table 2 shows that little research is conducted around activities (including effectiveness) that would occur in the Post Outsourcing phase.

Outsourcing Phase: IT Security Outsourcing Literature
Pre-Outsourcing: Cezar et al. (2010); Cezar et al. (2014); Cezar et al. (2017); Dhillon et al. (2017); Feng et al. (2019); Fenn et al. (2002); Hui et al. (2012); Hui et al. (2019); Karyda et al. (2006); Lee et al. (2013); Naicker and Mafaiti (2019); Oladapo et al. (2009); Samarasinghe et al. (2007); Sung and Kung (2017); Wu et al. (2021); Wilde et al. (2006); Zhang et al. (2021)
Actual Outsourcing: Cezar et al. (2014); Hui et al. (2012); Hui et al. (2019); Sung and Kung (2017)
Post Outsourcing: Rowe (2008)

Table 2: *Distribution of literature studies by the phase of outsourcing*

Gap 2: The Lived Experience of IT Security Outsourcing has not been Addressed

The following critical issues and variables were not considered in extant studies: organizational profile (size, scale, and industrial sector), risk profile, and the organizational context. This suggests researchers have not considered the lived experience (the organizational context) within which IT security outsourcing is conducted. One suspected reason for this gap, as shown in Table 3 could be that the scholars contributing to the literature regarding IT security outsourcing do not have an IT security background.

Literature Stream: IT Security Outsourcing Literature
Information Security: Fenn et al. (2002); Oladapo et al. (2009); Samarasinghe et al. (2007), Wu et al. (2021).
Economics of Information Security: Cezar et al. (2010); Cezar et al. (2014); Cezar et al. (2017); Feng et al. (2019); Lee et al. (2013); Liu et al. (2017); Zhang et al. (2021).
Information Security & Sociology: Dhillon et al. (2017); Hui et al. (2012); Hui et al. (2019); Karyda et al. (2006); Naicker and Mafaiti (2019); Sung and Kung (2017); Wilde et al. (2006).

Table 3: *Distribution of literature studies by theme*

An informal review of the researcher's backgrounds shows that most don't have a track record of IT security research and practice – hence a full understanding of the practice of IT security is missing from their interpretations. Rather, they tend to discuss IT security from a socio-economic perspective illustrating its economic considerations and social impacts.

Gap 3: Temporal Dimension of IT Security Outsourcing is Not Explored

The IT security outsourcing phenomenon changes over time, from insourcing to outsourcing and back to insourcing or part sourcing. The temporal dimensions of IT security outsourcing are not addressed within the IT security outsourcing literature. Therefore, how often

researchers need to revisit the question of studying outsourcing remains unclear. The temporal dimensions ensure that: IT security outsourcing is discussed as a phenomenon in research and researchers are cognizant of the changes in the climate in industry. Moreover, it ensures that researchers are keeping pace with market trends and industry changes. So, there is a need for alignment between changing trends in the industry and the studies done by the researchers to understand the IT security outsourcing phenomenon and how it is evolving.

Gap 4: A Multi-Stakeholder Perspective is Not Being Addressed

The role of stakeholders is key to understanding the holistic ecosystem, however the literature on IT security outsourcing focuses on the organizations deciding to outsource. The literature has either completely ignored primary stakeholders (e.g. insurance companies and the staff belonging to the outsourced function), or discusses stakeholders (e.g. MSSP, hackers, and Governing bodies) in terms of interest of the outsourcing company. This resulted in a single stakeholder perspective. The holistic view of the IT security outsourcing ecosystem may have revealed indirect reasons to outsource IT security like gaining market repute and utilizing a big brand name to win customer trust rather than functional and operational reasons for being secure.

Gap 5: The Impact of IT Security Outsourcing on IT security practices

There is considerable research on identifying organizational IT security practices (e.g., risk management, policy, training) (Alshaikh et al., 2014; Maynard et al., 2011). The impact of outsourcing IT security on said practices has not been studied. A particularly interesting case is that of incident response (Kotsias et al., 2022; Ahmad et al., 2021). The performance of an IT security incident response is measured in terms of agility (swiftness, flexibility, innovation) which is particularly challenging given that MSSPs tend to address IT security from a technology maintenance perspective rather than a business strategy perspective (Naseer et al., 2021).

Research Questions to Address Gaps in Knowledge

From all the gaps identified and discussed above, it can be concluded that the current state of research lacks maturity. Table 4 provides a summary of the gaps identified and the potential research questions that can be answered for addressing these gaps.

Section: Gap Identified	Potential Research Questions
4.1: The effectiveness of IT security outsourcing is not addressed	• What are IT security outsourcing success factors? • What is maturity in IT security outsourcing? • What is the strategic value of IT security outsourcing?
4.2: The lived experience of IT security outsourcing has not been addressed	• How is the effectiveness of outsourcing IT security influenced by organizational risk, organizational context, and the threat environment? • What are the effects of IT security outsourcing on internal security culture and in-house security functions of an outsourcing organization? • How often should IT security outsourcing contracts be reviewed (given the complex and evolving security landscape and organizational context)? • How can an outsourced IT security function be audited (considering the multiple stakeholder perspective)?
4.3: Literature does not consider the temporal dimension of IT security outsourcing	• How has IT security outsourcing evolved (given industry trends, norms, and expectations)? • What is the current state of IT security outsourcing within the broader landscape of evolving trends?
4.4: A multi-stakeholder perspective is not being addressed	• What is the role of stakeholders in IT security outsourcing (including insurance providers, regulators, and government)? • What expectations and requirements are imposed by parties involved in IT security outsourcing contracts? • How do MSSPs identify and assess their client's security requirements as part of operationalizing an IT security outsourcing contract? • What are the drivers (direct or indirect) for IT security outsourcing (e.g. contracting reputed MSSPs to improve shareholder confidence)?
4.5: The Impact of IT Security Outsourcing on IT security practices is Not Considered	• What is the impact of IT security outsourcing on IT security practices in organizations (e.g. strategy, policy, training, risk management)? • What is the impact of IT security outsourcing on the agility of incident response? How should command and coordination be structured and instituted across organizational boundaries?

***Table 4**: Summary of gaps identified and the potential research questions.*

CONCLUSION

This paper conducted a literature review and developed a research agenda on the factors influencing organizational decisions to outsource IT security. We found that there are managerial and legal factors that influence an organization's decision to outsource IT. The managerial factors were: (i) The need for state-of-the-art expertise and resources to provide IT security, (ii)

Cost-benefit, (iii) Internal security culture, (iv) Threat environment, (v) Characteristics of MSSP, (vi) IT value proposition, (vii) Outsourcing contract structure, and (viii) Outsourcing organization's IT governance structure. The legal factors were: (i) Regulatory/ legislative compliance, (ii) Data protection requirements, and (iii) Protection of Intellectual Property.

Our analysis of the literature led to the development of a research agenda based on five gaps in knowledge. We suggest future research into IT security outsourcing study effectiveness, lived experience, temporal dimensions, multi-stakeholder perspectives, and the impact on IT security practice, particularly agility of incident response. We have proposed a list of research questions for each knowledge gap. We believe that research addressing these questions will make substantive contributions to both theory and practice.

Finally, we articulate the key insights from this paper. We found that the industry practice of IT security outsourcing is primarily driven by financial considerations without due consideration of IT security risk. We found literature arguing the risk of information leakage/IP can offset cost savings made by outsourcing IT security. Further, there are considerable advantages in terms of cost efficiency, technical advantage, and legal compatibility in outsourcing IT security where the outsourced entity is a partnership between an MSSP and a technology vendor. Adopting a centralized IT governance structure when outsourcing IT security yields improved compliance and resource management benefits. Finally, evolving regulatory requirements are explain why organizations outsource their IT security.

REFERENCES

Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y. B., Al-Sai, Z. A., & Alhayja'a, S. A. (2021). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology*, *19*(1), 100059.

AVASANT. (2020). What's Behind The Five Year Upward Trend in IT Outsourcing? AVASANT. Retrieved from *https://avasant.com/report/whats-behind-the-five-year-upward-trend-in-it-outsourcing/*

Beel, B. G. (2009). Google Scholar's Ranking Algorithm: An Introductory Overview, *Proceedings of the 12th International Conference on Scientometrics and Informetrics (ISSI'09)*, *volume 1,* pp. 230–241. Rio de Janeiro (Brazil), July. ISSN 2175-1935.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices.

Bissell, k., Lasalle, M., Paolo, C. (2020). Lessons from leaders to master cybersecurity execution. Accenture Security. Retrieved from https://www.accenture.com/ae-en/insights/security/invest-cyber-resilience

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2010). Competition, speculative risks, and IT security outsourcing. In *Economics of information security and privacy* (pp. 301-320). Springer, Boston, MA.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2014). Outsourcing information security: Contracting issues and security implications. *Management Science*, *60*(3), 638-657.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2017). Sourcing information security operations: The role of risk interdependency and competitive externality in outsourcing decisions. *Production and Operations Management*, *26*(5), 860-879.

Computer Economics, Inc., a service of Avasant Research. (2021). IT Outsourcing Statistics 2020/2021. Outsourcing Trends and Cost/Service Experiences for 11 Key IT Functions. Retrieved from https://www.computereconomics.com/page.cfm?name=Outsourcing

Deloitte. (2019). The future of cyber survey 2019, Cyber Everywhere Succeed Anywhere. Deloitte Development LLC. Retrieved from *https://www2.deloitte.com/za/en/pages/risk/articles/2019-future-of-cyber-survey.html*

Deloitte. (2020). How Much Disruption? Deloitte Global Outsourcing Survey 2020. Deloitte. Retrieved from *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Process-and-Operations/gx-2020-global-outsourcing-survey-how-much-disruption.pdf*

Deloitte. (2021). Ask the PRO; How Managed Services Can be Leveraged to Move the Needle on Cyber Risk. Retrieved from https://www2.deloitte.com *https://www2.deloitte.com/us/en/pages/operations/articles/cyber-managed-services.html*

Delve. (2021, October 18). *The Essential Guide to Coding Qualitative Data*. Retrieved from www.delvetool.com/: https://delvetool.com/guide

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, *54*(4), 452-464.

East Carolina University Libraries. (2020, June 2). *Google Scholar: Advantages/Limitations of Google Scholar.* https://libguides.ecu.edu/c.php?g=89754&p=656912

Ernst & Young Global. (2019). *EY Norwegian IT Outosurcing Survey 2019*. Retrieved from www.digi.no.com: https://www.digi.no/filer/IT_Outsourcing_Survey_Norway_2019.pdf

Feng, N., Chen, Y., Feng, H., Li, D., & Li, M. (2019). To outsource or not: The impact of information leakage risk on information security strategy. *Information & Management*, *57*(5), 103215.

Fenn, C., Shooter, R., & Allan, K. (2002). IT security outsourcing: how safe is your IT security? *Computer Law & Security Review*, *18*(2), 109-111.

Hui, K. L., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems*, *29*(3), 117-156.

Hui, K. L., Ke, P. F., Yao, Y., & Yue, W. T. (2019). Bilateral liability-based contracts in information security outsourcing. *Information Systems Research*, *30*(2), 411-429.

Info-Security Europe. (2015). Information Security Breaches Survey 2015. Retrieved from *https://www.gov.uk/government/publications/information-security-breaches-survey-2015.* https://www.infosecurityeurope.com

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security*.

Lee, C. H., Geng, X., & Raghunathan, S. (2013). Contracting information security in the presence of double moral hazard. *Information Systems Research*, *24*(2), 295-311.

Liu, C. W., Huang, P., & Lucas, H. (2017). IT centralization, security outsourcing, and cybersecurity breaches: evidence from the US higher education.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248

Mathiassen, L., Saarinen, T., Tuunanen, T., Rossi, M., 2007. A contingency model for requirements development. *J. Assoc. Inf. Syst*. 8, 569.

Naicker, V., & Mafaiti, M. (2019). The establishment of collaboration in managing information security through multisourcing. *Computers & Security*, *80*, 224-237.

Oladapo, S., Zavarsky, P., Ruhl, R., Lindskog, D., & Igonor, A. (2009, August). Managing risk of IT security outsourcing in the decision-making stage. In *2009 International Conference on Computational Science and Engineering* (Vol. 3, pp. 456-461). IEEE.

PwC. (2017). Key Findings From The Global State of Information Security Survey 2017. PwC. Retrieved from *https://www.pwc.com/gx/en/consulting-services/information-security-survey*

Rowe, B. R. (2008). Will outsourcing IT security lead to a higher social level of security?

SYNTAX. (2021). 2021 IT TRENDS, A Year of New Industry Benchmarks. SYNTAX. Retrieved from *https://info.syntax.com/ebooks/3/syntax-it-trends-benchmark-report-2021*

Samarasinghe, K., Warren, M., & Pye, G. (2007, January). A conceptual model for security outsourcing. In *Proceedings of the 5th Australian Information Security Management Conference* (pp. 187-194). Edith Cowan University.

Sung, W., & Kang, S. (2017, June). An Empirical Study on the Effect of Information Security Activities: Focusing on Technology, Institution, and Awareness. In *Proceedings of the 18th Annual International Conference on Digital Government Research* (pp. 84-93).

Wu, Y., Duan, J., Dai, T., & Cheng, D. (2020). Managing security outsourcing in the presence of strategic hackers. *Decision Analysis*, *17*(3), 235-259.

Wu, Y., Fung, R. Y., Feng, G., & Wang, N. (2017). Decisions making in information security outsourcing: Impact of complementary and substitutable firms. *Computers & Industrial Engineering*, *110*, 1-12.

Wu, Y., Tayi, G. K., Feng, G., & Fung, R. Y. (2021). Managing Information Security Outsourcing in a Dynamic Cooperation Environment. *Journal of the Association for Information Systems*, *22*(3), 2.

Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review.

Wilde, W., Warren, M., & Hutchinson, W. (2006, January). The derivation of a conceptual model for outsourcing IT security. In *Proceedings of the IADIS International Conference e-Society 2006* (pp. 234-238). IADIS Press.

Zhang, C., Feng, N., Chen, J., Li, D., & Li, M. (2021). Outsourcing strategies for information security: Correlated losses and security externalities. *Information Systems Frontiers*, *23*(3), 773-790.