Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

The establishment of collaboration in managing information security through multisourcing

V Naicker[a,*], M Mafaiti[b]

[a] Cape Peninsula University of Technology, South Africa
[b] Unisa, Graduate School of Business Leadership, South Africa

ARTICLE INFO

Article history:
Received 3 April 2018
Revised 8 August 2018
Accepted 9 October 2018
Available online 12 October 2018

Keywords:
Multisourcing
Information security
Outsourcing
Knowledge sharing
Collaboration
Partnerships
Alliance

ABSTRACT

Purpose: As information security requirements evolve due to ever-changing business and regulatory requirements, and threat landscape, organisations have turned to multisourcing as a method of delivering information security services. This development has created opportunities for service providers which specialise in information security service provision to collaborate and deliver security services through multisourcing contracts. Therefore the research develops a collaboration framework for managing information security through multisourcing.

Methodology: This paper explores collaboration in multisourcing information security contracts through a qualitative case study that investigated the phenomenon from the views and experiences of a client organisation and its six service providers.

Findings: The research found that multisourcing contracts can effectively manage information security services through collaborative efforts from multiple service providers and technology vendors.

Practical implications: Theoretical insights into the use of collaboration and partnerships in the multisourcing of information security are non-existent. Therefore, the research contributes to practice by introducing a tripartite collaboration framework for multisourcing information security. This tripartite collaboration consists of client, service provider and technology vendors.

Originality value: The research demonstrates through the perspective of client organisation and service providers that collaboration in multisourcing information security contracts goes beyond the client and its service providers to include even technology vendors.

1. Introduction

The billion dollar sole-source megadeals that characterised outsourcing deals at the turn of the century are now outdated because of their lack of flexibility (Herz et al., 2011). Organisations have moved from outsourcing their services from sole-source agreements to identifying multiple service providers to work together with internal resources, a scenario known as multisourcing. Multisourcing offers the benefits of increased

* Corresponding author.
E-mail addresses: naickervi@cput.ac.za (V. Naicker), mmafaiti@gmail.com (M. Mafaiti).
https://doi.org/10.1016/j.cose.2018.10.005
0167-4048/

flexibility and quality and cost reductions through its best of the breed approach (Lacity et al., 2009; Siepmann, 2014). Consequently, multisourcing has been extended to support some sensitive areas such as information security services (Rhodes-Ousley, 2013).

2. Literature review

2.1. Definition of multisourcing

Multisourcing is defined as "the disciplined provisioning and blending of business and information technology (IT) services from the optimal set of internal and external suppliers in the pursuit of business goals" (Cohen and Young, 2006:1). After the failure of sole-source outsourcing arrangements, organisations have tried to move to insource some services while others have considered multiple service providers. The organisations choose to insource because of the need to maintain control over their complex and highly regulated activities (Cohen and Young, 2006). However even though outsourcing has failed in some cases, insourcing has still remained less prevalent. Particularly where information security is concerned, organisations have realised that all information security skills will not be found in a sole-source service provider or organisation. Therefore, there is a need to blend internal skills and external skills from various service providers in the delivery of IT or security services (IDC, 2014; Siepmann, 2014). Some researchers have characterised multisourcing with competition between suppliers, which will decrease costs (Lacity et al., 2009; Siepmann, 2014). Supplier competition in multisourcing contracts are viewed as a possible source of cost savings (Wiener and Saunders, 2014). However, cost saving through multisourcing is not always achievable. In fact the increase in outsourcing spending, does not link with estimated cost savings (Cohen and Young, 2006; Lacity et al., 2009). The inherent competition between suppliers also makes multisourcing sometimes untenable.

Capgemini (2008), one of the providers of consulting, technology and outsourcing services, holds the view that the fierce competition among service providers requires collaborative effort to achieve a mutually beneficial relationship. According to Currie and Willcocks' (1998), multisourcing leads to the formation of an alliance or partnership between suppliers. They state that the main reason is to deliver a service to an organisation and not hostile competition. Service providers must focus on their client's success in spite of the fact that they are competitors (Wiener and Saunders, 2014). This collaboration enables the client organisation to view multisource services as coming from one supplier in spite of the fact that there are a number of suppliers involved.

2.2. Collaboration in multisourcing contracts

The presentation of a diversified stakeholder base by Lacity and Willcock (2000), Cohen and Young (2006) and Wiener and Saunders (2014) demonstrates the need for a common approach to sourcing through collaboration. Collaboration is even more prominent in multisourcing, which brings together multiple service providers who are potentially competitors (Heitlager et al., 2010; Wiener and Saunders, 2014). According to Bapna et al. (2010), multisourcing contracts involve increased cooperation between service providers as they depend on each other to deliver services. Heitlager et al. (2010) call this dependency an IT service chain that consists of intra and extra organisational specialists who collaborate closely to deliver a quality service. Hence, service provider collaboration in problem solving brings about increased performance across the enterprise. In addition it can foster a culture of positive peer pressure, where no service provider wants to be identified as a laggard (ISG, 2014; Wiener and Saunders, 2014).

Such peer pressure is a source of healthy competition amongst service providers, which results in cost reduction for the client organisation (Heitlager et al., 2010). Therefore, both competition and co-operation are necessary for multisourcing contracts, giving rise to co-opetition (Wiener and Saunders, 2014). The client organisation plays an influential role in controlling competition and cooperation, a concept that Wiener and Saunders (2014) termed forced co-opetition. Wiener and Saunders' (2014) concept of forced co-opetition provides a view into the existence of both competition and cooperation in multisourcing contracts. However, they do not address how this is achieved to manage sensitive services such as information security, where the issues of intellectual property and secrecy are prevalent (Siepmann, 2014).

Conversely, collaboration facilitates knowledge sharing between the client and the service providers. According to Solli-Saether and Gottschalk (2010), knowledge sharing concerns how parties in the outsourcing deal, share and transfer their knowledge to one another. The key outcome of such knowledge sharing is the improvement of understanding of the services that are offered and the client organisation's business (Barthélemy, 2003; Solli-Saether and Gottschalk, 2010). Therefore, multisourcing requires a rethink of how to bring together different service providers and internal resources to work towards the same objective (Cohen and Young, 2006). A framework (see Fig. 1) that enables the delivery of a comprehensive information security service through a nexus of service providers is imperative to operationalising multisourcing contracts (Bacik, 2012; Siepmann, 2014; Capgemini, 2014).

2.3. Theoretical underpinnings of multisourcing and outsourcing

In order to understand how multisourcing contracts work and how to improve their efficacy in managing information security services, one has to understand the theoretical underpinnings that inform outsourcing. Literature on multisourcing is scant (Wiener and Saunders, 2014; Bachlechner et al., 2014) and for this reason theory from outsourcing is used to understand multisourcing. As a practical issue, general IT outsourcing is affected by organisational and management theories in order to improve its applicability (Solli-Sæther and Gottschalk, 2010).

The theories that are discussed are reviewed to strengthen the understanding of outsourcing and the motivations towards moving to multisourcing. Each theory represents a

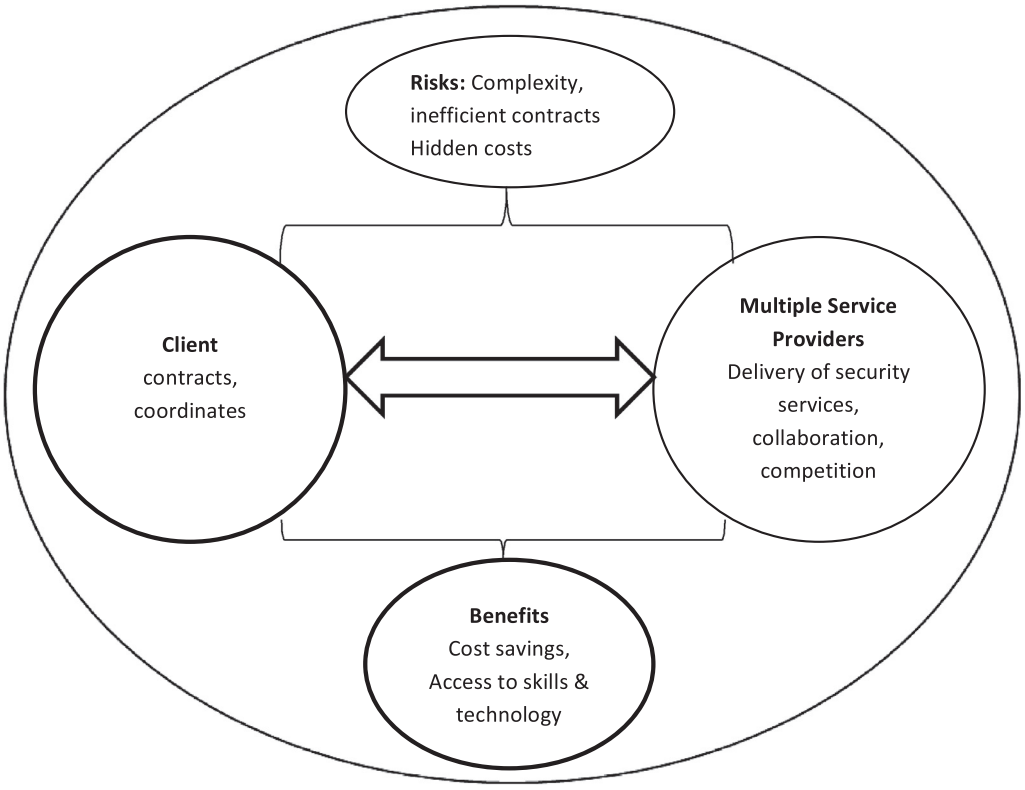

Fig. 1 – Multisourcing information security conceptual framework.

particular view on outsourcing and helps towards understanding the reason for considering outsourcing. The *Transaction Cost Theory* explains the boundaries of the firm, and what influences the purchase of a service or a product (Solli-Saether and Gottschalk, 2010; Beulen, 2011). Transaction costs are also affected by asset specificity, complexity and frequency (Solli-Saether and Gottschalk, 2010). In this case, idiosyncratic assets, highly complex services and frequent transactions result in more transaction costs.

The *Neo Classical Economic Theory* is based on the fact that every organisation is a production function, which is motivated by profit maximisation (Solli-Sæther and Gottschalk, 2010). Accordingly, organisations offer goods and services to markets where they have a cost or production advantage. Therefore, according to the neoclassical economic theory, organisations outsource IT activities in order to attain cost advantages from economies of scale and scope that are possessed by service providers (Ang and Straub, 1998; Gurbaxani, 2005).

The *Resource Based View Theory* states that successful organisations focus on their core competencies and enter strategic alliances to develop and extend their competencies (Dibbern and Heinzl, 2001). Another view of this theory claims that business functions that do not form part of core competencies are outsourced otherwise the company's competitive advantage is weakened (Stewart, 2002). The resource based view also states that companies have heterogeneous competencies and it is the heterogeneity that allows an organisation to earn good returns (Solli-Saether and Gottschalk, 2010). The *Resource Dependency Theory* implies that organisations depend on resources, which are acquired from other organisations (Konig and Beimborn, 2008). Cheon et al. (1995) argue that the resource dependency theory provides the basis for understanding why organisations outsource by stating that organisations outsource to obtain access to scarce human resources and technologies.

The *Partnership and Alliance Theory* describes the need for collaborative effort between two or more entities in order to achieve shared goals (Solli-Saether and Gottschalk, 2010). The partnership theory can assist to reduce the risks of inadequate contractual cover for complex and sensitive activities such as IT management (Das and Teng, 2003). However, the theory relies on many intangible qualities such as trust, comfort and understanding, which are difficult to assess before the identification and negotiation of partnerships (Solli-Saether and Gottschalk, 2010).

2.4. *Challenges in information security*

Information security is a discipline that is quite central to the operations of information technology and organisations' daily activities (Buecker et al., 2010). Organisations operate in an era of continuous collaboration, and information is required in real-time as means to make quick business decisions. The ability to compete in the current operational environment requires organisations to effectively access analyse and disseminate information to their stakeholders. These include suppliers, customers, consumers and industry regulators. Therefore, some information security assurance is required in order for organisations to rely on

available information for their key business decisions (Buecker et al., 2010). Furthermore, information security also affects the usability of information technology, and the experience that users have with their information systems (Sherwood et al., 2005). A non-functional information security service can damage an organisation's reputation beyond repair.

Future information security requirements for organisations go beyond merely detecting and responding to security threats, and also include predicting and preventing security threats (Rhodes-Ousley, 2013). Moreover, organisations are also overburdened by an increased security complexity because of the number of technologies that are used to deliver information security services (Burson, 2010; McAfee, 2016). Furthermore, training and retaining information security resources is a challenge in the world. According to a Security for Business Innovation Council (SBIC) report of 2012, there is a challenge in building an effective information security team owing to the variety of skills sets, which are required to run information security operations (RSA, 2012). This shortage of skills is exacerbated by the need for a new paradigm shift. This shift is from monolithic and technical skills sets such as protecting the perimeter and operating anti-virus solutions, to more diverse and business centric skills sets. The main focus being on business risks, asset valuations, threat and data analysis (RSA, 2012).

Hence the current security requirements and skills shortages present a formidable challenge that exceeds the internal organisation's competencies. These challenges have created opportunities for external organisations, namely service providers. These providers specialise in information security service provision and may take over the delivery of such services, hence resulting in the outsourcing of the service (Ding et al., 2005; Rhodes-Ousley, 2013). Consequently, organisations are considering external information security skills that they can blend with their internal competencies to deliver a secure environment for their businesses (Ding et al., 2005; Rhodes-Ousley, 2013). However, the general scarcity of information security resources across the world is not making it easy to find external partners. This implies that sought after information security skills and capabilities may not reside with one external partner. There is a need to consider more than one partner or service provider to provide information security services to one business and this concept is known as multisourcing (Cohen and Young, 2006).

2.5. *Multisourcing challenges*

Multisourcing in general has its own challenges, especially if it is not properly managed. According to Goolsby (2002), the results of strained sourcing relationships are high costs, operational disruptions and missed opportunities. However, from an information security perspective, the results are far more detrimental as it can mean fines, loss of intellectual property and permanent damage to the brand and the organisation's reputation. Therefore, managing information security through multisourcing is an extremely sensitive business, since it introduces new levels of business risk to the client organisation. The contractual relationship between the client organisation and the service provider is affected by hidden costs that many client organisations fail to identify and consider at the inception of the contracts (Barthélemy, 2003). Some of these hidden costs are: transaction costs, relationship management, transition costs and termination costs. Furthermore, client-service provider relationships are quite complex in any sourcing agreement. They consist of two parts, namely the formal contractual obligation and a psychological contract. Outsourcing contracts also define the service expectations from business through service level agreements (SLA) (Barthélemy, 2003; Goo, 2009). Therefore, there is a possible chance that one service provider's SLA might affect another within a multisourcing set up. However, there is a gap in literature on how to manage these complex multisourcing contracts, especially in terms of defining and enforcing SLAs on overlapping services.

Although some research has been done on the formation of partnerships and collaboration in IT multisourcing, most of it presents the phenomenon from a single perspective of the client. Theoretical insights from the service provider and the client's perspective into how collaboration and partnerships helps the multisourcing of information security are non-existent. Despite the lack of insights on this phenomenon organisations continue to approach multisourcing impulsively and indiscriminately resulting in huge losses and disappointment (Axelrod, 2004; Ding et al., 2005). Therefore the main objective of this research is to advance the understanding of how organisations collaborate and manage information security through multisourcing contracts by answering the following research question through a detailed scientific enquiry:

> How can organisations manage information security through collaboration in multisourcing contracts?

The research comprehensively studied collaboration in multisourcing information security through an exploratory case study of a South African client organisation and its six service providers culminating in the development of a framework (see Fig. 4).

The next section consolidates all the themes that have been discussed in the sections above into a conceptual framework to manage information security through multisourcing.

2.6. *Conceptual framework*

According to the conceptual framework below, management of information security through multisourcing involves two sets of players, the client and the multiple service providers. The client has a contractual expectation of service delivery from the service providers. The service providers in return deliver the service. Apart from these sets of players are two inherent factors, namely risks and benefits, which affect multisourcing. These risks include weak management, hidden costs, and inefficient contracts, among other issues. The benefits are access to knowledgeable resources and lowering of costs Managing these risks and benefits translates into the transaction costs as reinforced by the *Transaction Cost Theory*. Whereas the benefits are the main drivers of the multiosurcing decisions as described in the *Neo-Classical Economic Theory* and *Resource Based Theory*. Therefore, from a theoretical point of view, the conceptual framework captures the details of the multisourcing information security and increases the chances

of getting the desired outcomes, which benefit both the client organisation and the service provider.

The study analyses each theme from the client organisation and the multiple service providers' perspectives to gain a balanced view of the multisourcing of information security phenomenon.

The framework was subsequently refined as further analysis was performed and relations were identified between the multisourcing concepts. The conceptual framework serves as the reference point for the research design, empirical enquiry and analysis.

2.7. *The client organisation's background*

The client operates a multi-million dollar oil and chemicals business whose interests are spread across the world in five continents. There are ten business units in the company, and each business unit had its own IT organisation before 2010. The business lies in the petrochemical industry, which is at the heart of the critical infrastructure of the South African and the world's economy. The client's business is a strong and unique case of multisourcing, which is in line with the case study design that is outlined in the section below. The client offered the researchers a single opportunity to investigate the multisourcing phenomenon through the views of the service providers and the client organisation within a real life context. The client's petrochemical industry has also seen major investments in infrastructure security that is projected to rise from $18 billion a year in 2011 to $31 billion a year in 2021 (Frost and Sullivan, 2015). These huge infrastructure investments and the information security concerns have raised the researchers' interests, resulting in studies shifting from the technical aspects of information security to how organisations' interactions are shaped and defined around information security (Benbasat et al., 2002).

2.8. *Methodology*

The collaboration in multisourcing contracts is a qualitative study based on the interpretive paradigm. Qualitative methods are employed in this study because of their ability to comprehend complex and intangible social phenomenon (Lee and Baskerville, 2003; Beulen, 2011).

2.9. *Case study*

The case study method was selected for this study because of its ability to investigate the phenomenon of multisourcing within its real-life context of information security management (Yin, 1994). This case study used a variety of information sources, which include documents such as meeting minutes, artefacts such as policies and frameworks, unstructured interviews and observation of meetings to provide a rich view of the phenomenon (Yin, 2014; Cronin, 2014). Therefore, this case study results in the generation of new theory and description of collaboration in multisourcing of information security (Eisenhardt, 1989; Yin, 1994).The study follows the embedded case study design by focusing on the individual units of six service providers and the client organisation and then presenting the results as a holistic single case of multisourcing information security services (Eisenhardt, 1989; Yin, 1994).

2.10. *Sampling*

For this qualitative research, the purposive sampling technique was used to select the most productive sample in order to answer the research question (Coyne, 1997). This involved the researcher deciding on who would best provide the desired information based on the nature and needs of the study (Denzin and Lincoln, 2011; Løkke and Dissing, 2014). Therefore, information security practitioners and service delivery managers from the client organisation and service providers were selected to provide answers to the research question.

2.11. *Data collection*

One of the advantages of case studies is the rich detail, which emerges from a variety of information that is used to describe the case (Lee and Baskerville, 2003). These information sources include observations, documents, interviews, and participation (Wildemuth and Zhang, 2006). Hence, this research used multiple data collection methods, which included participant observation, document reviews and interviews to provide a rich insight of the case under investigation (Wildemuth and Zhang, 2006; Cronin, 2014).

2.12. *Interviews*

Unstructured interviews were suited for this interpretive paradigm, as they provided for naturalistic, explorative and in-depth enquiry, which allows for theory building (Wildemuth and Zhang, 2006). The most important aspect was for the researcher to build a better understanding of a new phenomenon of multisourcing information security services through the interviewee's perspective (Wildemuth and Zhang, 2006). The interview questions were compiled from prior theory that was revealed in the literature review into themes which were presented in the conceptual framework above. The unstructured interviews also included probing questions that assisted the researchers to capture real world experiences and further clarification on the topic (Perry, 1998a, b). To deal with this complexity, the researchers used two-person teams for interviews, as suggested by Eisenhardt (1989) and Perry (1998a, b). This implied that one researcher asked the questions and handled the dialogue with the interviewee, while the other took notes and observed the dialogue. Where this approach was not feasible owing to a lack of funds, the researchers used recording equipment, after obtaining permission from the informants, and took extensive notes (Eisenhardt, 1989; Cohen and Crabtree, 2008). Therefore, the type of data that was collected included field notes, audio recordings and transcripts. The interviews lasted between 40 min and 2 h. The unstructured interviews were conducted until new themes or explanations ceased to emerge from the data, a point that Herz et al. (2011) described as theoretical saturation. Longer interviews with key informants were divided into sessions of not more than an hour for logistical reasons, and to ensure maximum concentration and participation.

2.13. Observation

Observation of meetings, participation and site visits were used to augment the information from the interviews and document reviews (Yin, 2014). The resultant observations and discussions were captured as notes to produce qualitative data for this study.

2.14. Qualitative content analysis

This research used qualitative content analysis to analyse and interpret the content, which was gathered from interviews and reviewed documents. Qualitative content analysis was selected for this research because of its ability to offer subjective interpretation of the phenomenon under study while paying attention to its content and context (Miles and Huberman, 1994; Hsieh and Shannon, 2005). The qualitative content analysis consisted of directed and summative analysis techniques (Hsieh and Shannon, 2005). In directed content analysis initial coding is guided by theory and relevant research findings. The summative content analysis involves counting and comparisons of keywords, followed by interpretation of the underlying context.

Themes and categories of the phenomenon under enquiry were identified through direct content analysis by using the conceptual framework, reviewed literature and document analysis (Glaser, 1992; Beck and Schott, 2012). These conceptual themes were also identified according to their high frequency and were further refined through comparisons with relevant literature as part of summative content analysis (Beck and Schott, 2012). The final codes from this were analysed using QDA miner 4.1 and used to create a reconstruction of experience, and to write up theories of the multisourcing phenomenon.

2.15. Data analysis and coding

Data collection, coding and analysis occurred concurrently in this study. The following guidelines were developed a-priori to offer strategies and techniques followed during the data analysis. (1) Convergence of data from various sources were undertaken to understand the overall case and avoided treating each data source separately. (2) Analysis was performed in an iterative way to improve the study's ability to adequately answer the research questions. (3) Triangulation was achieved by using multiple sources of data and interviewing multiple participants in the organisation to increase the reliability and validity of the research. (4) A-priori coding of themes and patterns based on the case research instrument (Yin, 1994) was used and (5) theoretical saturation was reached when new sources of information resulted in a marginal improvement.

2.16. Rigor and credibility of the research

Generalisability is an essential feature of interpretive research that seeks to provide theoretical explanations of phenomena and not mere description .The study achieved this through the case study method, where the researcher records the different observations from the client organisation and service providers into first level constructs (Van Maanen, 1983). The first level constructs referred to understanding, which is held by participants in the enquiry. The reviewed literature and documents informed the theoretical formulations that culminate into second level constructs, which was the researcher's understanding (Van Maanen, 1983). The second level constructs were interpretations and theories that the research used to organise and explain what was observed from the interview responses. These constructs contributed to the formulation of a theoretical framework to manage information security services through multisourcing (Lee and Baskerville, 2003). Therefore, this case study did not seek to generalise across cases, but to build theory that could be generalised within the cases of similar contexts (Ferreira et al., 2012).

2.17. Validity, reliability and triangulation

According to Patton (2002), validity of a qualitative study owes its meaning to the information richness that is generated by the case study and the researcher's interpretations rather than by the size of a sample. In this research the interview questions were linked to the research questions. Each research question represented a section of the interview questions. Construct validity was also achieved by using the same questions for several informants to identify interesting constructs (Cronin, 2014). The researchers also employed multiple sources of evidence such as meeting minutes, governance frameworks and contract information to build construct validity (Eisenhardt, 1989; Yin, 1994). This study achieved external validity through seeking the perspective on multisourcing contracts from the client organisation and service providers. Presenting multisourcing of information security from both perspectives ensured that a comprehensive understanding and broader theory was built. The reliability of this study was demonstrated through comprehensive documentation of the data collection procedure and proper record keeping (Lee and Baskerville, 2003). Reliability was also achieved by adhering to the study's protocol, particularly the specific questions that the researchers had to remember to ask during data collection (Perry, 1998a, b; Yin, 2014). Triangulation is a combination of methodologies, data sources, and investigation or data analysis methods in the study of the same phenomenon (Denzin, 1989; Thurmond, 2001). Therefore, in this case study triangulation was achieved by reviewing other documentation such as contracts, annual reports, and participant observation to build an understanding of the multisourcing phenomenon, and to corroborate findings from the interviews (Yin, 2014; Cronin, 2014).

2.18. Findings and discussion

Based on the ethical considerations and requests by the study participants for anonymity, the researchers did not disclose the name of the client organisation, its Service Providers (SP) and the interview respondents. Therefore, for the purposes of this research, the organisation under study was referred to as the client and its service providers are referred to as SP-A, SP-B, SP-C, SP-D, SP-E and SP-F.

Table 1 – Overview of contracted information security services.

Service provider	Information security services
Client	Security architecture, security governance, security service management, operations management (after 2012)
SP-A	Anti-malware management, patch management, SOX compliance for application and file servers, email security.
SP-B	Security management, vulnerability management, risk management, reporting, process documentation (up to 2012)
SP-C	Anti-malware management, patch management, for workstations (desktops, laptops, mobile devices)
SP-D	Network infrastructure management (firewalls, switches and routers), identity and access management, encryption, web filtering
SP-E	Patch management for domain controllers, encryption, secure gateway, network security,
SP-F	Anti-malware management for domain controllers

2.19. *Multisourcing structure*

Around 2010 the client embarked on a consolidation journey, where all IT functions were performed by a single IT department. For almost ten years the client had one service provider for IT services, which included information security. However, in a bid to increase business agility and to improve IT services, the client departed from an outsourcing agreement that had become predictable and rigid towards a more flexible and robust multisourcing setup (Wiener and Saunders, 2014). The incumbent service provider had become inflexible and driven by the contract, leaving little room for innovation and response to business requirements. The idea was to have an information security service that would drive operational efficiency and innovation in the business.

In 2010 a decision was made to consider multisourcing IT to four service providers, namely SP-A, SP-B, SP-C and SP-D. SP-D went on to subcontract some of its services to SP-E and SP-F. The client retained some of the services such as security architecture and governance. The service providers were selected to bring value to the client by providing agile and innovative IT solutions, which include information security management. The service providers are described in the section below and a summary of their contracted services is presented in Table 1: Overview of contracted information security services.

2.20. *Service provider A (SP-A)*

SP-A is a big information technology service provider that used to be the only service provider for the client before it embarked on multisourcing contracts. In the new multisourcing dispensation, SP-A retained the responsibility to manage data centres, application and file servers, and the industrial information technology (IIT) or Operation Technology (OT) infrastructure. According to this arrangement, SP-A is also responsible for the information security aspect of their contract. As highlighted in the contract, the information security services comprise of anti-malware management and patch management on application and file servers, among other services. SP-A has most of the client's IT institutional memory because they once managed all IT for the client. The information security team from SP-A comprised of a principal information security specialist and a security specialist. These two are in charge of information security responsibilities that are contracted to SP-A.

2.21. *Service provider B (SP-B)*

SP-B is a big international information technology service provider and has a huge history in outsourcing across the world. SP-B mainly focuses on desktop services, systems integration, computing and network services, data centres, process modelling and SAP support. SP-B was in charge of the management of all service providers and service level reporting from 2010 to 2012. All contracted service providers reported to SP-B. SP-B had a service representative for each contracted service. Information security services were managed by an information security manager and an information security coordinator, who were both specialists in the discipline. Therefore, SP-B's team was in charge of managing the information security service providers on behalf of the client.

2.22. *Service provider C (SP-C)*

SP-C is part of the same company that owns SP-B; however, for the purposes of this multisourcing contract, they were treated as separate entities. SP-C is responsible for supporting information security on workstations, which are desktop computers and laptop computers, mobile devices (mobile phones) and printing services. SP-C's information security services include anti-malware support, patch management and the administration of all security applications that are deployed on the workstations. Therefore, SP-C has to work closely with all service providers that support different services that end up on workstations in a service chain (Heitlager et al., 2010).

2.23. *Service provider D (SP-D)*

SP-D is a big international telecommunications company, which started out with a low presence in South Africa. SP-D is in charge of network infrastructure security, which includes cabling, firewalls, routers and switches, and domain controllers (active directory). Most of the services that are contracted to SP-D are performed remotely or subcontracted to service providers, SP-E and SP-F. The security services from SP-D's contract also include antimalware support and patch management on domain controllers, network security, encryption, content filtering on emails and websites, among other services.

Table 2 – Distribution of interviewees across organisations.

Interviewee	Organisation	Work experience (Years)	Work experience at client (Years)
Security architect	Client	14	10
Security operations mgt	Client	10	6
Security governance	Client	8	3
Security strategy	Client	10	2
Service delivery manager	SP-A	18	8
Security specialist	SP-A	9	5
Service delivery manager	SP-B	20	4
Security specialist	SP-B	8	4
Service delivery manager	SP-C	15	4
Security specialist	SP-C	14	5
Service delivery manager	SP-D	17	3
Security specialist	SP-D	9	7
Security specialist	SP-E	6	2
Security specialist	SP-E	5	3
Security specialist	SP-F	5	3
Security specialist	SP-F	4	3

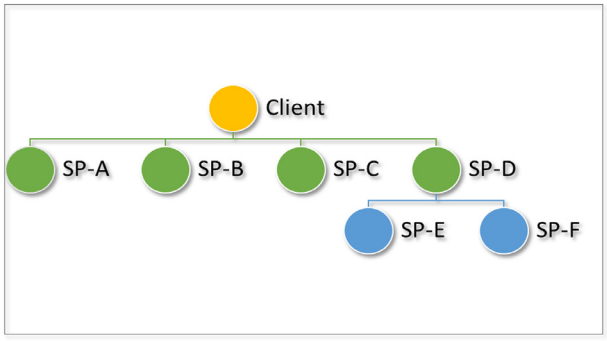

Fig. 2 – Multisourcing of information security structure.

2.24. *Service provider E (SP-E)*

SP-E is a big information technology outsourcing company that is a subcontractor to SP-D. SP-E is responsible for managing the network infrastructure (firewalls, routers and switches) and domain controllers on behalf of SP-D. SP-E does not have a direct contract with the client.

2.25. *Service provider F (SP-F)*

SP-F is an information security management company and a subcontractor to SP-D. SP-F is responsible for antimalware management on domain controllers on behalf of SP-D, and it also does not have any direct contract with the client.

The structure of the client and multiple service providers in the multisourcing of information security contract is depicted in Fig. 2 below.

2.26. *Distribution of interviews*

Table 2 below presents the demographic information and distribution of the interviewees across organisations.

2.27. *Code distribution and frequency*

The graph below (Fig. 3: Distribution of codes) shows the distribution of the codes that were identified from directed and summative qualitative content analysis techniques described in the section above. The coding categories are derived from the interview text; in directed content analysis initial coding is guided by theory or relevant research findings; while summative content analysis involved counting and comparisons of keywords, followed by interpretation of the underlying context. Therefore, direct content analysis and summative content analysis techniques were mainly used for the research's qualitative content analysis.

The above graph shows that the main codes, which emanate from the interviews and the review of the supporting documents, were collaboration (54.3%), communication (17.9%) and knowledge sharing (11.4%). Some of the codes, such as shared vision (3.3%) access to resources (8.8%) and quick completion of projects (3.3%), which had smaller frequencies, were used to identify the risks and benefits from multisourcing contracts or to support the main codes that stem from the research. The codes are now described in the section below as the main finding from the interviews and document reviews.

2.28. *Client coordinating collaboration*

The service providers and the client identified collaboration as a way to improve the management of information security through multisourcing. The client reported that collaboration allowed them to coordinate information security service delivery. All stakeholders, (client and service providers) were unanimous in their view that the collaboration agreement needs reinforcement and should cover all service providers, including subcontractors. The current contract has two subcontractors, namely SP-E and SP-F who assist SP-D in the delivery of their contracted services. Initially, the requirement for collaboration did not reach the two subcontractors. SP-B reported that some subcontractors were not aware of the need

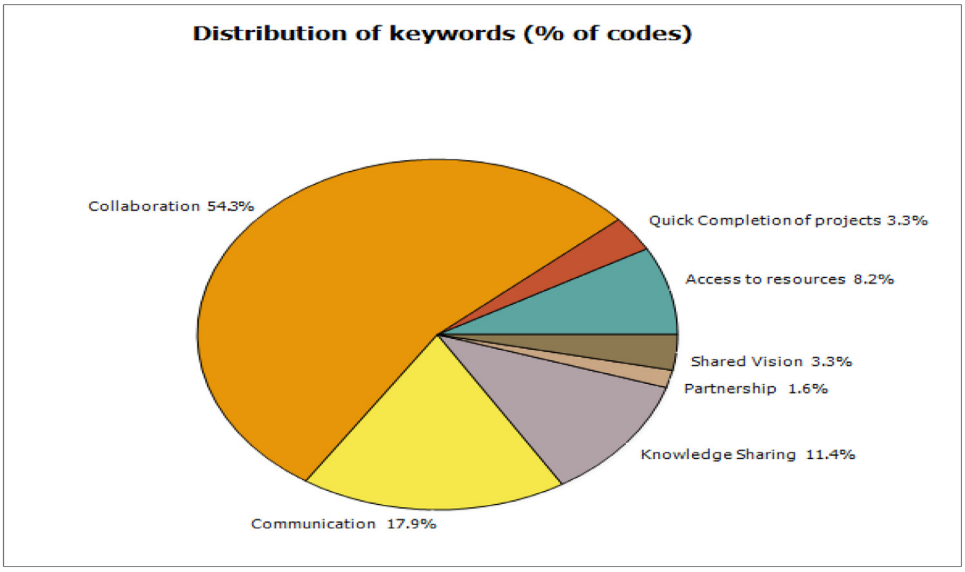

Fig. 3 – Distribution of codes.

to attend certain forums or to supply some reports. As one interviewee from SP-F explained:

> *"We were not aware that we must supply reports and attend some meeting at first because these expectations were not communicated to us by SP-D. We felt that we needed to report to SP-D only."*

To rectify this misunderstanding, SP-D had to ensure that both subcontractors were aware of the requirements of the multisourcing contract. Relying on SP-D's contract did not help because some of the requirements were not explicitly stated in the contract. Informal ways to improve collaboration were employed, and these included meeting with other service providers over coffee and lunch. Furthermore, the client played a leading role to attain this level of collaboration. The client emphasised the obligation on all suppliers to cooperate with other service providers in the statement below:

> *"We noticed that during the early days of multisourcing there was little collaboration. We were not actively involved in managing the service providers since the responsibility had been outsourced to SP-B. However we have now taken over the management and we have emphasised the need for collaboration with various account managers who represent the service providers. […] The need for collaboration had been specified in the contracts but it needed someone to enforce it during service delivery".*

The above extract also confirms that during the early days of the multisourcing contracts, SP-B could not enforce the need for collaboration because of the mistrust between service providers. Service providers were keen to protect their areas, and regarded SP-B and SP-C as competition, since they were from the same company. There were squabbles amongst service providers, late delivery of reports and finger pointing which led to service degradation.

2.29. *Overcoming the sense of competition through knowledge sharing*

SP-A also confirmed that at the inception of the multisourcing contracts in 2010 it was difficult for the service providers to share information on processes or security threats, because all this information was considered to be intellectual property. SP-B tried with extreme difficulty to get all the service providers to document and share their information security processes for their services. There was a deep sense of competition between the service providers and that prevented them from sharing information. For instance, SP-A highlighted that:

> *"At the inception of the multisourcing contracts, there was a general lack of trust in SP-B and other service providers, […] We viewed SP-B as fierce competition […] as a result we did not share any documents with them[…] However this has since improved because of the numerous intervention from both our management and the client. We can also see that the sharing of information is beneficial to our teams as well because it has become a very good platform for knowledge sharing […] we are able to share and compare threats information from the various technologies and our experiences from previous contracts."*

The above statements confirm that initial problems of collaboration were mainly caused by a lack of trust between the different teams. Reviewed reports and documents also confirm the lack of collaboration, which resulted in several information security findings during annual security audits. Several gaps in documentation were identified during annual security audits and assessments that were conducted by the client's external auditors. However, when the client took over the management of the service providers, after the cancellation of SP-B's contract, it resulted in the improvement of collaboration efforts. The client provided platforms for information sharing with all service providers. SP-A corroborated this development in the statement below:

"When the client took over the management of service providers from SP-B they managed to enforce the need for collaboration. We are interacting more with the client and among ourselves because new platforms for collaboration have been created. For example we now interact more during the newly introduced information security and architecture forums. Moreover the new CIO has introduced new platforms for communication for example road shows and monthly blogs, this has ensured that the information on the client is available to everyone. […] The technology vendors are also collaborating with us during the implementation of some technologies like vulnerability management".

The above extract confirms that, as part of improving collaboration, the client ensured that all service providers are fully informed about new initiatives through road shows and monthly blogs, where information on performance and new initiatives was presented. The establishment of information security and architecture forums also provided new platforms for further collaboration in discussing new solutions and strategies. The client emphasised that all processes and documents must be published on a portal, and should be accessible to all who worked on the contract. This portal became another platform for knowledge sharing. Apart from sharing documents and processes, knowledge sharing also takes place through monthly and quarterly information security meetings and some specific projects meetings, where service providers participate.

2.30. *The tripartite collaboration*

Collaboration came from technology vendors, Original Equipment Manufacturer (OEM), in the implementation of projects. The technology vendors are the original manufacturers of the security technologies of solutions that are used by the service providers to deliver information security services. This implied that the client benefited from other skills through the service providers' association with information security technology vendors. This benefit came from service providers' access to support and training from the technology vendors. For example SP-C explained the kind of support that they received from their technology vendors:

"We receive a lot of support and training from our technology vendors. During the implementation of the vulnerability management solution we received support from the technology vendor who understood the technology better than us. The Vendor helped with the architecture of the solution and performed a health check after the implementation enabling us to implement a quality solution."

This was one of the benefits of collaboration, which accrued to the client from using service providers who had a great partnership with a technology vendor. Where this service provider – technology vendor partnership did not exist initially it was forged during the implementation of some solutions. Hence to the service providers, working for the client opened the door to new opportunities for partnership with new technology vendors. Therefore, for the client, access to the service provider brought access to the technical skills from the vendor as well. The interviews also show that the new collaboration efforts enabled knowledge sharing about information security trends, threats and defence mechanisms and this was confirmed by the client's statement below:

"With improvements in collaboration we can now share information security intelligence and knowledge freely. Many service providers have access to different sources of information on security threats from their different technology vendors and this information is now shared with every member during the different security operations meetings. This has created a partnership with a shared goal and common interests. Given the proliferation of information security threats this collaboration is becoming helpful to our business"

The above statement confirms that the sharing of threat information through collaboration has improved the stakeholder's security posture. This improvement came with the assistance of technology vendors who provided threat intelligence from their technologies. The technology vendors particularly have this capability from their years researching and developing information security technologies.

3. Discussion

Feedback from the interviews, which appears above, point to a journey of collaboration that began with mistrust between service providers and which, ended with the client coordinating collaboration and knowledge sharing activities. When the management of service providers moved from SP-B to the client, it became easy to enforce the need for the service providers to collaborate with each other. The client identified platforms for collaboration and the main information that was required. The client also ensured that each service provider committed key resources to facilitate collaboration.

Service providers committed their senior security specialists and service delivery managers as the contact people for communication with other service providers and the client. Therefore, the findings show that the client made interventions that resulted in improved collaboration. A possible explanation for this development is that the client is ultimately accountable for the delivery of information security and, therefore, wields more power than a service provider such as SP-B (Bacik, 2012; Siepmann, 2014). Consequently, the client was able to enforce the required levels of collaboration.

Collaboration has also improved because each member's obligation and responsibility towards collaboration is clearly outlined in the contract. The types of information that service providers must contribute and the situations under which they must collaborate formed part of the definition of the conditions for collaboration. This development is in line with the partnership and collaboration theory which stipulates that flexibility, shared goals, proven abilities and regular communication cement collaboration.

For example, collaboration is required during problem management, incident management, vulnerability management, and change management. Therefore, every service provider and the client are represented during these meetings. This development demonstrates an improvement in the maturity of collaboration, which has created a huge information security alliance between the client and its service providers. This alliance has enabled the client organisation

to meet its strategic objectives (Solli-Saether and Gottschalk, 2010; Beulen, 2011). The client and its service providers can now view the information requirements and challenges as one team. Such a collaboration journey is in line with Das and Teng's (2003) three phases of alliance development processes, which are the formation, operation and outcome stages.

Collaboration proceeded through these stages and now it is at the outcome stage and benefits include reduction in high severity security incidents and high maturity of information security services (Beulen, 2011). According to Das and Teng (2003), there are four possible outcomes for an alliance and these are stabilisation, decline, reformation and termination. Evidence provided by service providers and the client confirm that collaboration has stabilised from the fractious relationship when SP-B managed the multisourcing contract.

When service providers collaborate there are low conflicts and high interdependency (Solli-Saether and Gottschalk, 2010). It becomes easy to leverage on each partner's strengths, which results in the client organisation benefiting from the best of the breed capabilities that are offered by multisourcing contracts (Cohen and Young, 2006; Wiener and Saunders, 2014). Such a scenario is important for information security management because it provides the client with stronger and skilled security teams at a time of security skills shortages (Axelrod, 2004; Ding et al., 2005; Bacik, 2012).

Interviewees stated that the client's ability to coordinate and set up formal structures that facilitated collaboration enabled them to mediate the fears of information sharing.

This finding concurs with Flores et al.'s (2014) finding that knowledge sharing of information security thrives in a scenario where there is full coordination and a formal arrangement. Hence, this research shows that formal structures provided an accountability framework. The accountability framework ensured that the service providers collaborated and behaved in a way that was consistent with the client's information security goals (ISG, 2014; Solli-Saether and Gottschalk, 2010). Coordination ensured the participation of service providers in knowledge sharing activities. The following section presents a framework for collaboration.

3.1. *Collaboration framework*

The research has shown that collaboration provides a common approach to information security management in diversified stakeholder environments that are presented by multisourcing contracts. Collaboration among the service providers and the client was reinforced by sharing information about information security threats and remediation tactics. This collaboration resulted in quick incident analysis and resolution. This development was an improvement from the initial mistrust between service providers during the early days of multisourcing. The client eventually managed to enforce the requirement for collaboration when they took over the management of service providers. In this case the finding on collaboration does not only corroborate with previous studies by Cohen and Young (2006) and Wiener and Saunders (2014), but also extends the requirement of collaboration to multisourcing information security services.

Meanwhile, multisourcing has always been discussed as involving collaboration between two parties, namely the client organisation and the service providers (Wiener and Saunders, 2014; Plugge and Bouwman, 2015). However, this research's findings point to a tripartite collaboration between the client, service providers and technology vendors in the delivery of information security services. The collaboration between the client, technology vendors and the service providers creates a hybrid information security organisation to respond effectively to information security threats.

This tripartite collaboration was demonstrated in this research when it was used to design and implement information security solutions for the client. Consequently, this ensures the correct and swift implementation of a technology solution for the benefit of the client organisation. Such a finding extends the knowledge of collaboration in multisourcing from the widely researched collaboration between the service providers and the client (Wiener and Saunders, 2014; Plugge and Bouwman, 2015) to the tripartite collaboration that involves the client, the service providers and the technology vendors.

Furthermore this tripartite collaboration, presented in Fig. 4 above, has been refined from the conceptual framework presented in Fig. 1 by adding the aspect of technology vendors. The new tripartite collaboration framework provides a way of sharing information security threat intelligence from across other industries in which the service providers work.

Technology Vendors bring their knowledge of the technology while the Service Providers bring their knowledge of service delivery. The client plays the co-ordination role and creates the platforms for collaboration. Hence, this tripartite collaboration facilitates the quick detection of new security threats, particularly in the petrochemical industry, which has seen rapid adoption of new technologies (Capgemini, 2008). The tripartite collaboration has provided the client organisation deep information security integration into the petrochemical business. Thus, the new level of collaboration enables the client to reap maximum benefits from multisourcing information security.

Therefore, it is important to note that collaboration results in the formation of an alliance or partnership based on shared goals which matures over time with improvement in experience that is gained from previous contracts (Rouse, 2009; Lacity et al., 2009). This is in line with the *Partnership* and *Alliance Theory* which provides for collaborative effort between two or more entities in order to achieve shared goals (Solli-Saether and Gottschalk, 2010).

The researchers have no doubt those partnerships that are formed from these tripartite collaborations will open doors for further expansion into possible coalitions for sharing information security threats and vulnerabilities across a wider community. Such examples of collaboration are already happening in countries such as the United States where laws promote sharing of information security threats and vulnerabilities (United States Government, 2015).

The research also revealed that multiple theories can be used to describe the multisourcing of information security journey. For example, the *Resource Based View* and the *Resources Dependency Theory* helps to understand the motivation and benefits of information security contracts, while the *Transaction Cost Theory* provides guidance through the contracting and some implementation phases.

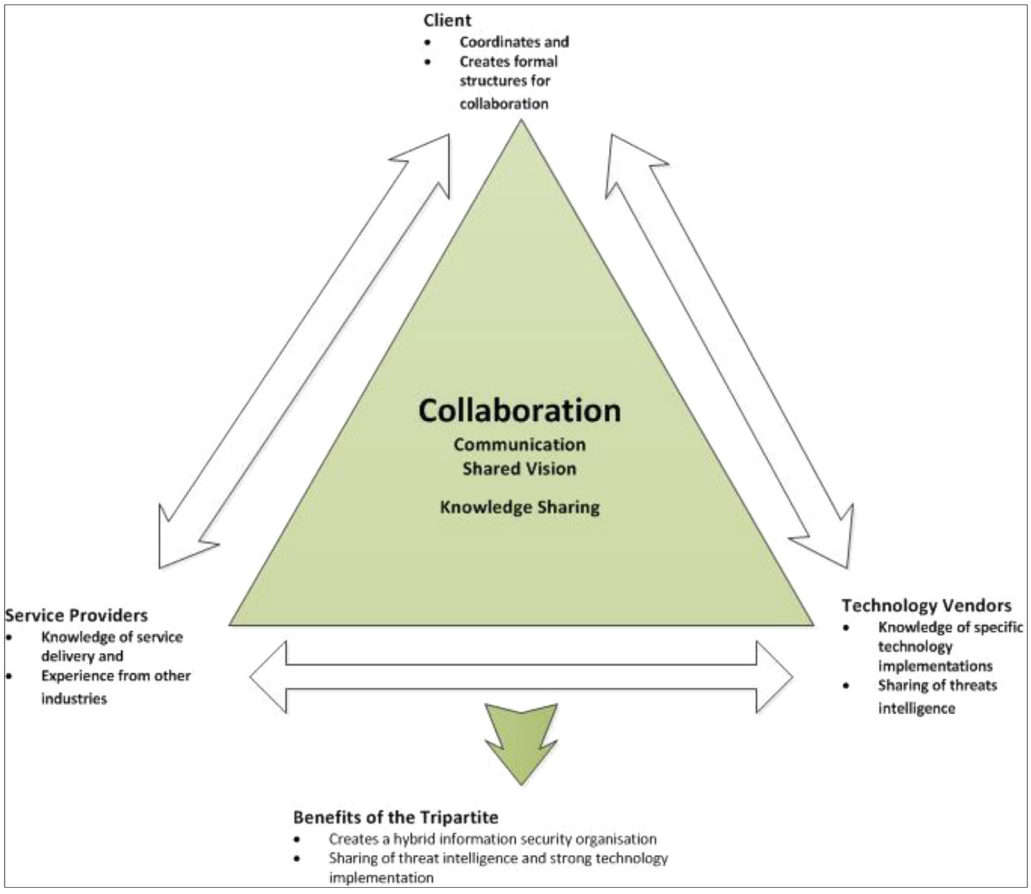

Fig. 4 – The Tripartite collaboration in multisourcing information security.

4. Conclusion and recommendations

Multisourcing introduces the best of the breed to manage specific information security services. The benefit of having the best of the breed in the environment is realised through collaboration. The researchers note that the tripartite collaboration between the client organisation, its multiple service providers and technology vendors creates a special interest group to address the client's business requirements through expeditious implementation of information security services.

As a result, one of the significant findings to emerge from the research is that collaboration enables multisourcing to create an information security community based on a shared responsibility of protecting the client's business. This level of collaboration develops over time as the client, service providers and technology vendors' interactions mature into a real partnership. Therefore, based on this finding, the researchers made the following conclusion:

Collaboration between the client organisation, its multiple service providers and technology vendors creates an information security community. This information security community is based on a shared responsibility of protecting the client's business through the expeditious delivery of information security services. Therefore the study contributes to literature and practice by extracting organisational decisions and practice that help the multisourcing of information security through tripartite collaboration between client, service providers and technology vendors.

5. Limitations of the research

The generalisability of these results is subject to certain limitations. For instance, the study uses data from one multisourcing setup. The multisourcing setup comprise of a sole-source client organisation in the petrochemical industry and its six service providers. This scenario creates a specific context for studying collaboration in multisourcing information security. While the service providers have exposure to a variety of industries, the main subject of the investigation, namely the client, is in the petrochemical industry. This might create some limitation of the applicability of the research in other industries, which might have different contexts.

Therefore, the study's generalisability could be improved by using data from multiple organisations' multisourcing contracts that cover information security management. The use of data from multiple organisations will further improve the understanding of multisourcing of information security through comparative studies that will identify new themes. While the scales of such contracts are low, the researchers have no doubt that in the near future more multisourcing contracts will be available for further studies, using quantitative methods.

REFERENCES

Ang S, Straub DW. Production and transaction economies and IS outsourcing: a study of the US banking industry. MIS Q 1998;22(4):535–52.

Axelrod C. Outsourcing information security. 1st ed. Boston: Artech House; 2004.

Bachlechner D, Thalmann S, Maier R. Security and compliance challenges incomplex IT outsourcing arrangements: a multi-stakeholder perspective, 40. Elsevier; 2014. p. 38–59.

Bacik S. Security outsourcing. In: Tipton HF, Nozaki MK, editors. Information security management handbook. London: CRC Press; 2012. p. 283–9.

Bapna R, Barua A, Mani D, Mehra A. Cooperation, coordination, and governance in multisourcing: an agenda for analytical and empirical research. Inf Syst Res 2010;IV(21):785–95.

Barthelemy J. The seven deadly sins of outsourcing. Acad Manag Exec 2003;17(2):87–98.

Beck R, Schott K. The interplay of project control and interorganizational learning: mitigating effects on cultural differences in global, multisource ISD outsourcing projects. Bus Inf Syst Eng 2012;1(4):183–92.

Benbasat I, Goldstein DK, Melissa M. An introduction to qualitative research in information systems. In: Myers MD, Avison D, editors. Qualitative research in information systems eds. London: SAGE Publications; 2002.

Beulen E. Maturing IT outsourcing relationships: a transaction costs perspective. In: Kotlarsky J, Willcocks LP, Oshri I, editors. New studies in global IT and business service outsourcing. Berlin, Heidelberg: Springer; 2011. p. 66–79.

Buecker A, Borrett M, Lorenz C, Powers C. Introducing the IBM security framework and IBM security blueprint to realize business-driven security. 1st ed. IBM Corp; 2010. sl.

Burson, S., 2010. Outsourcing information security. [Online] Available at: http://www.cio.com/article/2421303/security0/outsourcing-information-security.html.

Capgemini. The keys to successful multisourcing. Capgemini; 2008. s.l.

Capgemini. The multi-sourcing and service. Capgemini; 2014. s.l.

Cheon MJ, Grover V, Teng JTC. Theoretical perspectives on the outsourcing of information systems. J Inf Technol 1995;10(4):209–10.

Cohen L, Young A. Multisourcing – moving beyond outsourcing to achieve growth and agility. Boston: Harvard Business School Press; 2006.

Cohen DJ, Crabtree B. Evaluative criteria for qualitative research in health care: controversies and recommendations. Ann Fam Med 2008;6(4):331–9.

Coyne IT. Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries. J Adv Nurs 1997(26):623–30 Issue.

Cronin C. Using case study research as a rigorous form of inquiry. Nurse Res 2014;21(5):19–27.

Currie WL, Willcocks LP. Analysing four types of IT sourcing decisions in the context of scale, client/supplier interdependency and risk mitigation. Inf Syst J 1998;8(2):119–43.

Das T, Teng B. Partner analysis and alliance performance. Scand J Manag 2003;19(3):279–308.

Denzin NK, Lincoln YS. Handbook of qualitative research. 4th ed. London: Sage Publications; 2011.

Denzin N. The research act: a theoretical introduction to sociological methods. 3rd ed. New York: McGraw Hill; 1989.

Dibbern J, Heinzl A. Outsourcing of information systems functions in small and medium sized enterprises: a test of a multi-theoretical model. Wirtschaftsinformatik 2001;43:339–50.

Ding W, Yurcik W, Yin X. Outsourcing internet security: economic analysis of incentives for managed security service providers. In: Deng X, Ye Y, editors. Internet and network economics. Hong Kong: Springer; 2005. p. 947–58.

Eisenhardt KM. Building theories from case study research. Acad Manag Rev 1989;14:532–50.

Ferreira I, Ferreira S, Ramos I. The relevance of results in interpretive research in information systems and technology. Berlin, Heidelberg: Springer-Verlag; 2012. p. 80–9.

Flores WR, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Comput Secur 2014;43:90–110.

Glaser B. Basics of grounded theory analysis. Mill Valley, California: Sociology Press; 1992.

Goo J. Promoting trust and relationship commitment through service level agreements in IT outsourcing relationship. In: Hirschheim R, Heinzl A, Dibbern J, editors. Information systems outsourcing enduring themes, global challenges,and process opportunities. Berlin, Heidelberg: Springer-Verlag; 2009. p. 27–54.

Goolsby K. Growing beyond illusions: guidelines for changing and improving outsourcing relationships. White Paper Outsourcing Center; 2002. s.l.

Gurbaxani V. The value of information systems outsourcing arrangements: an event study analysis. UCLA; 2005. BIT Conference.

Heitlager I, Helms R, Brinkkemper S. Studying multi-sourced IT service chain arrangements: the relevance for mission critical outsourcing. Utrecht: University of Utrecht; 2010.

Herz T, Hamel F, Uebernickel F, Brenner W. Mechanisms to implement a global multisourcing strategy. In: Kotlarsky J, Willcocks LP, Oshri I, editors. New studies in global IT and business services outsourcing. Berlin, Heidelberg: Springer-Verlag; 2011. p. 1–20.

Hsieh H, Shannon SE. Three approaches to qualitative content analysis. Qual Health Res 2005;15(9):1277–88.

IDC. IDC reveals worldwide security predictions for 2015. Framingham: IDC; 2014.

ISG. Demand for specialists pushes outsourcing volume higher. Stamford: ISG; 2014.

König W, Beimborn D. Sourcing-trends im KMU-Kreditgeschäft der deutschen Banken. In: Kaib B, editor. Outsourcing in banken. Gabler Verlag; 2008. p. 183–209.

Lacity MC, Khan SA, Willcocks LP. A review of the IT outsourcing literature: insights for practice. J Strat Inf Syst 2009;18:130–46.

Lacity M, Willcocks L. Survey of IT outsourcing experiences in US and UK organizations. J Global Inf Manag 2000;8(2):5–23.

Lee AS, Baskerville RL. Generalizing generalizability in information systems research. Inf Syst Res 2003;14:221–43.

Løkke A-K, Dissing SP. Theory testing using case studies. Electron J Bus Res Methods 2014;12(1):66–74 Issue.

McAfee. McAfee labs threats report: March 2016. Intel Security; 2016. s.l.

Miles M, Huberman A. Qualitative data analysis. 1st ed. California: Sage Publications; 1994.

Patton MQ. *Qualitative* evaluation and research m*ethods*. 3rd ed. Thousand Oaks, CA: Sage Publications; 2002.

Perry C. A structured approach to presenting theses. Aust Mark J 1998a;6(1):63–86.

Perry C. Processes of a case study methodology for postgraduate research in marketing. Eur J Mark 1998b;32(9):785–802.

Plugge A, Bouwman H. In: Oshri I, Kotlarsky J, Willcocks L, editors. Understanding collaboration in multisourcing arrangements:

a social exchange theory perspective. Springer International Publishing; 2015. p. 171–86.
Rhodes-Ousley M. The complete reference guide: information security. 2nd ed. London: McGraw-Hill; 2013.
Rouse AC. Is there an "Information Technology Outsourcing Paradox"?. In: Hirschheim R, Heinzl A, Dibbern J, editors. Information systems outsourcing enduring themes, global challenges,and process opportunities. Berlin, Heidelberg: Springer-Verlag; 2009. p. 129–46.
RSA, 2012. Focusing on strategic technologies, https://www.rsa.com/en-us/perspectives/industry/security-business-innovation-council:RSA.
Sherwood J, Clark A, Lynas D. Enterprise security architecture: a business-driven approach. 1st ed. Boca Raton: CRC Press; 2005.
Siepmann F. Managing risk and security in outsourcing IT services. 1st ed. Boca Raton: CRC Press; 2014.
Solli-Saether H, Gottschalk P. Managing IT outsourcing performance. 1 ed. New York: IGI Global; 2010.
Stewart TA. The wealth of knowledge: intellectual capital and twenty-first century organization. 1st ed. London: Nicholas Brealey Publishing; 2002.
Thurmond V. The point of triangulation. J Nurs Scholarsh 2001;33(3):254–6.
United States Government, 2015. The White House. [Online] Available at: https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.
Van Maanen J. The fact and fiction in organizational ethnography, in. In: Van Maanen J, editor. Qualitative methodology. Beverly Hills: Sage; 1983. p. 37–55.
Wiener M, Saunders C. Forced coopetition in IT multi-sourcing. J Strat Inf Syst 2014;23:210–25.
Wildemuth BM, Zhang Y. Qualitative analysis of content. Philos Res Online 2006;1(2):1–12.
Yin RK. Applied case study research: design and methods. 2nd ed. Thousand Oaks: Sage; 1994.
Yin RK. Case study research design and methods. Thousand Oaks, CA: Sage Publications; 2014.

Prof Naicker is a National Research Foundation C3-rated researcher in Management Sciences, Business Management and ICT. He is currently a Full Professor and Chair of Department (*Business and Information Technology*) in the Faculty of Business and Management Sciences at the Cape Peninsula University of Technology. Prof Naicker specialises in ICT, computers and education, business management and retail management. His research interests are in artificial intelligence, business intelligence, green computing, big data, the internet of things and mobile computing. He is known nationally and internationally for his competence as a professional and inter-disciplinary researcher in the areas of ICT.

Dr Maclaud is a cyber/information security practitioner and consultant. An Industry thought leader who leads world-class cyber security organizations by building and implementing custom methodologies and frameworks that balance information security and business agility. He has a diverse background with cryptographic security providers, power utilities, petrochemical, mining, finance industry, airline, and governments. He combines executive business savvy with technical know-how to produce IT solutions and cyber security programs that are both realistic and effective.