Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments

Yudhistira Nugraha, Andrew Martin

Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments

Yudhistira Nugraha[1,2] and Andrew Martin[1]

[1]Centre for Doctoral Training in Cyber Security,
Department of Computer Science, University of Oxford, UK,
yudhistira.nugraha, andrew.martin@cs.ox.ac.uk,
[2]Directorate of Information Security, Indonesia,
yudhistira.nugraha@kominfo.go.id

Abstract. Many government agencies (GAs) increasingly rely on external computing, communications and storage services supplied by service providers (SPs) to process, store or transmit sensitive data to increase scalability and decrease the costs of maintaining services. The relationships with external SPs are usually established through service level agreements (SLAs) as trust-enhancing instruments. However, there is a concern that existing SLAs are mainly focused on the system availability and performance aspects, but overlook security in SLAs. In this paper, we investigated 'real world' SLAs in terms of security guarantees between GAs and external SPs, using Indonesia as a case study. This paper develops a grounded adaptive Delphi method to clarify the current and potential attributes of security-related SLAs that are common among external service offerings. To this end, we conducted a longitudinal study of the Indonesian government auctions of 59 e-procurement services from 2010-2016 to find 'auction winners'. Further, we contacted five selected major SPs (n=15 experts) to participate in a three-round Delphi study. Using a grounded theory analysis, we examined the Delphi study data to categorise and generalise the extracted statements in the process of developing propositions. We observed that most of the GAs placed significant importance on service availability, but security capabilities of the SPs were not explicitly expressed in SLAs. Additionally, the GAs often use the provision of service availability to demand additional security capabilities supplied by the SPs. We also observed that most of the SPs found difficulties in addressing data confidentiality and integrity in SLAs. Overall, our findings call for a proposition-driven analysis of the Delphi study data to establish the foundation for incorporating security capabilities into security-related SLAs.

Keywords: security, SLAs, trust, security capability, grounded Delphi method

1 Introduction

In recent years, many governments have been targets for a wide range of cyber attacks, by perpetrators ranging from unskilled individuals to foreign intelligence services. According to data from BAE Systems, 85% of the attacks have targeted high-profile organisations, such as government ministries (55%), embassies (15%) and public organisations (12%).[1] This statistical data is also supported by the Control Risks on Risk Map Report 2016, which pointed out that governments are the top sector targeted by

[1] Data was gathered from the slide,https://goo.gl/vumsm2, (Accessed March 2017).

cyber attacks (36% of total attacks). This is not surprising, as many governments generate, collect and store far more sensitive data than the private sectors, and this data is accumulated in more vulnerable systems. Consequently, some governments, notably the UK, the US and China require SPs to demonstrate compliance with government security requirements [14–16].

In fact, many government agencies (GAs) increasingly rely on external computing, communications and storage services supplied by service providers (SPs). The relationships with external SPs are usually established through service level agreements (SLAs) as trust-enhancing instruments. The concept of trust can be defined as a belief that a security capability will behave in an expected manner when demonstrating compliance with a security requirement according to particular threat. Whereas, a security capability is a combination of mutually-reinforcing security controls that are implemented by technical, physical and human elements [18]. In some cases, the level of *trust* is determined in relation to a specific *security capability* provided by external SPs [18]. For instance, an acceptable level of protection will be required depends on the trust that GAs place in external SPs [18] when using such external services. However, there is an absence of coherent approaches for preserving the confidentiality of sensitive data across GAs when using such SLAs. On top of that, most external SPs place a greater emphasis on the system availability and performance aspects, but overlook security in SLAs [3,4,7]. Also, they do not adequately incorporate security capabilities of the SPs into formulating security-related SLAs.

This study investigates the current and potential attributes of security-related SLAs that are common among external computing, communication and storage service offerings, using Indonesia as a case study. To this end, we conducted a longitudinal study of the government auctions of 59 e-procurement services to select major external SPs that provided Internet services, cloud-based services and data centre services across 80 GAs between 2010 and 2016. The selected SPs were then contacted to participate in a three-round Delphi study with group discussions and individual sessions to clarify security capabilities in SLAs. We analysed the Delphi study data using a grounded theory analysis [22–24], and synthesised findings, as follows: (i) perceived threats, (ii) government-specific security requirements, and (iii) service provider-specific security capabilities. We then postulate propositions for each research question.

In this paper, we claim three contributions. Firstly, we report a longitudinal study of the government auctions in Indonesia from 2010-2016. The insight will be useful to the government and other governments who make decisions. Secondly, we discuss how these findings can be used to improve such an understanding to incorporate the interplay of threats, security requirements and security capabilities into security-related SLAs. The insight will be used to develop a framework in the formulation of security-related SLAs as trust-enhancing instruments. Finally, we propose a grounded adaptive Delphi method to clarify existing security-related SLAs in service provision.

The reminder of this paper is structured as follows: Section 2 presents the research methodology. Section 3 reports key findings and discusses propositions. In Section 4, we discuss the implications of our findings, followed by the limitations of the paper and reflection with related work. We conclude our study in Section 5.

2 Research Methodology

This paper attempts to investigate the current and potential attributes of security-related SLAs that are common among external computing, communication and storage service offerings. Particularly, we attempt to clarify existing 'real world' SLAs with external SPs in terms of security guarantees to GAs, using Indonesia as a case study. As SLAs can be established with various interacting entities (i.e. customers, end-users, SPs, suppliers, integrators, standards bodies and accreditation bodies), this study was limited to GAs as customers who increasingly rely on such external services provided by SPs.

We use Indonesia as a case study because according to Article 12 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012, SPs have obligations to ensure agreements on minimum service level and information security when providing such external services to customers (e.g. GAs). Furthermore, *e-Government procurement systems* officially have been widely used since 2015 for procuring external information system products and services. For the purpose of this study, we aim to select representative SPs that supply external communications, computing and storage services to GAs through 59 e-procurement services in Indonesia.

Due to the inherent limitations of empirical studies of the scope of the current research, we developed a grounded adaptive Delphi method (GADM) that combines elements of the Delphi method and grounded theory (GT). Both the Delphi method and GT consist of simultaneous data collection and analysis, with each process being interrelated and iterative. The GADM varies in some respects from the two previous grounded Delphi methods [27, 28]. An important similarity between these methods is the integration of GT analysis and a group communication processes. One of the differences is that the GADM is based on a Policy Delphi approach [29] and an adaptive Wideband Delphi method [19], which aim to suit the different views of individual participants on specific matters, with greater generalisability across different participants. The GT analysis is well suited for capturing these different views from the participants.

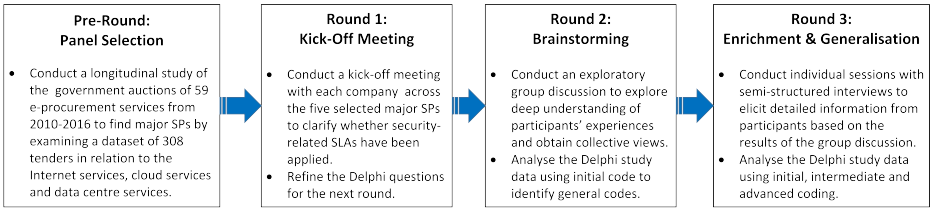

Fig. 1: The research method—a grounded adaptive Delphi method (GADM)

To this end, we conducted a longitudinal study of the government auctions in Indonesia to find "auction winners" or major external SPs, which were then contacted to do extensive face-to-face meetings as the application of GADM. In this paper, we adopted an adaptive wideband Delphi study [19] to enable the surveying of multiple panellists from major SPs through group discussions to clarify existing security-SLAs, along with individual sessions through semi-structured interviews to gather genuine knowledge and experiences in relation to the current and potential attributes of security-related SLAs. We analysed the Delphi study data using a grounded theory analysis to categorise and generalise the extracted statements.

2.1 Research Participants

Since the motivations and experiences of the participants directly affect the quality of the findings, the selection of participants is considered as an important aspect of a Delphi study. Consequently, a comprehensive selection criteria is necessary to select appropriate participants. In this study, particular attention was paid to the selection of SPs that provided external computing, communications and storage services to GAs through the government procurement system in Indonesia. To this end, we conducted a longitudinal study of the government auctions to find "auction winners" or major external SPs, which were then contacted to ask their participation in the data collection activities. We carried out the search process in the following steps.

Step 1:, We created and examined a dataset of 308 government tenders in relation to the Internet services, cloud-based services and data centre services from 59 e-procurement systems (SPSE) across 80 government agencies of which some agencies engage with other procurement services from other agencies.

Step 2:, We accessed the SPSE website for each government agency. Most of the the SPSE website follow the general format: lpse.[agency's website]/eproc/lelang]. We analysed 95944 government auctions from 2010 to 2016.

Step 3:, We used the automated search and applied the following *five* keywords, which were adopted from the Gartner Global IT Spending Forecast, to the site's search engine: 1) **Data Centre**, 2) **Cloud**, 3) **Co-location**, 4) **Internet**, and 5) **Network**). We initially extracted **273** for data centre category, **31** for cloud category, **17** for co-location category, **230** for Internet category and **236** for network category.[2]

Step 4:, We selected the set of e-procurement services, which could be relevant by reading the title of tender as well as identifying the relevant keywords in relation to the *five* keywords. Further, we searched by looking at information about the auctions that aimed to retrieve the requirements specifically for selecting external SPs.

Step 5:, Finally, we identified major external computing, communications and storage services that are widely procured across GAs. To understand the government's supply chain, we identified the SPs who were selected as auction winners.[3]

Further, we invited the five major selected SPs based on our longitudinal study to participate in a three-round Delphi study. We recruited our participants via an email containing an official invitation letter on behalf of the Indonesian ministry of communications and information technology. We typically corresponded with an organisational leader who then suggested potential participants according to the following the selection criteria: 1) work experience and background, 2) involvement in the government procurement auctions, and 3) a visible interest in the research topic. We also distributed the Delphi questions[4] to all potential participants across the five selected SPs before they agreed to take part in this study. Finally, we received 15 participants confirmed [P1–P15] who were representatives from the five selected SPs.

[2] e-Gov Procurement on IT Services, https://goo.gl/hzcHL9, (Accessed March 2017).
[3] Government Procurement Auctions, https://goo.gl/5LhWun, (Accessed March 2017).
[4] Delphi study questions, https://goo.gl/mIrQUk, (Accessed March 2017).

Although there is no need to meet certain number of participants [30], divergent opinions are required with more than two participants. Okoli and Pawlowski [31] suggest 10–18 participants on a Delphi panel. Other researchers suggest that the recommended size of the panel of experts varies from 5–20 participants [32], 10–15 participants [33] and 15–20 participants [34]. In this study, we aimed for a panel size of 6–11 participants for each round. The number of participants was sufficient for providing theoretical saturation. Although saturation occurred within the first twelve interviews, basic meta-themes became apparent after only six interviews [26].

Our participants are technical and regulatory compliance experts that have been working for many years at the five SPs {SP1, SP2, SP3, SP4, SP5}, which were selected as the winners of auctions, and provided Internet services, cloud-based services and data centre services to the GAs between 2010 and 2016. We spoke with our participants across the spectrum of general technical, procurement and security expertise.[5]

2.2 Data Collection: A Three-Round Delphi Study

We collected data primarily through a three-round Delphi study with 15 experts across the five selected SPs. We use some features of Delphi, such as group responses with face to face meetings for eliciting collective views and individual sessions with semi-structured interviews for collecting individual views where participants may not wish to elaborate in a group discussion [21]. Unlike other Delphi studies [27, 28], this study used group discussions and interviews instead of questionnaires as the instrument for data collection because the questionnaires are impractical for the purpose of eliciting genuine views or thoughts from busy participants, such as vice president and director.

Round 1: Kick-Off Meeting. We conducted a kickoff meeting with each company across the five selected SPs. However, one company did not take part in the first round due to some technical reasons. This round was intended to clarify the service providers' understanding of their obligations to ensure agreements on service level and information security. This stage was also important to refine the Delphi questions for the next round.

Round 2: Brainstorming Phase. We conducted an exploratory group discussion with representatives of participants from five selected SPs to explore a rich understanding of participants' experiences and beliefs, as well as to generate information on collective views [20]. We invited the 15 participants who initially agreed to participate in the study. However, only nine participants (*n=9*) from the five SPs attended the focus group.

Round 3: Enrichment and Generalisation Phase. We conducted individual sessions using semi-structured interviews to elicit detailed information from participants based on the results of the group discussion. We invited the 15 participants again to participate in the third round. However, we only conducted interviews and individual feedback with six participants (*n=6*) from two selected SPs. The two providers are the major SPs in Indonesia, and their network infrastructures were reported to be compromised according to Edward Snowden's revelations in 2013 [19].

[5] Participants information, https://goo.gl/dBSDcn, (Accessed March 2017).

2.3 Data Analysis: Grounded Theory Analysis

We applied the grounded theory analysis [22–25] to examine group discussion and interview transcripts, and to categorise and generalise the extracted statements. The process of developing a proposition was established after a thorough examination of the Delphi study data by establishing conceptual relations between categories.

In this study, the main researcher performed analysis of the Delphi study data. We conducted initial coding of a group discussion transcript to identify general codes. Further, we analysed the interview transcripts including the focus group discussion transcript, using initial coding, intermediate coding and advanced coding [25].

We used initial coding to identify topic of interest 'key-point coding' in which the researcher extracted useful sentences or statements and applied codes against the Delphi study data. In intermediate coding, we began to select categories from amongst topics of interest and found relationships among the initial codes (e.g. the most frequent or important codes) [24]. In advance coding, once categories were identified, we established the relationship between the categories to integrate them into a cohesive proposition regarding the interplay of threats, security requirement and security capabilities expressed in the formulation of security-related SLAs.

We can illustrate the grounded theory analysis with an example from this study. One participant commented that the greater threat to external `SPs` mostly come from DDoS attacks. We coded the following statement as 'deny access'.

> "*With regard to cases that hit banks around the world, such as SWIFT attacks, we, the service providers are required to protect against DDoS attacks*"(P1).

Unlike other qualitative studies where coding is performed by multiple researchers, the Delphi study data was coded only by the single researcher due to confidentiality reasons. However, the researcher discussed his findings with another researcher to receive feedback and comments on the findings.

3 Results and Analysis

In designing and analysing our research data, we will present our detailed findings for each primary research question, as follows:

1. What are the perceived threats to computing, communications and storage services as seen from the perspective of a service provider?
2. What are the government-specific security requirements when using external computing, communications and storage services supplied by service providers?
3. What are the security capabilities of the service providers used to mitigate the threats, and to demonstrate compliance with the security requirements?

We format the statements and challenges raised by participants in italics to distinguish them from our interpretations. We conclude each primary research question with propositions we derived from findings. By applying an appropriate qualitative analysis [24], we identify important codes and other observations present in the Delphi study data. We then report the raw number of participants who discussed a certain code to give an approximate indication of its prevalence amongst selected `SPs`.

3.1 Perceived Threats

We begin by examining specific threats that SPs are attempting to counter. Several statements have been made by participants to mitigate perceived threats to their service offerings. We noticed that consensus was obtained regarding a specific threat. For instance, many participants mentioned specific threats in relation to Deny Access. We highlight the perceived threats, as follows[6]:

Deny Access Many participants discussed this type of threat as the main security concern. This threat allows an adversary to prevent legitimate users from accessing the services. Thus, our participants paid much attention to mitigating the following threat:

> "*Our concern as a service provider is related to DDoS attacks because we can have three times the DDoS attacks in one month*" (P11).

Misuse Our participants were typically concerned with the weakest link (e.g. people). This threat allows an adversary to perform unauthorised use of assets. Some participants pointed out that authorised users could perform malicious actions to obtain sensitive data from the target. One of these participants indicated the following statement:

> "*We consider the highest risk is that authorised users that perform abuse or malicious stuff*"(P6).

Transmit Our participants discussed the importance of preventing unauthorised transfer of data, as this threat allows an adversary to transmit sensitive data externally. Only one participant indicated the threat (i.e. data exfiltration) in the following statement:

> "*An effort is needed so that data cannot be read and transferred by other people while data is in storage*"(P1).

Intercept A few participants reported that an adversary could intercept communication from the target people or devices, as indicated in the following:

> "*If the Internet is used by customers to send sensitive information without using a secure protocol, an attacker can intercept the communication*" (P1, P3).

Based on the aforementioned perceived threats, the extracted statements demonstrate challenges for offering an opportunity to specify security capabilities in SLAs. The most striking result to emerge from the Delphi study data is that the GAs often consider service availability the highest priority because DDoS attacks are currently targeting government services. We then postulate two propositions, as follows:

Proposition 1 *Identifying **[perceived threats]** is correlated with the concept of formulating **[security requirements]**.*

A strong relationship between threat models and security requirements has been reported in the literature [35]. As we learned from this study, our participants confirmed that such an understanding of the present and future perceived threats would help GAs and external SPs to formulate security requirements. In other words, external SPs can concern about specific perceived threats and/or vulnerabilities to express security

[6] Perceived threats, https://goo.gl/IdNKZj, (Accessed March 2017).

requirements, and to specify security capabilities used in the formulation of security-related SLAs, which can provide trustworthy services to GAs [17].

Proposition 2 *The current information about [**perceived threats**] is correlated with the concept of applying [**security capabilities**] to mitigate threats.*

Mitigating perceived threats plays an important role to deliver more secure products, services, or technologies. Our participants revealed that the GAs did not specify specific security capabilities for mitigating particular threats when using such external services. In most cases, the GAs are often less careful in terms of security objectives other than service availability. Our participants pointed out that although specific security objectives were not demanded by the GAs, the SPs employed minimum security capabilities, without additional cost of security services, to help ensure the services remain available based on the SLAs. Therefore, it can be assumed that the SPs will make their best effort to ensure their security posture when they provide such services to the GAs whether the agencies consider the need for security capabilities to mitigate possible threats, or not.

3.2 Government-Specific Security Requirements

Understanding the perceived threats can drive security requirements. Thus, security requirements play an important role in mitigating threats, such as unauthorised disclosure data by foreign intelligence services [19, 35]. However, our participants confirmed that understanding the government security requirements was essential in offering trustworthy services to the GAs. However, several challenges were described by participants, such as there were no specific security requirements from the GAs of what security capabilities the SPs would implement when processing, storing or transmitting sensitive data. We highlight the government-specific security requirements[7], as follows:

`Availability` All participants placed significant importance on availability and an overall guaranteed availability of approximately 99.5%. The provision of availability also addresses the reliability of the services to guarantee uninterrupted services that meet the availability requirement, as a key requirement from the GAs, as follows:

> "*If consumers ask for 95% availability, then we will provide a specific topology, such as dual homed gateway to meet the requirements*" (P1).

> "*As part of the availability requirement, we also provide a 24x7 monitoring service, response time, and resolution time. Additional requirements are related to the availability of Firewalls, IDS, IPS and Anti-DDoS Attacks*"(P1,P9).

`Access Control` Our participants typically reported relatively strong support for availability. Similarly, our participants reported that access control mechanisms were also often used to control access to networked resources and data. Several participants specifically mentioned access control mechanisms, as follows:

> "*How to get an access to the data centre's room? Is there a Log Book, whether the shelf is caged, and how to get the key to the caged rack?*" (P1).

> "*What kind of traffic is allowed in or out*" (P1, P3).

[7] Government Security Requirements, `https://goo.gl/eGtLRi`, (Accessed March 2017).

Authorisation Several participants reported that they had determined the access rights of an entity. Three participants mentioned that authorisations were used to manage who can read data at a higher security level etc. as follows:

> "*To access the data, the user must be registered, and the role must be permitted by the owner of the data*" (P6).

> "*As a service provider, we can only perform certain commands based on our privileges provided by the customer*" (P1, P3).

Non Repudiation Our participants indicated that SPs were required to maintain logs for monitoring and auditing purposes, as described in the following statement:

> "*To take precautions against unauthorised access, non-repudiation requirements can be added to record all activity on the devices*"(P1)

Confidentiality Many participants had no idea when we asked them whether they had implemented specific security capabilities in relation to confidentiality requirements and objectives in their services. However, our participants pointed out that specific security requirements from the GAs could impose such data confidentiality, as follows:

> "*When it comes to confidentiality of data, data classifications are of paramount importance to define. We also need to know whom the owner of that data is to determine the authorised user*" (P5).

> "*When encryption has been performed at the provider side, the customer should hold the key in terms of key management*" (P1).

From the above discussion, several challenges were described regarding the government-specific security requirements. The participants confirmed that the GAs did not demand specific security requirements for external SPs, which supply such services to them. However, the GAs placed particular security standard, namely ISO 27001 as the key security consideration for the government procurement (see footnote no.3). We then define the following propositions:

Proposition 3 *Service providers with a clear understanding of* ***[security requirements]*** *will be more likely to provide an appropriate level of trust by implementing specific* ***[security capabilities]****.*

It was hypothesised that formulating security requirements plays an important in mitigating perceived threats. However, our findings shown that very little was found on the adoption of security considerations in the government procurement because of the difficulty of specifying all security requirements [2]. Despite the strong need for compliance with the security standards (e.g. ISO *27001*), there is also the need for minimum security requirements in place when selecting external SPs (e.g. cloud services). Another lesson learned from this study is that existing regulations do not adequately support security procurement language for the government auctions. For instance, the Internet services, which are widely used in day to day government businesses, are still reliant on external SPs (considering ISO *27001* as a common security examination designed for

government procurement). Such external services are selected annually for for every year's budget. However, we identified a lack of basic technical protection to mitigate common threats when providing such external services to the GAs. This finding, while preliminary, suggests that it is necessary to classify security capabilities according to threats to establish the level of trust required between the GAs and external SPs.

Proposition 4 *Formulating **[security requirements]** is a fundamental part of incorporating appropriate **[security capabilities]** into the formulation of security-related SLAs.*

The results of this study indicate that all participants reported no specific security requirements were considered as instruments of selecting external SPs that provide such services to the GAs. Interestingly, another lesson learned from this study is that the GAs do not initially know what they want, or come up with new ideas about what and how to protect, what types of threats to mitigate, what types of security requirements that need to be defined, and which security capabilities that need to be employed. In some cases, most of the GAs rely on the ISO *27001/2* standards to form a strong security foundation. Indeed, it is not possible for the SPs to identify a complete security requirements up-front because security incidents occur many times and come later. The participants suggested that the GAs need to define the high-level security requirements up-front. Detailed security requirements are gathered as needed. It is evident that the diversity of security requirements can address unreasonable risks that were unlikely to occur.

3.3 Provider-Specific Security Capabilities

Some security capabilities are in place to demonstrate compliance with the government-specific security requirements. The statements made by participants indicate that threat-mitigation techniques have been normally conducted through technology capabilities because the GAs consider applying security requirements for such external services by implementing security technologies. From the Delphi study data, whether or not SPs had experienced perceived threats, our participants reported that they had implemented some security capabilities, including technical elements, physical elements and human elements. We summarise the specifically mentioned security capabilities mentioned, and mapped each to security requirements [35] (Availability, Integrity, Non-Repudiation, Confidentiality, Authentication, and Authorisation).[8]

`Technology Elements` In most cases, our participants mentioned using security technologies to protect their communication and information systems, as described in the below mentioned statements. We highlight provider's use of specific security technologies, as follows:

> "*We provide related requests, such as firewall, IDS, IPS and Anti-DDoS*" (P5)
>
> "*For data in motion we can do encryption, using SSL, IPSec or VPN. For data at rest, we can make use of data encryption and data loss prevention, and for more advanced technologies for cloud customers, we can provide storage encryption or hardware security module*" (P4)

[8] Security Capabilities, `https://goo.gl/zuCt18`, (Accessed March 2017).

`Physical Elements` Since all participants were industrial experts; we were particularly interested in other security capabilities that they have developed to protect their information system services (e.g. computing, communications and storage services). Several participants mentioned physical security measures used, such as doors, locks and surveillance tools, to deny unauthorised access to facilities and resources. For example, several participants pointed out that some security capabilities in relation to physical elements, as follows:

> "*We guarantee the availability of CCTV devices, door access and visitor access management*" (P2).

> "*We log all activity that occurs to monitor and track all user activity*" (P1).

`Human Elements` We also uncovered a number of human elements as mitigation strategies, such as people, process, and procedures that they have developed to protect their infrastructure. For example, most participants pointed out that people and process elements are necessary to be considered, as follows:

> "*A set of controls should have to comply with controls in ISO 27001, as the controls do not only discuss technology but also process and people*" (P5).

> "*It would be great if the customer already has a security policy and user access matrix to mitigate unauthorized access*" (P1, P3).

Note that the above statements demonstrate challenges for classifying security capabilities according to threats. We found that most of the `SPs` were reliant on the ISO *27001:2013* standard for providing better security services to the `GAs`. Our findings is consistent with our earlier observations, which showed that the `SPs` were required to hold the ISO *27001* certification for the government auctions at the value above *IDR 5 billion*, (see footnote no.3). Consequently, the `SPs` must have such security certification when they provide such external services to the `GAs` particularly for high-assurance services. However, such certification cannot contribute to addressing emerging threats [2]. We then derive the following propositions:

Proposition 5 *There is a need for an approach that addresses the interplay of* ***threats****,* ***security requirements*** *and* ***security capabilities*** *in the formulation of security-SLAs.*

Based on the Delphi study data, the `GAs` heavily rely on the experience of the external `SPs` in defining security requirements and implementing appropriate security capabilities to defend government data against a range of applicable threats. Our participants confirmed that certifications schemes, such as ISO *27001*, were necessary for meeting agreed-upon security capabilities for protecting government data (see *footnote no.3*). However, there are several issues with relying on the ISO *27001*, as this certification scheme is not sufficient to address specific threat that the `GAs` and `SPs` are attempting to counter [2]. Furthermore, the `SPs` reported that most of the `GAs` had no idea how to mitigate particular threats. One unanticipated finding was that implementing basic security capabilities is part of the `SPs`' initiatives to ensure the services remain available to the `GAs` based on SLAs. It seems that there is a connection between the *level of trust* and security capabilities of the `SPs` used to demonstrate compliance with the security requirements and to mitigate the perceived threats.

Proposition 6 *Classification of [**security capabilities**] specified in security-related SLAs according to [**perceived threats**] will be more likely to asses what is being claimed and achieved by service providers.*

Concerning this issue, we have learned that it is not possible to address every threat we have found. The results of this study show that security capabilities-related defensive technologies are commonly used for the GAs to mitigate threats. The findings further support the idea of technology-level implementation of defensive strategies are the fastest and easiest way to address one or more threats [35]. In this case, the GAs often take simple ways to address threats through technology-level implementations of mitigation strategies. However, despite the strong need for technology solutions, there is also the need for a perspective on human elements, which might still be a vulnerability, as the weakest link. Also, the participants reported that technology capabilities can be a major consideration, but it is not the only method in mitigating threats. It may be the case that the formulation and classification of security capabilities provided by the the SPs can help the GAs to select appropriate security capabilities according to threats.

4 Discussion

We discuss the implications of our findings for governments, service providers and researchers working on security-related SLAs, and summarise the limitations of our study. We then discuss the relationships with related work.

4.1 Implications

The interesting finding was that most of the GAs placed significant importance on service availability. However, other security requirements, such as data confidentiality and integrity were not demanded by the GAs. To help explain this, concerns over data confidentiality and integrity in the use of such external services are already seen as inhibiting the adoption of data centre services and cloud-based services in the government procurement auctions (see footnote no.2). However, it is apparent that ISO *27001* is often the only available way to demonstrate compliance with the government security requirements to provide a degree of security assurance, particularly for the government auctions at the value above *IDR 5 billion (GBP 320 thousand)*, (see *footnote no.3*). Based on our findings, specification of other **security requirements**, particularly with regards to data confidentiality and integrity, are not considered in the existing SLAs, as it brings some security challenges, such as the cost of security services associated with data confidentiality and integrity specified in security-related SLAs. Interestingly, the SPs have incorporated other **security requirements** in terms of the availability of security facilities, such as firewalls, intrusion detection and access management.

So far, the total cost associated with the interplay of **perceived threats**, **security requirements** and **security capabilities** in the formulation of security-related SLAs becomes a more difficult calculation since it encompasses liability and compensation. Furthermore, our findings reveals that several assumptions have been made to understand the current challenges with expressing the **security requirements** and **security capabilities** in SLAs according to specific **perceived threats**. Our propositions will be used in future research as a foundation for developing such a conceptual framework,

including how the **security capabilities** can be incorporated into the formulation of security-related SLAs.

Overall, identifying the **perceived threats** can drive the **security requirements**, which can impose appropriate **security capabilities**. In other words, *level of trust* between the GAs and external SPs can be determined by using specific **security capabilities** according to specific **perceived threats**.

4.2 Limitations

This study has three main limitations. Firstly, these results may be applicable only to the domain and context being studied [24]. The results are, to some extent, dependent on the research participants selected for this study and how participants described their experiences. Our qualitative data relies on the statements of the participants, which might be subjective. However, we limit its effects by conducting a series of data collection activities using a three-rounds Delphi study. While the demographics of our participants were representative of major SPs particularly in Indonesia, we did observe that our participants had a deficit of experiences in the formulation of security-related SLAs, particularly with regards to data confidentiality and integrity. Secondly, the internal validity of this study is determined mainly by the evidence we have used to generate our propositions. To limit these weaknesses, we recorded the audio of group discussions, transcribed the recorded audio, and sent the results to the participants before the individual sessions began. Finally, this study was subject to the paucity of participants who participated in each round (6-11 participants), as our participants were limited to those who were permitted to participate. However, the number of participants is still acceptable, as basic elements for meta-themes were present as early as six interviews [26]. We could increase the confidence in our propositions by asking more experts working at major SPs that provide external computing, communications and storage services to the GAs in Indonesia or in different countries. However, this study was not designed to be largely generalizable, but it aimed to clarify existing 'real world' SLAs and explore how the SPs implement security-related SLAs within service provision.

4.3 Reflection with related work

An SLA is a binding agreement between a service provider and a customer that is widely used in a variety of contexts to claim the obligation of external SPs to deliver services according to service requirements [1, 3]. The concept of security-related SLAs was first proposed by Henning [5], who pointed out that security-related SLAs have a lack of tangible and measurable services because security is not quantifiable and has not been expressed in such concrete terms in SLAs. The authors pointed out that it is not trivial to address the cost of security service required in contracts or SLAs, as security is challenging to measure and quantify.

This view is supported by Monahan and Yearworthy [6] who argue that statistical measures need to be captured and understood by customers and SPs to develop meaningful security-related SLAs. The authors explored basic examples, such as the measurable distribution of anti-virus signatures and how the formulation of security-related SLAs can be incorporated with certain legal and contractual instruments.

Similarly, Bernsmed et al. [3] asserted that existing security mechanisms should be formalised into a contract language, such as an SLA. With emerging remote services, such as cloud-based services, the authors pointed out that the absence of security properties in SLAs makes it impractical for external SPs to offer trustworthy services to their customers, especially when external SPs along with their suppliers are involved. However, the authors found that there are still many unresolved issues associated with the formulation of security-related SLAs.

Moreover, Jaatun et al. [4] pointed out that security-related SLAs are necessary for Internet services to help ensure that customers and external SPs have a shared understanding of security considerations expressed in SLAs for which customers receive the required level of security services. In most cases, the authors found that many SPs offer QoS guarantees (e.g. service availability) as part of their contracts. However, the lack of guarantees for security properties, such as data confidentiality and integrity, is a major drawback from the customers point of view.

Guesmi and Clemente in [7] described security-related SLAs in relation to problems arise in cloud-based services. The authors noted that external SPs should be able to describe what they can supply regarding security capabilities specified in SLAs according to security requirements, which help the providers to convince the customers regarding their security capabilities. However, the authors found that existing cloud SPs do not adequately express security requirements in cloud SLAs.

Some consortia have proposed standards to generate security-related SLAs between customers and external SPs to comply with the customers requirements, particularly in cloud computing, such as the Secure Provisioning of Cloud Services based on SLA Management (SPECS) [9], the Multi-Cloud Secure Applications (MUSA) [12], SLA-Ready [11] and SLALOM [10]. The SPECS project aims at offering a solution for such problems, developing and implementing an open source framework to offer Security-as-a-Service, by relying on the notion of security parameters specified in SLAs. The SPECS project is linked to a further project, called MUSA, a framework for facilitating security in multi-cloud applications. Similarly, SLA-Ready is a European initiative that aims to deliver a reference model for cloud SLAs that are designed for small and medium-sized enterprises (SMEs). SLALOM is another European initiative established to develop standardised SLAs and contract terms for cloud-based services, which is built on ISO standards as a baseline with the SLALOM templates.[9]

Questions have been raised by Luna et al. in [13] about the lack of assurance and techniques to quantify security. The authors noted that it is difficult to understand what security capabilities the customers have been paying for, when considering particulars services. The authors introduced techniques to assess quantitatively the security level of protection offered by cloud SPs to allow customers to compare with other SPs, based on their security-related SLAs. However, it is necessary to implement advanced security metrics expressed in SLAs to improve assurance and trustworthiness in remote services, such as cloud-based services.

[9] More details of research gaps, https://goo.gl/8i0ISC, (Accessed March 2017).

So far, there is a concern that the existing SLAs are usually limited to defining guarantees and regulations in terms of service availability and quality. Consequently, many external SPs to date have tended to focus on the system availability and performance aspects rather than security aspects (e.g. data confidentiality and integrity). This study focuses on the idea of investigating 'real-world' SLAs in terms of security guarantees. In so doing, GAs can understand the service capabilities regarding security that are provided by external SPs.

5 Conclusion

This paper has investigated existing 'real world' SLAs in terms of security guarantees across the five major selected SPs that provided external computing, communications and storage services to the GAs between 2010 and 2016, using Indonesia as a case study. We found that most of the SPs did not incorporated the security capabilities adequately into their SLAs, except for defining guarantees and regulations in terms of service availability and quality. This study has shown that most of the GAs placed significant importance on service availability, including response time and resolution time. One of the more significant findings to emerge from this study was that there were no security considerations expressed in existing SLAs. Another major finding was that most of the GAs applied the provision of service availability to demand additional means of confirming the security services supplied by the SPs. For example, the GAs require the availability of security facilities, such as the availability of firewalls, access controls, visitor access management, intrusion detection systems (IDS), intrusion prevention systems (IPS) and closed circuit television (CCTV). Hence, the results of this study indicate that there is a need for methods supporting security capabilities addressed in security-related SLAs to enhance the level of trust in service provision, as all participants confirmed that they encountered challenges to address data confidentiality and integrity in SLAs. Also, this study provides additional evidence with respect to the lack of formulation and classification of security capabilities specified in SLAs according to particular threats. Although this study is based on a selective sample of participants, the findings can illuminate security concerns for other governments to incorporate the interplay of threats, security requirements and security capabilities into SLAs.

6 Acknowledgements

This work was supported in part by the Indonesian Ministry of Communications and Information Technology under the Directorate of Information Security, and the Indonesia Endowment Fund for Education Scholarship (LPDP).

References

1. Ferrer et al.:The Role of SLAs in Building a Trusted Cloud for Europe, In: IFIP International Conference on Trust Management, pp. 262-275, Springer, (2015)
2. Bhme, R.: Security audits revisited. In: International Conference on Financial Cryptography and Data Security, pp. 129-147, Springer Berlin Heidelberg, (2012)
3. Bernsmed et al.:Security SLAs for federated cloud services, In: International Conference on Availability, Reliability and Security, pp.202-209, IEEE, (2011)
4. Jaatun et al.: Security SLA - An idea whose time has come?. In: Multidisciplinary Research and Practice for Information Systems, pp. 123-130, Springer, (2012)

5. Henning, R.R.: Security service level agreements: quantifiable security for the enterprise?. In: Proceedings of the 1999 workshop on New security paradigms, pp.54-60, ACM, (1999)
6. Monahan, B., Yearworth, M.: Meaningful security SLAs. Technical report, HP Labs, (2008)
7. Guesmi et al.: Access control and security properties requirements specification for clouds' SECLAS. In: IEEE Conference on Cloud Computing Technology and Science, (2013)
8. Takahashi et al.:Tailored security: Building nonrepudiable security service-level agreements. In: IEEE Vehicular Technology Magazine, pp.54-62, (2013)
9. Rak et al.:Security as a service using an SLA-based approach via SPECS. In: IEEE Conference on Cloud Computing Technology and Science, pp. 1-6, (2013)
10. SLALOM Project. The SLALOM project website, 2015.
11. SLA Ready Consortium. The SLA ready project website, 2015.
12. Rios et al.:Towards Self-Protective Multi-Cloud Applications, (2015).
13. Luna et al.: Quantitative Reasoning About Cloud Security Using Service Level Agreements. In: IEEE Transactions on Cloud Computing, pp. 1-1, (2015)
14. Cabinet Office.: Procurement policy note-use of cyber essentials scheme certification. (2016)
15. Hadeka, S., Scheimer, M.: DoD Amends its DFARS Safeguarding and Cyber Incident Reporting Requirements with a Second Interim Rule. (2016)
16. Bird et al.: China introduces new cybersecurity for rules for banking procurement, (2016)
17. Nugraha, Y.:Security Assurance Requirements Engineering (STARE) for trustworthy service level agreements, In: IEEE Conference on Requirements Engineering, pp. 398-399, (2015)
18. NIST 800-53.: Security and privacy controls for federal information systems and organisations, (2013)
19. Nugraha, et al.: An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements. In: IEEE Transactions on Emerging Topics in Computing, pp.47-59, (2016)
20. Harrell et al.: Data Collection Methods, RAND Corporation, (2009)
21. Paul et al.:Methods of data collection in qualitative research, In: Nature, pp.291295, (2008)
22. McGregor, et al.: Investigating the computer security practices and needs of journalists, In 24th USENIX Security Symposium (USENIX Security 15), pp. 399-414, (2015)
23. Egelman, et al.: Are you ready to lock?. In: ACM CCS, pp. 750-761, (2014)
24. Charmaz, K.: Constructing grounded theory, Sage, (2014)
25. Melanie Birks and Jane Mills. Grounded theory: A practical guide. Sage, (2015)
26. Guest et al.:How many interviews are enough? In: Field methods, pp.5982, (2006)
27. Pivrinta et al.:Grounding theory from Delphi studies. In: International Conference on Information Systems, pp. 2022-2035, (2011)
28. Howard, K.:Educating cultural heritage information professionals for Australia's galleries, libraries, archives and museums: A grounded Delphi study, PhD dissertation, QUT, (2015)
29. Turoff, M.: The design of a policy Delphi. In: Technological forecasting and social change, 2(2), pp.149-171, (1970)
30. Schmidt et al.: Identifying software project risks: an international Delphi study. In: Journal of management information systems, 17(4), pp.536, (2001)
31. Okoli et al.: The Delphi method as a research tool.In: Information and Management, (2004)
32. D Forsyth. Delphi technique. In: J.Levine, M.Hogg (Eds.), Encyclopedia of group processes intergroup relations, pp.196198. SAGE Publications, (2010)
33. Delbecq et al.: Group techniques for program planning, Scott Foresman, (1975)
34. Hsu, C., Sandford, B.: Delphi technique. In: Neil J. Salkind (Ed.), Encyclopedia of Research Design, pp. 344247. SAGE Publications, (2010)
35. Shostack, A.: Threat modeling: Designing for security, John Wiley & Sons, (2014)