NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

Assessing Cybersecurity Service Quality in Corporate Environments

Rui Norberto Barcoso Guerreiro

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

ASSESSING CYBERSECURITY SERVICE QUALITY IN CORPORATE ENVIRONMENTS

by

Rui Norberto Barcoso Guerreiro

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management with specialization in Information Systems and Technologies Management.

Supervisor: Prof. Dr. Tiago Oliveira

ACKNOWLEDGEMENTS

I wish to express my deepest gratitude towards Prof. Dr. Tiago Oliveira. His advices, insights and guidance have undoubtedly promoted the development and conclusion of this work.

ABSTRACT

This study assess the quality of Cybersecurity as a service provided by IT department in corporate network and provides analysis about the service quality impact on the user, seen as a consumer of the service, and on the organization as well. In order to evaluate the quality of this service, multi-item instrument “SERVQUAL” was used for measuring consumer perceptions of service quality. To provide insights about Cybersecurity service quality impact, DeLone and McLean information systems success model was used. To test this approach, data was collected from over one hundred users from different industries and partial least square (PLS) was used to estimate the research model. This study found that SERVQUAL is adequate to assess Cybersecurity service quality and also found that Cybersecurity service quality positively influences the Cybersecurity use and individual impact in Cybersecurity.

KEYWORDS

Cybersecurity, service quality, SERVQUAL, IT Service

INDEX

INDEX OF FIGURES

INDEX OF TABLES

1. INTRODUCTION

Organizations are increasingly relying on information systems (IS) to enhance business operations, facilitate management decision-making, and deploy business strategies (Kankanhalli et al., 2003). Facing pressures of organizational cost containment and external competition, many companies are rushing headlong into adopting IT without carefully planning and understanding the security concerns (Dhillon & Backhouse, 2000). With technology evolution and business being provided by means of Internet (e.g. e-commerce, transactional portals, and B2B software solutions) and adoption by users of BYOD concept into their way of life, corporate IT environment suffers several threats. Merely plugging in a mobile phone in a company's building can introduce malware into a secure environment (Hiller & Russell, 2013). As a result, regulators, investors, employees, customers and vendors are concerned about the safety and privacy of their organizations' information and IT (Hardy, 2006).

Cybersecurity has become a matter of global interest and importance (von Solms & van Niekerk, 2013) and, according to literature, adds dimensions as cost, return of investment, information recovery and loss of 'good will' between companies and clients (Steele & Wargo, 2007). Although IT executives have frequently identified the security of information as an important but not critical issue (Whitman, 2003), professional and managerial reasons support the interest in understanding the quality of the security provided by corporate organizations. Our research identified several studies about security on information systems and also studies about the quality of services but none considering the quality of Cybersecurity provided as a service by organizations. In order to fill that gap, Parasuraman (Parasuraman, Berry, & Zeithaml, 1988) multiple-item scale for measuring consumer perception of service quality (SERVQUAL) will be used to assess the quality of Cybersecurity service provided by organizations. Furthermore, we will study the individual and organizational impact of the measured service quality. Considering the regulators approach (e.g. Sarbanes-Oxley Act of 2002) and

professional's efforts to bring international standards as a framework (e.g. COBIT[1]) we believe that this study will promote an increased awareness about Cybersecurity.

This paper is organized as follows. In the next section we provide a detailed approach to Cybersecurity topic and describe the theoretical foundations of the study. The conceptual model and hypotheses are presented in section 3. The research method is discussed in section 4 and its results are analyzed in section 5. Section 6 discusses the major findings of the study, practical implications, theoretical contributions, study limitations and future research. In the last chapter, study conclusions will be presented.

[1] http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

2. LITERATURE REVIEW

2.1. CYBERSECURITY

In recent research, is stated that Cybersecurity and information security is often used interchangeably and that there is a substantial overlap between these two terms. Although information security can be defined in a number of ways, the boundaries of Cybersecurity as a concept are wider than those of information security in terms of how it is formally defined (von Solms & van Niekerk, 2013). Information security, at times referred to as computer security, is defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability (CIA) of information system resources (Zafar, 2013). Cybersecurity can be defined as the protection of cyberspace itself, the electronic information, the information and communications technologies (ICTs) that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace (von Solms & van Niekerk, 2013). Furthermore, Solms and Niekerk (2013) state that the security of underlying data is at large extent reliant on the overall security of the information system on which the data resides therefore identifying a sub component of information security considering technology security. This has a direct reflection on security information range of action because has to consider, not only issues regarding the security of the information itself but also flaws and possible threats inherited from the technology that supports it broaden the range and possible attacks. In other words, this “relationship” has a drawback: the gaps and flaws identified on the technology have exposed organizations to threats resulting in costly information security incidents and failures leading to substantial revenue losses.

As stated by Garfinkel (2012), attackers have the luxury of choice. They can focus their efforts on the way our computers represent data, the applications that process the data, the operating systems on which those applications run, the networks by which those applications communicate, or any other area that is possibly subverted. These considerations promotes a ‘sub-level’ of security called ICT security and is defined as all aspects relating to defining, achieving and maintaining the confidentiality, integrity,

availability, non-repudiation, accountability, authenticity, and reliability of information resources.

Just one successful security breach, theft, error, hack or virus attack on a company's IT can result in serious financial and reputation damage (Hardy, 2006). A company's cyber risk is a function of threats, vulnerabilities, the Cybersecurity environment, and company-specific mitigation (Hiller & Russell, 2013). Aside from the systems administrators and information security specialists, the greatest information security risk to the organization is not from professionals with narrowly-defined responsibilities. It is from the end-user (Wood, 2004). Research has found that security can oppose to day-by-day operations as in a busy working day of many demands, information security is given a lower prioritization than other work tasks (Albrechtsen, 2007; Steele & Wargo, 2007).

The end-user not following the information security policies, for whatever reason, is the weakest link in information security, and this user omissive behavior can seriously compromise the organizational information security posture (Cox, 2012). The evolution of computer science breaking barriers as distance and time has promote the scope of security to expand addressing data, means and users. Computing practices of system administrators and users continue to be one of the greatest challenges that the information security arena faces, yet there are no easy ways to improve these practices (Schultz, 2005). Thus, organizations are consequently more aware of information security risks and the need to take appropriate action. In order to be both efficient and effective with our information security efforts, every organization needs to adopt standard approaches to information security which applies across the organization, and in some cases, which apply on a multi-organizational basis (Wood, 2004). Banks, universities, hospitals, navies, and humane societies need very different kinds of information security programs (Anderson, 2003; Steele & Wargo, 2007).

So, organizational and business contexts in which information security serves must be considered and it is important to maintain the wholeness of systems because organizations depend so heavily upon information for their success (Dhillon & Backhouse, 1996).

2.2. CYBERSECURITY IN CORPORATE ENVIRONMENT

For organizations, information and communication technologies (ICTs) are means to be more efficient and productive and its adoption has been so profound that its value has become intrinsic with mission critical functions they support (Baker & Wallace, 2007). As organizations increasingly rely on information systems as the primary way to conduct operations, keeping such systems (and the associated data) secure receives increasing emphasis (Rees, Bandyopadhyay, & Spafford, 2003). Over the last 10 to 15 years, organizations have spent billions building strong perimeter defenses to protect their data from hackers and other out-side attackers (Steele & Wargo, 2007). The consequences of a security breach have negative implications for customers' privacy, investors' lost profits, business IP theft and industry competitiveness, and loss of jobs in the economy (Hiller & Russell, 2013). A single database breach incident can lead to millions of dollars in recovery costs and erode stakeholder and customer confidence (Steele & Wargo, 2007).

Security breaches can also result from operational decisions for instance when addressing cost reductions tactics as remote work or out-sourcing. Security requires time and money, and any security program will fail without management support (Steele & Wargo, 2007). Thus, security is a management problem and as a result, the investigation of security culture should also have a management focus (Ruighaver, Maynard, & Chang, 2007). This is obviously an evolution of the perspective of security information where in corporate organizations in the corporate world, information security is generally seen as being of interest to the IT department (Dhillon & Backhouse, 2000) and so many professionals do not give adequate importance to the security concerns of an organization. Something also observed by Whitman (2003), stressed that Information security continues to be ignored by top managers, middle managers, and employees alike.

2.3. IT SERVICE

From literature, our research has come across several definitions of IS service. For instance, Parasuraman et al. (2005) define electronic service quality as 'the extent to which a web site facilitates efficient and effective shopping, purchasing and delivery'. Peppard (2003) has pointed that the concept of IT service management that is typically encountered in the literature has come to mean the services that are necessary to keep the computer systems running. These include configuration management, change management, release management, access control, security management and capacity management.

Services-oriented thinking is one of the fastest-growing paradigms in technology management, with relevance to many other disciplines, such as accounting, finance, marketing, computer science, information systems, and operations (Bardhan et al., 2010). Peppard (2003) provides several keen considerations regarding services provided by IT departments to corporate users, referring to those using the service that can be at all levels in the organization. Being this service provided inside of the company's premises or to it related (e.g. branch office, remote worker, etc.) corporate users could be viewed as 'clients' of this service.

Based on these statements, one can infer that not only information technology departments are considered 'service providers' but they can offer their services not only to external consumers by forms of outsourcing where firms share knowledge (including technology, know-how, and organizational capability) (Yakhlef & Sié, 2012) but also internal consumers i.e. corporate users by form of services including those that enable communication and collaboration (i.e. email, desktop videoconferencing, instant messaging), data capture (i.e. point of sale [POS] systems, Internet-based data entry systems, business intelligence, customer portals), processing (i.e. order processing, invoicing, contract management, account management), storage (i.e. data centers and databases with information about customers, inventories, assets, etc.), access (i.e. ad hoc queries, report writing), and analysis (i.e. analytics, modeling) (Peppard, 2003). Summarizing, IT departments provide two kinds of services to its organization: Information-handling services and other services that are required in order for these

information-handling services to be made available to users. Security services or Cybersecurity services are considerer to belong to last service type provided by IT.

Since our study is basing the evaluation of the quality of Cybersecurity service on measurement scales of 'traditional' services an assessment to understand if information technology services have the same basis as 'traditional' services must be undertake. Parasuraman et al. (1985) stressed in their work, three well-documented characteristics of services: intangibility, heterogeneity and inseparability. First, as noted by these researchers, from previous work is pointed that 'most services are intangible' and most services cannot be counted, measured, inventoried, tested, and verified in advance of sale to assure quality. Some observations can be made to IS service and, in particular, to information security service. Information security service is, usually something one cannot touch, feel or manipulate. Passwords, antivirus, information access level to name a few are not 'things' that users can physically manipulate. Second, services, especially those with high labor content, are heterogeneous: their performance often varies from producer to producer, from customer to customer, and from day to day. The same can be considered either for IS services in general or for information security service. Both are highly dependable of people directly (e.g. support provided by Helpdesk) or indirectly (e.g. technology vendor support) for delivering the service. Third, production and consumption of many services are inseparable and in labor intensive services, for example, quality occurs during service delivery, usually in an interaction between the client and the contact person from the service firm (Parasuraman et al., 1985). Many information, systems and technology services are at least to some extent produced and consumed simultaneously. For example, support from a helpdesk is generally provided and utilized immediately (Peppard, 2003). The case applies in information security service in situations where end-user must engage with service-delivery-people (e.g.: user account lock, defining information access levels, performing antivirus actions, etc.).

Poon and Lee (2012) have found several e-services concepts: e-service is a transaction, that is, the customer pays for the goods or services (the hard e-service), and the supplier is responsible for delivering on time; e-service as a form of interactive services, which relates to the interaction between customer and service provider, thus

creating a relationship, usually a one-on-one experience; e-service as information service which is basically a customer's interactions with a Website; and finally e-service from the technology experts' viewpoint, which is the natural extension of Web-based functionality focusing on the soft e-service aspects, for example, Website design, Web content, security, accessibility, and reliability. These differences in concept could be justified by (as stated) 'include unit of analysis, research objectives, and scope of study; and each service component may encompass an array of elements influencing the heterogeneity of customer expectations, experiences, and perception'.

2.4. QUALITY ASSESSMENT

Previous research presented quality as "zero defects—doing it right the first time" (Parasuraman et al, 1985). But this definition results from early papers and strongly connected to goods sector but considered inadequate for the quality definition in services. To address this issue several studies have been made for the last thirty years and some addressed security (or as in several exercises 'privacy') as a dimension to be evaluated but not as a service to be consider (Bauer et al., 2006; Parasuraman et al., 2005; Poon, 2008; Wolfinbarger & Gilly, 2003).

Parasuraman et al. (1985) approached the subject of service quality by defining a service quality model that provided a framework on the area resulting from empirical studies in several industry sectors (Parasuraman & Berr, 1991). These researchers (Parasuraman et al., 1988) identified 10 service quality dimensions (reliability, responsiveness, competence, access, courtesy, communication, credibility, security, understanding/knowing the customer, and tangibles). After reevaluation, these researchers reduced the number of dimensions to five due to overlaps identified in empirical investigations. Therefore, the refined SERVQUAL presents five service quality dimensions:

- Tangibles - this dimension deals with the physical environment. It relates to customer assessments of the facilities, equipment, and appearance of those providing the service;

- Reliability - this dimension deals with customer perceptions that the service provider is providing the promised service in a reliable and dependable manner, and is doing so on time;

- Responsiveness - this dimension deals with customer perceptions about the willingness of the service provider to help the customers and not shrug off their requests for assistance;

- Assurance - this dimension deals with customer perceptions that the service provider's behavior instills confidence in them through the provider's courtesy and ability;

- Empathy - this dimension deals with customer perceptions that the service provider is giving them individualized attention and has their best interests at heart.

SERVQUAL observation is based on the assessment of 22 items, where each item is measured according to the performance of the service provided and the expectations for the service. The score is calculated as the difference between performance and expectations. The greater the scores, the higher the perceived service quality (Ladhari, 2010). In the absence of objective measures, an appropriate approach for assessing the quality of a firm's service is to measure consumers' perceptions of quality (Parasuraman et al., 1988). The SERVQUAL instrument assesses the gap between what is expected and what is delivered, using two seven-point scales: one to measure general expectations about companies in a service sector, the other to measure perceptions about a particular company.

The value for the use of Parasuraman SERVQUAL is stressed by several papers. It allowed researchers to use it for benchmarking or as a diagnostic tool (Kettinger et al., 1997). Previous research has second that SERVQUAL could be used for IS service quality measurement (Parasuraman & Berry, 1991; Van Dyke, Kappelman, & Prybutok, 1997). For instance, Barnes and Vidgen (2001) worked in the development of WEBQUAL 2.0, an instrument to evaluate Internet bookshop Web sites. This instrument was an evolution from the original WebQual instrument (WebQual 1.0) through SERVQUAL research and insight.

SERVQUAL also served as base to develop two scales for assessing electronic service quality: E-S-Qual and E-RecS-Qual. These two scales were developed for service quality delivered by Web sites on which customers shop online (Parasuraman et al., 2005). Previous research also seconds the use of this tool for intrafirm context (Kettinger et al., 1997).

3. CONCEPTUAL MODEL AND HYPOTHESES

3.1. THE CONCEPTUAL MODEL

In order to accomplish what has been proposed, two concerns must be addressed: i) Cybersecurity service quality measure; ii) impact of service quality in the individual and on the Organization itself. To address the first concern, SERVQUAL instrument will be used as been observed as suitable to assess electronic service quality. To provide an observation regarding the impact of the service quality on the user (as an individual) and on the organization, DeLone and McLean model will be used. Figure 1 presents the adapted model steamed from the earlier mentioned instruments.

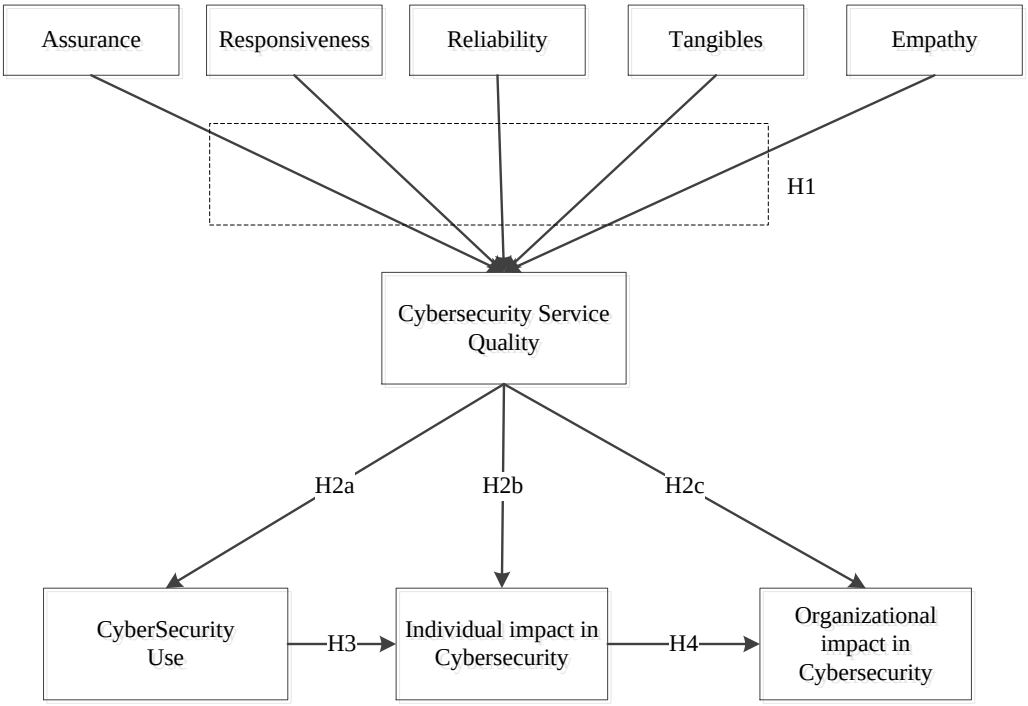

Figure 1 - The Research Model

3.2. HYPOTHESES

From Parasuraman et al. study (Parasuraman et al., 1988), five indicators define and allow the measurement of the quality of service: empathy (EMP), reliability (REL), responsiveness (RES), assurance (ASS), and tangibles (TAN). Although developed from a marketing perspective (Parasuraman et al., 1988; Pitt et al., 1997), over the last three decades it has been used by several researchers to measure specific kind of services (Bauer et al., 2006; Dinget al., 2011; Parasuraman et al., 1988, 2005).

H1 – 2nd order constructs (assurance, responsiveness, reliability, tangibles and, empathy) estimate Cybersecurity service quality

Information-handling services are delivered via the organization's portfolio of applications that are implemented on its technology platform (Peppard, 2003). Intuitively, in a healthy Portfolio, all of the important systems will have good technical quality and be used regularly (Weill & Vitale, 1999). Generally speaking there are two kind of IS services: information-handling services such as communication and collaboration, data capture, storage, processing, access and analysis; and, services around the specification of technology and applications, services concerned with design and construction of the technical infrastructure, services eliciting and analyzing user requirements, services focused around user and management education, training and support, services centered around security and disaster recovery, services focused on software development, project management services, vendor and contract management services, and maintenance services that are required in order for these information handling services to be made available to users (Peppard, 2003). Cybersecurity is a supportive service to Information-handling services.

Quality was clearly identified has a category of I/S success (W. H. DeLone & McLean, 1992), either the characteristics of IS itself which produces the information (System Quality) or in the desired characteristics such as accuracy, meaningfulness and timeliness related to Information quality. While IS managers may want to know how they compare to other IS departments, nowadays many want to compare themselves to

other excellent service providers, especially those serving external customers (Pitt et al., 1997). The use of information system reports, or of management science/operations research models, is one of the most frequently reported measures of the success of an IS or an MS/OR model (W. H. DeLone & McLean, 1992) therefore, relating quality to use. Additionally, technical quality has long been suggested as an important factor that influences IS use and performance (W. H. DeLone & McLean, 1992). The relation between quality and use, was also noted in SaaS (Software as a Service) literature: given a growing service orientation in the IS Industry and with SaaS-based software delivery quickly gaining importance, it has become critical for companies to regularly assess the service quality factors of SaaS services and their importance for continued IS usage (Benlian, Koufaris, & Hess, 2011).

H2a - Cybersecurity service quality has a positive influence on Cybersecurity use

The failure to fulfill customers' expectations regarding service quality, such as application availability or vendor responsiveness, may thus have critical consequences not only for the customers but also for the vendors (Benlian et al., 2011). As concluded by Etezadi-Amoli and Farhoomand (1996) in their study about end user computing satisfaction and user performance, performance may change a user's perception of application software and subsequently affect the degree of his/her satisfaction. In this study is also stated that user performance should enable companies to assess the degree of success of a given application software in improving work environment. As can be seen in DeLone and McLean study (2003), performance is a measure for quality observed. From the above, the correlation between Cybersecurity service quality (SQ) and individual impact in Cybersecurity is suggested.

H2b - Cybersecurity service quality has a positive influence on individual impact in Cybersecurity

Field studies and case studies which have dealt with the influence of information systems have chosen various organizational performance measures for their dependent variable (W. H. DeLone & McLean, 1992). In other words, Information Systems characteristics have an impact in the organizations. Rivard & Huff, in 1984, interviewed data processing executives and asked them to assess the cost reductions and company profits realized from specific user-developed application programs. Benefits from an IS can come from a variety of sources. Since information systems are deployed through IS services has mentioned earlier, is inferred that benefits from IS services, also having several sources, can influence positively (benefits) corporate activity.

H2c - Cybersecurity service quality has a positive influence on organizational impact in Cybersecurity

Individuals may use technologies to assist them in the performance of their tasks (Goodhue & Thompson, 1995). Inferences from this observation alone provide theoretical support. Nevertheless, as stated in previous work (Thompson, Higgins, & Howell, 1991) when use is optional, however, having access to the technology by no means ensures it will be used or used effectively. This observation links information systems use or the information systems service use to the will of company users. Even when the use is “mandatory” the way that user relates to the IS service is still a user domain. In a research conducted by Rivard and Huff (1984) it was found that one of the measure of user satisfaction to IS services was “Improvement in user productivity and in decision making outcomes due to user developed applications (UDA)”. Individual impacts were measured in terms of job performance and decision-making performance (DeLone & McLean, 2003).

H3 – Cybersecurity use has a positive influence on individual impact in Cybersecurity

Measures of individual performance and, to a greater extent, organization performance are of considerable importance to IS practitioners (W. H. DeLone & McLean, 1992). Organizational impact represents the firm-level benefits received by an organization because of IS applications (Gorla et al., 2010). Benbasat and Dexter (1986) have study the impact on managers due to an technological evolution. The objective was to test the effects of color and graphics on decision making performance under differing time constraints; Managers were told that their performance would be evaluated based on the amount of profit they obtained from budget allocation decision.

H4 – individual impact with Cybersecurity has a positive influence on organizational impact in Cybersecurity

4. METHODOLOGY

4.1. MEASUREMENT

To test the model presented earlier in Figure 1, we conducted a survey where respondents from different industry were invited to participate. The instrument adapted from SERVQUAL was slightly adapted to Cybersecurity context and translation issues were not found. The inquiry was divided in two phase: first, was considered a sample of thirty (30) respondents to validate language and interpretation issues and also to test the reliability and validity of the instruments scale. After careful consideration and feedback analysis from phase one, some respondents reported difficulties in responding some questions due to "lack of technical knowledge" or even "lack of knowledge about the theme". Being these issues not related to the questionnaire items itself, second phase was started where a larger group of individuals were invited to participate. The resulting survey instrument and measurement items are shown in the Appendix.

The variable Cybersecurity service quality was measured as a IT service provide inside corporate premises as discussed over section 2. Using SERVQUAL (Parasuraman et al., 1988), second order constructs were used to measure quality of this service: empathy (EMP), reliability (REL), responsiveness (RES), assurance (ASS), and tangibles (TAN) slightly adapted to Cybersecurity context. Cybersecurity service quality (CSQ) dependent variable was measured in terms of user friendly, easy to use, system accuracy and satisfaction regarding system accuracy according to previous works on the subject (Doll & Torkzadeh, 1988). These items were also adapted to Cybersecurity context.

The Cybersecurity use was measured by four items considering the work of (Thompson et al., 1991) where system use were observed in terms of intensity of use, frequency of use, system use introduction and new system introduction in the organization (William H. DeLone & McLean, 2003). The Individual Impact in Cybersecurity evaluation was captured by four items according to the approach of Izak Benbasat & Dexter (1979) study regarding usefulness, easy understanding and problem

solving tool. This reading ensures an observation regarding change in behavior of the consumer of Cybersecurity service.

Organizational impact in Cybersecurity followed the approach preconized by studies on the subject (W. H. DeLone & McLean, 1992; William H. DeLone & McLean, 2003) were this impact was measured in four items considering managerial concerns i.e. cost reduction, increase work volume, increased effectiveness and staff reduction (Danziger, 1979).

4.2. DATA

Data was collected using an online survey over a six weeks period (October to November 2014). Although over 203 respondents accepted the survey invitation, only 111 complete answers were collected. Table 1 provides information regarding the sample. Related IT respondents 36% and Non-IT respondents 64% could support the lack of complete answers. The sample covered a wide range of industries where "services" represented 63.1% of the complete answers collected.

	(%)	Obs.
Type of Industry		
Services	63.1%	70
Human Health and Social Work Activities	4.5%	5
Wholesale and retail trade	4.5%	5
Construction	1.8%	2
Manufacturing	5.4%	6
IT and Communications	16.2%	18
Academy	4.5%	5
Respondents Title		
IT Respondents	36,0%	40
Non-IT Respondents	64,0%	71

Table 1 – Sample Characteristics

5. RESULTS

According to the work of Henseler et al. (2009) in order to examine the casual relationships of the conceptual model, we used partial least squares (PLS) to estimate the research model. First, we review our motivations as those pointed as being as the most important to use PLS: exploration and prediction, since PLS path modeling is recommended in an early stage of theoretical development in order to test and validate exploratory models. Second, due to PLS path modeling characteristics: i) PLS path modeling avoids small sample size problems and can therefore be applied in some situations when other methods cannot; ii) PLS can handle both reflective and formative measurement models. Nevertheless, before testing the structural model, we examined the measurement model to assess reliability and validity.

5.1. MEASUREMENT MODEL

The results of the measurement model are provided by tables 2 and 3. Construct validity, indicator validity, convergent validity, and discriminant validity have been assessed.

	CR	EMP	TAN	REL	RES	ASS	CSQ	USE	IIS	OIS
EMP	**0.963**	**0.915**								
TAN	**0.923**	-0.442	**0.866**							
REL	**0.953**	-0.491	0.783	**0.895**						
RES	**0.913**	0.741	-0.346	-0.423	**0.852**					
ASS	**0.945**	-0.537	0.709	0.857	-0.429	**0.900**				
CSQ	**0.680**	-0.738	0.835	0.920	-0.644	0.899	**NA**			
USE	**0.964**	-0.456	0.706	0.779	-0.379	0.676	0.766	**0.934**		
IIS	**0.947**	-0.348	0.624	0.702	-0.369	0.649	0.688	0.701	**0.904**	
OIS	**0.927**	-0.220	0.505	0.646	-0.213	0.496	0.552	0.677	0.745	**0.873**

Table 2 – Correlation matrix and composite reliability

Note:

(i) CR – composite reliability, EMP – empathy, TAN – tangibles, REL – reliability, RES – responsiveness, ASS – assurance, USE – Cybersecurity use, IIS – individual impact in Cybersecurity and OIS – organizational impact in Cybersecurity

(ii) NA – Not Applicable

CONS	Item	EMP	TAN	REL	RES	ASS	USE	IIS	OIS
EMP	EMP1	**0.934**	-0.426	-0.444	0.698	-0.484	-0.458	-0.319	-0.224
	EMP2	**0.909**	-0.456	-0.479	0.741	-0.477	-0.462	-0.371	-0.242
	EMP3	**0.948**	-0.444	-0.486	0.694	-0.539	-0.456	-0.385	-0.262
	EMP4	**0.932**	-0.348	-0.425	0.675	-0.475	-0.383	-0.311	-0.170
	EMP5	**0.849**	-0.339	-0.405	0.572	-0.480	-0.312	-0.188	-0.091
TAN	TAN1	-0.404	**0.814**	0.696	-0.283	0.650	0.617	0.551	0.442
	TAN2	-0.364	**0.879**	0.612	-0.307	0.501	0.606	0.497	0.432
	TAN3	-0.411	**0.866**	0.756	-0.347	0.699	0.641	0.584	0.480
	TAN4	-0.347	**0.903**	0.631	-0.254	0.587	0.575	0.520	0.387
REL	REL1	-0.427	0.710	**0.888**	-0.395	0.730	0.716	0.652	0.617
	REL2	-0.408	0.590	**0.874**	-0.343	0.805	0.561	0.567	0.504
	REL3	-0.465	0.709	**0.911**	-0.393	0.802	0.712	0.600	0.527
	REL4	-0.474	0.741	**0.937**	-0.393	0.792	0.733	0.656	0.604
	REL5	-0.419	0.748	**0.861**	-0.369	0.707	0.757	0.663	0.638
RES	RES1	0.497	-0.173	-0.213	**0.752**	-0.217	-0.248	-0.299	-0.243
	RES2	0.604	-0.282	-0.342	**0.888**	-0.304	-0.338	-0.320	-0.222
	RES3	0.621	-0.256	-0.346	**0.880**	-0.377	-0.280	-0.258	-0.077
	RES4	0.753	-0.412	-0.480	**0.881**	-0.498	-0.394	-0.370	-0.202
ASS	ASS1	-0.479	0.640	0.827	-0.398	**0.928**	0.656	0.637	0.474
	ASS2	-0.530	0.685	0.804	-0.433	**0.947**	0.610	0.571	0.426
	ASS3	-0.450	0.510	0.634	-0.336	**0.823**	0.483	0.445	0.325
	ASS4	-0.470	0.701	0.806	-0.374	**0.897**	0.670	0.667	0.546
USE	CUPS1	-0.437	0.631	0.723	-0.339	0.612	**0.944**	0.635	0.654
	CUPS2	-0.417	0.661	0.768	-0.369	0.659	**0.949**	0.673	0.654
	CUPS3	-0.435	0.701	0.704	-0.378	0.630	**0.943**	0.648	0.590
	CUPS4	-0.413	0.644	0.711	-0.327	0.621	**0.897**	0.661	0.628
IIS	IIS1	-0.275	0.547	0.618	-0.330	0.544	0.652	**0.891**	0.662
	IIS2	-0.352	0.595	0.668	-0.330	0.605	0.662	**0.873**	0.666
	IIS3	-0.383	0.575	0.665	-0.366	0.623	0.650	**0.928**	0.658
	IIS4	-0.244	0.538	0.584	-0.305	0.572	0.569	**0.922**	0.704
OIS	OIS1	-0.168	0.381	0.537	-0.149	0.417	0.545	0.659	**0.886**
	OIS2	-0.202	0.470	0.598	-0.231	0.441	0.664	0.714	**0.923**
	OIS3	-0.300	0.543	0.674	-0.275	0.560	0.646	0.667	**0.887**
	OIS4	-0.078	0.355	0.426	-0.066	0.295	0.494	0.546	**0.791**

Table 3 – Loadings and cross-loadings for the measurement model

Note:

i) EMP – empathy, TAN – tangibles, REL – reliability, RES – responsiveness, ASS – assurance, USE – Cybersecurity use, IIS – individual impact in Cybersecurity and OIS – organizational impact in Cybersecurity.

The construct validity was tested using the composite reliability coefficient. As shown in Table 2, all the constructs have a composite reliability above 0.7 (Straub, 1989) indicating that the scales have internal consistency. The indicator reliability was evaluated based on the criteria that the loadings should be greater than 0.70, and that

every loading lesser than 0.4 should be eliminated (Henseler et al., 2009). Overall, the instrument presents good indictor reliability.

Average variance extracted (AVE) was used as the criterion to test convergent validity and it should be higher than 0.5 so that the latent variable explains more than half of the variance of its indicators (Henseler et al., 2009) has shown in Table 2 – all constructs have AVE higher than 0.5 satisfying this criteria. Constructs discriminant validity was assessed using Fornell-Larcker criterion and Cross-loadings. The first criterion indicate that the square root of AVE should be greater that the correlations between the construct (Fornell & Larcker, 1981). The second criterion mandates that the loading of each indicator should be greater than all cross-loadings. As seen in Table 2, the square roots of AVEs are higher than the correlation between each pair of constructs (off diagonal values). Patterns of loadings are greater than cross-loadings as can be seen in Table 3. Therefore, both measures are satisfied. The assessments of construct reliability, indicator reliability, convergent validity, and discriminant validity of the constructs are satisfactory indicating that the reflective constructs can be used to test the conceptual model. The five formative constructs (assurance, responsiveness, reliability, tangibles, and empathy) that modeled Cybersecurity service quality, had absolute weight value between 0.141 and 0.352, and all are statistically significant at 0.01. Regarding multicollinearity, the VIF for each indicator was computed range between 2.25 and 4.98. For all items, the VIF is below the cut-off value of 10 (Hair et al., 2010). Consequently, constructs can be used to test the conceptual model.

5.2. STRUCTURAL MODEL

The structural model was assessed using R^2 measures and the level of significance of the path coefficients. Figure 2, presented below, shows the model results. The calculated R^2 values of dependent variables reveals that our models explain: 100% of variation in Cybersecurity service quality (CSQ); 59.0% of variation in Cybersecurity use (USE); 55.9% of variation in individual impact in Cybersecurity (IIS); and 58.7% of variation in organizational impact in Cybersecurity (OIS). The significance of the path coefficients was assessed by means of bootstrapping procedure (Henseler et al., 2009) with 500 resampling.

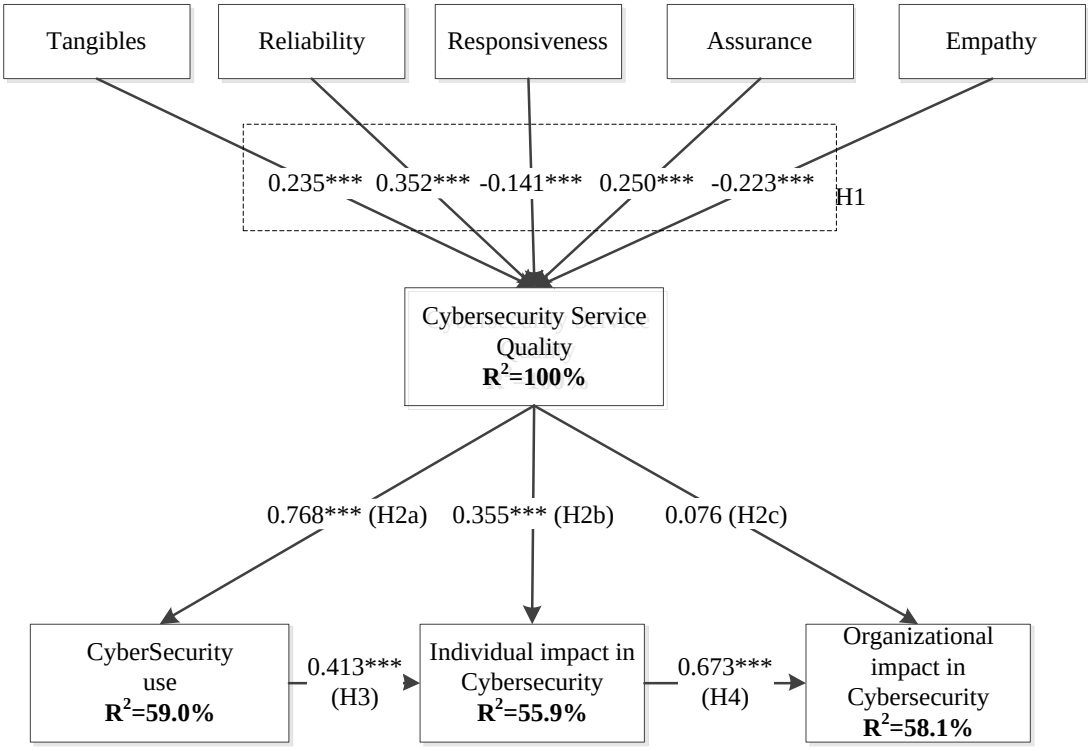

Figure 2 – Results of the Conceptual Model

Our study found that, regarding the second order formative constructs, tangibles ($\hat{\beta}$=-0.141; p<0.01), reliability ($\hat{\beta}$ =0.352; p<0.01), responsiveness ($\hat{\beta}$=0.235; p<0.01), assurance ($\hat{\beta}$=-0.223; p<0.01) and empathy ($\hat{\beta}$ =0.23; p<0.01) are statistically significant, therefore supporting hypothesis H1.

Cybersecurity service quality is statistically significant to explain Cybersecurity use ($\hat{\beta}$=0.768; p<0.01) and individual impact in Cybersecurity ($\hat{\beta}$=0.355; p<0.01), supporting both hypotheses H2a and H2b. In other hand, Cybersecurity service quality is not statistically significant to explain organization impact in Cybersecurity ($\hat{\beta}$=0.076; p>0.10). Hence hypothesis H2c is not supported.

Cybersecurity use is statistically significant to explain individual impact in Cybersecurity ($\hat{\beta}$=0.413; p<0.01), consequently hypothesis H3 is confirmed. Individual impact in Cybersecurity is statistically significant to explain organizational impact in Cybersecurity ($\hat{\beta}$=0.673; p<0.01). Therefore, hypothesis H4 is confirmed.

6. DISCUSSION

The research model presented in this paper has assessed Cybersecurity service quality and contextualized, through DeLone and McLean IS success model, providing individual impact and organizational impact insights. The use of this model was carefully considered and the analysis of service quality impact to the organizational has been seen as a major contribution. The interpretation of the results based on the empirical findings is presented next.

6.1. MAJOR FINDINGS

The study shows that all constructs for the second order construct Cybersecurity service quality (CSQ) are statistically significant. While "reliability", "assurance" and "tangible" constructs positively influence CSQ, "empathy" and "responsiveness" contribute in opposite way, promoting a negative influence. This can be explained by the measured items: "empathy" was observed as customer perceptions that the service provider is giving them individualized attention and has their best interests at heart. As seen by Peppard (2003) there could be a situation where a smaller help desk, staffed by friendly service staff is perceived as providing a better service to users than a larger desk with unfriendly staff. Our findings are in line with previous works that also observed that the dimension of 'empathy' is less important in the electronic service quality context because the online environment lacks personal human interaction (Gefen, 2002; Ladhari, 2010). Regarding "responsiveness", the measured items dealt with customer perceptions about the willingness of the service provider to help the customers and not shrug off their requests for assistance; Igbaria & Tan (1997) found that external computing support was related to perceived system usefulness, but that internal computing support was not related to perceived usefulness.

Prior service quality studies have observed a relation between "responsiveness" and loyalty (Akinci, Atilgan-Inan, & Aksoy, 2010; Marimon, Petnji Yaya, & Casadesus Fa, 2012; Wolfinbarger & Gilly, 2003). Cybersecurity use is explained by Cybersecurity quality service (R^2=59%) confirming other studies on the theme (W. H. DeLone & McLean, 1992; William H. DeLone & McLean, 2003). This means that service quality

largely explains the use of the Cybersecurity service. The research model validates the relationship between Cybersecurity service quality (CSQ) and individual impact in Cybersecurity (IIS) and also validates the relationship between Cybersecurity use (USE) and individual impact in Cybersecurity (IIS). Both variables explain 55.9% of variation in the IIS.

Finally, the research model explains 58.1% of variation in organizational impact in Cybersecurity (OIS) being individual impact in Cybersecurity the only construct statistically significant to explain OIS. This means that, when regarding to organization impact in Cybersecurity, the behavior of the individual has greater influence than the quality of the Cybersecurity service provided by the organization.

6.2. Practical Implications

We consider that this study has brought to light several important considerations regarding service quality assessment in corporate environment, individual impact and organization impact. From the results, it can be inferred that SERVQUAL is a valid instrument to assess this kind of service in order with several studies that have been using this multi-item instrument to assess service quality in electronic context (Benlian et al., 2011; Ding et al., 2011; Parasuraman et al., 2005; Wolfinbarger & Gilly, 2003). The DeLone and McLean model to address IS success has contextualized the service assessment results and provided insights relating the quality of the service and service use to the user. Study results also provided insights regarding the service quality and individual impact to the organization, useful when addressing Cybersecurity programs.

6.3. Theoretical Contributions

Our study presents several contributions to further increase the service quality knowledge in general and quality in information security in particular. To notice a pioneer study to assess quality measurement in a specific IS service that until now, to our recollection, it hasn't been attempted.

Using a well-known instrument (SERVQUAL) we continue in the long tradition of service quality research by developing, refining, and testing a service quality instrument (SaaS-Qual) for a specific context (SaaS) (Benlian et al., 2011).

Furthermore, by contributing to augment the knowledge about service science, we assure a better understanding of the issue as suggested by other researchers (Van Dyke et al., 1997) and respond to the calling to provide more experimental and behavioral approaches in service science research, specifically to answer questions on customer experience […] (Bardhan et al., 2010).

7. CONCLUSIONS

This study has used a multi-item instrument developed in 1988 to assess the quality of Cybersecurity as a service provided in corporate environment. The result posits that SERVQUAL is suitable to assess electronic service quality, in this case Cybersecurity service. The result also shows that all first order constructs contribute to explain the Cybersecurity service quality (second order construct). “Reliability” and “tangibles” are the greatest contributors with a positive influence on Cybersecurity service quality. From the model results is also possible to conclude that the quality of the Cybersecurity service provided explains 59% of variation of Cybersecurity use. By using the DeLone and McLean IS success model to contextualize Cybersecurity service quality, this research presents a holistic approach for future studies on Cybersecurity and its impacts. For practitioners, we consider that this research presents valuable insights for developing and implementing Cybersecurity corporate strategies.

8. BIBLIOGRAPHY

Akinci, S., Atilgan-Inan, E., & Aksoy, S. (2010). Re-assessment of E-S-Qual and E-RecS-Qual in a pure service setting. *Journal of Business Research*, *63*(3), 232–240. http://doi.org/10.1016/j.jbusres.2009.02.018

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276–289. http://doi.org/10.1016/j.cose.2006.11.004

Anderson, J. M. (2003). security, 308–313.

Baker, W. H., & Wallace, L. (2007). Is Information Security Under Control? *IEEE Security & Privacy Magazine*, (January/February), 36–44.

Bardhan, I. R., Demirkan, H., Kannan, P. K., Kauffman, R. J., & Sougstad, R. (2010). An Interdisciplinary Perspective on IT Services Management and Service Science. *Journal of Management Information Systems*, *26*(4), 13–64. http://doi.org/10.2753/MIS0742-1222260402

Barnes, S. I., & Vidgen, R. (2001). An Evaluation of Cyber-Bookshops: The WebQual Method. *International Journal of Electronic Commerce*, *6*(1), 11–30.

Bauer, H. H., Falk, T., & Hammerschmidt, M. (2006). eTransQual: A transaction process-based approach for capturing service quality in online shopping. *Journal of Business Research*, *59*(7), 866–875. Retrieved from http://www.sciencedirect.com/science/article/pii/S0148296306000646

Benbasat, I., & Dexter, A. (1986). An investigation of the effectiveness of color and graphical information presentation under varying time constraints. *MIS Quarterly*, (March), 59–83. Retrieved from http://www.jstor.org/stable/248881

Benbasat, I., & Dexter, A. S. (1979). Value and Events Approaches to Accounting: An Experimental Evaluation. *Accounting Review*, *54*(4), 735. Retrieved from http://www.lib.lsu.edu/apps/onoffcampus.php?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=4489006&site=ehost-live&scope=site

Benlian, A., Koufaris, M., & Hess, T. (2011). Service Quality in Software-as-a-Service: Developing the SaaS-Qual Measure and Examining Its Role in Usage Continuance. *Journal of Management Information Systems*, *28*(3), 85–126. http://doi.org/10.2753/MIS0742-1222280303

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. http://doi.org/10.1016/j.chb.2012.05.003

Danziger, J. N. (1979). Technology and Productivity: A Contingency Analysis of Computers in Local Government. *Administration & Society*, *11*(2), 144–171. http://doi.org/10.1177/009539977901100202

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research*, *3*(1), 60–95. http://doi.org/10.1287/isre.3.1.60

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success : A Ten-Year Update. *Journal of Management Information Systems*, *19*(4), 9–30. http://doi.org/10.1073/pnas.0914199107

Dhillon, G., & Backhouse, J. (1996). Risks in the Use of Information Technology Within Organizations. *International Journal of Information Management*, *16*(1994), 65–74.

Dhillon, G., & Backhouse, J. (2000). Security Management in the New Millennium, *43*(7), 125–128.

Ding, D. X., Hu, P. J.-H., & Sheng, O. R. L. (2011). e-SELFQUAL: A scale for measuring online self-service quality. *Journal of Business Research*, *64*(5), 508–515. http://doi.org/10.1016/j.jbusres.2010.04.007

Doll, W. J., & Torkzadeh, G. (1988). The Measurement of End-User Computing Satisfaction The End-User Computing. *MIS Quarterly*, (June), 259–275.

Etezadi-Amoli, J., & Farhoomand, A. F. (1996). A structural model of end user computing satisfaction and user performance. *Information & Management*, *30*(2), 65–73. http://doi.org/10.1016/0378-7206(95)00052-6

Fornell, C., & Larcker, D. F. (1981). Evaluation Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(February), 39 – 50.

Garfinkel, S. L. (2012). Inside Risks The Cybersecurity Risk. *Communications of the ACM*, *55*(6), 29–32. http://doi.org/10.1145/2184319.2184330

Gefen, D. (2002). Customer Loyalty in E-Commerce. *Journal of the Association for Information Systems*, *3*, 27–51. http://doi.org/10.1016/S0022-4359(01)00065-3

Goodhue, D. L., & Thompson, R. L. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, *19*(2), 213. http://doi.org/10.2307/249689

Gorla, N., Somers, T. M., & Wong, B. (2010). Organizational impact of system quality, information quality, and service quality. *The Journal of Strategic Information Systems*, *19*(3), 207–228. http://doi.org/10.1016/j.jsis.2010.05.001

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis, 7th Ed., Upper Saddle River, NJ, USA: Prentice-Hall*.

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, *11*(1), 55–61. http://doi.org/10.1016/j.istr.2005.12.004

Henseler, J., Ringle, C. M., & Sinkovics, R. (2009). The use of partial least squares path modeling in international marketing. *Advan in International Marketing*, *20*(2009), 277–319. http://doi.org/10.1108/S1474-7979(2009)0000020014

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, *29*(3), 236–245. http://doi.org/10.1016/j.clsr.2013.03.003

Igbaria, M., & Tan, M. (1997). The consequences of information technology acceptance on subsequent individual performance. *Information & Management*, *32*(3), 113–121. http://doi.org/10.1016/S0378-7206(97)00006-2

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. http://doi.org/10.1016/S0268-4012(02)00105-6

Kettinger, B. W. J., Lee, C. C., & Perdue, F. P. (1997). Pragmatic Perspectives on the Measurement of Information Systems Service Quality, (June), 223–241.

Ladhari, R. (2010). Developing e-service quality scales: A literature review. *Journal of Retailing and Consumer Services*, *17*(6), 464–477. http://doi.org/10.1016/j.jretconser.2010.06.003

Marimon, F., Petnji Yaya, L. H., & Casadesus Fa, M. (2012). Impact of e-Quality and service recovery on loyalty: A study of e-banking in Spain. *Total Quality Management & Business Excellence*, *23*(7-8), 769–787. http://doi.org/10.1080/14783363.2011.637795

Parasuraman, A., & Berry. (1991). Refinement and Reassessment of the SERVQUAL Scale. *Journal of Retailing*, *67*(4), 420–452.

Parasuraman, A., Berry, L., & Zeithaml, V. (1988). SERVQUAL : A Multiple-Item Scale for Measuring Consumer Perceptions of Service Quality. *Journal of Retailing*, *64*(1).

Parasuraman, A., Zeithaml, V., & Malhotra, A. (2005). E-S-QUAL: A Multiple-Item Scale for Assessing Electronic Service Quality. *Journal of Service Research*, *7*(3), 213–233. http://doi.org/10.1177/1094670504271156

Parasuraman, A., Zelthami, V. A., & Berry, L. L. (1985). A Conceptual Model of Service Quality and Its Implications for Future Research, *49*(1979), 41–50.

Parasuraman, & Berr. (1991). More on Improving Service Quality Measurement. *Journal of Retailing*, *69*(1), 140–147.

Peppard, J. (2003). Managing IT as a Portfolio of Services. *European Management Journal*, *21*(4), 467–483. http://doi.org/10.1016/S0263-2373(03)00074-4

Pitt, L. F., Watson, R. T., & Kavan, C. B. (1997). Measuring information systems service quality: concerns for a complete canvas. *MIS Quarterly*, *21*(June), 209–222. http://doi.org/10.2307/249420

Poon, W.-C. (2008). Users' adoption of e-banking services: the Malaysian perspective. *Journal of Business & Industrial Marketing*, *23*(1), 59–69. http://doi.org/10.1108/08858620810841498

Poon, W.-C., & Lee, C. K.-C. (2012). E-Service Quality: An Empirical Investigation. *Journal of Asia-Pacific Business*, *13*(3), 229–262. http://doi.org/10.1080/10599231.2012.690682

Rees, J., Bandyopadhyay, S., & Spafford, E. (2003). PFIRES: a policy framework for information security. *Communications of the ACM*, *46*(7), 101–106. Retrieved from http://dl.acm.org/citation.cfm?id=792706

Rivard, S., & Huff, S. L. (1984). User Developed Applications: Evaluation of Success from the DP Department Perspective. *MIS Quarterly*, *8*(1), 39–50. 12p. 1 Diagram.

Ruighaver, a. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56–62. http://doi.org/10.1016/j.cose.2006.10.008

Schultz, E. (2005). The human factor in security. *Computers & Security*, *24*(6), 425–426. http://doi.org/10.1016/j.cose.2005.07.002

Steele, S., & Wargo, C. (2007). An Introduction to Insider Threat Management. *Information Systems Security*, *16*(1), 23–33. http://doi.org/10.1080/10658980601051334

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(June 1986), 147–169. http://doi.org/10.2307/248922

Thompson, R., Higgins, C., & Howell, J. (1991). Personal computing: toward a conceptual model of utilization. *MIS Quarterly*, (June 1989), 125–144. Retrieved from http://www.jstor.org/stable/249443

Usa. (2002). SOX act of 2002. *Public Law*, *2*, 1–670. Retrieved from http://www2.ed.gov/policy/elsec/leg/esea02/107-110.pdf

Van Dyke, T. P., Kappelman, L. A., & Prybutok, V. R. (1997). Measuring Information Systems Service Quail ity : Concerns on the Use of the SERVQUAL Questionnaire. *MIS Quarterly*, (June), 195–208.

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. http://doi.org/10.1016/j.cose.2013.04.004

Weill, P., & Vitale, M. (1999). Assessing the health of an information systems applications portfolio: An example from process manufacturing. *MIS Quarterly*, *23*(4), 601–624. Retrieved from http://www.jstor.org/stable/249491

Whitman, M. E. (2003). Information Security. *Communications of the ACM*, *46*(8), 91–95.

Wolfinbarger, M., & Gilly, M. C. (2003). eTailQ: dimensionalizing, measuring and predicting etail quality. *Journal of Retailing*, *79*(3), 183–198. http://doi.org/10.1016/S0022-4359(03)00034-4

Wood, C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*. Retrieved from http://www.sciencedirect.com/science/article/pii/S1361372304000193

Yakhlef, A., & Sié, L. (2012). From Producer to Purchaser of IT Services: interactional Knowledge. *Knowledge and Process Management*, *19*(2), 79–90. http://doi.org/10.1002/kpm

Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. *Human Resource Management Review*, *23*(1), 105–113. http://doi.org/10.1016/j.hrmr.2012.06.010

9. APPENDIX – SURVEY QUESTIONNAIRE

Constructs		Items		Source
Cybersecurity service quality	assurance	ASS1	I can trust the IT Department cyber security members of my organization.	(Parasuraman et al., 1988)
		ASS2	I feel secure in my interactions with my IT Department people.	
		ASS3	IT Department cyber security technicians of my organization are polite.	
		ASS4	Employees get adequate cyber security support from the IT Department of my organization to do their jobs well.	
	responsiveness	RES1	The IT Department of my company does not tell users exactly when cyber security services will be performed.	(Parasuraman et al., 1988)
		RES2	I do not receive prompt cyber security service from the IT Department of my company.	
		RES3	IT technicians from the IT Department of my company are not always willing to help users when cyber security issues arise.	
		RES4	IT technicians from the IT Department of my company are too busy to respond to user's cyber security requests promptly.	
	reliability	REL1	When IT Department people promise to do something regarding cyber security by a certain time, they do so.	(Parasuraman et al., 1988)
		REL2	When I have cyber security issues, my IT Department technicians are sympathetic and reassuring.	
		REL3	Regarding cyber security, the IT Department of my company is dependable.	
		REL4	IT Department provides its cyber security services at the time it promises to do so.	

Constructs		Items		Source
		REL5	The IT Department of my company keeps its security records accurately.	
	tangibles	TAN1	The IT Department of my company has up-to-date cyber security equipment.	(Parasuraman et al., 1988)
		TAN2	The IT Department of my company has physically secure facilities that are visually appealing.	
		TAN3	The IT Department of my company has employees who appear professional with respect to security.	
		TAN4	The appearance of the physical facilities of the IT Department of my company is in keeping with the type of cyber security services provided by it.	
	empathy	EMP1	IT People do not give me individual attention on cyber security issues.	(Parasuraman et al., 1988)
		EMP2	Cyber security technicians from my organization do not give me personal attention.	
		EMP3	IT Department people of my organization do not know what my cyber security needs are.	
		EMP4	With respect to cyber security, IT Department people do not have my best interests at heart.	
		EMP5	Operating hours of IT Department for cyber security support are not convenient to all their users.	
Cybersecurity use		CUSP1	There is intensity of use of my company's cybersecurity solution.	(Thompson et al., 1991)
		CUSP2	In my company we frequently use the cybersecurity solutions.	
		CUSP3	In general, my organization has supported the introduction of cybersecurity solutions.	

Constructs	Items		Source
	CUSP4	The senior management of this business unit has been helpful in introducing cybersecurity solutions.	
Individual impact in Cybersecurity	IIS1	The reports provided by the cybersecurity systems of my company are very useful for identifying and defining cybersecurity problems.	(I Benbasat & Dexter, 1986)
	IIS2	The cybersecurity solutions in use in my company are very easy to understand.	
	IIS3	The cybersecurity solutions in use in my company are useful for selecting among alternative courses of action.	
	IIS4	The cybersecurity reports in use in my company are very useful in formulating solutions to the problem.	
Organizational impact in Cybersecurity	OIS1	The Cybersecurity solutions in use in my company have reduced the cost of operations.	(Danziger, 1979)
	OIS2	The Cybersecurity solutions in use in my company allow handling a greater volume of service without corresponding increases in cost.	
	OIS3	The Cybersecurity solutions in use in my company have increased the effectiveness of my company. (reversed question from original)	
	OIS4	The Cybersecurity solutions in use in my company have reduced the number of people necessary to perform cybersecurity tasks.	