Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2014 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2014

A TYPOLOGY OF TECHNOLOGICAL ENABLERS OF WEBSITE SERVICE FAILURE PREVENTION

Alireza Nili
School of Information Management, Victoria University of Wellington, New Zealand, alireza.nili@vuw.ac.nz

Mary Tate
Victoria University, Mary.tate@vuw.ac.nz

Guy G. Gable
Queensland University of Technology, g.gable@qut.edu.au

A TYPOLOGY OF TECHNOLOGICAL ENABLERS OF WEBSITE SERVICE FAILURE PREVENTION

Alireza Nili, School of Information Management, Victoria University of Wellington, Wellington, New Zealand, alireza.nili@vuw.ac.nz

Mary Tate, School of Information Management, Victoria University of Wellington, Wellington, New Zealand, mary.tate@vuw.ac.nz

Guy G. Gable, Information Systems School, Queensland University of Technology, Brisbane, Australia, g.gable@qut.edu.au

Abstract

An increasing range of services are now offered via online applications and e-commerce websites. However, problems with online services still occur at times, even for the best service providers due to the technical failures, informational failures, or lack of required website functionalities. Also, the widespread and increasing implementation of web services means that service failures are both more likely to occur, and more likely to have serious consequences. In this paper we first develop a digital service value chain framework based on existing service delivery models adapted for digital services. We then review current literature on service failure prevention, and provide a typology of technologies and approaches that can be used to prevent failures of different types (functional, informational, system), that can occur at different stages in the web service delivery. This makes a contribution to theory by relating specific technologies and technological approaches to the point in the value chain framework where they will have the maximum impact. Our typology can also be used to guide the planning, justification and design of robust, reliable web services.

Keywords: Service failure prevention, service value chain framework, typology, technological enablers.

1 INTRODUCTION

Services are an increasingly large and important sector of the world economy, and are estimated by the World Bank to make up approximately two thirds of the total world Gross Domestic Product (GDP) (World Bank 2012). The nature of services and service delivery is also changing, becoming increasingly digitized, with an increasing emphasis on the user's role in self-service, service co-creation, and service recovery (Tate et al., 2014, Tate and Evermann 2009, 2010). For example, the New Zealand government has a goal that 70% of common transactions between citizens and government will be conducted online by 2017 (State Services Commission 2014). The increasing volume, complexity, and importance of digital service delivery means that service failures are both more likely to occur, and more likely to have serious consequences. Therefore automated solutions are increasingly used for error detection and service failure prevention as well as for service failure recovery (Kasabov & Warlow 2009; Kasabov 2010). Considering the consequences of service failure and its effects on customers' overall service quality perception and customer satisfaction, preventing service failure, and delivering reliable, robust web services is a critical business competency. However, services (including digital services) are increasingly diverse, and are "as different from each other, and from products, as products are from each other" (Edvardsson et al. 2005, p. 119), so there is no "one-size-fits-all" prescription for delivering reliable online services.

The concept of service failure is based in Expectation-Confirmation Theory (ECT) (Oliver 1980), and is defined as the gap that occurs when customers' perceived quality of service delivery does not match their service expectations (Lin et al. 2011; Sabharwal & Soch 2011; Zhu et al. 2013). This can be due to system error, staff error, or the consumers' own mistakes (Casado-Dı´az & Nicolau-Gonza´lbez 2009; Dabholkar & Spaid 2012; Van Vaerenbergh et al. 2012; Zhu et al. 2013). Since many service failures happen due to system errors, fast identification and correction of these errors (which sometimes can be done in seconds, or less, through dynamic and automatic error detection and recovery) can prevent them from becoming a real service failure in the minds of customers, since they are corrected before the customer is aware they have occurred. Due to the nature of some technical errors and the time needed to analyse them (e.g., through 'root cause analysis' or through analysis of failure related data stored in databases), some failures cannot be prevented at the time. However, technologies can enable service providers and customers to prevent similar service failures occuring in the future. Moreover, some technology enablers (e.g. online chat capabilities, social media, and online tutorials) can empower customers and service providers to communicate and interact in a way that can prevent, or at least minimize, the probability of service failures occurring.

In order to more appropriately manage digital service failure prevention, a deeper understanding is required of the nature and characteristics of digital service failure, and the technological enablers of service failure prevention that firms and customers can employ to avoid various service failure types. This study contributes to the Information Systems literature and practice by developing a typology of the technological enablers (including the technologies and technological approaches) for service failure prevention.

A typology is defined as "a classification according to general type"[1]. A typology is distinct from a taxonomy in that while a taxonomy develops increasingly fine levels of classification, where lower level nodes share all the properties of the higher level nodes (Marradi 1990), a typology groups objects of a set into several subsets according to the perceived similarities in their states on one or more *properties* (Marradi 1990). We use multiple *properties* for classifying enablers of digital service failure prevention, based on leading models from multiple disciplines. We classify prevention technologies according to the *type of failure* they are aimed at: system failure (sub-categorized into network and security failures); information failure; and functionality failure (recognizing that one type of failure may lead to another). We also classify prevention technologies according to the *point in the value chain*[2] at which they can be utilized. Finally, we classify prevention technologies according to wheth-

[1] http://www.oxforddictionaries.com/definition/english/typology

[2] We develop a new value chain framework for digital service delivery

er they are *usable by customers or organizations*. These properties, in combination, provide rich and actionable insights for customers and website managers aiming to reduce failure and improve their service experience.

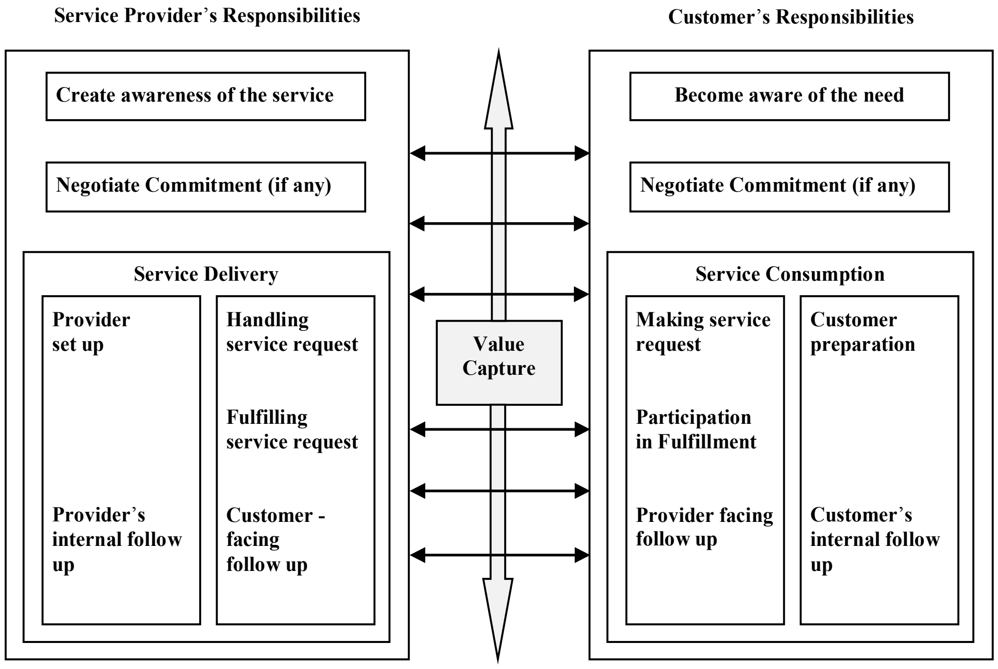
The rest of this paper is organized as follows. We first offer an integrative literature review and framework development section. We propose a service value chain framework suitable for web services, based on two leading models. We then identify different digital service failure types. Following this, we apply the service failure types to different stages of the service value chain framework. In the next section, we then develop our typology using this framework, to classify digital service failures, and website service failure prevention technological enablers, from the perspective of the customer and the service provider. This is followed by a discussion and a conclusion.

2. LITERATURE REVIEW AND FRAMEWORK DEVELOPMENT

In this section, we first present the development of our digital service value chain framework in order to use it to organise our typology. It also enables us to use customer or organizational responsibility as an additional classification property in the typology. The framework is based on leading models of service delivery in multiple disciplines, adapted for a digital services context. Next, we review the service quality and service failure literature to present our classification of website service failure types and provide a detailed list of technological enablers (both technologies and technological approaches) of service failure prevention.

2.1 Service Value Chain Framework

The service value chain framework presents a view of service-related activities in many service industries. However, some of these activities are not important for some service systems (Alter 2008). Based on the co-production view, Alter (2008) developed a service value chain framework that presents the service provider’s and the customer’s roles and responsibilities (figure 1).



Service Provider’s Responsibilities
Customer’s Responsibilities
Create awareness of the service
Become aware of the need
Negotiate Commitment (if any)
Negotiate Commitment (if any)
Service Delivery
Service Consumption
Provider set up
Handling service request
Fulfilling service request
Provider’s internal follow up
Customer - facing follow up
Value Capture
Making service request
Participation in Fulfillment
Provider facing follow up
Customer preparation
Customer’s internal follow up

Figure 1. Service value chain framework (adapted from Alter 2008)

In addition to Alter (2008), Eshghi et al. (2012) offered a service value chain framework (figure 2); however, their framework consists of three very general steps (one of which is service recovery) and it does not apply the concept of co-production in the service setting. Also, it does not develop service recovery in any depth and does not consider service failure prevention. Moreover, we argue that considering service failure recovery as the last step is over simplified as, different types of service failure are likely to happen at different stages of service activities.

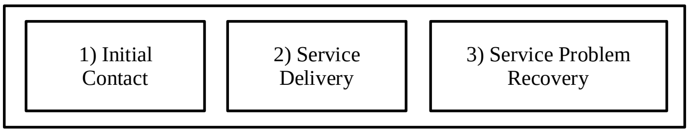


Figure 2. Consumer service value chain (Eshghi et al. 2012)

While these models are valuable, they have some limitations for our purposes. Considering the fact that services are often co-produced by service providers and customers, Alter's (2008) is the most appropriate service value chain framework from this perspective; however it does not specifically address *website* service activities. Similarly, it provides a very general view of service activities for all types of service industries, and therefore, does not necessarily provide actionable insights for specific types of services and technologies. For example, the conceptualisation of "negotiation commitment" by Alter (2008) is more suitable for traditional ways of delivering and receiving service. In a digital context, it can be performed just by clicking the appropriate option on the dedicated webpage to determine the Service Level Agreement (e.g., how much data and for how long a consumer aims to purchase from an ISP). Therefore, we felt that a new and more granular digital service value chain was required for the purposes of our study.

We propose a new framework based on the two leading models including the service value chain framework (Alter 2008) which we have adapted in Figure 1, and the customer purchase decision-making model (Elliott et al. 2010), adapted as Figure 3.

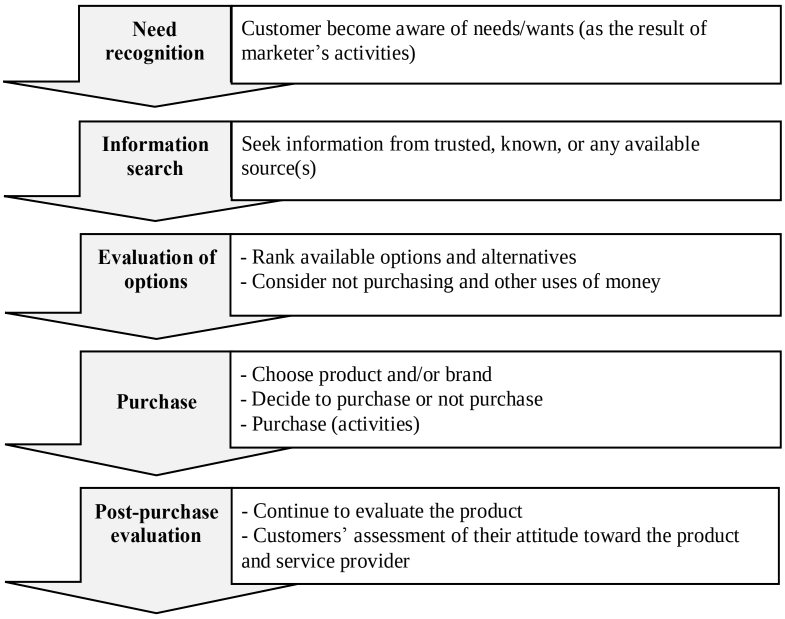

Need recognition
Customer become aware of needs/wants (as the result of marketer's activities)
Information search
Seek information from trusted, known, or any available source(s)
Evaluation of options
- Rank available options and alternatives
- Consider not purchasing and other uses of money
Purchase
- Choose product and/or brand
- Decide to purchase or not purchase
- Purchase (activities)
Post-purchase evaluation
- Continue to evaluate the product
- Customers' assessment of their attitude toward the product and service provider

Figure 3. Customer purchase decision-making model (adapted from Elliott et al. 2010)

The stages of customer purchase decision-making model complement the stages of service value chain framework proposed by Alter (2008); therefore, a modified combination of these two models provides a suitable service value chain framework for digital service delivery via websites. This enabled us to provide richer insight into service failure by classifying the exact stage at which a consumer's expectation of the service is formed (i.e., evaluation of products and brands) and the stage (i.e., making service request) from which service failures may happen. Figure 4 illustrates our framework.

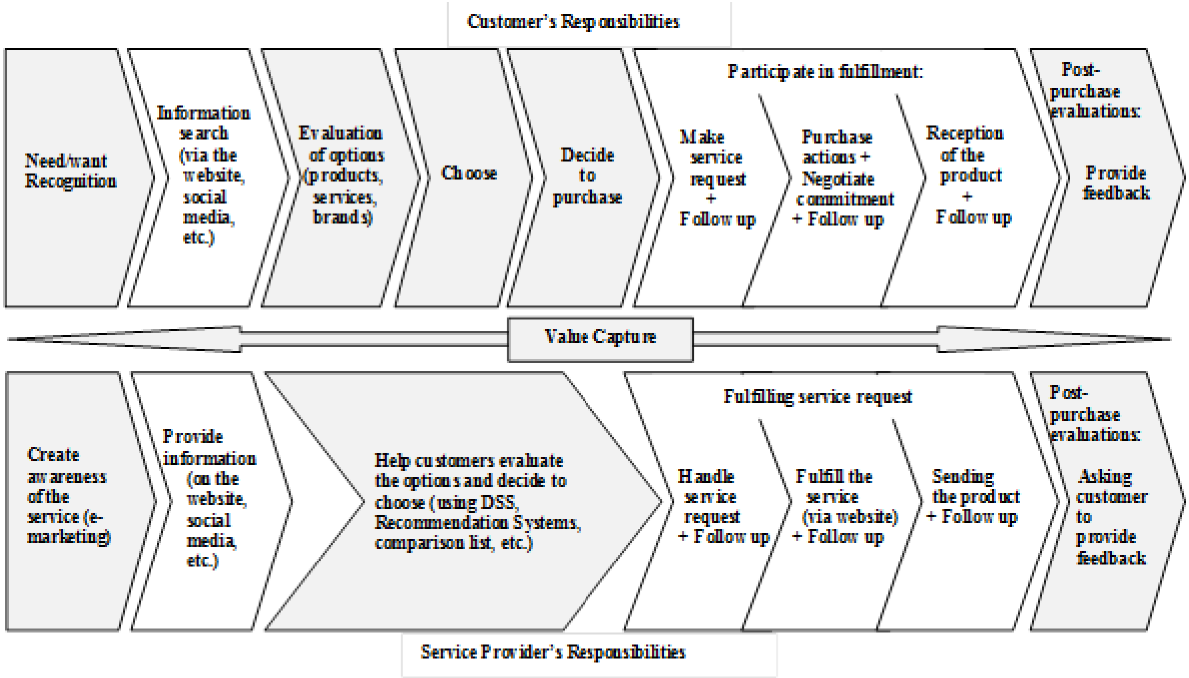

Customer's Responsibilities
Need/want Recognition
Information search (via the website, social media, etc.)
Evaluation of options (products, services, brands)
Choose
Decide to purchase
Participate in fulfillment:
Make service request + Follow up
Purchase actions + Negotiate commitment + Follow up
Reception of the product + Follow up
Post-purchase evaluations:
Provide feedback
Value Capture
Create awareness of the service (e-marketing)
Provide information (on the website, social media, etc.)
Help customers evaluate the options and decide to choose (using DSS, Recommendation Systems, comparison list, etc.)
Fulfilling service request
Handle service request + Follow up
Fulfill the service (via website) + Follow up
Sending the product + Follow up
Post-purchase evaluations:
Asking customer to provide feedback
Service Provider's Responsibilities

Figure 4: Digital service value chain framework

2.2 Types of Website Service Failures

We use the categorization and definitions of digital service failures developed by Tan et al. (2011) as it is the most relevant, comprehensive, and contemporary study we were able to identify. According to this categorization, there are three types of service failures associated with website performance namely, Informational Failures, Functional Failures, and System Failures. Functional failures happen when the functionalities provided on the website are unable or insufficient to support customers in the accomplishment of transactions (e.g., insufficient payment options or occasional problems in payment due to the system security issues). Informational failures happen if the information provided on the website is incapable of conducting customers in the accomplishment of transactions and fully benefiting from the website functionalities (e.g., irrelevant, inconsistent or incomplete information). System failure is the situation when the functionalities provided on the website are not delivered properly (e.g., due to the website navigational problems, lack of interactivity, or problems in the networking security), therefore customers will be unable to benefit from the website functionalities and accomplish their transactions satisfactorily. We emphasize that a functional failure is a failure in meeting user's functional requirements/expectations. Note that by functional requirements we mean the user's goal for using the service system. An example is the user may have a requirement to communicate with a community of other customers and respond to threads via a discussion forum.

According to the general definition of service failure from expectation confirmation theory, and the specific definitions for each type of service failure by Tan et al. (2011), we can see that functional failures are the central type of digital service failures and are caused in turn by: 1) absence or insufficiency of required website functionalities to complete the expected service satisfactorily; 2) functionalities that are present, but do not function satisfactorily due to system failures; 3) functionalities that are present, but do not function satisfactorily due to informational failures (e.g., misleading information before and/or while completing the service.

The next section presents a comprehensive review of the technological enablers to prevent from different types of service failures and describes each of them briefly.

2.3 Technological Enablers for Website Service Failure Prevention

This section considers the technological enablers (i.e. specific technologies and technological approaches) that can be used to prevent website service failure. Sources included articles in Information Systems (IS), e-Commerce, and Service Management fields within ProQuest Computing, ACM Digital Library, Web of Science, ScienceDirect, and SpringerLink databases and the AIS Electronic Library (AISEL). In order to find the appropriate articles from these resources, search terms including service failure; e-service failure; service problem; e-service problem; service recovery; e-service recovery, service failure prevention, and service problem prevention were employed. As we discussed, functional failures are the central type of service failures and are caused in turn by "system failures", "informational failures", and/or "lack or insufficiency of the required website functionalities". Accordingly, in order to prevent website functional failures, service providers can employ the following types of technological enablers. We note this includes the situation where they are used to provide self-help for customers.

- Technological enablers to prevent system failures.
- Technological enablers to prevent informational failures.
- Technological enablers to identify the lack or insufficiency of required website functionalities and provide them on the website (i.e. preventing repetition of this type of failure in future)

2.3.1 Technological enablers to prevent website functional failures as the result of system failures

In the general context of technological enablers (technologies and technological approaches) for website functionalities and capabilities improvement, Napier et al. (2003) classifies the system related technological enablers into the enablers for "networking" and "security" (including internal, external, and transactional security). Therefore, for the specific context of technological enablers for system-related service failure prevention, we categorise these technological enablers into:

- Prevention from "networking" related failures
- Prevention from "security" (internal, external and transactional security) related failures

This section provides a description for the technological enablers including both the specific technologies and technological approaches to prevent "networking" and "security" related failures, separately. We start with a brief description of the technological approaches to prevent "networking" related failures. As these approaches provide fast (real-time error detection and recovery) solutions for service providers, they can prevent or minimise the possibility service failure occurring in the mind of customers. Note that in keeping with the focus of our paper, we describe briefly the business functionality provided by each technological enabler. References are provided to enable readers to access more in-depth technical descriptions.

The technological approaches to prevent from "networking" related failures include:

- Content Caching and Streaming Media Caching: Online service providers can store and move frequently requested content closer to customers (i.e., content caching). This reduces traffic to the original server and therefore, handling of the customers' requests and purchases can be performed more quickly. A similar process can be used for streaming media caching which allows service providers to prevent from unsatisfactory waiting time for customers when downloading video and audio content (Napier et al. 2003, p.233; Lamberti & Sanna 2007).
- Multiple Stage Adaptation: In order to acquire and retain customers, e-businesses have to modify or increase service options; therefore, they may experience changes in network configurations and quality of service (QoS) offerings. In this situation, failure of component services and other negative consequences will be probable (Chafle et al. 2006). Multiple Stage Adaptation helps the system to adapt itself and react effectively to these changes by employing a different type of service or different template of services for a fast compensation of failed service. See Chafle et al. (2006) for more information on this approach.
- Dynamic Substitution and Control Flow Intervention: Control Flow Intervention is an automatic service substitution at runtime in a service composition. It dynamically replaces faulty services by semantically equivalent ones (Mo¨ller & Schuldt 2010). Like the previously mentioned dynamic

and automatic approaches, as this approach provides a fast solution for service providers, it can prevent occurrence of a real service failure in the mind of customers.

- Backup Path: A backup path (second path) can be created for each service in a service composition; therefore, if the optimal path fails to accomplish the purpose, the current and future executions can continue through the second path (Yu & Lin 2005). See Yu and Lin (2005) and Feng, Wu, Wang, Ren and Guo (2007) for more information on this approach.
- Multiple QoS Constraints: Many web services are a composition of multiple technical services from multiple providers (e.g. network, merchant, and bank). Since for each of the services in the composition a different quality of service (QoS) may be specified by different SLAs, there will be the possibility of a service failure as the result of this complexity. The Multiple QoS Constraints approach dynamically finds a new path that starts from the preceding service by maximising or minimising some QoS values (Feng, Wang, Wu & Zhou 2007). See Feng, Wu, Wang, Ren and Guo (2007) for more information on this approach.
- Rebinding: In order to meet the requirements of a QoS in the situations like unavailability of a service, this approach is capable of early run-time re-binding for functionally equivalent services in a service composition. See Canfora, et al. (2008) for more information on this approach.
- Performance Prediction: Online services are offered through the dynamic and changing environment of the Web (e.g., changes in data transmission speed) which leads to frequent changes in the QoS. Dai et al. (2009) used performance prediction approach and proposed a self-healing solution that dynamically finds a backup during the execution. As this approach minimises the re-selections during the execution, the system is capable of healing itself fast.
- Region Reconfiguration: In a service oriented architecture, many service processes are composed of services from some other service providers. Therefore, if an error happens in a service, it may cause a failure for end-to-end QoS constraints. Using an iterative algorithm, this approach prevents from a failure in the whole service process by dynamically replacing that service by some of its neighboring services in the region of that QoS (Lin, Zhang, Zhai & Xu 2010). See Lin et al. (2010) for more information on this approach.

The specific technologies to prevent from “networking” related failures include:

- Cache Servers and Content Delivery Networks: Using cached servers (between the origin servers and customers in content delivery network), service providers can store and move frequently requested contents closer to customers. As the traffic to the origin server is reduced, handling customer’s requests and purchase process can be performed with less waiting time. A similar process can be done for streaming media caching for video and audio content delivery (Napier et al. 2003, p.233; Lamberti & Sanna 2007).
- Watchdog systems: dynamically prevent software or hardware failures that may lead to a failure in the efficiency of the system by periodically checking the signals sent through the system components (Ibrohimovna & Groot 2010). Also, they can be used to monitor the attempts to access websites from different locations periodically and inform service providers of access failures through online reports (e.g., via email).
- SLA Monitor and SLA Management System: SLA monitors can be used to ensure that the service (especially cloud services) fulfills the QoS requirements of SLA by observing the runtime performance. SLA management system processes this data (gathered by the SLA monitor) to be used for SLA reporting metrics and control. Watchdog system and this technology are used together by many digital service providers for the purpose of fast and dynamic error detection and failure prevention (Mosallanejad et al. 2014).

The technological enablers (technologies and approaches) to prevent “networking” related failures (as a subset of system failures) were described above. The technological enablers to prevent “security” related failures (as the other subset of system failures) are described in the following section.

In addition to the technologies (e.g., password, biometric, and smart card identification systems for authorised access) and approaches (e.g., disaster recovery plans, backup and restore policies, risk management processes, email/spam filtering, and employee education and awareness) that can be employed to prevent “internal” security risks originating from inside the business, technological enablers that can prevent from “external” and “transactional” security related failures must also be considered by the firms. External security related failures can happen because of infections resulting from viruses, worms, and Trojan horses or because of unauthorized access that may lead to fraud (stolen data is misused or modified), or network intrusion by hackers. For e-businesses, other security failures are Denial of Service Attacks (disabling the network by flooding it with confusing traffic) and Website Defacement (i.e., changing the contents of webpages by for example modifying the HTML). Eavesdroppers, DNS attacks, Input Validation attacks, and Script Attacks are some of the others. For detailed information on different types of attacks such as the ones posted to servers and the appropriate counter measures for detecting and recovering them see Rane et al. (2012) and Gehling and Stankard (2005).

In addition to the internal and external security failures, e-business transactional related failures can lead to serious negative consequences for the customers' trust in transactions with service providers. In the context of e-business, the necessities of transactional security include confidentiality, authentication, integrity, and nonrepudiation. As explained below, among the technological enablers (the technologies and technological approaches) for preventing from security related failures, security protocols, Public Key Infrastructure (PKI), digital signature, and digital certificates are the ones that can prevent from e-business transactional related failures. Other technological enablers such as firewalls and proxy servers are used for more general security purposes. The technological approaches that can prevent from security (external and transactional security) related failures include:

- Security Protocols: includes the communication and payment protocols specially, Secure Socket Layer (SSL) and Transport Layer Security (TLS) for securing communication channels, and the protocols including Secure Electronic Transactions (SET), e-Cash, Secure Payment Application (SPA), and 3D Secure for securing payment data from alteration during transmission (Yasin et al. 2012; Kizza 2013, p.369; Niranjanamurthy & Chahar 2013; Manakshe et al. 2014).
- Public Key Infrastructure (PKI): E-businesses who participate in a PKI and use the digital certificate (explained further below) can check the public keys of other organizations in the network. PKI creates digital certificates, securely stores them in a public repository and disproves them if necessary (Napier et al. 2003, p. 280; Tyagi & Srinivasan 2011; Kizza, 2013 p.240).
- Technical Security Audits and Penetration Tests: In addition to assessment of the security plans and procedures (i.e., organisational audit) and the assessment of physical security of hardware (i.e., physical audit), a complete security audit scans the network security internally and externally (penetration tests) to identify the potential weaknesses (i.e., technical audit) (Napier et al. 2003, p. 288; Gehling & Stankard 2005; Tyagi & Srinivasan 2011; Marchany & Tront,2011; Yasin et al. 2012; Niranjanamurthy & Chahar 2013; Kizza 2013, p.165).

In addition to updated antivirus software to prevent from system infections, the specific technologies that can prevent from the security related failures include:

- Firewalls, VPN, Proxy Server, Network Address Translation (NAT), and Filters: Firewalls (generally categorised as packet-filtering, circuit-level, and application-level firewalls), VPN (a combination of firewalls, public and private key encryption and digital certificates), Proxy Servers and NAT (can be separately used to protect the user's IP address), and filters (to block the spurious traffic in a distributed denial of service attack) are common technologies used by many digital service providers to prevent from the system security related failures. The SSL protocol and digital certificates are described in this section. See Kizza (2013), Gehling and Stankard (2005) and Niranjanamurthy and Chahar (2013) for more information.
- Network Scanning and Network Intrusion Detection Software: help to detect weaknesses of the network security and also can identify the hacker attack threats. Moreover, this can be done in the form of "vulnerability monitoring" that is a continuous scanning to find potential problems that match the characteristics of the known threats in the 'threat database'. The data can help to resolve the problem and also can be used to analyse patterns of suspicious behavior. Some of these tools can also help to develop Threat Models when developing the system to help preventing exploits in future (Napier et al. 2003, p. 273; Tyagi & Srinivasan 2011; Marchany & Tront 2011; Yasin et al. 2012; Niranjanamurthy & Chahar 2013; Kizza 2013, p.271).
- Information Security Software / Shareware Tools: Many information security management solutions are now sold in the form of the tools such as software for website traffic analysis, proxy

server reporting, quality control, monitoring and recovery for limited or unlimited number of devices, and also to build secure payment systems (Tyagi & Srinivasan 2011; Marchany & Tront 2011; Yasin et al. 2012).

- Cookies 'marked as secure': cookies are primarily used to store authentication and users' information and preferences. Also, they can be used to track users' activities; therefore, using the cookies that store encrypted data and passing them through SSL enhances a secure online shopping experience (Niranjanamurthy & Chahar 2013).
- Digital Signature: Depended on the type of an e-business, digital signature may be necessary for the negotiation phase of the purchase process between service providers and their customers. A digital signature provides the recipient the proof of authentication, non-repudiation, and integrity of the message (i.e., the message has not been altered during the transmission) (Tyagi & Srinivasan 2011; Marchany & Tront 2011; Niranjanamurthy & Chahar 2013; Kizza 2013, p.242).
- Digital/Electronic Certificate: is a digital credential of an e-business on the Web. It is issued by a certificate authority to provide this security assurance for the e-businesses that if they are going to exchange encrypted data with other parties, these parties are actually who they claim (Yasin et al. 2012; Niranjanamurthy & Chahar 2013; Kizza 2013, p.240).

According to the above descriptions, PKI, digital certificate and also technical security audits and penetration tests are useful for precautionary considerations that should be considered *before* starting service transactions. For example, customers may check the digital certificate of a service provider during the "evaluation of options" (e.g., services, products, brands, service providers) phase of the service value chain framework (i.e., before starting and receiving a service from a specific service provider). In summary, they are not included among the technological enablers that can prevent website service failures once a customer has started a service transaction by requesting a service.

2.3.2 Technological enablers to prevent website functional failures as the result of informational failures

Sometimes functional failures occur not because of the system failures, but because of informational failures. However, it is always possible that the information provided by the website and service provider is complete and presented properly, but due to occasional customers' mistakes (e.g., not paying attention to guidance or warning/error messages), the consumer does not fulfill his/her intended actions satisfactorily. Customers have an essential role in co-production when using self-service technologies such as websites, and therefore in service failure prevention. Service providers can use appropriate technology enablers (e.g., online chat capabilities, creating online community of users webpages, links to the firm's social media pages, online tutorials, etc.) on the website to communicate with customers and/or educate them to help them prevent, or at least minimize the possibility of some functional failures.

- Self-Help Resources: Dedicating a part of the website to frequently asked questions (FAQs), customers' community webpages, links to the (service provider's) social media pages, online video training sessions and tutorials for the purpose of educating customers and prevent from customers' mistakes that can lead to service failure. It is important to mention that although sometimes service failures happen because of the customer's mistakes when working with technology, it is the responsibility of the service providers to educate customers and provide facilities for them to avoid from these mistakes (Kasabov & Warlow 2009; Kasabov 2010; Nili & Keramati 2012).
- Automated Messages and Pop-Up Windows: can provide guidance and directions for customers while they are proceeding through the purchase process. Therefore, they can help to prevent from some potential customer's mistakes during the purchase activities (e.g., preventing from mistakes in selecting the same product twice and being charged more than what they were expecting).
- Social Media Pages, Online Chat Sessions (with service personnel), and Instant Messaging: These can help customers and service providers to interact in a way that they can prevent from the occurrence of service failures due to either of customer's or service provider's mistakes (e.g., answering to the customers' general enquiries or specific enquiries when they detect a potential problem with the website or informing customers to avoid using the website until a problem is resolved) (Kasabov & Warlow 2009; Kasabov 2010; Nili & Keramati 2012).

- Online Feedback Forms: for receiving customers' feedback about the quality of the services, product, and also their comments on how to improve design quality and therefore, preventing from occurrence of similar failures in future (Kasabov & Warlow 2009; Kasabov 2010).
- Electronic Status Reports: can be used in the form of a webpage, automated email or messages to explain the current status of the recovery process (for an already happened system error). This can help to minimise the risk of occurring a real service failure in the mind of customers (customer's perception of service failure) as they become aware of the service providers attempts for a fast resolution (Kasabov & Warlow 2009; Kasabov 2010).

2.3.3 Technological enablers to prevent from "lack/insufficiency of the website functionalities"

According to Napier et al. (2003), Kizza (2013), Kasabov and Warlow (2009) and Kasabov (2010), the technological enablers to identify the failures related to the "lack or insufficiency of the website functionalities" and prevent from repeating them in future include:

- Genetic Algorithms, Neural Networks, and Fuzzy Logic: to classify and route the service failure causes for analysis and design improvement (i.e., root cause analysis) for the purpose of preventing their repeated occurrence in the future.
- Data Warehousing and Data Mining: separate databases can be used for maintaining "value failure data" and to help analysis of service failures to prevent from their occurrence in future.
- Online Feedback Forms: for receiving customers' attitudes toward the quality of the services, product, and also for receiving comments on how to improve the quality of the website design and therefore, preventing from occurrence of similar failures in future.
- Intelligent Agents (IA): Can provide the capabilities such as personalization of the website contents, as they gather and analyze individuals' preferences based on their shopping behaviour. These IAs can be used as shopping assistants to help finding a desired item without the need to browse many webpages. This ability can help to prevent a (perceived) long time delay needed to find a desired item (i.e., a perceived service failure by some customers). Moreover, in the event of service failure IAs can be used to earmark severe failures. This helps service providers in analyzing data related to these failures and prevent from them in future.

The previous sections presented the technological enablers that service providers and/or customers can use to prevent from website service failures. However, it is important to mention that perceived service failures (from the customers' perspective) can still occur when the website has all of the required functionalities, there is no problem with the system and the necessary information is available for customer's purchase activities. This can be due to the problems on the customer's side (e.g., an out of date version of web browser that is not supported, or lack of required software). Although in this case, there is no problem with the website itself, it is always the service providers' responsibility to ensure that they have provided all of the means required for a convenient service experience and failure-free services for customers. Web browser Plug-Ins are the technology enablers that can help to overcome this issue by adding new features and capabilities to customers' web browsers (e.g., the ability of playing video for the online self-help tutorials). In addition to this, e-businesses can provide links to a specific web browser, required software or their latest version; therefore, customers will benefit from the website functionalities with higher efficiency and less probability of dissatisfaction.

3. A TYPOLOGY OF TECHNOLOGICAL ENABLERS FOR PREVENTING FROM WEBSITE SERVICE FAILURES

In this section, we first elaborate the type of service failures that can occur at each point in our website value chain framework (Table 1). Then, we provide a typology of the technological enablers (both technologies and technological approaches) based on their suitability for preventing from each type of service failure that may occur in each phase. As we explained, services (especially the ones offered via websites) are often co-produced. Therefore, we present our typology based on the technological enablers that can be used by *service providers* (see table 2) and also based on the technological enablers that can be used by *customers* (table 3) for each type of service failure.

Consumer’s Roles in Co-Production by Websites arranged by phase in the Digital Service Value Chain:			
Participate in fulfilment			Post-purchase Evaluations
Make service request + Follow up	Purchase actions + Negotiate commitment (e.g., SLA) + Follow up	Reception of the product + Follow up	Providing feedback
Service Provider’s Roles in Co-Production by Websites arranged by phase in the Digital Service Value Chain:			
Handle service request + Follow up (e.g., automated messages or confirmation)	Fulfil consumers’ purchase activities + Fulfil Negotiate commitment + Follow up	Sending the product (electronically or to residential address) + Follow up	Asking customers to provide feedback on the service delivery
Examples of Service Failures Leading to Website Functional Failures from a customer perspective:			
Informational Failures			
Listing an unavailable item in the list of available items, not enough self-help resources (e.g., FAQs, instructions) to gain information on the purchase process.	Lack or misleading guidance and directions during purchase, no information on the current status/stage of service delivery	No receipt of payment and/or product specification	Not providing an estimation of the time needed to fill in the feedback form
System Failures			
Communication security issues, compatible only with a specific web browser, host overload (due to high number of requests)	Navigation problems, delay in loading a webpage, communication and payment security issues	Unacceptable waiting time for downloading a software or a video file	Problem with submission of feedback
lack/insufficiency of the website functionalities			
Search capabilities are not provided	Lack/insufficient payment options	Lack of options/methods of receiving the product	Lack of feedback form or any channel of communication with service provider

Table 1. Examples of the service failures that may occur in each related phase of the website service value chain Framework

We note that based on the definition of service failure (i.e., a service failure happens if customer’s perception of service delivery falls below their prior expectation), our website service value chain framework shows that customer’s expectation of service delivery is formed in the “evaluation of options” phase, while the possibility that a service failure may occurs from the “making service request” phase of the website service value chain framework onward. Therefore, each of the tables 2 and 3 presents our typology of technological enablers to prevent from these service failures, starting from the “making service request” phase of the framework.

Service provider’s roles in co-production by websites:			
Handle service request (by the provided website) + Follow up (e.g., automated messages or confirmation)	Fulfill consumers’ purchase activities + Negotiate commitment (if needed) + Follow up	Sending the product (e.g., via download) + Follow up	Asking customers to provide feedback on the quality of service
Technological enablers to prevent from the website functional failures as the result of Informational Failures:			
1) Providing links to the (service provider’s) social media pages, customers’ community webpages, FAQs, and online video training and tutorials and instructions. 2) Automated messages and pop-up windows to provide guidance /directions 3) Providing online chat sessions (with service personnel), instant messaging, and social media pages 4) Electronic status reports via webpage, automated email or messages			5) Service provider’s social media pages, online feedback forms, online chat capabilities, and customers’ community webpages
Technological enablers to prevent from the website functional failures as the result of System Failures:			
1) Web browser plug-ins 2) Links to a compatible web browser or required software and/or their latest version	3) Digital Signature	4) Caches Servers and Content Delivery Networks 5) Content Caching and Streaming Media Caching	6) Service provider’s social media pages, online feedback forms, online chat capabilities, and customers’ community webpages
7) Firewalls, VPN, Proxy Server, Network Address Translation (NAT), and Filters 8) Network Scanning and Network Intrusion Detection Software 9) Information Security Software / Shareware Tools 10) Cookies ‘marked as secure’ 11) Security protocols 12) Backup Path 13) Performance Prediction 14) Dynamic Substitution and Control Flow Intervention 15) Multiple Stage Adaptation 16) Multiple QoS Constraints 17) Rebinding			

18) Dynamic/Region Reconfiguration 19) Watchdog system 20) SLA Management System and SLA Monitor	
Technological enablers to prevent from the website functional failures as the result of "lack or insufficiency of the website functionalities" and preventing from repeating them in future:	
1) Genetic Algorithms, Neural Networks, and Fuzzy Logic 2) Data Warehousing and Data Mining 3) Intelligent Agents 4) Service provider's social media pages, online feedback forms, and online chat capabilities (for receiving feedback during the purchase process).	5) Service provider's social media pages, online feedback forms, online chat capabilities, and community webpages

Table 2. A typology of the technological enablers that can be used by service providers for website service failure prevention

We note that in typology development, the researcher only develops "a" typology, not "the" typology. There is no restriction on the range of properties that can be used for classification purposes, or their theoretical origins. However, it is necessary that the properties used for classification, and the classification process, is clear, consistent, intuitive and theoretically sound. Therefore to validate our classification process, our three classification tables were work-shopped and validated with eight academic experts, including three from information systems, three from e-commerce, and two from computer science, at a university in New Zealand. We first explained that the columns (i.e., consumer's and service provider's roles starting from the "making service request" phase of our service value chain framework) present the criteria for the typology. Next, we asked participants to add, remove, or revise any column of the three tables. Also, we asked them to add, remove, and/or revise the contents of each column of each table. The only changes include removal of one of our service failure examples from table 1 by a participant in the e-commerce field (also confirmed by other participants) and adding two new examples by two participants in the IS field. No new ideas appeared for tables 2 and 3 (i.e., our proposed typology) and they were confirmed by all participants.

Consumer's Roles in Co-Production by Websites:			
Participate in fulfillment			Post-purchase Evaluations
Make service request + Follow up	Purchase actions + Negotiate commitment (e.g., SLA) + Follow up	Reception of the product + Follow up	Providing feedback
Technological enablers to prevent from the website functional failures as the result of Informational Failures:			
1) Using the links to the (service provider's) social media pages, customers' community webpages, FAQs, and online video training and tutorials and instructions. 2) Paying attention to the guidance/directions provided by the automated messages and/or pup-up windows 3) Using the online chat sessions (with service personnel), instant messaging, and social media pages 4) Paying attention to the electronic status reports via webpage, automated email or messages			5) Service provider's social media pages, online feedback forms, online chat capabilities, and customers' community webpages
Technological enablers to prevent from the website functional failures as the result of System Failures:			
1) Using/accepting Web browser plug-ins (if needed) 2) Links to download a specific web browser or software and/or their latest version (if needed) Paying attention to whether the service provider uses: 3) The security protocols for communication and/or payment 5) Cookies 'marked as secure' (if needed) 6) and whether uses digital signature (if needed)			5) Service provider's social media pages, online feedback forms, online chat capabilities, and customers' community webpages
Technological enablers to prevent from the website functional failures as the result of "lack or insufficiency of the website functionalities" and preventing from repeating them in future:			
1) Using links to the (service provider's) social media pages, customers' community webpages, FAQs, and online video training and tutorials and instructions. 2) Using social media pages, online chat sessions (with service personnel), and instant messaging			3) Service provider's social media pages, online feedback forms, online chat capabilities, and customers' community webpages

Table 3. A typology of the technological enablers that can be used by customers for website service failure prevention

4. DISCUSSION AND CONCLUSIONS

In this paper we developed a typology of the technological enablers for preventing different types of website service failures, including both the specific technologies and technological approaches. In doing so, we adapted the set of digital service failure types from Tan et al. (2011) and identified the technological enablers of service failure prevention through a comprehensive review of the IS and e-commerce literature. However, when we aimed to further classify these enablers according to the stage of the service life-cycle at which they can be applied, we realised that due to the different nature of the service activities via websites (i.e., more co-produced and integrated service activities) no existing framework provides a suitable view of these activities. Therefore, we presented a new service value chain framework that considers these aspects. In addition to help presenting and organising our typology, this new framework helped us to find the exact phase of formation of customer's expectation of service (i.e., evaluation of options) and the phase from which service failures may occur (i.e., making service request).

This paper contributes to both IS theory and practice by presenting a service value chain framework specifically designed for the services offered via websites and presenting a typology of the technological enablers including both the technologies and technological approaches that can be used by firms and/or customers to prevent from different types of website service failures. We also provided a brief description for each of these technological enablers from a business perspective, and references to resources where a more detailed technical explanation can be obtained.

As our typology clearly shows, an interesting finding is that among these technological enablers, social media can be widely used by both customers and service providers to prevent from service failures at many stages of the framework (even at the "post-purchase evaluations" stage). Different types of social media have different characteristics (e.g., information richness and cultural issues) and can have variety of forms many of which are free and also are capable of being provided through dedicated webpages of a website. As these features can show the high potential of wider use of social media for the purpose of service failure prevention, we encourage future research to consider these different characteristics in how social media can be effectively used at different stages of our framework. Another major conclusion is that effective service management requires deep understanding and cooperation between business and IT specialists. Our paper contributes to this by bridging technical and managerial (customer service) perspectives on preventing service failure. Therefore, as our second suggestion for future research, we suggest deeper investigation of the business and technology service management issues involved in each stage of our service value chain framework, and the inclusion of other relevant enablers such as managerial enablers of service failure prevention.

References

Alter, S. (2008). Moving toward a service metaphor for describing, evaluating, and designing systems. In Proceedings of the European Conference on Information Systems (ECIS). Paper 142. http://aisel.aisnet.org/ecis2008/142

Canfora, G. Di Penta, M., Esposito, R. and Villani, M. L. (2008). A framework for QoS-aware binding and re-binding of composite web services, Journal of Systems and Software, 81, 1754–1769.

Casado-Díaz, A. B. and Nicolau-Gonzálbez, J. L. (2009) Explaining consumer complaining behaviour in double deviation scenarios: the banking services, The Service Industries Journal, 29 (12), 1659-1668.

Chafle, G., Dasgupta, K., Kumar, A., Mittal, S. and Srivastava, B. (2006). Adaptation in web service composition and execution, in IEEE International Conference on Web Services (ICWS). Chicago, USA: IEEE Computer Society, September, 549–557.

Dabholkar, P.A and Spaid, B.I. (2012) Service failure and recovery in using technology-based self-service: effects on user attributions and satisfaction, The Service Industries Journal, 32 (9), 1415-1432.

Dai, Y., Yang, L. and Zhang, B. (2009). QoS-driven self-healing web service composition based on performance prediction, Journal of Computer Science and Technology, 24, 250–261.

Edvardsson, B., Gustafsson, A. and Roos, I. (2005). Service portraits in service research: a critical review. International Journal of Service Industry Management, 16 (1), 107-121.

Elliott, G., Rundle-Thiele, S. and Waller, D. (2010), Marketing. John Wiley and Sons Australia.

Eshghi, A., Gangui, S. and Nasr, N. (2012) Service quality in hybrid services: a consumer value chain framework, Journal of Services Research, 12 (1), 115-130.

Feng, X., Wang, H.,Wu, Q. and Zhou, B. (2007). An adaptive algorithm for failure recovery during dynamic service composition, in Pattern Recognition and Machine Intelligence, ser. Lecture Notes in Computer Science, A. Ghosh, R. De, and S. Pal, Eds. Springer Berlin / Heidelberg, 4815, 41–48.

Feng, X. Wu, Q., Wang, H., Ren, Y. and Guo, C. (2007). ZebraX: A model for service composition with multiple QoS constraints, in Advances in Grid and Pervasive Computing, ser. Lecture Notes in Computer Science, C. Ce´rin and K.-C. Li, Eds. Springer Berlin / Heidelberg, 2007, 4459, 614–626.

Gehling, B. and Stankard, D. (2005). eCommerce security, Information Security Curriculum Development Conference , ACM, September 23-24, 2005, Kennesaw, GA, USA, 32-37.

Holloway B.B and Beatty, S.E. (2003) Service failure in online retailing A recovery opportunity, Journal of Service Research, 6 (1), 92-105.

Ibrohimovna, M. and Groot, S.H.D. (2010). Reputation-based Systems within Computer Networks. Fifth International Conference on Internet and Web Applications and Services, IEEE Computer Society, 96-101.

Kasabov, E. (2010) The Compliant Customer, MIT Sloan Management Review, 51 (3), 17-19.

Kasabov, E. and Warlow, A.J. (2009) Automated marketing and the growth of ‘customer compliance’ businesses, Journal of Direct, Data and Digital Marketing Practice 11 (1), 30-50.

Kizza, J.M. (2013). Guide to computer network security, 2nd Edition. © Springer-Verlag London, 1617-7975.

Lamberti, F. and Sanna, A. (2007). A streaming-based solution for remote visualization of 3D graphics on mobile devices. IEEE Transactions on Visualization and Computer Graphics, 13(2), March/April 2007, 247-260.

Lin, H.H., Wang, Y.S. and Chang, L.K. (2011) Consumer responses to online retailer’s service recovery after a service failure: A perspective of justice theory, 21 (5), 511-534.

Lin, K.-J., Zhang, J., Zhai, Y. and Xu, B. (2010). The design and implementation of service process reconfiguration with end-to-end QoS constraints in SOA, Service Oriented Computing and Applications, 4 (3), 157–168.

Manakshe, A.R., Jirkar, S., Wakhare, P. and Buram, V. (2014). Analysis of secure electronic transmission (SET) system for electronic transactions. International Journal of Research in Advent Technology, 2 (3), 12-15.

Marchany, R.C. and Tront, J.G. (2002). E-commerce security issues. Proceedings of the 35th Hawaii International Conference on System Sciences, 1-9.

Marradi, A. (1990). Classification, typology, taxonomy. Quality and Quantity, 24, 129-157.

Mo¨ller, T. and Schuldt, H. (2010). OSIRIS Next: Flexible semantic failure handling for composite web service execution, in Fourth International Conference on Semantic Computing (ICSC). Los Alamitos, CA, USA: IEEE Computer Society, September 2010, 212–217.

Mosallanejad, A., Atan, R., Murad, M.A. and Abdullah, R. (2014). A hierarchical self-healing SLA for cloud computing. International Journal of Digital Information and Wireless Communications (IJDIWC), 4 (1), 43-52.

Napier, H. A., Judd, P., Rivers, O., and Adams, A. (2003). E-business technologies. Boston, MA: Thomas Course Technology.

Nili, A. and Keramati, A. (2012) Customer retention programs of CRM and customer retention in E-banking, International Journal of E-Entrepreneurship and Innovation, 3 (1), 18-32.

Niranjanamurthy, M. and Chahar, D. (2013). The study of e-commerce security issues and solutions. International Journal of Advanced Research in Computer and Communication Engineering, 2 (7), 2885-2895.

Oliver, R.L. (1980). A cognitive model for the antecedents and consequences of satisfaction. Journal of Marketing Research (17), 460-469.

Rane, P.B., Kulkarni, P., Patil, S. and Meshram, B.B. (2012). Authentication and authorization: tool for ecommerce security. IRACST – Engineering Science and Technology: An International Journal (ESTIJ), 2 (1), 150-157.

Sabharwal, N. and Soch, H. (2011) Confirmatory factor analysis of determinants of service recovery, Global Business Review, SAGE Publications, 12 (2), 297–318.

State Services Commission. (2014). Retrieved from http://www.ssc.govt.nz/bps-interaction-with-govt

Tan, C.W., Benbasat, I. and Cenfetelli, R.T. (2011). Understanding e-Service failures: formation, impact and recovery, In Proceedings of the Special Interest Group on Human-Computer Interaction (SIGHCI). Paper 5. http://aisel.aisnet.org/sighci2011/5

Tate, M., & Evermann, J. (2009). Descendents of ServQual in Online Services Research: The End of the Line? Paper presented at the Americas Conference in Information Systems (AMCIS), San Francisco.

Tate, M., & Evermann, J. (2010). The End of ServQual in Online Services Research: Where to from here? e-Service Journal, 7(1), 60-85.

Tate, M., Furtmueller, E., Gable, G., & Gao, H. (2014). Reconceptualizing Digital Service Quality: A Call-to-action and Research Approach. Paper presented at the Pacific-Asia Conference on Information Systems (PACIS), Chengdu, China.

Tyagi, N.K. and Srinivasan, S. (2011) Ten-stage security management strategy model for the impacts of 'security threats on e-business'. International Journal of Computer Applications. 21 (5).

Van Vaerenbergh, Y., Larivière, B. & Vermeir, I. (2012). The Impact of Process Recovery Communication on Customer Satisfaction, Repurchase Intentions, and Word-of-Mouth Intentions. Journal of Service Research, 15, 262-279.

World Bank (2014). Retrieved from http://data.worldbank.org/indicator/NV.SRV.TETC.ZS

Yasin, S., Haseeb, K. and Qureshi, R.J. (2012). Cryptography based e-commerce security: a review, International Journal of Computer Science Issues, 9 (2), 132-137.

Yu, T. and Lin, K.-J. (2005). Adaptive algorithms for finding replacement services in autonomic distributed business processes, in The 7th International Symposium on Autonomous Decentralized Systems (ISADS), April 2005, 427–434.

Zhu, Z., Nakata, C., Sivakumar, K. and Grewal, D. (2013) Fix it or leave it? customer recovery from self-service technology failures, Journal of Retailing 89 (1), 15-29.