INFORMATION SECURITY VALUE IN E-ENTREPRENEURSHIP

Sérgio Nunes

ISEG School of Economics and Management

Abstract

This paper researches the information security value in e-entrepreneurship by revising the literature that establishes the entrepreneurial domain and by relating it with the development of technological resources that create value for the customer in an online business. It details multiple paradigms regarding consumer's values of information security, while relating them with common practices and previous researches in technological entrepreneurship. This research presents and discusses the benefits of information security standards in e-entrepreneurship. It details and discusses the ISO 27001 and PCI-DSS information security standards that can be used to differentiate security initiatives to achieve competitive advantage, while preserving information leadership as a critical resource for online business success. Based on the literature review, a theoretical research model is presented and research hypotheses are discussed. This model believes that information security affects information leadership and that information leadership, as a unique resource in e-business, contributes to e-entrepreneurship success. The adoption of information security standards affects customer's trust in e-business, which also benefits e-entrepreneurial strategy.

Key Words: e-entrepreneurship, technological resources, online business, information security standards, information leadership.

Introduction

What is e-entrepreneurship? E-entrepreneurship is nothing more than an entrepreneurial initiative performed over the Internet. It has similar characteristics to those of traditional entrepreneurial actions, but it differs in others, which will be enumerated throughout the paper. The typical definition of entrepreneurship, as the creation of a new venture also applies to e-entrepreneurship. A fundamental core competence for e-entrepreneurship is the dependence on information technology (IT) as the vital theme that differentiates business success from failure. When creating a new e-business, the question is not the adoption of information technology to achieve competitive advantage, but how to deploy it to establish a distinctive strategic positioning (Porter, 2001). How can a new enterprise established in the Internet achieve competitive advantage over its competitors? The concept of information leadership (Kollmann, 2006) has always played an important part in the process of entrepreneurship and information knowledge is viewed as being an intangible resource form a resource-based point of view (Barney, 1991) and is studied deeply in, and enhanced by the knowledge based view (Grant, 1996). Information has been identified as being a source of competitive advantage for the traditional business (Porter and Millar, 1985), and business on the Internet is no exception. Information leadership for a business established on the Internet creates value for customers, as an information resource deviates from the classical support function in the production process of a traditional enterprise, turning it into the core competence, which brings added value to the business. The enterprise that has information superiority and transforms that information into organizational knowledge is more likely to succeed in e-business.

A major impact of the Internet is the rapid decline in the costs of information, as well as the technology needed to acquire, store, and transmit information. The role of gathering, preserving and presenting information using technology should be performed in such a way that is as user-friendly as possible. Everyone knows that information on the Internet is just a mouse click away, and the usability of a platform is a significant step towards a happy customer. The initial technology investment barrier is now minimized with the use of cloud computing, where resources are elastic and acquired as a service that can grow as the business demands. The benefits from online crowd funding can also be used to gather the initial technological investment, as it favors risk-sharing among investors. But money does not appear without a price, and giving away e-business equity is one necessary burden, although investors also demand transparency in business management, and adequate governance control.

But what happens when the customer is malicious and wants access to more information than is authorized? Who knows whether behind that customer there is a competitor seeking unauthorized information? What happens to the e-business if information technology fails? The benefits that turn e-entrepreneurship quickly into a success from a massive exposure can also quickly remove a new e-venture from

the Internet and kill its reputation. Information as the key to a new e-business is just waiting to be stolen, or the opportunity is imitated, or the product is substituted by a competitor around the world. The new product combinations that present a unique entrepreneurial opportunity are dependent on information technology as the vehicle for added value. The physical barriers that constrain the imitation of a product, or information leaking in a traditional business, do not exist for e-business. Nowadays, there are multiple cases of news related to the disclosure of sensitive information, namely credit cards and personal information. E-entrepreneurship demands a business platform as soon as possible with time to market expectations, but is the platform behind the elegant look and feel secure? Due to the exposure of e-business to multiple threats, security tests should be undertake before going live and should ensure that secure coding best practices are taken into account by the developers. The e-business process is more visible to the customer than a traditional process, and thus the threats that affect it are intensified, as in the case of a malicious individual.

How does one achieve information security for an e-entrepreneurship? Does information security present an added value to the business, and is it transferred to the end user? Information security is the accomplishment of three basic pillars: confidentiality, integrity, and availability of information. The confidentiality of information deals with information not being disclosed to unauthorized people, and it is normally accomplished by the use of encryption. Integrity of information invalidates the tampering and destruction of data. Some security measures allow information to be changed or corrupted while traveling in electronic format, but they preserve the integrity by detecting it, and by requesting information replay, until it becomes integrity-intact. The availability of information requires that when such information is needed, it can be accessed in a timely manner. Availability on the Internet is not easy to guarantee, as multiple sites are being more often subjected to denial of service attacks from multiple sources. How long does an e-entrepreneurship last under attack until it is completely out of business?

Security mechanisms should be deployed to mitigate risk to an acceptable level by top management. The mitigation of risk should be performed following a business impact analysis which prioritizes technological assets in terms of business criticality. This analysis measures how long an e-business can last offline before going bankrupt or damaging its reputation to a point of no return. Using this quantitative evaluation, metrics exist that support the necessary cost benefit analysis when implementing new security safeguards.

Trust is a fundamental value in e-business, as customers are not buying products or services face to face (Corbitt et al., 2003). Some people still have doubts and fears about using e-commerce (Lee and Tan, 2003). This is where trust comes in, as if the customers trust the enterprise where they are buying, then they will propagate their trust to their circle of influence. This behavior can be seen in online banking for example, where the bank assures that is taking all the measures necessary for

ensuring information security, in order to protect the customer's assets. The perceived security and privacy risk weighted by the customer are fundamental factors that function as impediments to the adoption of online banking (Liao and Cheung, 2002; Tan and Teo, 2000). The problem with trust in e-business is that it can be quickly shattered with a single and unique information disclosure or fraud event. The propagation of such an event is multiplied with the spreading of information in social networks and reputation loss cannot be easily recovered.

How can e-entrepreneurship prove that it takes care of its information security in order to differentiate its behavior from its competitors? There are multiple information security standards that assure that a company employs adequate measures to safeguard information security. One example is the ISO 27001 standard, where a company can be certified by an independent auditor that verifies multiple security procedures, ranging from the definition of a security policy, to the control of employment security. Another example developed specifically for e-business is PCI-DSS, which is a standard that defines requirements for online transactions involving credit cards, seeking to unify security procedures for online shopping. Online enterprises are adopting these standards more and more, to establish a competitive advantage over their competitors and usually present the certification information on their online site for the customer to notice. These standards also provide governance control, which ensures the accountability and traceability required to provide investors the necessary assurance of adequate due care.

The problem of privacy also plays an important role when buying products online, as online marketing techniques are used to presenting similar products to the customer, taking into account their latest purchases. While this can be seen as being an advantage of e-business for most customers, there should always be an option to stay anonymous. Personal data should only be stored if necessary, and it should follow secure storing procedures, such as database encryption. This personal data should only be accessed for additional and necessary information related to that same transaction.

Usability is a key factor for the acceptance of information technology, and security mechanisms are sometimes seen as deterrent controls that negatively influence the use of information technology. This also happens in e-business, where security mechanisms have to be weighed against usability, to achieve the psychological acceptability of the customer (Saltzer and Schroeder, 1975). If the mechanisms used to mitigate information security risks limit the usability of a service, and if that aspect is noticeable to the customer, then they will search for the next competitor to buy goods from. E-business should develop information security awareness campaigns among customers, in order that they can see the added value of information security.

The theme of cloud computing closed the barrier of high initial capital funding that was necessary for e-entrepreneurship, but it brought additional problems regarding

information security. Many countries have established privacy and information protection laws which e-business must be in compliance with, however, with cloud computing, where does the information reside physically? If a crime is committed and the local legislator needs access to the data, is it possible to access it? How can a legal entity verify compliance with certain e-business laws? There is also the problem of the lock-in of information, where the cloud supplier does not facilitate the migration of data to another supplier if the e-entrepreneurship owner is not satisfied with the service and wants to terminate it. What happens to the data if the cloud supplier goes bankrupt? Most of the cloud service providers have a shared infrastructure for multiple e-businesses, and it is difficult to assure that competitors are not sharing a virtualized infrastructure, and that the principle of separation of duties is guaranteed, by physically limiting access to information of a different competitor.

The next section analyzes related work on entrepreneurship and technological entrepreneurship, and the information security standards sections then details the objectives and requirements of standards that can enhance information security in e-business. Next a research model is presented and the research hypotheses are enunciated. Finally, the conclusion summarizes the main points of this paper and presents future research topics.

Related work

This section details the related work that formed the basis of entrepreneurship, and after this, it details the subject of entrepreneurship in information systems or those related with information technology.

Entrepreneurship

The definition of entrepreneurship has evolved and diverged along multiple research, without a clear accepted definition of what entrepreneurship actually is. It is fighting for a separate domain of investigation as it is connected directly with research in management, economics, sociology and psychology. Entrepreneurs were synonyms with businessmen in initial management articles (Kilby, 1971), and were not directly related to the foundation of new business ventures, or even to the correct identification and exploration of business opportunities.

The heart of entrepreneurship is viewed by Schumpeter (1934) as being directly related with innovation, in the sense that the entrepreneur is a person who innovates to create a new business venture, by carrying out new production combinations and they lose this trait when their business is correctly established. These combinations are the introduction of a new product that the consumers are not familiar with, the introduction of a new inexperienced method of production, discovering a new market, or the conquest of a new source of supply. Given this

point of view, entrepreneurship cannot occur in an organization that is already functioning, and among different team members.

Are the traits of an entrepreneur unique, or is it the way that they exercise their beliefs that differentiates them from a regular manager? Kirzner (1978, 1999) enumerates some of the traits that define an entrepreneur: alertness by noticing errors in the normal operation of a market to discover hidden profit opportunities, and creativity to exploit that disequilibrium. Gartner (1988) advocates that entrepreneur traits are auxiliary to their behavior, and that research should focus on what they do, instead of who they are. He simply defines entrepreneurship as being the creation of new organizations. Low and MacMillan (1988) define entrepreneurship in the same way, and argue that entrepreneurship research tries to find out the role of a new enterprise during the process of economic progress. Another research stream worth discussing is the results or consequences of an entrepreneur's actions. The main streams of entrepreneurship research can be characterized as: why the entrepreneurs act, how they act, and what happens when they act (Stevenson and Jarillo, 1990). Entrepreneurs influence economic growth by the way that they explore productive means (Baumol, 1990).

What is the status of entrepreneurship when we analyze strategic management actions? Both entrepreneurial and strategic management actions can be seen as being complementary domains to form the concept of strategic entrepreneurship. Strategic entrepreneurship is characterized by using the opportunity-seeking and uncertainty-capturing characteristics of entrepreneurship and the advantage-seeking perspective to increase the organization's performance from a strategic management point of view (Hitt et al., 2002; Ireland et al., 2003). It can be seen as an entrepreneurial action, which is carried out with a strategic mindset. Not all opportunities are worth being explored, and thus a strategic perspective helps to identify those that establish competitive advantages which lead to wealth creation (Hitt et al., 2001). The strategic entrepreneurship approach differs from earlier definitions, as it is not only the basis for new ventures, but it also considers the entrepreneurial mindset in an already-established enterprise. It foments entrepreneurial thinking, not only among top management, but also among teams which may spot new business opportunities by promoting a free speech and constructive feedback environment. This approach of entrepreneurship within an already established organization is named by some authors as being 'corporate entrepreneurship' (Dess et al., 2003; Ireland et al., 2009; Zahra et al., 1999). It deals with entrepreneurship within an established organization, instigating internal innovation that may lead to new business diversification, using joint ventures or acquisitions.

Social networking plays a fundamental role in entrepreneurship, as opportunities can be identified within communities and can simplify the exploration of resources among peers, which thus leverages a new production process (Greve and Salaff, 2003). Social networks also function as an advisory role for entrepreneurs, by

sharing experiences and by helping gather the necessary resources for venture creation. Another concept is 'entrepreneurship education', which deals with the problem of how to teach entrepreneurship by deviating from the myth that entrepreneurs are born with the right traits, and that entrepreneurship cannot be taught (Jones and English; Kuratko, 2005). Entrepreneurship where profit is not at stake is called 'social entrepreneurship' (Austin et al., 2006; Felício et al., 2012). Some authors also analyzed the regional, national or international expansion of the business that is performed, using an entrepreneurship perspective (Coviello and Jones, 2004; McDougall and Oviatt, 2000; Oviatt and McDougall, 2005).

Shane and Venkataraman (2000) present a conceptual framework of entrepreneurship. They explain that entrepreneurship is the "discovery and exploitation of profitable opportunities". The occurrence of entrepreneurship is due to a different point of view from an entrepreneur to an opportunity by facing the challenges with an optimistic attitude. If all entrepreneurs had the same mindset, then the incentive to pursue new opportunities would be useless, as everyone would transform the market needs of the same product or service by exploring the opportunity with no added value.

Venkataraman and Sarasvathy (2001) explain that both the fields of strategic management and entrepreneurship "seek to describe, explain, predict and prescribe how value is discovered, created, captured, and perhaps destroyed". They state that entrepreneurship contains the recognition, discovery and creation of opportunities that if exploited lead to new economic artifacts. It is the matching process that combines products of imagination with human aspirations to create new markets for goods and services. They use a metaphor with Romeo and Juliet, whereby Romeo is the entrepreneur, and the balcony represents the strategy to explain that entrepreneurship cannot progress without strategic management, and vice versa. In the paper they enumerate entrepreneurial aspects of strategic management, such as the human creativity that contributes to effectuation. Effectuation involves transforming aspirations into defined objectives and choosing between them. Another aspect is the emphasizing of control that "consists in analyzing the history and structure of the environment to make predictions about future trends, which then form the basis for strategic decisions". Near-decomposability deals with dividing complex systems into small connected parts that function as components, which can be further enhanced independently. This aspect provides the ability to respond quickly to new opportunities and to adapt the firm structure to multiple changes and challenges. The authors give the following example to explain the effect of effectuation and near-decomposability: "While effectuation stitches together pieces of entrepreneurial fabric into economic quilts that continue to make sense in an interactive and dynamically changing environment, near-decomposability identifies lines of tearing, so that pieces can be re-worked in synchrony with the overall pattern as the needs imposed by the environment change".

Gartner (1988) discusses that focusing on the traits of the entrepreneur is the wrong approach as the question the personality is irrelevant, as the main point of research in entrepreneurship is the actions behind the creation of organizations. He compares the research on entrepreneurship with leadership, where he argues that the evolution of leadership began when the research focused on the behavior of leaders, to evaluate their actions and decisions, instead of the traits that leaders possess. He gives the example of a baseball team to support his point of view, by explaining that the selection of a baseball player is based on the surmise that he is good at playing baseball and not his mental or physical characteristics, although they help. He concludes by saying that "the entrepreneur is not a fixed statement of existence, but rather entrepreneurship is a role that individuals undertake to create organizations".

Ketchen et al. (2007) argue that collaborative innovation is the key to strategic entrepreneurship, as large firms have difficulties of thinking outside of the box, and by partnering with small firms that lack resources and have limited knowledge they are able to develop new ideas, both as opportunity and advantage seeking activities. They explain that wealth creation by fomenting collaborative innovation is consistent in network, learning, resource-based and real options theories.

Foss et al. (2008) explain that "entrepreneurs use imagination to interpret economic data and anticipate future market conditions." They characterize entrepreneurship both as alertness, where opportunities are waiting to be discovered and explored to introduce new services, and judgment, where the entrepreneur reveals a new product to the market by believing they are right and going against the tide by having a different perception of reality. The authors emphasize that subjectivism is a key element for theory development in entrepreneurship and strategy research, because it connects the missing links between the insight from the Austrian economics, Penrose's resources approach, and also the modern resource-based view. They focus on entrepreneurship as a team effort and state that diverse team membership, heterogeneous mental models, positive team dynamics, rewarding creative thinking with experimentation, and resource learning are all key factors that increase team entrepreneurship in organizations.

Dyer et al. (2008) analyze the attributes of innovative entrepreneurs. They define an innovative entrepreneur as being: "the founder of a new venture that offered a unique value proposition relative to incumbents (e.g., a new or different feature set, pricing, convenience, customizability); and the person who came up with the original idea to start the venture." They started by conducting interviews with 25 innovative entrepreneurs and 25 senior executives in large companies, in order to differentiate the behavioral patterns of acquiring information. They identified 4 patterns: questioning by challenging the status quo; observing in search of new ideas; experimenting, and; idea networking by testing the ideas with people with different knowledge and background.

Felício et al. (2012) present a model that explains the effect of social entrepreneurship and transformational leadership on social value that affects organizational performance of non-profit social organizations. They conclude that organizational performance is explained equally by social entrepreneurship and social value, and that transformational leadership contributes to a lesser extent. They also state that the socio-economic context affects the influences of these constructs.

Multiple authors attempt to define entrepreneurship, and there is no general accepted definition among researchers. Trends in entrepreneurship research are divided among the study of an entrepreneur's traits, the behavior that motivates the actions of an entrepreneur, and the consequences of entrepreneurial initiatives. Multiple research domains claim entrepreneurship to be a discipline of their own, while others advocate that entrepreneurship should be isolated in its own domain. Earlier studies by Gartner (1988); Kirzner (1978); Low and MacMillan (1988); Schumpeter (1934) provide the basis for entrepreneurial research, and they have been used and cited intensively by newer researches. A recent article that summarizes the multiple entrepreneurship approaches is "A general review of entrepreneurship research (1998 to 2010): Theoretical implications, management applications and future research directions" by Cai et al. (2012). They review the entrepreneurship literature from 1998 to 2010, and classify 359 entrepreneurial articles according to research theme, methodology and level of analysis. They classify the articles among the following research themes: entrepreneur, team, opportunity, resource, networking and environment. They also differentiate as to the type of study (conceptual, empirical and experimental) and the scope of the study (individual, team, firm or macro). They also present a list of different theories applied in entrepreneurial literature, divided by the economics, management, sociology and psychology domains. Analyzing each theme individually, they state that the "research on entrepreneur focused on aspects that included entrepreneurial demography, personality, human capital, human resources, as well as the entrepreneur's behavior and decision-making". Entrepreneurial resources research focuses on the resource-based view, and the research focus is moving from static to the dynamic management of resources. That research branch is divided by the effect of the resources on outcomes and the management of new venture resources. When the focus is the entrepreneurial team, they segmented the research material among multiple areas: research on team entrepreneurship theory; the training process of the new venture team and influence factors; the study team dynamic management process; the relationship between entrepreneurial team and performance, and; the influence of new venture team on venture capital decision making. They divided the research on entrepreneurial networks into two branches: "entrepreneurial networks as an impact factor, and discussion of its function in the process of new venture creation and growth", and networks as a research object (dynamic evolutionary process and network governance) and the effect of social capital on new ventures. Regarding the perception of the entrepreneurial environment, the

research is centered in three aspects: environmental elements, by analyzing the impact of those elements on entrepreneurial activities; environmental characteristics positioned at firm level, using contingency or resource dependent theory, and; institutional environments by looking at entrepreneurial activities within that frame. At the end of the article they identify the literature gaps and describe future research directions for each of the research themes. Some of the research directions are: what are the contextual factors that influence an entrepreneur's human capital; how does the interaction of individual differences in entrepreneurs affect the processes of opportunity exploitation; how do human resource management practices affect organizational performance in new ventures; how will members' entry or departure influence the formation of new ventures, and; what is the effect of environmental characteristics on new ventures.

Technological entrepreneurship

Kollmann (2006) defines e-entrepreneurship as being: "establishing a new company with an innovative business idea within the Net Economy, which, using an electronic platform in data networks, offers its products and/or services based upon a purely electronic creation of value. Essential is the fact that this value offer was only made possible through the development of information technology". He explains that the achievement of information leadership leverages superiority over competitors, by the knowledge provided by the information about customers and by the market. Information technology has changed from being a mere support function, into the core competence of e-entrepreneurship, being a part of the preparation, negotiations and conclusion phases of business processes. The author discusses the electronic creation of value, by including the following aspects: creation of value with the structuring of information to simplify the customer's overview; the selection value that enables the customer to search and locate the product they need among multiple information; the optimization of the transaction value, fomenting cooperation among various vendors to interlink themselves, and; the communication among different customers with opinions and product reviews. He explains that the electronic value creation process involves three phases: 1) the information gathering that is elaborated by creating the e-entrepreneurship mindmap; 2) information processing by transforming it in a product for the customer, and; 3) information transfer, where knowledge is implemented in an online platform. He details that e-entrepreneurship requires a high amount of capital to be funded with the acquisition of information technology, both in the case of software and hardware. He also warns that information technology is constantly evolving, and thus capital investment will always be necessary, and will not just be an initial financial contribution. He enumerates some of the differences between traditional entrepreneurship and e-entrepreneurship: type of the company established; added value through the use of information technology; information as a competitive factor in e-business, and; increased growth potential and uncertainty of the constantly changing information technology environment. The competences

of the e-entrepreneurs are also pointed out as being distinctive in the e-venture process, namely: know-how regarding computer science to understand the core resource of information technology; the capability of information management; the knowledge necessary to administer a business, and; experience in the business specific target industry.

Kollmann (1998) analyzes the three steps necessary for electronic commerce success: 1) obtaining information; 2) processing information, and; 3) transferring information. The author explains that the process of information management is the key to the success of e-business, as e-business deals with interactive information directly provided from, and to the customer, as part of the e-business internal processes. He details four factors that influence information: cost; quality; speed, and; flexibility. He points out barriers that constrain an effective information management process: short term return on investment, dismantling or changing existing traditional commercial structures and becoming actively involved in the customer interactive communication. He provides an example that setting a static webpage describing products is normally the step deployed by enterprises which do not see the advantage of information management in e-business.

In Amit and Zott (2001), the authors' aim is to fill the theoretical gap by identifying the sources of value in e-business. They present a business model for the creation of value in e-business, based on four dimensions: efficiency, complementarities, lock-in and novelty. They characterize virtual markets as having high connectivity, being focused on transactions, the availability of detailed information, and being centered on information goods and networks. In virtual markets the provider versus customer relation is straightened with the reduction of intermediaries and the direct communication provided via constant online feedback, which leads to transaction cost reduction, which in turn creates added value. The first value dimension is efficiency, and this dimension is related with transaction cost efficiency and information richness, as it supports faster and reliable customer decision making. This selection process is simplified, as the customer does not have to search for additional information regarding a product. Complementarities bring added value, by presenting bundles of interrelated products, which individually do not bring that much value. Another dimension to take into account is lock-in, which is represented by the benefit of a customer performing multiple transaction for the same e-business. This behavior creates trust, and is measured in order to reward loyal customers and thus encourage customer retention, while seamlessly preventing customer migration to a competitor. This sort of behavior can also occur in sites where the lock-in effect increases with the addition of other customers, creating a community where the consumer also contributes with content, which in turn increases information leadership. The interface of the e-business also presents a form of lock-in, as the customer gets used to carrying out the transaction in a familiar way, as humans are known to resist change, which, in this case, is the change from altering the interface by using a competitor's e-business. Product customization by the customer is also proposed by the authors as a lock-in method,

as people always like products which are customized by their needs, which gives the notion of product uniqueness, or an especially-tailored product. Cross-selling by exchanging preferences and analyzing past purchases along with updated customer product reviews also increases the lock-in effect. The novelty dimension deals with the innovation regarding the structuring of transactions in e-business. The authors state that: "the unique characteristics of virtual markets (i.e., the removal of geographical and physical constraints, possible reversal of information flows from customers to vendors, and other novel information bundling and channeling techniques) make the possibilities for innovation seem endless". The partnering with online third-parties to develop affiliate programs to promote te-business and to diversify the product offer also intensifies the first mover experience.

Fillis and Wagner (2005) present a conceptual framework for e-business development. They enumerate some measures to overcome the barriers that constrain e-business: operational barriers that can be surpassed through the use of data transfer of online documentation, and product and market barriers that can be suppressed by online market research, and by improving customer orientation through online feedback. Other barriers that are more difficult to overcome are "security and privacy worries, costs of consultants and lack of IT competence". Competences in e-business play a central role, with the competence portfolio not only being represented by technical kills, but also by soft skills, like entrepreneurial marketing. Networking in e-business should also be regarded as a key factor for success, as the traditional word to mouth that favors real business is converted to virtual to mouth recommendations. This behavior occurs because: the Internet offers a potential new approach to customer-relationship management, with particular emphasis on communication". Among other e-business benefits, the authors enumerate: "improved communications, cost savings, greater visibility, ability to develop new markets and greater levels of information retrieval". They conclude that the lack of technical skills negatively affects e-business success, but these have to be balanced with judgmental, managerial knowledge and business experience.

Colombo and Delmastro (2001) analyze the characteristics of technological entrepreneurs. The research sample is 241 entrepreneurs, whot created 116 firms in Italy between 1984 and 1999. They concluded that the institutional setting was determinant in influencing the entrepreneurial decision that led to self-employment. They explain that the entrepreneurs were in their middle 30s, and that they were not necessary educated in a technological field. The expectation of a substantial income increase is another point that e-entrepreneurs take into account when deciding to move into e-business.

Wang and Swanson (2007) analyze the role of institutional entrepreneurs in designing and implementing professional services automation. They relate this theme with the discussion as to why some IT innovations are more easily adopted by business than others, and propose a model that "shifts the focus of IT innovation

research from assessing institutional effects, to understanding institution-building". They state that the success of IT innovations is dependent on the entrepreneur that creates institutional favorable conditions for this success to occur, namely the struggle against technological change that hinders the acceptance of IT, and the leadership skills that achieve mobilization towards the legitimation of the innovation, and also the establishment of a community that supports it.

Keeney (1999) uses value-focused thinking to develop a comprehensive list of customer values related to Internet commerce, as the value proposition of a product can be higher or lower if bought online. These values are transformed into objectives composed by: a decision context, an object and a direction of preference. By using customer values, a company can adapt their products to fit the needs of the buyer, but as customers may have different values, a value proposition in one product for a customer, may be different for another. Values can also be prioritized by asking the customers to decide on the importance between fundamental objectives, and therefore achieve knowledge to create and redesign products. This knowledge allows the creation of a framework for addressing company decisions that carry out business over the Internet. The values of prospective customers that were identified in this research will allow for the forecast of Internet commerce for a new company.

Garud and Karnøe (2003) defend that technology entrepreneurship is the product of a body of entrepreneurs. They argue that "skills and resources required to take an idea from its inception to commercial use have to be mobilized by drawing upon the generative impulses of actors from multiple domains". Each entrepreneur, or actor, possesses bits of inaccurate or contradictory knowledge that must be discussed among the entrepreneurial body, in order to generate a momentum that foments technology entrepreneurship. This shaping of entrepreneurial ideas in real-time also shapes the different individual visions of an entrepreneur, leading to a unique entrepreneurial strategy which is accepted among a community that mobilizes the technological change necessary for entrepreneurship.

Information Security Standards

This section details two information security standards used by e-business to achieve competitive advantage over its competitors regarding the assurance of information security. These standards assure that a continuous improvement process takes place, and that their requirements are audited independently in order to establish management accountability.

ISO 27001

The ISO/IEC 27001 (ISO/IEC27001, 2005) is an international standard that provides a model for establishing an Information Security Management System

(ISMS) as a strategic organization decision. The word system does not imply a real asset, but a defined and monitored methodology, or a security program. The ISMS is formed by tools, processes, templates, documents and best practices. The establishment of the ISMS is performed according to the plan, do, check, act (PDCA) model. It reveals the present snapshot of the organization's security posture, called "as-is", and establishes the target objective to plan for the "to-be", using the information from a gap analysis and developing a transition plan.

The objective of an organization being certified in this standard is compliance with the effective information security processes in place, instead of applying non-repeatable ad-hoc procedures. The certification issued by an independent third party serves as evidence that the security controls exist and function according to the standard requirements. This evidence can serve as a competitive advantage, and can respond to the compliance requests of some customers and assures that business security follows best practices, which generates a trust relationship.

The ISMS can be defined as an overall management system from a business risk perspective, that has to be established, implemented, operated, monitored, and maintained (Arnason and Willett, 2008). It mandates that the organization systematically examines its risks, taking into account threats and vulnerabilities, implements control procedures to deal with those risks, and adopts a continuous improvement information security management process that continuously responds to business security needs (Calder and Watkins, 2008).

ISO/IEC 27001 is used in conjunction with ISO/IEC 27002, formerly known as ISO/IEC 17799 (ISO/IEC17799, 2005), which establishes the code of practice for information security management. This code of practice contains specific controls for dealing with most requirements of ISO/IEC 27001, including technical security, but ISO/IEC 27001 expects these measures to have already been taken care of, and focuses on the mandatory requirements of an Information Security Management System. ISO 27001 focuses on the ISO/IEC 17799 control objectives in Appendix A:

- Security policy: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- Organization of information security:
    - Internal Organization: To manage information security within the organization.
    - External Parties: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
- Asset management:

  - Responsibility for assets: To achieve and maintain appropriate protection of organizational assets.
  - Information classification: To ensure that information receives an appropriate level of protection.

- Human resources security:
  - Prior to employment: To ensure that employees, contractors and third party users understand their responsibilities, are suitable for the roles they are considered for, in order to reduce the risk of theft, fraud or misuse of facilities.
  - During employment: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, in order to reduce the risk of human error.
  - Termination or change of employment: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

- Physical and environmental security:
  - Secure areas: To prevent unauthorized physical access, damage and interference to the organization's premises and information.
  - Equipment security: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

- Communications and operations management:
  - Operational procedures and responsibilities: To ensure the correct and secure operation of information processing facilities.
  - Third party service delivery management: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
  - System planning and acceptance: To minimize the risk of systems failures.
  - Protection against malicious and mobile code: To protect the integrity of software and information.
  - Backup: To maintain the integrity and availability of information and information processing facilities.
  - Network security management: To ensure the protection of information in networks and the protection of the supporting infrastructure.

- Media handling: To prevent unauthorized disclosure, modification, removal or destruction of assets, and the interruption of business activities.
- Exchange of information: To maintain the security of information and software exchanged within an organization and with any external entity.
- Electronic commerce services: To ensure the security of electronic commerce services, and their secure use.
- Monitoring: To detect unauthorized information processing activities.

- Access control:
  - Business requirement for access control: To control access to information.
  - User access management: To ensure authorized user access and to prevent unauthorized access to information systems.
  - User responsibilities: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.
  - Network access control: To prevent unauthorized access to networked services.
  - Operating system access control: To prevent unauthorized access to operating systems.
  - Application and information access control: To prevent unauthorized access to information held in application systems.
  - Mobile computing and teleworking: To ensure information security when using mobile computing and teleworking facilities.

- Information systems acquisition, development and maintenance:
  - Security requirements of information systems: To ensure that security is an integral part of information systems.
  - Correct processing in applications: To prevent errors, loss, unauthorized modification or misuse of information in applications.
  - Cryptographic controls: To protect the confidentiality, authenticity or integrity of information by cryptographic means.
  - Security of system files: To ensure the security of system files.
  - Security in development and support processes: To maintain the security of application system software and information.
  - Technical Vulnerability Management: To reduce risks resulting from exploitation of published technical vulnerabilities.

- Information security incident management:

- Reporting information security events and weaknesses: To ensure information security events and weaknesses associated with information systems are communicated in a manner that allows timely corrective action to be taken.
- Management of information security incidents and improvements: To ensure a consistent and effective approach is applied to the management of information security incidents.

- Business continuity management:
  - Information security aspects of business continuity management: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.

- Compliance:
  - Compliance with legal requirements: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
  - Compliance with security policies and standards, and technical compliance: To ensure compliance of systems with organizational security policies and standards.
  - Information systems audit considerations: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

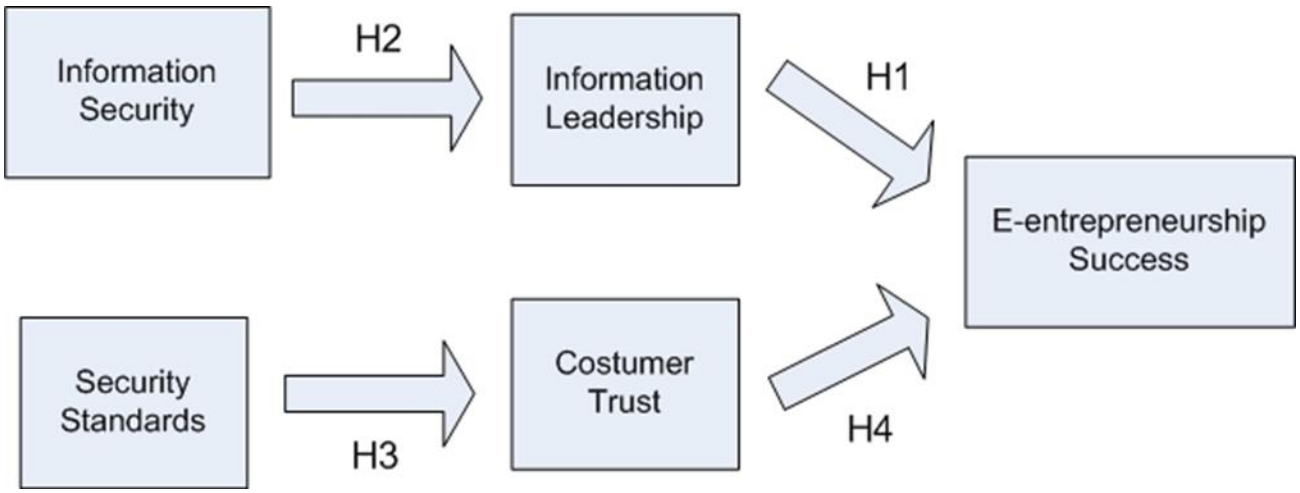

Figure 1. Research Model

PCI-DSS

The payment card industry data security standard (PCI-DSS, 2008) was developed to assure cardholder data security and to unify consistent data security measures globally. It was created by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to establish requirements for the security of the payment card industry affecting everyone who stores card payment data, including common online commercial transactions. It is guided by a continuous process, as it can be seen in Figure, to ensure adequate monitoring and the improvement of requisites by assessing, remediating and reporting procedures. It has six control objectives and establishes twelve requirements for compliance:

- Build and maintain a secure network
- Install and maintain a firewall configuration to protect cardholder data;
    - Not to use vendor-supplied defaults for system passwords and other security parameters;
- Protect cardholder data
    - Protect stored cardholder data;
    - Encrypt transmission of cardholder data across open, public networks;
- Maintain a vulnerability management program
    - Use and regularly update anti-virus software or programs;
    - Develop and maintain secure systems and applications;
- Implement strong access control measures
    - Restrict access to cardholder data by business need-to-know;
    - Assign a unique ID to each person with computer access;
    - Restrict physical access to cardholder data;
- Regularly monitor and test networks
    - Track and monitor all access to network resources and cardholder data;
    - Regularly test security systems and processes;
- Maintain an information security policy

- Maintain a policy that addresses information security for employees and contractors;

Discussion

ISO 27001 contains general requirements that embrace most of the departments and processes of a business model. A company wishing to be certified in this standard can size the effort for the ISMS implementation, by detailing scope of the certification in the statement of purpose document. In this way, the standard has the flexibility to include only some processes in the certification scope. The establishment of an information security policy that documents the ISMS strategy by top management serves as a milestone for the implementation of the additional requirements. Information classification allows for the prioritization of security measures by documenting the importance of information from a business perspective, rather than from a technology-centered vision. The human resources security section details requirements for the employment lifecycle, starting during the hiring process by looking, for example, at the criminal record, through to the termination of duties by revoking all accesses to the organization. Although human resources security is not applicable initially to e-entrepreneurship, due to the limited number of employees, it should be taken into account as soon as the business grows. E-business logical security access needs to be taken into account right from the beginning, but there should also be concerns regarding physical security, as there are bypass mechanisms for logical security access for operators, who have physical access to the technological assets. Communications and operations management, logical access control, systems development and incident management detail the specific requirements that apply directly to e-entrepreneurship from the beginning to establish customer trust with increasing added value and to achieve competitive advantage. These sections details the requirements that affect the business core: the online platform, from system development and maintenance through to the assurance of network security and the readiness to respond to security incidents. Business continuity ensures that the business tolerates both physical and logical disasters that affect the availability of information. The compliance section details the aspects necessary for compliance with legal and internal requirements and provides the management control evaluation which is established by independent auditors.

The PCI-DSS standard is more focused on e-business than ISO 27001. Its control objectives are more technical in nature, e.g. by providing detailed requirements for the configuration of the firewall, the use of anti-virus, and the storing and transmission of cardholder data. Secure application development is present with the requirement to develop and maintain secure systems and applications and to test these systems from a malicious point of view, which is also called penetration testing or ethical hacking, in order to evaluate existing code vulnerabilities.

Monitorization is another factor to take into account, as it enables the early detection of security incidents that can jeopardize access control, based on the need-to-know principle. This standard is mostly mandatory for establishing partnerships with online payment entities and is not just a vehicle to earn customer trust.

Research Model

Based on the literature review and using the evaluation of information security standards, this section presents the research model that visually supports the research hypotheses, as it can be seen in Figure 1.

Nowadays, information is seen to be the primary core resource for e-entrepreneurship in order to achieve competitive advantage. The information leadership fully supports e-entrepreneurship success, as it has provided added value to the customer since its foundation. It supports the lock-in customer aspect, while producing added value for transactions during the information gathering, processing and transference process. Therefore I hypothesize:

H1: Information leadership affects e-entrepreneurship success.

E-entrepreneurship needs to maintain information leadership for as much time as possible in order to impose barriers to new businesses and to differentiate from competitors. As e-business presents a huge margin for growth, due to the lack of geographical barriers, and it also can be ruined by the loss of reputation caused by sensitive information disclosure, or the unavailability of information technology. With this context in mind, I present the following hypothesis:

H2: Information security affects information leadership.

Strategically, most e-businesses are starting to realize the importance of information security, not only for the daily operations, but also as a marketing technique for earning the consumer's trust and loyalty, in a virtual world where trust is deposited in an entity that is not always trustworthy. This lack of face-to-face contact that improves human trust is not available online, and therefore the customer needs to trust an independent auditing entity that assures that appropriate security controls are put in place. These controls are derived from information security standards that safeguard the consumer's interests regarding information security. Current practices show that, with the rise of cloud computing, some e-businesses are technically managed by a third party, so the adoption of these standards promote e-business accountability regarding customer data. This mindset leads to the following hypothesis:

H3: The adoption of information security standards affects customer's trust.

The customer's trust is directly related with e-entrepreneurship success, as it enhances the price that a customer is willing to pay for an online transaction, as customers tend to be loyal to an e-business they trust and it improves the lock-in

aspect that enables multiple transactions and gets them used to the e-business interface. Therefore the following hypothesis is proposed:

H4: Customer's trust affects e-entrepreneurship success.

Conclusion

This research bridges the theoretical gap that exists regarding information security value for e-entrepreneurship. Information plays the leading role in supporting e-business and therefore security safeguards need to be taken in order to support the integrity, confidentiality and availability of information. Customers value the due care responsibility that e-entrepreneurship shows by employing best practices from security standards such as ISO 27001 and PCI-DSS, in order to demonstrate that adequate security measures have been put in place to protect the customer's stored personal information, and to secure the data during e-business transactions. Information security enables the competitive advantage for e-entrepreneurship, whilst establishing an effective governance of information that foments customer trust, due to an adequate security control framework. Future research relies on testing the research model by collecting data from recent e-entrepreneurship initiatives, both successes and failures, via a questionnaire, in order to evaluate how the theoretical research model fits into real e-business and whether the research hypotheses are supported. If e-entrepreneurship founders have the availability to conduct face-to-face interviews, then the research can take a triangulation approach. This approach consists of supporting the literature review conclusions by conducting in depth interviews with open-questions in order to qualitatively enhance the research model, followed by conducting the questionnaire in order to quantitatively corroborate the results from the interviews.

References

Amit, R. and C. Zott: 2001, 'Value creation in e-business'. *Strategic Management Journal* 22(6-7), 493-520.

Arnason, S. T. and K. D. Willett: 2008, *How to Achieve 27001 Certification*: *An Example of Applied Compliance Management*. Auerbach Publications.

Austin, J., H. Stevenson, and J. Wei-Skillern: 2006, 'Social and Commercial Entrepreneurship: Same, Different, or Both? Entrepreneurship Theory and Practice 30(1), 1-22.

Barney, J.: 1991, 'Firm Resources and Sustained Competitive Advantage'. *Journal of Management* 17(1), 99-120.

Baumol, W. J.: 1990, 'Entrepreneurship: Productive, Unproductive and Destructive'. *Journal of Political Economy* 98(5), 893-921.

Cai, L., Q. Liu, S. Deng, and I. Alon: 2012, 'A general review of entrepreneurship research (1998 to 2010): Theoretical implications, management applications and future research directions'. *African Journal of Business Management* 6(2), 474-492.

Calder, A. and S. Watkins: 2008, IT Governance: *A Manager's Guide to Data Security and ISO 27001 / ISO 27002*. Kogan Page.

Colombo, M. G. and M. Delmastro: 2001, 'Technology-based entrepreneurs: does internet make a dierence?' *Small Business Economics* 16(3), 177-190.

Corbitt, B. J., T. Thanasankit, and H. Yi: 2003, 'Trust and e-commerce: a study of consumer perceptions'. Electronic Commerce Research and Applications 2(3), 203 - 215. Selected Papers from the Pacific Asia Conference on Information Systems.

Coviello, N. E. and M. V. Jones: 2004, 'Methodological issues in international entrepreneurship research'. *Journal of Business Venturing* 19(4), 485-508.

Dess, G. G., R. D. Ireland, S. A. Zahra, S. W. Floyd, J. J. Janney, and P. J. Lane: 2003, 'Emerging Issues in Corporate Entrepreneurship'. *Journal of Management* 29(3), 351-378.

Dyer, J. H., H. B. Gregersen, and C. Christensen: 2008, 'Entrepreneur behaviors, opportunity recognition, and the origins of innovative ventures'. *Strategic Entrepreneurship Journal* 2(4), 317-338.

Felício, J. A., H. M. Gonçalves, and V. C. Gonçalves: 2012, 'Explaining Social Value and Organizational Performance in Social Non-Profit Organizations: Social Entrepreneurship, Leadership and Social Context Effects'. In: 1st GIKA Conference Proceedings, Global Innovation and Knowledge Academy, Valencia, Spain, July 10-12.

Fillis, I. and B. Wagner: 2005, 'E-business Development: An Exploratory Investigation of the Small Firm'. *International Small Business Journal* 23(6), 604-634.

Foss, N. J., P. G. Klein, Y. Y. Kor, and J. T. Mahoney: 2008, 'Entrepreneurship, subjectivism, and the resource-based view: toward a new synthesis'. *Strategic Entrepreneurship Journal* 2(1), 73-94.

Gartner, W. B.: 1988, '"Who is an Entrepreneur? is the Wrong Question". University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship.

Garud, R. and P. Karnøe: 2003, 'Bricolage versus breakthrough: distributed and embedded agency in technology entrepreneurship'. Research policy 32(2), 277-300.

Grant, R.: 1996, 'Toward a knowledge-based theory of the rm'. *Strategic Management Journal* 17, 109-122.

Greve, A. and J. W. Salaff: 2003, 'Social Networks and Entrepreneurship'. *Entrepreneurship Theory and Practice* 28(1), 1-22.

Hitt, M., R. Ireland, S. Camp, and D. Sexton: 2002, *Strategic Entrepreneurship: Creating a New Mindset*. Oxford, UK: Blackwell Publishing.

Hitt, M. A., R. D. Ireland, S. M. Camp, and D. L. Sexton: 2001, 'Strategic entrepreneurship: entrepreneurial strategies for wealth creation'. *Strategic Management Journal* 22(6-7), 479-491.

Ireland, R. D., J. G. Covin, and D. F. Kuratko: 2009, 'Conceptualizing Corporate Entrepreneurship Strategy'. Entrepreneurship Theory and Practice 33(1), 19-46.

Ireland, R. D., M. A. Hitt, and D. G. Sirmon: 2003, 'A Model of Strategic Entrepreneurship: The Construct and its Dimensions'. *Journal of Management* 29(6), 963-989.

ISO/IEC17799: 2005, 'Information Technology - Security Techniques - Code of Practice for Information Security Management'. http://www.iso.org.

ISO/IEC27001: 2005, 'Information Technology - Security Techniques – Information Security Management Systems - Requirements'. http://www.iso.org.

Jones, C. and J. English, 'A contemporary approach to entrepreneurship education'. *Education + Training* 46(8-9), 416+.

Keeney, R. L.: 1999, 'The Value of Internet Commerce to the Customer'*. Management Science* 45(4), 533-542.

Ketchen, D. J., R. D. Ireland, and C. C. Snow: 2007, 'Strategic entrepreneurship, collaborative innovation, and wealth creation'. *Strategic Entrepreneurship Journal* 1(3-4), 371-385.

Kilby, P.: 1971, *Entrepreneurship and economic development*. Free Press.

Kirzner, I.: 1978, *Competition and Entrepreneurship, Phoenix edition*. University of Chicago Press.

Kirzner, I.: 1999, 'Creativity and/or Alertness: A Reconsideration of the Schumpeterian Entrepreneur'. *The Review of Austrian Economics* 11, 5-17.

Kollmann, T.: 1998, 'The information triple jump as the measure of success in electronic commerce'. *Electronic Markets* 8(4), 44-49.

Kollmann, T.: 2006, 'What is e-entrepreneurship? Fundamentals of company founding in the net economy'. *International Journal of Technology Management* 33(4), 322-340.

Kuratko, D. F.: 2005, 'The Emergence of Entrepreneurship Education: Development, Trends, and Challenges'. *Entrepreneurship Theory and Practice* 29(5), 577-598.

Lee, K. S. and S. J. Tan: 2003, 'E-retailing versus physical retailing: A theoretical model and empirical test of consumer choice'. *Journal of Business Research* 56(11), 877 - 885. Strategy in e-marketing.

Liao, Z. and M. T. Cheung: 2002, 'Internet-based e-banking and consumer attitudes: an empirical study'. *Information & Management* 39(4), 283 - 295.

Low, M. B. and I. C. MacMillan: 1988, 'Entrepreneurship: Past Research and Future Challenges'. *Journal of Management* 14(2), 139-161.

McDougall, P. P. and B. M. Oviatt: 2000, 'International Entrepreneurship: The Intersection of Two Research Paths'. *The Academy of Management Journal* 43(5), pp. 902-906.

Oviatt, B. M. and P. P. McDougall: 2005, 'Defining International Entrepreneurship and Modeling the Speed of Internationalization'. Entrepreneurship Theory and Practice 29(5), 537-554.

PCI-DSS: 2008, 'Payment Card Industry Data Security Standard Version 1.2'. http://www.pcisecuritystandards.org.

Porter, M. E.: 2001, 'Strategy and the Internet.' *Harvard Business Review* 79(3), 62-78, 164.

Porter, M. E. and V. E. Millar: 1985, 'How information gives you competitive advantage'. *Harvard Business Review* 63(4), 149-160.

Saltzer, J. H. and M. D. Schroeder: 1975, 'The protection of information in computer systems'. Proceedings of the IEEE 63(9), 1278-1308.

Schumpeter, J. A.: 1934, *The Theory of Economic Development*. Harvard University Press.

Shane, S. and S. Venkataraman: 2000, 'The Promise of Entrepreneurship as a Field of Research'. *Academy of Management Review* 25(1), 217-226.

Stevenson, H. and J. C. Jarillo: 1990, 'A Paradigm of Entrepreneurship: Entrepreneurial Management'. *Strategic Management Journal* 11, 17-27.

Tan, M. and T. S. Teo: 2000, 'Factors influencing the adoption of Internet banking'. *Journal of the AIS* 1(1es), 5.

Venkataraman, S. and S. D. Sarasvathy: 2001, 'Strategy and entrepreneurship: Outlines of an untold story'. Darden Business School Working Paper No. 01-06.

Wang, P. and E. B. Swanson: 2007, 'Launching professional services automation: Institutional entrepreneurship for information technology innovations'. *Information and Organization* 17(2), 59-88.

Zahra, S. A., D. F. Jennings, and D. F. Kuratko: 1999, 'The Antecedents and Consequences of Firm-Level Entrepreneurship: The State of the Field'. *Entrepreneurship: Theory and Practice* 24(2), 45-65.