WEB ASSURANCE

Information Security Management for e-commerce

LES LABUSCHAGNE

RAU Standard Bank Academy for Information Technology

Rand Afrikaans University, South Africa

LL@na.rau.ac.za

Key words: Information security, e-commerce, web assurance, privacy, security services, consumer protection

Abstract: Most organisations considering the adoption of electronic commerce (EC) need to undergo a paradigm shift. The rules that usually govern business change when engaging in cyber trade. In terms of security, a similar paradigm shift needs to take place. In EC, security is no longer the protector, but has become the enabler. This article looks at what it takes to become EC-enabled and what the real security challenges are. Based on these challenges, the role of security in EC is analysed, leading to a wider view called Web assurance. Web assurance consists of three components, namely security, privacy and consumer protection. Security managers in EC-enabled organisations will have to expand their existing skills and knowledge to effectively combat the onslaught of EC.

1. INTRODUCTION

Information security is identified by many surveys as the biggest inhibitor to electronic commerce (EC), yet when looking at security technologies, this does not seem to hold true. Many tales of horror as well as success abound, making it difficult to judge whether or not security is adequate. When a car is stolen with locked doors but open windows, it is not the security technologies that failed, but rather the ineffective or partial use thereof. Car theft, however, does not deter people from using it as a mode of transport. Its functional value outweighs its security risks.

Before attempting to evaluate the adequacy of security technologies, it is necessary to look at what makes an organisation EC-enabled. Based on these characteristics, the security challenges of EC can be defined and understood.

This article is intended to provide a framework for EC security management, based on the above-mentioned challenges, to assist a security manager in covering all the bases and, at the same time, contribute to the successful acceptance thereof. This EC security management framework is referred to as Web assurance as it encompasses more than just security [ACCE01]. EC security should not be an inhibitor of EC but rather become an enabler.

2. WHAT ARE THE SECURITY PROBLEMS ASSOCIATED WITH ELECTRONIC COMMERCE?

Before embarking on any EC initiative, it is crucial that an organisation understands the security implications. To comprehend the security implications, the nature of EC has to be analysed. EC organisations differ substantially from one another, ranging from small retailers to large multinational corporations. Despite the differences, there are some common elements to be found in all EC organisations. There are six factors that govern an EC-enabled organisation as depicted in Figure 1 below [ROSS01]:

Figure 1 – EC elements

1. **Convergence** – In EC, the convergence of business and technology drives the organisation. Technology has become a business enabler and creates new business opportunities. Information technology no longer plays just a supporting role but has worked its way up into senior management circles. Most successful companies have a Chief Information Officer (CIO) on the board.

The security challenge associated with convergence is the integration of information security architecture into the business architecture. Few business people understand information security to the extent that it is included during business strategy planning.

Furthermore, convergence leads to EC organisations becoming totally reliant on technology, and any security breaches - unlike those in physical organisations - could lead to the demise of such an organisation. CDUniverse is an example of an EC business that had to close down after it was discovered that several credit card numbers had been stolen from it.

2. **Streamlining** – All business processes, both internal and external, must constantly be analysed for ways to make improvements. Streamlining also involves the creation of new business processes, which, in turn, might require new or additional infrastructure. Organisations can no longer function in electronic isolation of customers, partners and suppliers.

The security challenge of streamlining is the integrated nature of EC, which means that total security is no longer within the complete control of the organisation. This is especially a problem in business-to-business (B2B) EC. If a customer or supplier is negligent with passwords, no level of security is going to protect the organisation from hackers. There are many reported cases where hackers break into one organisation just to use it as a launch pad for an attack on someone else.

3. **Technology awareness** – The EC-enabled organisation must keep abreast of technological developments, as such developments create new opportunities. CEOs of the future will need a solid understanding of both the business and technological aspects affecting their organisations and industry.

The security challenge of new technologies is that they come with new vulnerabilities. The integration of different technologies also makes it difficult to find all vulnerabilities, as it is impossible to test all possible combinations of technologies. The ever-changing environment also makes it very difficult, if not impossible, to do proper risk analysis on these systems. Employees are becoming more technologically capable and can find and exploit weak spots within systems. The abundance of hacking-related Web sites and the decline in organisational loyalty all augment the problem.

4. **Flat-and-flexible organisational structure** – The EC industry is a fast-paced one with little time for bureaucracy. The organisational structure needs to be adapted to become mobile and flexible in response to change. Employees must be empowered to make decisions and utilise opportunities. This means that the functional organisational structure of the past is inadequate and that new structures, such as project and matrix organisation structures are required.

The security challenge with a flat-and-flexible organisational structure is that employees are now empowered to take advantage of opportunities. Less control, therefore, is possible within organisations that are having difficulty enforcing policies and procedures. Little time is spent on doing proper risk analysis before venturing into new endeavours. The balance between security and business opportunity is becoming more difficult, especially in view of point 1 above. Thus the line between accountability and responsibility becomes very hazy.

5. **Information-centricity** – EC differentiates itself from traditional commerce in the sense that information, rather than a physical product, is the primary asset. A more aggressive approach, therefore, needs to be followed for information gathering, storage and retrieval. For this purpose, more organisations are starting to use data warehousing and data mining. Information centricity also means that organisations are becoming more dependent on technology to provide the information in a timely manner.

The amount of information that has to be stored makes the security classification thereof very difficult. Access control to the information becomes problematic especially in the light of point 4 above. The availability of information is crucial to the organisation, and as such, requires well-tested disaster recovery and business continuity plans. The security issues in data warehousing – spread across several platforms – present a new area that is yet to be understood.

6. **Customer-centricity** – The focus of EC is on the individual customer, rather than on the anonymous masses. This is sometimes referred to as mass-customisation where products and services intended for the masses are packaged for the individual. Customers want to be treated as individuals, which means that organisations must get to know their customers as individuals.

To do this requires substantial private information. Possessing large amounts of private information increases the responsibility on the organisation in terms of complying with data privacy legislation. Organisations are now also more vulnerable to legal action by disgruntled clients. The socio-ethical issues in EC are unexplored and undefined territory.

The above list is by no means exhaustive but serves as a general understanding of what makes an organisation EC-enabled. The next section looks at what can be done to address some of the security problems discussed above.

3. **WHAT IS ELECTRONIC COMMERCE SECURITY**

Much research has been done in this field and various methods, models and approaches have been recommended. The general consensus is that EC

security incorporates more than the traditional five security services of identification and authentication, authorisation, integrity, confidentiality and non-repudiation [GREE00]. EC security must address both technical and business risks if it is to be accepted. Furthermore, it must be integrated into the EC strategy, as it is an enabler for EC and not just an add-on. When comparing the security requirements for EC to those of the physical world, it becomes clear that additional requirements must be satisfied [LABU00].

In the physical world, a consumer would walk into a business and immediately make a decision on the level of trust to be placed in the organisation's transactional abilities. If it is a well-known business that has been around for some time, a trust relationship would have been built up and the consumer would not hesitate to perform transactions. The trust is further increased by the business's physical presence. The consumer has little fear that the business would disappear overnight without a trace. Talking to people face-to-face also increases the level of trust. Most consumers would also have trust in the transactional process of a physical business because, as a legal requirement, they must be audited regularly. Although irregularities might still slip through, most people feel secure in concluding transactions with physical businesses. The use of credit cards as a method of payment at restaurants, clothing shops and super-markets is common for most people.

In the realms of e-commerce, all of the above is challenged. Many new EC initiatives spring up overnight and a number of these close down just as quickly.

The lack of trust in a Web enterprise is, therefore, not unfounded, as stories of stolen credit card numbers, unfulfilled procurement and unsatisfactory products and services abound. There is no physical presence, no real people, and most importantly, no way of telling what the transactional capabilities are of the Web enterprise. This not only holds true for business-to-consumer (B2C) EC, but in some cases, also for business-to-business (B2B), business-to-government (B2G) and government-to-government (G2G) [TURB00].

Organisations wishing to engage in EC must, therefore, focus on establishing trust. One mechanism for doing this is information security. Different security mechanisms and tools can be used to provide trust in different aspects of EC, but unless a holistic approach is taken, the levels of trust will not be sufficient for clients to engage in any form of transaction [TRIA00].

Another approach is to look at Web assurance. Web assurance generally means looking at security, privacy, and consumer protection [TURB00]. Security refers to the required technology to protect transactions; privacy refers to the way in which personal information is stored and used; and consumer protection is assuring the client that the transactional processes followed are correct and that the consumer has certain recourse in the event of an unsatisfactory transaction.

Figure 2 illustrates the components making up Web assurance.

Figure 2 -Web assurance components

Following is a more detailed discussion of the Web assurance components.

3.1 Security

Different mechanisms can be used to provide the five basic security services. An additional security service that becomes very important is availability. In the realms of EC, an organisation must be able to conduct transactions 24 hours a day, 7 days a week. Business continuity planning

(BCP) and disaster recovery planning (DRP) are usually used for this purpose. Each of the 6 security services can be provided with existing technology [LABU00].

What is more important is that the client can be given the assurance that the necessary security measures are in place and being used effectively. To accomplish this, both a technical and a process assessment must be done. The technical assessment is done using penetration testing, network health checking, ethical hacking and/or configuration management auditing. Part of this assessment includes verifying if the security in the EC systems complies with the organisation's security architecture [GREE00].

The process assessment is done by verifying that the organisation complies with some baseline standards, such as the BS7799, ISO 13335, ISF or Cobit, for example [ERNS01]. Part of this assessment includes verifying whether or not the security in the EC systems complies with the organisation's security policies and procedures.

3.2 Privacy

Privacy refers to the way information is stored and retrieved within the organisation as well as how information is used by the organisation [DEPA00].

Ensuring privacy on a technical level can be achieved by means of authorisation. Not everyone needs access to all information regarding a client or transaction and the principle of least privileges can be applied. Access control can be provided through access control lists, storing the information in encrypted form and keeping logs of who accesses which information.

Also of importance is the ethical use of private information. This refers to what the organisation does with the information it has about its clients and transactions. In most cases, people would not want their private information to be given or sold to others outside the context of the original transaction. Despite legislation in many countries, spamming is still a large problem, especially for many of the free email service providers such as Hotmail and Freemail. The policy statement of the organisation determines the ethical use of private information [TURB00].

3.3 Consumer protection

Consumer protection is a concept that exists within the physical business domain as well. The main goal of consumer protection is to ensure that business is conducted in a manner that is fair to all parties involved. It is based on trust and in EC this becomes even more difficult due to its global nature. In most cases, trust can only be established through the combined use of both technical and non-technical means [TURB00].

A basic level of trust can be established by using security mechanisms such as SSL. The consumer has the assurance that all information being communicated is done so in a confidential manner, but it still provides no assurance of what the organisation is going to do with it.

An even higher level of trust can be achieved by means of non-repudiation. Non-repudiation consists of two parts, namely non-repudiation of the customer and non-repudiation of the merchant. By using digital signatures and asymmetric encryption, proof of a transaction exists that prevents any party from denying any wrongdoing. Both parties must, therefore, take responsibility for their actions and can be held accountable for any breach of contractual obligations [GREE00].

The above only provides subsequent trust in the transaction mechanism. Initial trust must first be established before a transaction will actually take place. As discussed in the introduction, initial trust is more difficult in EC. It has become necessary to find a mechanism that will establish initial trust. One mechanism that can be used for this purpose is to have the organisation and its processes audited by a trusted third party. An EC organisation can, therefore, be certified as being legitimate and following sound business principles and processes. A stamp-of-approval is given to the organisation if it complies with all the audit requirements [ARTH01].

This is becoming a prerequisite for B2B EC, as many organisations are not prepared to take the risk of dealing with 'untrusted' organisations, processes and technologies. In principle, this is similar to an organisation refusing to deal with those who do not comply with certain quality standards such as ISO 9000.

4. CONCLUSION

Due to its particular nature, information security management for EC is becoming a specialist field. It requires a good understanding of three areas, namely security, technology and business. With EC, security cannot be treated as an afterthought or add-on as it forms part of the core of any EC initiative.

This article refers to EC security as Web assurance, based on the fact that it is more comprehensive in nature and that it is an enabler, not an inhibitor. The purpose of web assurance is to enable EC by providing clients, be they individuals, organisations or government departments, with the necessary peace of mind to make use of it. Web assurance consists, mainly, of three interwoven components namely security, privacy and consumer protection.

Security in EC should not be the limiting factor that it is currently perceived as, but should rather be viewed as an enabler.

5. REFERENCES

- [ACCE01] Accenture, <http://www.accenture.com/>, eCommerce Division, 2001
- [ARTH01] Arthur Andersen, Confidence, Taking the right steps, Assurance Services, <http://www.arthurandersen.com/website.nsf/content/MarketOfferingsAssurance?OpenDocument>, 2001
- [DEPA00] Department of Communications – Republic of South Africa, Green Paper on E-Commerce, Published by the Department of Communications – Republic of South Africa 2000
- [ERNS01] Ernst & Young, Meeting Changing Information Technology Needs, Information Systems Assurance and Advisory Services, http://www.ey.com/global/gcr.nsf/South_Africa/ZA_-_Welcome_-_ISAAS, 2001
- [GREE00] Greenstein M. & Feinman T.M., Electronic commerce — Security, Risk Management and Control, , McGraw-Hill Higher Education, ISBN 0-07-229289-X, 2000
- [LABU00] Labuschagne L., A framework for electronic commerce security, Information Security for Global Information Structures, p. 441 – 450, Kluwer Academic Press, ISBN 0-7923-7914-4, 2000
- [ROSS01] Rossudowska A., The EWEB Framework – A guideline to an enterprise-wide electronic business, Rand Afrikaans University, Masters thesis, Rand Afrikaans University Library, South Africa, 2001

- [TRIA00] Worthington-Smith, R., The E-commerce Handbook: Your guide to the Internet revolution and the future of business, Trialogue, ISBN 0-620-25915-9, 2000
- [TURB00] Turban E. et al, Electronic Commerce: A Managerial Perspective, Prentice Hall Inc., ISBN 0-13-975285-4, 2000