LEGAL AND SOCIAL ASPECTS OF E-COMMERCE

Dr. Daphyne M. Saunders Thomas, James Madison University, thomasds@jmu.edu
Dr. Karen A. Forcht, James Madison University, forchtka@jmu.edu

ABSTRACT

This paper presents concerns and considerations from a legal and social perspective relating to the growth of e-commerce. Issues discussed include security, control and monitoring of an e-commerce site.

Keywords: cookies, e-commerce security, digital signatures, on-line authentication, social engineering, regulatory restrictions, intellectual property, private key

INTRODUCTION

When a customer walks into a local grocery store, they are immediately recorded by one of the overhead cameras. The cameras follow the customer down the isles as they put items in the shopping cart. As the items are scanned into the machine, a database recalls the price and adds it to the total sale. The database is updated to reflect changes in inventory and watches for missing inventory. When the customer swipes their credit card, the machine verifies the validity of the card and only then is the customer allowed to leave with their items. This should sound familiar, but what is perhaps less familiar is that in online electronic commerce, many of the same things are going on behind the scenes.

When a customer enters an electronic commerce website, a cookie will be immediately placed on their computer, usually without their knowledge. Cookies among other things, allow a website to track movement through a site and can store information about a person for use the next time they visit the website. This is comparable to the security cameras present in the stores. Adding things to an online shopping cart is only possible if the site has that item in its online catalogue (which displays available items similarly to the shelves in a store. When the customer purchases something online, the site will verify the credit card much in the same way the grocery store would. And just as the store won't let you leave without paying, an e-commerce website won't send your shipment unless the credit card is verified. E-commerce is fundamentally very similar to regular commerce, while allowing for some totally new ways of thinking about business. Traditional costs of modifying, printing, and shipping catalogues, as well as maintaining a store and the stores' employees, are being traded for costs that streamline business processes, and utilize the information that is gathered more efficiently.

Building an E-commerce Website

According to <**www.howstuffworks.com**> (in a brief tutorial on where to start in creating an e-commerce site), you must have the following elements to conduct e-commerce:

- A product
- A place to sell the product-for e-commerce; a website displays the products in some way and acts as the place to sell the product

- A way to get people to come to your website
- A way to accept orders- normally an on-line form of some sort
- A way to accept money- normally a merchant account handling credit card payments. This piece requires a secure ordering page and a connection to a bank, or you may use more traditional billing techniques either on-line or through the mail.
- A fulfillment facility to ship products to customers (often out-source-able). In the case of software and information, fulfillment can occur over the Web through a file download mechanism.
- A way to accept returns
- A way to handle warrantee claims, if necessary.
- A way to provide customer service (often through e-mail, on-line forms, on-line knowledge bases, FAQs, etc. (2)

E-commerce Security in Business

Since the Internet exploded in the early nineties, many thousands of e-commerce businesses have come and gone. Also, during this time, there have been many highly publicized attacks on computer systems by hackers, virus writers, and other malicious computer users. “Any computer user should protect themselves from computer viruses. When you run an eBiz, the stakes are much higher. Security should be one of your highest priorities.” (10)

It would seem that ten years after the Internet explosion that all companies involved in e-commerce would have installed high level security systems to protect themselves and their customers from such attacks. The truth, however, is that many companies are moving to a security plan as an afterthought instead of a priority. “ You can think of a company’s attitude toward an issue like security as a procession through four stages. First is ignoring it; second is talking about it and hoping employees do the right thing; third is putting procedures in place to deal with it, and fourth is really bearing down to solve the problem” (1). As the big companies are subject to larger and larger attacks, it is hoped that they realize the scale to which they need to implement an e-commerce security plan. Perhaps the smaller companies will follow suit, thereby making the Internet a safer place.

Even the giants of the computer and e-commerce industry are leaving themselves open to attack because of large security holes. Although depended upon by millions of users, Microsoft is guilty of leaving security holes in both its software and its member sites such as its email service, hotmail. “Security experts have long criticized Microsoft for the inherent security weaknesses in some of its products.” (6)

E-commerce Security Measures and Applications

An adequate security system for e-commerce transactions is an absolute necessity in today’s age of global marketplaces and terrorism. Without a secure system in place, a company is at risk to lose customers and revenue and without a secure system in place, a company exposes itself legal liability issues. Because of these risks, the very best security technology and their providers are essential for a successful e-commerce business. To ensure a reliable e-commerce system, the security of the LAN, firewall, Internet and many other components of a networked system must be validated and assured.

A leading security product is on the market today that is a very simple, but efficient and comprehensive method to assist in the security of network components. The product is called the e-Security Toolkit. This product is comprised of a collection of electronic items and documents to assist in a company's security functions. The collection includes "a LAN/Network security questionnaire, a complete checklist for e-security, which encompasses everything from firewalls to data access, and security questionnaires covering virus management, network routers, contingency, and system access."(9) The e-Security Toolkit offers not only a foundation for the assessment of a company's e-commerce capabilities and limitations, but is also designed for a company to find its own specific security risk exposures. It allows a company to efficiently review and audit its e-commerce network and aid in identifying the needs or shortcomings of the current system.

Another security product is an innovative, new technology being developed by Microsoft, VeriSign, and WebMethods to make it easier to use digital signatures and other online security devices for e-commerce transactions. The technology is called the XML (Extensible Markup Language) key management specification (XKMS). These formidable software giants are hoping to make XKMS the industry standard. The technology's XML-based framework has a superior advantage because it allows the capabilities of XKMS to link a company's wide rage of network applications together. "XML is a Web standard that has quickly become the language for e-business, allowing businesses to exchange data."(4)

The current software security measures, such as digital signatures, online authentication, and data encryption, are employed by e-commerce businesses to secure transactions completed in their online sites. The growing popularity of these e-commerce businesses and the emerging on-line marketplace is definitely raising the importance for an official authorization to be accessible for companies and consumers transacting business on-line. A digital signature is an ideal solution for the growing need of a personal validation and authentication of a transaction and "with the XKMS specification, software developers will be able to combine some of these newer technologies, like digital signatures, into their Web-based applications."(4) XKMS is expected to become a new standard for the XML based e-commerce activity by building trust through stronger verification methods and helping to fulfill XML's promise of an expanded and growing e-commerce world.

One of the most important components of e-commerce applications is the security of payment for electronic transactions. Reliable e-commerce payment methods are an essential security need-area to promote e-commerce consumers to use and endorse the on-line marketplace. The CommerceNet community maintains that a viable Internet payment system is within the grasp of the e-commerce world. "CommerceNet is a global, not-for-profit organization of leading business, government, technology, and academic minds working together for the advancement of eCommerce worldwide."(11) CommerceNet asserts that the technology for a payment system is already available, however standards of reliance and assurance for the operation of the system must be created. CommerceNet believes that the possibility of integrated payments into e-commerce transaction flows is a realistic hope.(11)

Social Aspects of E-commerce Security

Information security measures are designed to prevent unauthorized individuals or systems from affecting viewing, accessing or preventing access to organizational systems or data. Proper technical solutions, such as the e-Security Toolkit, can hinder technical threats from an adversary. Unfortunately, these threats are not solely limited to technical infiltration but rather affect a number of social aspects including: legal issues, retaining expertise, removable data, and social engineering.

Legal Issues

“Business transactions over the information superhighway, the domain of EC, have no precedent defining potential legal obligations, risks, and liabilities.”(7) Time, distance and regional regulations associated with traditional forms of commerce often do not apply to electronic commerce. Traditional commercial law must now be extended to consider the unique circumstances of conducting business via electronic commerce. Organizations planning to engage in electronic commerce should carefully consider the following key legal issues:

- *Regulatory restrictions* are rules and regulations that describe conduct for domestic and international business transactions. However, since electronic commerce resides in “ a society without borders”, organizations planning to engage in international electronic commerce must maintain existing precedence for international business conduct.(8)
- *Reliability of commercial records* is concerned with appropriate standards for record maintenance. As a result, organizations with customers in multiple jurisdictions will need to adhere to multiple regulatory requirements.
- *Data transmission* issues should be negotiated between all parties involved. Due to the decentralized nature of networks and Internet, transactions may travel among multiple carriers. Careful review of chosen carriers should be conducted to avoid using undesirable jurisdictions.
- *Intellectual property protection* pertains to organizations maintaining rights of ownership to systems and services offered electronically. Electronic services are often replicated so organizations should be prepared to enforce their intellectual property rights.(5)
- *Segregation of privileged information* protects the identities and confidentiality of information associated with electronic commerce business transactions. Organizations are held accountable to contain such information or risk liability.

Retaining Expertise

Electronic commerce information security is a “complex process requiring expertise and knowledge to succeed in guarding organizational assets while not compromising their net value.(7) Electronic commerce security implementations are often maintained through technological measures. This knowledge can only be maintained within the minds of those individuals involved. Effective management of human capital for the purpose of retaining expertise is crucial in any successful information security management. Three guidelines for achieving this include:

- Choose partners with demonstrated abilities

- Build strategic relationships with partners who have access to sensitive security configurations
- Re-evaluate staff selection compensation based on currently available skills in the marketplace(7)

Removable Data

Data access is no longer viewed strictly from a central computing facility. Laptops, remote mail, data warehouses and electronic commerce are a few examples of applications that have created a world of removable data. Although a number of benefits coincide with removable data, problems develop when inappropriate access is gained. Data must be managed in a manner that addresses all potential threats. Virus protection, personal encryption and backup can be effective mechanisms against threats. However, the use of a private key escrowed PKI is the only effective manner in which removable data can be controlled.(14) All users or systems that manage removable data should own a public and private key. The PKI is effective because it maintains copies of these keys to ensure that the organization is capable of retrieving the contents of the removable repository.

Social Engineering

In computer security, social engineering is a term that describes "a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures."(3) Social engineering tactics do not follow any one method. Appeal to vanity, appeal to authority, and old-fashioned eavesdropping are the more common used techniques of social engineering. Social engineering can be effectively averted with the following controls:

- *Security awareness programs* are an effective first level protection. Attention must be drawn to security-related issues and the implications they may have on the organization. These issues should be outlined in a security policy.
- *Security escalation systems* must be implemented to prevent repeating attacks.
- *Social engineering penetration tests* are effective in examining security policy to reveal possible weaknesses within the organization.(3)

CONCLUSION

Although tight information security is slow to be viewed as a necessity for all e-commerce businesses, the concept is well on its way. There are laws in the works that may require websites to uphold certain security standards similar to laws of the FCC and the Food and Drug Administration. Having these laws will not prevent hackers and malicious users from existing, but the hope is that with more focus on the Internet, business online will be safer in years to come.

REFERENCES

1. Barr, Adam. "Microsoft's New Security Focus." OsOpinion.com. http://www.osopinion.com/perl/story/15879.html
2. Brain, Marshal. "How E-commerce Works." HowStuffWorks.com. http://www.howstuffworks.com/ecommerce.htm.
3. Chen, Anne. "PKI Starts To Deliver." *Eweek.* April 2, 2001. http://www.eweek.com/article/0,3658,s=703&a=9303,00.asp.
4. Farmer, Melaine Austria. 2000. Microsoft, VeriSign team on e-commerce security. *CNET News.com.* http://news.com.com/2100-1017-249145.html?legacy=cnet.
5. Fine, Scott. "Legal Advisor-Contracts 101." *Computer User.* January 2001. http://www.computeruser.com/articles/2001,5,37,1,0101,01.html
6. Grant, Elaine. "Microsoft Gets Serious About Security." http://www.osopinion.com/perl/story/15845.html.
7. Keen, Peter, and Craigg Balance. Electronic Commerce Relationships. New Jersey: Prentice Hall PTR, 2000.
8. May, Paul The Business of E-Commerce. Boston: Cambridge University Press, 2000.
9. Unknown 2001. Network and e-Commerce Security: The e-Security Toolkit. *E-Security and E-Commerce Security Partners.* http:// www.e-security-e-commerce-security.com.
10. Unknown 2002. Security. Ebiz101.com. http://www.ebiz101.com/security.htm
11. Unknown. 2002. Security and Internet Payment. C*ommerceNet.* http://www.commerce.net/initiatives/sipayment/.
12. Unknown. "Social Engineering." Visited on April 26, 2002. http://www.askjeeves.com/main/metaAnswer.social+engineering&dt.