Global Information Assurance Certification Paper

Customer Information Privacy Within Electronic Commerce

Don Burlack
October 18, 2000

The Significance of Privacy Within E'Commerce

Electronic commerce growth is exploding around the world. Many believe that the big bang has yet to come. Within this ever-changing environment, merchants, consumers, and local, national & international governing bodies have accepted a fundamental. All parties concur that information privacy is the cornerstone upon which lies success or failure of an e'commerce implementation.
Repeated polls have shown that persons not embracing e'commerce have concerns for the confidentiality of their personal information. Consumers are primarily concerned about four privacy issues[1]:

1) When one's information will be used, by whom, and for what purpose
2) Choice about whether or not to volunteer one's personal information
3) Ability to access one's information to perform corrections and /or updates
4) Protection of their information from third parties who may steal it for unauthorized purposes.

A report released by the Pew Internet & American Life Project [2] studied the public's views on online privacy. The report found that the public shares two common views:

1) Internet users want a guarantee of online privacy
2) Many consumers are not versed on how privacy invasions occur and what technological solutions are available to prevent them.

Industries and governments have unanimously agreed that information security policies must be applied within cyber economies. These policies have identified the need for cyber laws within various layers of government and jurisdictions. To name but a few:

- In 1995 Europe adopted The European Community Data Directive[3]. Over 30 articles lay out the guidelines for member states to follow in protecting privacy of data. Article 1, "Object of the Directive" states:

  "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

- The US has Federal Statutes and cyber laws in every state. Interestingly, the Federal Trade Commission and Clinton Administration have supported self regulation in the Internet industry – but their patience has been tested by some companies' slowness to meet customer privacy needs. As a result, the US federal government is considering online privacy legislation[4].
- Canada has the Canadian Criminal Code plus recently introduced Bill C6 (http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_3/C-6_cover-E.html). This new bill makes it illegal for anyone to digitally

collect personal information without the person's consent[5].

These and a long list of other countries with corresponding cyber laws and guidelines strongly emphasize the importance of online information privacy controls.

Policy Requirements

Any organization or person(s) building or maintaining an online transaction service will need to ensure that privacy is treated as a high priority. A policy is required – a policy that reflects the organization's business needs. In e'commerce, these business needs would include support for privacy of customer information.
Whether we are assessing the effectiveness of existing policy, or if we are in the process of policy creation, some basic questions[6] should be answered:

- Do/will the policies identify the organization's internal privacy practices and expectations for management of customer/user/client information?
- Is there a process in place to ensure that these policies are communicated to all employees? Plainly said, the best policy in the world is useless if no one knows about it.
- Are customer information privacy expectations communicated to the customer through an online privacy policy? Because of it's significance, some detail will be presented on this item.

The Online Privacy Policy: This is a document that **must** be clear and concise. It should be assumed that the reader might not be technically learned. The following components are essential in an online privacy policy[6]:

- Openness – practices and policies concerning personal information should be openly discussed.
- Purpose - the purpose of personal information collection should be openly and clearly communicated
- Collection limitation – a declaration that the method of information collection will be lawful and fair. Only information for a stated purpose will be collected.
- Use limitation – a declaration that personal information will not be disclosed to other parties without consent of the person or law enforcement agencies.
- Individual participation – individuals will be enabled to review and correct their personal information.
- Security safeguards – individuals should be informed of security measures that have been implemented to protect their personal information

A wide range of quality is found within existing online privacy policies. A sample of a good policy can be found at the Better Business Bureau website[8] (http://www.bbb.org/about/privacy.asp). Bad examples, unfortunately, are numerous and can be found with little effort. A study conducted by the Federal Trade Commission in May 2000 found that 42% of the 91 most popular Web sites, and only 20% of 335 Web sites in its random sample, offer consumers the types of privacy protection the agency

deems essential.

Moving Beyond Words

An impressive policy statement will accomplish nothing without the support and dedication of senior management. The organization must "put it's money where it's mouth is" through implementation and maintenance of controls that fulfill the policy statement. While it is far beyond the scope of this document to detail all controls necessary to secure an e'commerce environment, some key points[7] for securing a website are listed:

- Security should never be perceived as an add-on after the site goes into production. It should be included as one of the necessities during the design stage.
- Employ firewalls to secure servers. Utilize a DMZ to isolate internal network resources from the Internet (or other external systems/networks).
- Ensure that production and test environments are kept separate.
- Never forget that the test system(s) should not be less secure than the production system(s). Many breaches on production systems have been the result of lax security on test systems that contain identical access control lists and configuration details.
- Ensure that logging is enabled on all pertinent activities and services (logins, HTTP, FTP, etc.)
- Minimize the amount of services on the hosts. If possible, utilize separate machines for web, news, email, FTP and others. Avoid placing applications and databases on the same machine. Each host should be configured to run only the bare essentials (i.e.: don't run services like telnet, sendmail and ping if there is no significant need for them).
- Implement robust encryption on files/databases containing sensitive and/or valuable information.
- Regularly conduct vulnerability scans on servers and network elements (or as new vulnerabilities become known).
- Use Secured Socket Layer (SSL) to collect sensitive customer information.
- Consider implementing the Platform for Privacy Preferences (P3P) specification to ensure that users are informed about privacy policies before they release personal information[9]. For more information on P3P see the World Wide Web Consortium site at http://www.w3.org/TR/2000/WD-P3P-20000510/
- Carefully screen CGI scripts for errors and vulnerabilities.
- Disable directory listings to avoid disclosure of files and directory structure.
- Employ an intrusion detection mechanism (automated or manual depending on the complexity of the environment).
- Ensure that all employees (especially customer service personnel) are aware of and adhere to the privacy and information security policies.
- Ensure that systems development, operations and administration personnel are

adequately trained and knowledgeable in security.

Going Forward

Privacy of customer information in a global network is a complex issue with many variables. Laws and standards (technical and political) will require significant development before customer confusion and doubt can be replaced by a level of trust that can sustain large-scale e'commerce. Will it happen? Certainly… the big bang IS coming.

Internet References

1. Lawson, "Sen." Katherine T. "United States Internet Privacy Laws and the European Community Data Directive". 1999. URL: http://ils.unc.edu/~lawsk/policypaper.html (12 Sept. 2000)

2. Pew Research Center. "Pew Internet & American Life Project". 21 August 2000. URL: http://www.researchengine.org/reports/reports.asp?Report=19&Section=ReportLevel1&Field=Level1ID&ID=43 (12 Sept. 2000).

3. The European Parliament and the Council of the European Union. The Council Brussels. 2 February 1995. URL: http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html (12 Sept. 2000).

4. Thibodeau, Patrick. "Privacy concerns rankle industry". 29 May 2000. URL: http://www2.computerworld.com/home/print.nsf/all/000529E3EE (9 Oct. 2000).

5. The House of Commons Of Canada. "Bill C6". 26 October 1999. URL: http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_3/C-6_cover-E.html (12 Sept. 2000).

6. Merkow, Mark. "Information Privacy: The Other Side Of The E-commerce Coin". 24 September 1999. URL: http://ecommerce.internet.com/outlook/article/0,1467,7761_207511_2,00.html (20 Aug. 2000).

7. Raigaga, Haridas. "Security And Governance For eCommerce". 15 February 2000. URL: http://www.dqindia.com/feb1500/eCommerce.html (20 Aug. 2000).

8. "The Better Business Bureau Online Privacy Policy". Better Business Bureau. 22 April 1998. URL: http://www.bbb.org/about/privacy.asp (12 Sept. 2000).

9. Rosencrance, Linda. "Microsoft, others unveil tools to protect online privacy". 21 June 2000. URL: http://www2.computerworld.com/home/print.nsf/(frames)/000621EADE (6 Oct. 2000).