

Trends in e-Commerce Security Practices

a report by

**Brent Lahaise, Lise Jansen, Andrew Kissman, Kumar Mahadevan
Mike Saumure, E Wayne Boone and Joanne Reid**

Assisted by **Brian Sanderson and Mandana Ghadaksaz**

Ottawa – Canada Chapter, Information Systems Security Association (ISSA)

“Shopping online is safe, safer than shopping offline if you buy from a responsible and reputable business over a secure Web server.” Royal Canadian Mounted Police

In spite of the Royal Canadian Mounted Police’s (RCMP’s) assurance of safety in online shopping, business-to-consumer (B2C) transactions and the use of credit cards over the Internet is not what e-commerce pundits had predicted a few years ago. Compared with bricks-and-mortar retail sales, credit card transactions at e-tailers are quite insignificant.

The Internet was in use for educational and military purposes long before its widespread use for commercial and personal purposes. The Internet was built for robustness rather than security. The Transmission Control Protocol/Internet Protocol (TCP/IP) (used as the Internet communication standard) offers open connections that are the strength of the Internet. It is also the weakness of the Internet from the point of view of commerce. This openness allows imaginative attackers to discover new exploits in commercial products and websites with ease.

Security deficiencies are often discovered by the underground hacker community well before the vendors uncover them. The most famous example is the widespread use of an illegal hacker tool called Back Orifice in the underground hacker community. This tool was not known to the security professionals, network administrators and other legitimate information technology (IT) professionals for more than two years after its initial use by the hacker community.

Hacker attacks on major e-tailers in 2000, along with more recent flaws discovered in Berkeley Internet Name Domain (BIND), which is a popular version of Domain Name Server (DNS), have increased public concern about Internet security. The media has compounded the fear of lax security with headlines that approach the scare tactics of “Recent Vulnerabilities Spell the Demise of the Internet”.

Security, however, is not just about technology. The other major requirement for establishing trust

between partners in e-commerce transactions is security practices. People are the weak link in an organisation’s security architecture. The lack of security policies and procedures to deal with new vulnerabilities weakens the ability of online vendors to keep ahead of potential attacks. Without demonstrably solid policies and practices, e-tailers will not be able to gain the trust of customers or business partners.

A Brief History of Security Decision-making Paradigms

In the beginning, there was chaos. Security was an afterthought and tended to be a simplistic ad hoc reaction to breaches. As such, the security measures adopted did not typically address the over-arching organisational weaknesses.

Advances in IT, and the corresponding increases in complexities and vulnerabilities, led governments to panic. They sought solace in rules and regulations and, thus, rule-based security was born. In the Canadian government, this led to the creation of several policy bodies such as the Government Security Policy (GSP), as well as a host of baseline technology standards. All departments, agencies and crown corporations, large and small, had to obey these rules.

This, however, led to a backlash. Many departments did not have information that was truly critical to protect. For instance, Parks Canada does not have the same security requirements as the Department of National Defence. The question arose as to why they should have to follow the same security rules. In the private sector, this trend was exaggerated among businesses that were not held to these types of rules. Unless there was a solid business case for it, money would not be spent on security.

Risk-based security decision-making was the reaction to this situation. Business cases for security would be built on analyses of threats, vulnerabilities, assets and overall risks. The mantra became “only as much security as necessary and no more”, which was good enough for a short while.

However, as the information systems of organisations begin to interact more and become more interdependent, businesses realise that their business partners' security practices (or lack thereof) can hurt them. They need assurance that these interactions will not unduly expose their information assets. As a result, there is an increasing demand for third-party certification of information systems and audits of security policies and practices to provide this assurance.

The Trend Towards Standardised Codes of Practice

There are several business needs driving the trend towards following standardised codes of information security practices (standards) in e-commerce.

The main need is that for assurance of trustworthiness between business partners that will gain the trust of customers. If 'Business A' knows that 'Business B' follows a trusted standard, then A can extend that trust to B. This is especially important for transactions across national borders, and between organisations that know little about each other. Examples of this are Visa, with its requirement that participating merchants follow its Account Information Security Standard,¹ and the EU, which requires that not only must European organisations comply with International Organization for Standardization (ISO)-17799, but that any business partners with which they share citizens' personal information must also comply with this standard. The banking industry, being fairly conservative, will likely follow suit with their business customers soon.

A second growing need is for standards in Certificate Policies and Certification Practice Statements (CP/CPS) to allow for cross-certification of certificate authorities (CAs) and interoperability among public key infrastructures (PKIs). Divergence between organisations' CP/CPSs and other security practices will likely end up being more of a barrier than technical issues to interoperability of PKIs.

It becomes a management decision based on trust. If Business A does not follow as stringent a set of policies and practices as Business B, then B cannot trust A, and will not cross-certify with A. The greater the push to make all PKIs interoperable and to have all major CAs cross-certified, the greater the push towards adopting a more stringent standard. Different levels of CP/CPS can be established for certificates that provide different levels of trust, but these too will require internationally agreed upon standards.

Another growing driver is the insurance industry. As more insurance companies start offering 'anti-hacking' policies, they will look more closely at their customers' security policies and practices, as well as their technical safeguards and their industry's inherent risks, to determine rates. Insurance companies will then likely specify standards with which their customers must comply.

Last and probably least of these drivers is potential savings in time and effort on the part of an organisation's information security managers. They will not have to re-invent the wheel when developing a security plan, and their decision-making effort will be reduced as they will have defined rules to follow.

Existing Standards

The leading standard at this time is the recently released ISO-17799 (formerly known as BS-7799). It has gained a significant amount of support in the information security industry globally, and has been adopted as a national standard in several countries, with many more planning to follow suit. European companies may soon be in the legal position that they must ensure that any company with which they share customers' personal information also complies with ISO-17799. Since e-commerce transactions involve customers' personal financial data, global transactions may require organisations to demonstrate compliance with ISO-17799, whether their government demands it or not.

There are already some well-established tools available to measure compliance with ISO-17799, such as COBRA. The Information Security Institute of South Africa (ISIZA) has proposed an incremental approach to ISO-17799 certification, as they believe that "a staged approach is required, which gives organisations an entry-level commitment to information security practices, which they can then develop further as (they) grow"²

The ISIZA approach has five levels, each representing a subset of the full set of ISO-17799 standard practices. Level 1 consists of a few basic security controls, while Level 5 will be a full implementation of ISO-17799. ISIZA will create a board to define the controls required for each level. This approach will permit organisations to obtain certification much faster by being audited for a subset of the ISO-17799.

Another standard gaining popularity, at least among IT auditors, is Control Objectives for Information

1. Visa, "Account Information Security Standards".

2. R H (Basie) von Solms, "Institutionalising Information Security", Business Briefing: Global InfoSecurity, *World Markets Series*, January 2001.

and Related Technology (COBIT), whose third edition was published in 2000.³ The major proponent of this standard is Information Systems Audit and Control Association (ISACA), and its membership (as well as the contributors to COBIT) is also international in scale. Any organisation facing an external auditor will want to become familiar with this standard. One of COBIT's advantages is that it has a built-in capability-maturity model (CMM), which explains in detail what is required to achieve each level as part of the explanation of each objective.

Visa now requires that its members/participating merchants meet its Account Information Security Standards Manual. Visa also supplies a guide to best practices, which are based on the American National Standards Institute (ANSI) Information Security for Financial Organizations Guidelines, X9/TG-5 (1992) and the ISO/TR 13569 Banking and Related Financial Services Information Security Guidelines. In 2001, Visa is piloting this requirement in the US. It is expected that all the major credit card companies will develop similar requirements worldwide by 2003.

When and Where the Pendulum will Stop

The trend towards standardisation of security practices will reach its peak by around 2003. The small backlash will be mostly absorbed, until the pendulum stops (more or less) by 2005.

The end result will likely see a new ISO standard, which will be even more comprehensive than the current one. This new version will be the result of collaboration between the ISO committee, ISACA and several other major players to incorporate the best/most features of all the previous individual standards, as well as some well-defined guidelines for measuring compliance.

This more comprehensive standard will be flexible. It will have more than a dozen subsets, including five or six generic subsets, plus several specialised ones for industries with unique needs. This will balance the desire for industry-specific practices on the one hand, and a universal standard on the other. That, and the incorporated use of CMMs, will tell them what level of trust to extend to that organisation.

Risk management will be a required element of every subset, and will remain a key tool that will be used daily to deal with new threats as they arise.

Maximising Identification and Authentication

The Federal Trade Commission (FTC) website, Consumer Sentinel,⁴ lists credit card fraud as one of the most prevalent problems. A common example includes sites that provide adult images online for free. Fraudulent promoters request a credit card number as proof of age and subsequently apply charges to the card.

Security Management Online cites the top four consumer complaints up to April 2001 as involving "Internet services and computer complaints; prizes, sweepstakes and lotteries; Internet auctions; and advance-fee loan and credit protection/repair."

A report concerning unlawful conduct on the Internet advocates a three-pronged approach to mitigate unlawful conduct on the Internet – regulation, law enforcement and user education.⁵ While the first two are long-term solutions, dealing with the criminal element, the latter is much more immediate.

What causes users to fear using their credit cards on the Internet is the lack of understanding the threats, little or no knowledge of the vulnerabilities of their home personal computers (PCs) and lack of education on how to adequately mitigate those risks in an increasingly technical world. The purchaser of a family PC with colour-coded connectors and all software pre-loaded really cannot be expected to install and configure a firewall, upgrade a browser to 128-bit encryption and conduct e-commerce in a secure fashion.

A brief summary of the risk-mitigating tips on the RCMP website for online purchasers includes dealing with known companies, reading terms and conditions, looking for a privacy policy, ensuring the complaint or cancellation process is fair, ensuring the transaction is secure, remembering that e-mail messages are not private, checking for endorsement, avoiding spam and educating children.⁶ Industry Canada's site and the American FTC site offer similar advice.^{7,8}

3. ISACA/IT Governance Institute (2000), Control Objectives for Information and Related Technology, 3rd ed., July 2000, <http://www.isaca.org>

4. <http://www.ftc.gov/sentinel>

5. "The Electronic Frontier: The Challenge of Unlawful Conduct Involving The Use of The Internet," a Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000. <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>

6. "Shopping Online", Royal Canadian Mounted Police, <http://www.rcmp.gc.ca>

7. "Shopping on the Internet", Industry Canada, <http://www.ic.gc.ca/>

8. "Top Ten Dot Cons", US Federal Trade Commission, <http://www.ftc.gov>

Security versus Privacy

The challenge that e-tailers face is in finding a way of proving that the purchaser is really the credit card owner, without asking an intrusive number and intensity of questions that people will not be willing to answer.

Most e-commerce security efforts to date have focused on validating the transaction between points A and B, as well as validating against repudiation, authenticity and tampering (the PKI model). Once this is done, there is a sense that the transaction itself is now fully secure.

The fact of the matter is that two areas still leave a lot to be desired in terms of security. First, transaction information and logs have been stolen from websites and misused. This is not caused by the electronic transaction itself but rather the unsecured storing of related information. Secondly, although the transaction may be valid, the identity of the person initiating the transaction must be verified to reach a fully secure state. Passwords are often compromised because people write them down or choose passwords that are too easy to guess.

Biometrics is surfacing as the means to authenticate the originator of such a transaction. Inherently, biometrics cannot be compromised (stolen or guessed) as with passwords. This makes them a potential solution to the identity issue. However, a number of hurdles are being slowly overcome towards full acceptance of biometrics in the community. They include realistic expectations from implementers, proper deployment, sampling approach and user interface, and adequate training for eventual users.

Conclusion

There are several standards, old and new, as discussed above that attempt to reduce fear in the realm of Internet security. Unless B2C e-tailers and banks who play in the B2C arena understand and implement frameworks to manage residual security risk, understand that the security in B2C transactions is derived from end-to-end security and implement policies and procedures around the people who use such technologies, the level of trust in B2C vendors will remain low.

As an example, and pursuant to the discussion of the Visa standard, if B2C e-tailers and banks do not educate their customers on the need to secure the devices they use for conducting B2C transactions with personal firewalls and other necessary mechanisms, the Visa standard will only provide a partial security solution.

On the other hand, if the B2C e-tailers and banks do not have well-written and communicated policies and procedures on their side, then the trust in the entire B2C transactional system is undermined.

B2C is in jeopardy unless security practitioners can effectively manage the inherent risks of the way the Internet is designed and security vulnerabilities in popular products. Strict policies and procedures are required to strengthen the technology used in B2C transactional systems. Without such policies, the general public will not gain enough trust in the system to conduct critical transactions over the Internet. ■

References

British Standards Institute (1999), BS 7799: Information Security Management, Part 1: Code of Practice for Information Security Management; and Part 2: Specification for Information Security Management Systems.

Warwick Ford and Michael Baum (2001), *Secure Electronic Commerce, 2nd ed.*, Prentice Hall.

John P Hopkinson (1999), "The Relationship Between the SSE-CMM and IT Security Guidance Documentation", draft paper, EWA-Canada.

Laura Pearlman, "Client Side Security", World Wide Web Security, <http://www.w3.org>

Simon Rogerson and Sara Wilford, "Identity and Authentication", IMIS Journal, June 2000, as posted on Centre for Computing and Social Responsibility (CCSR), <http://www.csr.cse.dmu.ac.uk/resources/general/ethicol/Ecv10no3.html>

Bruce Schneier, "The Insurance Takeover", Information Security Magazine, February 2001, http://www.infosecmag.com/articles/february01/columns_sos.shtml

US Federal Trade Commission, "FTC Consumer Alert", <http://www.ftc.gov>

US Federal Trade Commission, "Guide to Online Payments", March 1999, <http://www.ftc.gov>

Further BS 7799/ISO17799 information came from:

Timothy Stacey, "Toward Standardization of Information Security: BS 7799", SANS Institute, 2000, <http://www.sans.org/infosecFAQ/policy/standardization.htm>

<http://www.securityauditor.net/iso17799/what.htm>

<http://www.pcorp.u-net.com/bsintro.htm>