E-Commerce Fraud

Before any discussion can take place about fraud specifically or cyber crime in general, it is useful to take an overview of the entire market that is currently being dealt with. Regardless of the soothsayers, prophetic utterances and futurists, there are some important urban legends to destroy.

The Internet is not "global" as in "it reaches everyone". It's global only so far as it can connect people internationally, but 48% of the people on the Internet come from North America, which represents only 5% of the total population "globally".

E-commerce is not defined. If you took the word "e-commerce" to mean "electronic commerce" in the same way we look at e-mail being "electronic mail," then using a fax machine to take an order would qualify as an "e-commerce" solution.

ONLINE SALES UP 43% IN 2001

Statistics Canada says Canadian businesses received $10.4 billion in revenue from on-line sales in 2001, 78% from sales to other businesses. On-line sales were up 43.4% from 2000 but were still only 0.5% of total business revenue for the year.

The terminology is convenient, a buzzword, a phenomenom, but hardly revolutionary. Futurists were wrong when they said that television was going to replace newspapers, or that facsimiles would replace sales people and the Internet will replace your neighbourhood store.

E-commerce has three basic models. The ease of complexity of the venue is dependent on the amount invested in the solution. Full-blown enterprise solutions can cost hundreds of thousands of dollars to build and advertising budgets for the site can be in the millions of dollars. Simple commerce websites can be developed with off-the-shelf software for a few hundred dollars and some time. All of these venues can easily fall within the three models.

The first model is to use the electronic version of an order form. This is a very low risk extension of the sales process allowing known and established customers the convenience of research products and ordering online at a time and often a place that is convenient. This convenience can translate into a wider customer base simply because the order desk operates 24/7. Dealing with established customers minimizes risk, since the "transaction" part of the sales process is handled by established protocols including pre-approved authorization, spending limits and regular credit checks. Good examples of this are restaurants, bakeries and other businesses where the hours of operation for the business do not match the hours of operation of the vendors.

The second model is to extend the sales process through electronic transactions. This is a high-risk model equivalent to serving a customer at a storefront where the customer is wearing a paper bag over their head and the transaction is subject to a high risk on the part of the merchant. Typically the transaction is done by credit card and a credit card carries only a $50 risk to the cardholder, no risk to the issuing bank, and liability for the

entire transaction on the merchant with the possibility of additional charges involved in the charge-back process should it be a stolen or unauthorized credit card.

Killer Apps

"Ask people whether they would rather give up e-mail or the phone, and the responses will typically be split.

However, when a similar choice is offered between the web and e-mail, there is no contest.

This is true for both individuals and large organizations. Intranets are all the rage, but it is e-mail that makes enterprises run."

http://www.angustel.ca/teleman/tm00e-07.html"

The third model currently being deployed is the use of the electronic medium as an adjunct to the sales process. Customer retention and customer service management is handled through an electronic interface. The assumption, of course, is that a substantial portion of your customer base is connected and willing to use this medium. Since the number of new users on the Internet is expanding exponentially the net result is that most of the customers while having access to new technologies are in fact new users and still on a learning curve. Anecdotal information rather than hard-core research is the *de rigueur* method of education and, not surprisingly, contributes to the confusion and misuse of the resources.

Regardless of the method used stating a 43% growth in online sales to $10.4 billion sounds impressive until you realize like “the Internet is global” the impact per business is very small. E-commerce still accounted for only .5 of a percent of sales volumes.

While there are some advantages of being an early adopter of technology, there is also a time to reflect on how much impact the adoption of electronic commerce is going to affect the bottom line.

It is important to remember this adage: “During a gold rush only a few prospectors strike gold. The people who go home with money in their pockets are those that sell pickaxes, shovels and gold pans.”

The decision for a company to go into e-commerce and the expectancy of what the venue will accomplish for the business is best decided around a table with people who have done their due diligence rather than rely on a sales rep’s PowerPoint presentation full of speculation and marketing hype.

The dot-com crash has reminded us of one truth: The only permanent thing is change.

The Internet is a great tool, but like most tools it can be abused. Most of the frauds that are committed are just jump-overs. They existed as frauds before, now they have a brand new suit.

These frauds are the same kind that moved from the phone to the fax machine and now show up in e-mail or on some of the web sites on the Internet.

Some of these include:

- Phony Advertising Space – solicitations for advertising or web space that doesn't exist or is so over subscribed that it might as well not exist.
- Bargain Corporate Travel Packages requiring a pre-pay or prepaid fee for services.
- Office Furniture and Office supplies that advertise deep discounts but are either inferior quality or they just don't exist. Office supplies also include computers and electronic equipment.
- Speciality Advertising Products like pens, key chains etc.
- Solicitations for Charities that have names that are close to recognized charities.
- Phony invoices or solicitations that are made up to look like invoices.
- Solicitations to remove your name from advertising and marketing lists (809/900 scam)
- Advance fee business loans, insurance, consulting services – in fact, advance fee anything.
- Identity Theft, hijacking, impersonation, and trading on a business' good reputation.
- Vandalism, Malicious Intent, Nuisance, Junk Mail and Junk Faxes as well as other thefts of resources.
- False Authority and misleading information (mud slinging and lies)

Convenience should not overshadow diligence

The problem with these frauds when they jump over into cyberspace is that it is much easier for the criminal to hide, and much more difficult to find them.

Since the only change with these frauds is the method of delivery, the standard rules of fraud prevention and awareness apply. Convenience should not overshadow diligence.

Tips:

- Never pay for advertisement in directories and journals that are not industry specific or known to you.
- Check vendors before purchasing products. The further they are away from you the harder it is to "fix" a problem. Be especially cautious if you have to cross borders. You might be left with no one who will be able to help.
- Order samples of advertising specialities to check quality before you buy.
- Deal with known charities or local ones that you can get all of the information on. If they are claiming Canadian charitable status verify their status at http://www.ccra-adrc.gc.ca/tax/charities/list/chtysr-e.html
- Flow invoices, bills and purchase orders and shipping receipts through a single department so that you are not paying for something you didn't order or didn't receive.

- Have your local Telco speak to the organization about things like toll fraud and other crimes committed using your phone service.
- Simply make it a rule that you do not respond to unsolicited faxes and e-mails. If they are sent locally phone and ask them to remove them. Do not respond to remove requests from e-mail. They are often used to "verify" that they have a valid e-mail.
- Funnel all inquiries about the company, the equipment in the company and all surveys and questionnaires to the most sceptical manager that you have.
- **NEVER ACCEPT SOLICITATIONS OR REQUESTS FROM NON-ISP BASED E-MAIL**. Services like hotmail.com, yahoo.com, mail.com etc are difficult or almost impossible to trace who the owner is. When in doubt replace the username with www and the @ with a dot in your browser and see if it takes you to an actual site, or an e-mail forwarding or free e-mail service. I have about 1000 of these services downloadable in an *.rtf document at www.heads-up.ca/nonispmail.rtf. Since virtually all fraud is committed using these kinds of service, refusing to do business with those using these mail services will eliminate virtually all of the fraud.
- Vendors who want to sell to you will have no problem in you doing your "Due Diligence," in fact they want you to be assured that they are legitimate and forthright in their dealings. Individuals who want to buy from you should also be free with their information.

There are frauds that are somewhat unique in cyberspace include:

It is ironic that @ has become a trendy mark of Internet awareness since it is a very old symbol, derived from the latin preposition "ad" (at).

Giorgio Stabile, a professor of history in Rome, has traced the symbol back to the Italian Renaissance in a Roman mercantile document signed by Francesco Lapi on 1536-05-04.

www.dictionary.com

Merchandise Fraud using Internet or Network related products and services. (Web Development and Hosting Services, Security and Security related products and services, Consulting, and Vaporware.

Since the Internet is unregulated and new, it is difficult to assess what "real value" is when you are buying these new products. These companies should have additional ways for you to contact them, verifiable "real" addresses, ways to verify their work, and references for you to contact.

It is the same for the credentials of those holding themselves out to be "experts". An Engineer is an individual with an Engineering Degree from a recognized University yet I have seen the term attached to Systems, Security, Networks, Software and Sales. Ask for credentials, references and full information. If they are nervous, agree to sign an NDA that will allow you to continue to investigate and at the same time keeping their information confidential.

Credit Card Fraud is increasing over the Internet. The incident of credit card fraud has been estimated to be between 6 and 10 times greater than credit card fraud in the retail environment.

The liability to the cardholder is limited to $50.00. The liability to the bank is nothing since they will simply charge back the merchant and will often include a charge-back fee. So the cardholder pays $50.00 to the bank, and the merchant pays the charge-back fee to the bank, and the bank withdraws the revenue from the merchant. The perp has the goods and the merchant is left "holding the bag".

Tips:

- Get full information, address, phone number etc.
- Use a disclaimer on your website stating you will not process orders from non-ISP mail services
- Phone verify the order.
- Use HTTP_USER_AGENT and the REMOTE_ADDR code in the form handler to record information about the computer and the IP address used for the order.
- Reconsider using "real time" transactions. The convenience might be outweighed by the risk associated with this type of transaction.
- Consider using a "fax-back" form to verify the order and obtain a signature for the order.
- Check the first six digits with your credit card processor to check the name and address of the issuing bank. (Orders in Russia using a US based bank credit card).

Apr 08 2002: Newsbytes reports that nearly 90 percent of US businesses and government agencies suffered hacker attacks within the past year.

Identity Fraud has a number of forms that are used against business. These include using names that are close to the corporate identity, hijacking the website to steal client information, using your web supplied corporate logo's and information to create phony company ID cards, business cards and stationary.

"Whois" searches will give you additional information, so will looking at usenet postings where people post using corporate e-mail addresses. Deja.com can give you information that employees might have given, and people can assume the identity of a corporate employee and spread lies, slander and rumours with impunity.

Dumpster Diving, Police Accident Reports, all can be used with or without Internet support or can be done by an associate. (All papers should be shredded).

Vendor Fraud is another area where fraud has benefited by the anonymity that the Internet affords. All merchandise frauds including phony invoice scams, office supplies and "deep discounts" and bait and switch scams can be carried out using Internet resources.

Since anonymity is the most important consideration for the fraudster, anything that is done to identify and authenticate the vendor and the willingness of the vendor to share information is generally your primary tool.

Prevention costs are substantially less than damage recovery. Recovery can also involve foreign jurisdictions in which case recovery is not likely. Creating a corporate culture that is "fraud aware" will go a long way to preventing Fraud. Since many of the social engineering hacks are directed at the front line people (receptionists or call centres) it is important for these people to realize that while the "customer comes first" they owe a duty to the company to also be diligent and aware of fraud crime, methodologies and techniques.

Protecting the Assets is an aspect of security that is generally overlooked. While " building security" is understood and the costs are "part of doing business" network security is often viewed as an expense with little or no understanding of the risk to the business.

The problem is not the recovery of hardware and software (which is achieved by insurance) but the data and Intellectual property that is created using the hardware and software, which can involve thousands of hours of work. All documents and work should be placed on a secured file server and backed up on a daily basis. Most important and overlooked in this process is the testing of the back-ups to insure that they are functional and complete. Testing during a recovery operation is not an option, it is too late.

Typical measures to protect the network include:

What it is…	What it is like…
Firewall	Locked Doors and Windows
IDS (Intrusion Detection Systems)	Motion Detectors
Monitoring	Video Surveillance
Username / Passwords	Keys for the Locked Doors
Acceptable Use Policies	Legal and Legitimate use of corporate resources and the consequences of abuse
Access Policies	Trust Levels and Checks and Balances insuring a division of duties enhancing control

Network Audit	Review of the topology, physical layout, and testing of the network by a peer review. (A network is an engineered product; an appropriate Engineer should audit it).

Internal Fraud and theft still is where the majority of the cyber fraud is going to take place. The most compromised information is the Intellectual Property of the company. This can include things like client lists, client information, billing habits, marketing campaigns, vendors and vendor pricing, designs, bids, quotes, and staff. There really isn't a department that does not have information that if released would not have a detrimental effect on the company.

Your employees have access to information that is valuable to someone else. A competitor, espionage, terrorists all can be well funded and willing and able to offer an incentive for your employee to "provide" this information. The network and your Internet connection can be used as a pipeline for that information and using commonly available compromises your entire network can be laid open to your competitor with a few simple downloads and keystrokes.

E-Commerce is new, the use of the Internet is new, in essence the global cyber community is still on one big learning curve. However like the grand technologies of previous times, it's impact will not overtake current technologies, but rather enhance what we, as humans, would normally be doing.

Success is a lousy teacher; it seduces people into thinking that they can't lose. And it's an unreliable guide to the future. What now seems the perfect business plan or latest technology may soon be as out of date as the eight-track tape paper, the vacuum tube television or the mainframe computer.
—Bill Gates