The Net Present Value of Information Security: A Paradigm Shift for INFOSEC and E-commerce.[1]

by M. E. Kabay, PhD, CISSP-ISSMP[2]

Version 17

1 Introduction

Electronic commerce has been growing rapidly since the inception of the World wide Web in the early 1990's. E-commerce is forcing a change in the traditional view of security, which has long been viewed as an annoying, intrusive and expensive set of mechanisms for risk reduction.

Today, we see an evolving recognition of the positive value of security; for e-commerce, security enables many aspects of business and it can improve organizational strength.

This white paper is written for managers and explains the critical role and positive benefits of information security for e-businesses.

2 What's happening in e-business?

2.1 Transformation of the business model

Over the last decade, we have seen an explosion in the types of businesses conducting transactions electronically. Where electronic commerce was once restricted what was called electronic data interchange (EDI) and limited to huge organizations such as automobile manufacturers and their suppliers, today even Mom and pop stores can sell goods and services to anyone on the Web--even to kids.

Peter G. W. Keen[3] has succinctly summarized the evolution of business in the age of the Internet[4]. He points out that the early phase of e-commerce focused on the user interface and provided shopping at one site at a time. Growing price competition then led to an emphasis on personalization — using cookies, for example, to give each visitor a suitable mixture of advertisements, product pointers, advice and hints. As personalization became more effective and far-reaching, many organizations moved towards becoming portals. "Build a relationship brand so customers park at your site to explore the Web, the way shoppers park at Wal-Mart and then shop the rest of the mall." At the present time, writes Keen, the complex and dynamic mixture of services offered by Web storefronts necessarily involves "on-the-fly communication among sites about inventories, status, prices, catalogs and specials." Keen concludes, "This business model turns the Web into a market of tightly linked supply chains."

Mark Doll, National Director of E-commerce at Ernst & Young < http://www.ey.com >, has defined a model for e-business called 3P: presence, penetration and profit[5]. Because the business-to-business (B2B) is already larger than the business-to-consumer (B2C) market (he quotes figures of $114 B vs. $36 B in 1999), Doll predicts that market penetration will increase massively in 2000 and

---

1 This is a modified version of what later became a paper published with Karen Worstell and Mike Gerdes of AtomicTangerine and published on the now-defunct *SecurityPortal* Web site. The original version was later published in *the Journal of E-Business & IT* 2(1):13-28 in 2003. Over the years I have made minor corrections and additions.

2 Program Director, MSIA & CTO, School of Graduate Studies; Associate Professor & Program Director, BSc in Computer Security & Information Assurance, Division of Business and Management; Norwich University, Northfield, VT 05663-1035 USA

3 Author of *Electronic Commerce Relationships: Trust by Design* (Prentice Hall, ISBN: 0-130-17037-2).

4 Keen, Peter G.W. (1999). E-commerce: Chapter 2. *Computerworld* (Sep 13, 1999):48

5 Anonymous (1999). Interview with Mark Doll. *Inter@ctive Week* (Oct 4, 1999) 6(i41):40

2001 for B2B. In this stage of development, Doll argues, "B2B players, like B2C players, must focus on getting the business model 80 percent right. Business customers may be more forgiving (it's someone else's money!) than consumers, but management execution is still critical, and industry expertise becomes a differentiator."

According to *Computer Weekly* columnist Danny Bradbury, "One of the biggest areas for IT spending in the next few years will be e-commerce. Now that network standards have emerged and the Internet has grown into a unifying medium, e-commerce has become a sales channel that businesses can't afford to ignore."[6]

In *InformationWeek* Editor Stephanie Stahl's opinion, "Electronic business is quickly becoming part of everyone's business model-and it's forcing dramatic change."[7]

According to Irving Wladawsky-Berger, General Manager for IBM's Internet Division, giving the keynote address at the December 1999 eBusiness Conference and Expo in New York City, the exponential growth of e-commerce and the Internet is as important as the life-changing technological revolutions caused by electricity and the automobile. He added that e-business is forcing companies into total integration: "The real magic of the Internet comes from putting things together. It's really important to connect the dots, to ensure that processes work together."[8]

Buell Duncan , General Manager of IBM Global Business Partners, says of his strategic focus, "We are obsessed with transforming IBM from traditional computing to e-business computing because the growth in e-business is on average four times faster. Compounded out over five years, that's pretty significant."[9]

The Goodyear Tire & Rubber Company has seen such massive acceptance of online ordering and e-mail communications by their dealers that as of now (mid 2000), the firm is eliminating all of its paper mailings to its dealers. Gary Hargreaves, Manager of E-commerce for the North American tire business unit, said, "It would be hard to fathom doing business any other way."[10] In the opinion of *InformationWeek* writers Clinton Wilder and Marianne Kolbasuk McGee, ". . .[M]aybe it's time to drop the 'E' from E-business and acknowledge that soon — sooner than anyone expected — all business, or at least a part of every business process, will be conducted online."

In a recent interview, Mark Hogan, President of General Motors' new eGM Electronic-Commerce Division, spoke about his vision of commerce in the age of the Net: "[The Internet is] touching us end to end . . . . The business-to-consumer piece is getting big inasmuch as more than 50% of prospective customers are going to the Net for information about automotive purchases before they purchase. So having a strong presence with accurate information on the Net's very important. And. . . the functionality of that shopping/buying experience online is really important, too. . . . The net goal of our alliances with AOL and Net-Zero will. . . generate 10 to 15 times the number of leads going into GM Buy Power today. We've got 600,000 hits a month at Buy Power today. So it tells you

---

6 Bradbury, D. (1999). What next for Y2K staff. *Computer Weekly* (Oct 21, 1999):34

7 Stahl, S. (1999). E-Business Is Everyone's Business. *InformationWeek* (Nov 8, 1999): 8

8 Smith, E. (1999). The Next E-Biz Generation; Integrating e-commerce services is key to success, says IBM's Net honcho. *Network World* (Dec 20, 1999):NA

9 DeMarzo, R. & M. Kindley (2000). IBM Becomes The E-Business -- Here's how IBM's Buell Duncan is answering Big Blue's e-business wake-up call. *VARbusiness* (Jan 10, 2000):44

10 Wilder, C. & M. K. McGee (2000). Cover Story -- Putting The "E" Back In E-Business -- It's Time To Realize That All Business Will Soon Be Online. *InformationWeek* (Jan 31, 2000):45

how massive the improvement's going to be, and we expect that increased leads will lead to increased sales for GM."[11]

So we see that today's business environment is becoming a matrix of interrelations both B2B and B2C. Mistakes and outages in our electronic business infrastructure now have massive and immediate repercussions, as we shall see in more detail in this White Paper.

2.2 Explosive growth

The rate of growth of e-commerce has been astounding. For example, Dell Computer filled its first online order in June 1994; sales reached $1M per day through Internet orders in 1997. E-sales rose to $5M a day in 1998, $10M per day by the beginning of 1999 and reached $33M a day by the end of the 3rd quarter of 1999[12].

According to *InfoWorld's* Editor in Chief, Michael Vizard, e-businesses are having to cope with a doubling of their trade every three months.[13]

Even so, writes Leon Kappelman of *InformationWeek*, "online retail activity in the fourth quarter of 1999 accounted for less than 0.65% of total retail business ($5.3 billion of $821.2 billion, according to the Commerce Department)."[14] We are not even close to reaching any kind of limit on the growth of e-business. And that doesn't even take into account the potential for international trade, says Kappelman. "About 4.6% of the world's population (275 million of 6 billion) had Internet access as of February 2000, up from 3.3% a year earlier. North America has about 5% of the world's population but about half its online population. It's projected that worldwide Internet access will increase during the next four years to about 10% and that there will be more than 700 million Internet-connected devices by 2003, up from 200 million last year."

The value of electronic commerce between businesses alone was recently forecast by brokerage Goldman Sachs to rise to $1.5 trillion in 2004, from $114 billion in 1999[15].

3 So what is information security all about?

The goals of information security as defined by Donn Parker, winner of a Lifetime Achievement Award from the U. S. National Computer Security Center, are to protect confidentiality, control, integrity, authenticity, availability and utility.

Confidentiality is a wider concept than disclosure. For example, certain files may be confidential; the data owner may impose operating system controls to restrict access to the data in the files. Nevertheless, it may be possible for an unauthorized person to see the names of these files or find out how often they are accessed. Changing a file's security status may be a breach of confidentiality. Copying data from a secure file to an unsecured file is a breach of confidentiality.

Control or *Possession* means control over information. When thieves copy proprietary software without authorization, they are breaching the owner's possession of the software.

---

11 LaMonica, M. (2000). eGM head pursues broad e-commerce plan. *InfoWorld* (Mar 6, 2000) 22(i10):18

12 Lammers, D. (1999) Bones and e-commerce. *Electronic Engineering Times* (Sep 6, 1999):26

13 Vizard, M. (2000). FROM THE EDITOR IN CHIEF: In e-business, as in war, the edge goes to those who have the best technology. *InfoWorld* (Mar 13, 2000) 22(i11):97

14 Kappelman, L. A. (2000). Working In The Global -- Because the Internet blurs boundaries, doing E-business subjects you to a host of unfamiliar jurisdictions, laws, taxes, cultures, and even technologies. *InformationWeek* (Mar 20, 2000):150

15 Ledwith, S. (1999). Internet Crime Causes Problems for Law Enforcers. Reuters news wire RTir 12-7-99 9:38 PM GMT.

Integrity refers to internal consistency. For example, if the summary field in an order contains a total of $5,678 for all items purchased but the actual sum of the costs that were bough ought to be $6,789 then the data structure is logically corrupt; it lacks integrity.

Authenticity refers to correspondence between data and what the data represent. For example, if electronic mail is sent with a false name, there has been a loss of authenticity. For an e-business, such a breach would occur if a computer program showed a customer the total cost of their order but actually showed the company's internal costs for the order.

Availability means that data can be gotten to; they are accessible in a timely fashion, convenient, handy. If a server crashes, the data on its disks are no longer available; but if a mirror disk is at hand, the data may still be available. If customers expect to see their account balance within 5 seconds but it actually takes 50 seconds, there is a problem of data availability. If such poor service continues, there will soon be a problem of availability of customers.

Utility refers to the usefulness of data for specific purposes. Even if the information is still intact, it may have been transformed into a less useful form. Parker gives as an example the unauthorized conversion of monetary values in a database; seeing prices in the wrong currency reduces the utility of the data. Can you imagine the confusion if US customers were being shown prices in Deutschmarks and German customers saw the same prices in Indian Rupees?

3.1 So security does matter after all

The basic reasons we care about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, the if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

3.2 Threats to information security

It is very difficult to estimate precisely what causes damage to information systems. Managers should be skeptical of any statistics about information security if they show very precise numbers. The problem is twofold: people don't recognize crimes or damage, and when they do they usually don't report them anywhere that collects statistics. Despite these problems, information security experts generally agree on some rough guesses about how damage occurs.

3.2.1 Internal dangers

Perhaps half of all the damage caused to information systems comes from authorized personnel who are either untrained or incompetent. Another quarter or so of the damage seems to come from physical factors such as fire, water, and bad power. Maybe a fifth of the damage comes from dishonest and disgruntled employees. Computer viruses cause another few percent, and maybe about 5 or 10 percent of the damage is caused by external attack.

3.2.2 External threats

Who are the people attacking computer systems? There seem to the two major classes: amateurs and professionals. Amateurs include poorly-supervised children, rebellious and badly-socialized adolescents, and psychologically disturbed or ideologically warped adults. Some amateurs cloak their destructive badly-protected computer systems in the language of social responsibility; they claim to have the best interests of their victims of heart. Their actions belie their words, however: well-meaning people do not place obscenities and insults on other people's property as these cybervandals do on many a Web site.

Professionals are harder to characterize, since there are probably fewer of them and they may be harder to catch; however, some criminal hackers are earning a living with their skills. Some professionals use public and illegal sources of information to help unscrupulous private investigators. Some computer criminals steal credit card numbers and sell them to the criminal underground or participate in theft of services from telephone and mobile-phone companies. An unknown number may be involved in industrial espionage.

Some criminal hackers have set up shop as security consultants and offer penetration analysis and consulting services for their clients. There is a serious question about the trustworthiness of people who used to break the law and now claim that they no longer do so; some security experts argue that leopards have indelible spots, whereas others are willing to believe that there is such a thing as an ex-hacker. I strongly urge managers who are considering hiring such people to ensure that their contracts include severe penalty clauses if any of their employees are found to be damaging their clients in the course of their duties.

3.2.3 Attractive targets

Several factors influence the likelihood of attack. For example, a small, obscure tool-and-die company with eight employees is unlikely to be as attractive to any external attacker as a major corporation with thousands of employees and a significant share of its market. It is possible that having a public Web site makes an organization an attractive target for cybervandals. Any site proclaiming its tight security is likely to attract the attention of the amateurs who were trying to prove their prowess; for example, security organizations are under constant daily attack. Some amateurs deliberately attack financial institutions and military systems to demonstrate the sites' weaknesses and ostensibly to force improvements. Finally, some hackers ("hactivisits") attack sites for political purposes; for example there have been recently been concerted attacks on the World Trade Organization Web sites by anti-WTO activists, and mainland Chinese and Taiwanese hackers have been damaging official sites in each others' countries for the last few years.

3.3 What kinds of breaches hurt e-commerce?

Perhaps one of the most damaging problems a business can encounter is to have customer data revealed to criminals. For example,

- In 1997, Drew Dean reported on a hacker incident in which someone sent 2,300 customers of the ESPN Sportzone and NBA.com Web sites copies of the last eight digits of the victims' credit card numbers. The accompanying message said, "You are the victim of a careless abuse of privacy and security. This is one of the worst implementations of security we've seen." It seems

that the hackers were not, however, malicious: no one reported fraudulent use of their cards. Dean suggested that the fault was likely to lie in bad CGI programming[16].

- A thief who ran a packet sniffer to capture 100,000 credit card numbers from a dozen on-line commerces was arrested in May 1997 when he tried to sell it to the FBI for $260,000[17].
- In 1998, an employee of a Japanese bank offered to sell detailed customer records to a mailing-list company. Happily, that firm immediately contacted the bank and the scam was stopped[18].
- The Canadian consumer-tracking service Air Miles inadvertently left 50,000 records of applicants for its loyalty program publicly accessible on their Web site for an undetermined length of time. The Web site was offline as of 21 January 1999 until the problem was fixed[19].
- In February 1999, an error in the configuration or programming of the F. A. O. Schwarz Web site resulted paradoxically in weakening the security of transactions deliberately completed by FAX instead of through SSL. Customers who declined to send their credit-card numbers via SSL ended up having their personal details — address and so forth — stored in a Web page that could be accessed by anyone entering a URL with an appropriate (even if randomly chosen) numerical component[20].
- World famous cryptographer and security expert Prof. Ross Anderson of Cambridge University analyzed requirements on the AMAZON.COM online bookstore for credit card number, password, and personal details such as phone number. He identified several risks: (1) merchant retention of credit card numbers poses a far higher risk of capture than of capture in transit; (2) adding a password increases the likelihood of compromise because so many naïve users choose bad passwords and then write them down; (3) even the British site for Amazon contravenes European rules on protecting consumer privacy; (3) such practices make it easier for banks to reject their clients' claims of fraudulent use of their credit-card numbers[21].
- In April 1999, Joe Harris, a computer technician at the Seattle-area "Blarg! Online" ISP, discovered that improperly-installed shopping-cart software used widely on the Net to simplify shopping can allow anyone to see confidential data such as credit-card numbers. Security analysts pointed out that the plain ASCII file where such data are stored should not be on the Web server at all, or if it is, the file should be encrypted. Initial evaluation suggested that the weakness affects at least several hundred and possibly many thousands of e-commerce sites where the software installations were improperly done[22].
- In another recent case, CD Universe customers were shocked when a Russian hacker calling himself Maxus was able to access the CD distribution company's customer credit-card database in December 1999. The criminal then tried to extort $100,000 (and later $300,000) from the firm in exchange for not publishing the numbers. When CD Universe refused to pay him, the

---

[16] RISKS FORUM DIGEST 19(24): < http://catless.ncl.ac.uk/Risks/19.24.html#subj5 >

[17] *New York Times* May 23 ,1997

[18] RISKS FORUM DIGEST 19(53): < http://catless.ncl.ac.uk/Risks/19.53.html#subj3 >

[19] RISKS FORUM DIGEST 20(18): < http://catless.ncl.ac.uk/Risks/20.18.html#subj13 >

[20] Glave, J. (1999). FAO Schwarz Springs a Leak. *Wired* press service Feb 3, 1999 16:30 PST

[21] RISKS FORUM DIGEST 20(20): < http://catless.ncl.ac.uk/Risks/20.20.html#subj10 >

[22] Wilson, J. (1999). Shopping Software May Be Flawed. Associated Press newswire 06:48 PM ET 04/22/99

scoundrel posted the stolen numbers on a Web site and allowed anyone to have one credit card number at a time. Criminals were able to make fraudulent charges on the cards.[23]

A similar breach of confidentiality that can be disastrous is to have trade secrets revealed to competitors. For example,

- In a settlement of one of the few documented cases of industrial espionage involving intercepted e-mail, the Alibris company paid a $250K fine for the firm it acquired in 1998. That company, Interloc, admitted intercepting and copying 4,000 e-mail messages sent to Amazon.com through its own ISP, Valinet. Prosecutors said that the e-mail was intercepted to gain a competitive advantage against Amazon in Interloc's own book business. The managers of Interloc steadfastly denied any wrongful intention but failed to explain why they copied the e-mail[24].
- In the first case of a lawsuit involving industrial espionage by lawyers, Moore Publishing of Wilmington, DE sued Steptoe & Johnson of Washington, DC for allegedly breaking into its computer systems more than 750 times while simultaneously using a stolen user-ID and password to penetrate the victim's network. In addition, the suit alleges a systematic cyberwar involving misinformation posted on newsgroups through a HotMail account that was eventually traced to the defendants. The suit demanded damages of at least $10M[25].

There have been some spectacular software quality-assurance failures in recent years; in one particularly humiliating case, a programming error generated the largest single accounting error in the history of the space time continuum (as far as we know, that is).

As for breaches of integrity, Web vandalism is so common it is no longer news. Web defacement has become a sport, with hordes of children called script-kiddies blindly using hacking tools that exploit known and usually very old vulnerabilities[26]. If you can stomach pornography, obscenity and really bizarre spelling, you can even look at the images of the hacked pages by clicking on the links at that location. For e-businesses, the scary aspect of these cases is that in many of them, technical personnel had no idea they had been hacked until someone phoned them or sent them e-mail to ask about the peculiar pictures and words on their Web pages.

Infections by viruses and worms also cause breaches of integrity; for example, back in 1996, there was a widely-distributed MS-Word macro virus that inserted the word "Wazzu" at random into infected documents. Having a damaged document on one's Web site would be pretty embarrassing. Well, a careful search (careful to exclude phrases such as "up the wazoo" and references to Washington State University – known as Wazzu) by IBM researchers revealed many sites that had "Wazzu" in their documents[27]. Even today, one can find documents with ectopic "wazzu" in them; e.g., as I was writing this paper I found a music review with the sentence, "Confined to the piano seat wazzu for the duration this was unlike any other performance by Nick Cave in Melbourne. . . ."

If anyone with an e-business needs yet more to worry about, then worry about viruses that can alter numbers at random — like, for example, prices. To get a sense of the kind of damage such alterations can cause consider the case of the unusually cheap Hitachi monitors. For unknown reasons, in February 1999 the BUY.COM online store Web site listed a $588 Hitachi monitor at only $164.50 -- and staff failed to notice the error until two days later, by which time there were 1,600

---

[23] Smetannikov, M. & L. Trager (2000). Credit-Card Fraud Hits Web. *Inter@ctive Week* (Jan 17, 2000) 7(i2):8

[24] Internet e-mail intercepted. United Press International UPn 11-23-99 2:25 PM

[25] Computer Hacking Suit Escalates Against Top U.S. Law Firm. WASHINGTON, Nov. 11 /PRNewswire/

[26] For a long list of recently-hacked Web pages, see the AntiOnline archives < http://www.antionline.com/archives/pages/ >.

[27] See <http://www.av.ibm.com/1-3/Features/Cover/> for the results of this research by Morton Swimmer.

orders for this incredible bargain. The potential cost in lost revenue was $677,600 and the real cost depended on the markup. Attempting to refuse to sell the monitors could lose the company enormous customer good will, not to speak of resulting in an investigation for fraud and possible civil lawsuits for breach of contract. Analysts speculated on the cause of the error. One intriguing possibility: the BUY.COM online store has a policy of underbidding any price on the Net and may possibly use knowbots (automated agents) to scour the Web looking for prices of products it sells. If a competitor were accidentally or deliberately to post a bad (excessively low) price, the unsupervised knowbot could very well poison the Web site database. The same technique could be used in an information warfare attack to ruin a competitor.

It is trivially easy to alter the originating address that appears on e-mail messages; there have already been many cases in which lies have been distributed on the Internet and attributed to the wrong source. A business can be targeted by a flood of false advertising, abusive messages, or even announcements about nonexistent discounts — all apparently coming from the victim and causing enormous problems with customer relations. All such breaches of authenticity would cause serious damage to the reputation of the victim. In 1997, a Texas student named Craig Nowak used "flowers.com" as his return address in a flood of junk e-mail. His victim, Flowers.Com, received thousands of angry and even abusive e-mail messages and many cancellations of accounts from customers and prospects who thought the flower company had abused their e-mail addresses. Luckily, in that case, it was possible to track the miscreant down and he was fined $18,910 plus court costs for his fraud; in other cases it has been difficult or impossible to track down the originator of this kind of cyber-slander[28]. Even today, countless firms are falling prey to charlatans and crooks who claim that unsolicited bulk e-mail is a good method of marketing — and are suffering monetary losses and loss of reputation as a consequence[29].

Consumers expect appropriate response from e businesses; there have been many examples of disastrous cases of slow response due to inadequate resources, downtime due to errors and downtime due to denial-of-service attacks. Firms consistently fail to plan for peak loads; they omit effective backup systems for electrical power and telecommunications systems; they lack real-time recovery for disk failures and server outages. And every time a customer leaves a non-responding Web site in disgust, there's a good chance they will turn to a competitor the next time they start their online shopping.

On a fundamental level, e-business naturally depends on the utility or usefulness of its user interface. For example, people become irritable when faced with clumsy, inconsistent and non-intuitive Web designs. A customer who cannot reverse a mistake or get help quickly will soon be an ex-customer.

Losing control over information is also a problem. Some companies have been subjected to extortion, in which criminals have threatened to reveal confidential information war to destroy critical systems unless they are paid[30]. Visa International, for example, admitted in January 2000 that criminal hackers had broken into several servers in its global network in July 1999 and stolen information (although, according to them, not credit-card numbers or consumer data). In December 1999, the criminals contacted Visa demanding a ransom in return for the data. Although it is very difficult to have confirmed evidence of such cases, there have been widespread reports of this kind

---

[28] RISKS FORUM DIGEST 19(19):9 < http://catless.ncl.ac.uk/Risks/19.19.html#subj9 >

[29] RISKS FORUM DIGEST 20(21) < http://catless.ncl.ac.uk/Risks/20.21.html >and *Wired* online < http://www.wired.com/news/news/business/story/17803.html >

[30] Harrison, A. (2000). Visa Reveals July Break-ins; Suggested: Credit card company says crackers tried to extort money. *Computerworld* (Jan 31, 2000):6

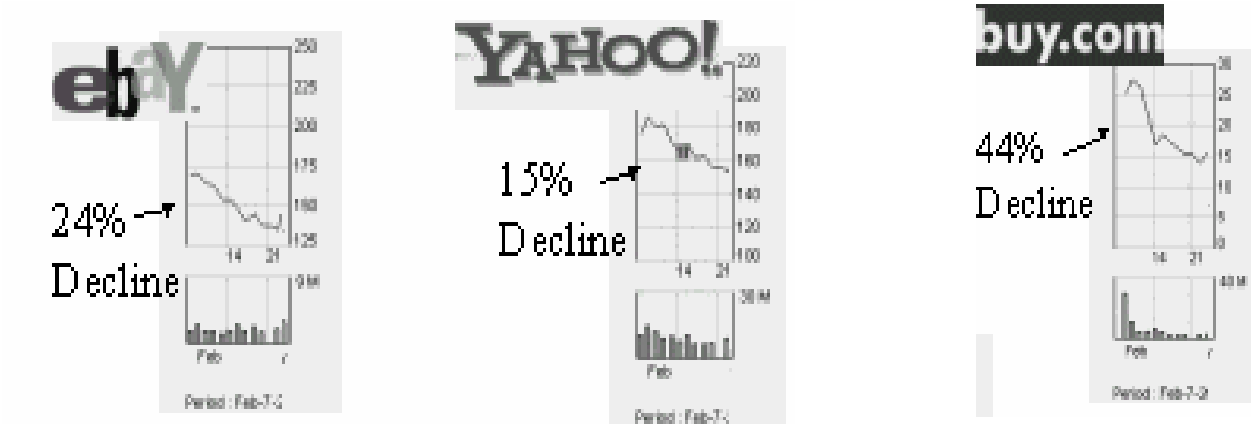
of extortion, especially in the financial world where companies are reluctant to admit that their systems have been penetrated.[31]

3.4 The problem of downstream liability

Another kind of loss of control occurs when a system is used to launch damaging attacks against other systems. For example, in mid-February 2000, Internet users suffered the consequences of distributed denial-of-service (DDoS) attacks on several major e-commerce sites[32]. These attacks involved two types of victims: the initial and the final.

The final victims were the sites receiving a flood of fraudulent and useless packets that crashed servers and saturated inbound bandwidth keeping customers away.

Amazon, Buy.Com, CNN and eBay users experienced serious delays in getting service from these Web sites. Investors in these companies' shares may have lost over a billion dollars in paper value of their stocks. The following graphs tell their own story:



However, the floods of packets in such a DDoS originate from hundreds of other victims — call them the initial victims — whose integrity is compromised by criminal hackers. The DDoS attacks involve tools such as trin00, Tribe Flood Network (TFN), Stacheldraht and TFN2K, widely available on the Internet due to the irresponsibility and stupidity of programmers with less social conscience than the average bacterium. In each case, the criminal hacker takes as long as required to break into many ill-secured computer systems to install programs known as soldiers, slaves or zombies. These slave programs respond to instructions sent in encrypted form from a master program directly under the control of a criminal hacker. The slaves serve as amplifiers for the denial-of-service attacks, allowing criminal hackers to put together an unauthorized parallel-processing system to abuse their victims. There are even scanners available to help locate weak systems

---

[31] But see Komisar, L. (1999). Russian Cons and New York Banks. *Village Voice* (December 1 - 7, 1999) < http://www.globalpolicy.org/nations/russ993.htm > for an exposé on the lax state of controls in today's international banking industry.

[32] See for example:

- Yasin, R (1999). Rise In Intrusions Sparks Concern -- CERT Responds To Increase In Distributed Denial Of Service Attacks. *InternetWeek* (Dec 6, 1999):18
- Fonseca, B. (1999). Zombies attack networks: Denial-of-service attack uses multiple PCs to hit system. *InfoWorld* (Dec 13, 1999) 21(i50):14
- Farrow, R. (2000). Distributed Denial of Service Attacks. *Network* (Jan 1, 2000)
- Featherly, K. (2000). Denial Of Service Attacks Continue - Reports 02/09/00. *Newsbytes* (Feb 9, 2000)

automatically; it is possible to infect yet another new host once every few minutes or faster, depending on the bandwidth available to the criminal[33].

Tracing an attack back to one of the slaves is not much of a problem; however, going back to identify the person who installed the slave programs is very difficult. While law enforcement officials, including the FBI and the RCMP, searched for the perpetrators, the usual rag-tag band of lunatics crawled out of the woodwork to claim responsibility for this disruption of Internet commerce. Some of these fools even claimed a political agenda; supposedly spewing useless packets at their victim was a demonstration of their feelings about the commercialization of the Internet[34]. Eventually the RCMP in Canada arrested a nameless 15 year-old Montreal boy with the on-screen pseudonym "MafiaBoy" and charged him with breaching Canadian computer-crime laws.

But regardless of who is causing these DDoS attacks, there's an issue that has concerned security specialists and tort lawyers for many years: the question of whom to sue for damages when an attack is launched from a site that has itself been victimized by criminal hackers.

Now, I am not a lawyer, and this article is not legal advice; for legal advice, consult an attorney qualified to discuss tort law. That said, I have been following cyberspace law developments for a long time. At several professional meetings, I have heard attorneys specializing in the law of cyberspace discuss the concept of downstream liability in hacking incidents. Simply put, whom would you rather sue: some impecunious wretch sitting in a basement cackling over his latest DDoS attack or a real business with assets?

In a *PC Week* article, columnists Jim Kerstetter and John Madden wrote, "The recent distributed denial-of-service attacks on seven of the Web's busiest sites could not have happened without lax security on possibly thousands of other Web servers around the world. The owners of those sites could face legal trouble, since the attitude exists that you are responsible for the material on your site, regardless of its origin.[35]"

In my opinion, if DDoS attacks become a significant impediment to e-commerce, there are bound to be lawsuits against the owners and administrators of the first-line infected hosts harboring the DDoS slaves. I guess that the argument presented by tort lawyers will be that the slave-infected systems demonstrate contributory negligence by the people who ought to have a secured their systems so that the slaves could not have been implanted in the first place. Conceivably, a victim might sue all of the hundreds of infected sites in the hope of collecting settlements or awards from several of them.

What arguments would the plaintiffs' attorneys use in laying blame on the first rank victims? A strong case could be made using expert witnesses who would show that the vast majority of security breaches on sites linked to the Internet derive from out-of-date software and from inadequately configured defenses. The witnesses would testify that fixes for well-known vulnerabilities have been available for years at no cost from software manufacturers, security firms, and from volunteers freely

---

[33] For more technical information about distributed denial-of-service attacks see Dave Dittrich's extensive resource page at < http://staff.washington.edu/dittrich/misc/ddos > and also the SANS Institute's excellent and practical guide, "Help Defeat Denial of Service Attacks: Step-by-Step" < http://www.sans.org/dosstep/index.htm >.

[34] Klein, N. (2000). My Mafiaboy. *The Nation* (Mar 13, 2000) < http://www.thenation.com/issue/000313/0313klein.shtml >

[35] Kerstetter, J. & John Madden (2000). Web security breakdown —'Zombie' Web servers were unwitting partners in denial-of-service spree. *PC Week* (Feb 14, 2000):1
See also
Weil, N. (2000). Real denial-of-service hack victims weren't Web sites. *Network World* (Feb 14, 2000)

exchanging solutions. If subpoenaed, some of the network administrators from the slave-infested sites would testify that they knew that their sites were vulnerable, they knew where to get the fixes, but they just didn't have time to get the fixes installed. At that point, a clever attorney would ask, "Why not?"

Why not? Because there are well-known, respected firms where a single overworked network administrator is responsible for hundreds or even thousands of nodes with capital value estimated in the million-dollar range; where despite regular pleas from desperate people trying to get their work done, managers consistently refuse to allocate adequate resources to develop and implement sound security policies.

And so we are back to downstream liability. If it makes sense to sue the organizations whose computer systems harbor slave programs for contributory negligence rather than to pursue the hackers who infected them, doesn't it make sense to sue the managers who decided to leave their systems inadequately secured rather than pursue the network administrators who tried and failed to do their job in the face of managerial malfeasance?

4 The public cares about security

Consumers and fellow businesses have finally grasped that information security matters to *them*. Survey after survey confirms that one of the key impediments to increased consumer usage of online purchasing is fear: fear of losing control over their credit card numbers and fear of losing control over their privacy.

- In a study of 1,001 respondents selected at random among the general public, most people expressed suspicion about the security of online transactions. Highlights: 58% of consumers do not consider any financial transaction online to be safe; 67% are not confident conducting business with a company that can only be reached online; 77% think it is unsafe to provide a credit card number over the computer; and 87% want e-commerce transactions confirmed in writing. The National Technology Readiness Survey was carried out by Rockbridge Associates over a two-year period[36]. The 95% confidence limits for such responses range from around ±3% in the middle to around ±0.5% at the extremes.
- The e-commerce firm CyberSource commissioned a survey of online merchants; the work was carried out by Mindwave and interviewed over 100 online businesses. The findings, reported in December 1999, showed that 75% of the respondents rated credit-card fraud as "a concern" but only 59% knew that they would be liable for restitution in cases of fraud. About 72 percent of online merchants surveyed believed that sales would increase if online shoppers were not worried about fraud. The 95% confidence limits for percentages in a sample of 100 are approximately ±10% at worst[37].
- In April 2000, the Angus Reid Group (a national polling agency) released results of 1,125 interviews with Canadian Web users. The overall conclusion was that most Internet users in Canada have never shopped on-line because they fear their credit card information will be accidentally leaked or stolen. Tyler Hamilton, reporting for the *Globe and Mail* newspaper, wrote, "Such on-line shopping jitters represent a massive barrier to e-commerce,. . . preventing billions of dollars from flowing into the country's digital economy. . . .The perception that such

[36] *E-Commerce Times Online* Jun 21, 1999
[37] Dennis, S. (1999). INTERNET FRAUD A GROWING CONCERN TO ONLINE MERCHANTS. *Newsbytes* Dec 6, 1999

information will be misused or stolen is cited as the main reason 74 per cent of all Canadian Internet users have stayed clear of on-line shopping." Steve Mossop, senior vice-president of Angus Reid and head of the firm's Canadian Internet practice, called the numbers "staggering." He said privacy and security issues on the Internet have gained a higher profile over the past year, largely because of recent hacker incidents and Web site breaches. The top fears holding back consumers: 62% are "very concerned" about the security of databases holding their credit-card information; 57% believe that credit-card data are can be easily used for unauthorized transactions; 54% think their credit card data can be intercepted in transit by hackers[38].

5 Consequences of security failures for e-businesses

All right, let's take stock. Here are some brief reminders of the kinds of problems that will occur for e-businesses hit by security problems:

- immediate loss of business due to unavailability
- long-term loss of business due to loss of trustworthiness and reputation
- loss of stock value
- financial liability for breach of contract
- legal liability for contributory negligence
- loss of management credibility
- embarrassment of employees
- lowered employee morale
- increased employee turnover
- difficulty hiring competent staff
- incitement to abuse of security policies.

So far, this is the usual gibbering and fist-shaking that all of us information security specialists get into when trying to explain why our contributions are valuable.

The news is that we can now go beyond gibbering and fist-shaking. In today's e-commerce environment, effective information security can actually increase business and increase profits, not merely reduce risk.

6 Defining the Net Present Value of Information Security

Tom Nelson, VP and Chief Strategy Officer of AtomicTangerine has defined the Net Present Value of Information Security (NPVSec) as follows: "NPVSec is the value protection and value creation that is realized when barriers to e-Business are removed through mechanisms that ensure business integrity, service availability and customer/consumer confidentiality and privacy. Value creation examples include: new distribution channels, new revenue streams, new business models, among others."

[38] Hamilton, T. (2000). Web sales stunted by security fears - survey - 84% of web users worry when personal information goes on-line. *Toronto Globe and Mail* (Apr 27, 2000).

In other words, instead of viewing information security solely as a risk-avoidance measure — like a kind of insurance policy that never actually pays anything back — we are forced by the nature of e-business to accept that security actually *supports* and *enables* e-business.

As we have seen in our review, e-business has brought security to the forefront of strategic thinking for successful businesses. Business leaders can no longer tolerate the view that security is an add-on feature relegated to the end of the design process. Security is a process, not a product or a state; security affects every e-businesses bottom line in a positive way. Security is no long a cost center, it's part of your repertoire for meeting the legitimate needs of your public. Instead of seeing security as solely the purview of the technical staff in your organization, you should ensure that your marketing and public relations departments are well versed in the principles of information security and can communicate effectively to an anxious public about the measure you are taking to safeguard your customers' privacy and their money. Be sure that your Web site has clear and appropriate privacy policies; don't sell or trade visitors' and customers' information without their explicit opt-in permission.

Secure your systems and you will secure your future.