

NPV:

information
security



atomictangerine™

Proprietary Information Statement

The words AtomicTangerine and associated logo are trademarks of AtomicTangerine, Inc. All other brands and product names are trademarks or registered trademarks of their respective owners.

©2000 AtomicTangerine, Inc. All rights reserved.



Contents

The Net Present Value of Information Security:	
Executive Summary.....	1
Introduction.....	1
All Business Will Be E-Business.....	2
The Need to Establish New Ground Rules for E-Business	3
No Legal Recourse.....	4
Security Is a Critical Enabler for E-Business	4
The NPV of Information Security.....	5
What Information Security Brings to the Table	5
How Security Helps Companies Create Value	6
Leverage the Value of Information.....	7
Improve the Customer Experience.....	7
Create New Distribution Channels.....	8
The Impact of Poor Security	8
Denial of Service.....	8
Breaches of Consumer Confidence.....	9
Lost Business and Third-Party Liability	10
Lack of Consumer Trust	10
A Security Checklist	11
Conclusion.....	15
Notes.....	15



The Net Present Value of Information Security: Executive Summary

Information security is critical to e-business. In a twist on an old business paradigm, security is no longer relegated to just providing asset value protection for e-firms; it has now become a vital part of the core business processes. When it is incorporated into business strategies, information security can help organizations create additional business value by leveraging information assets, improving the customer experience, enabling new avenues of competitive advantage and opening new market channels.

This is not to say that value protection is no longer an important part of an overall information security program. To the contrary, it is now more important than ever. Recent events underscore the continued need for information security and highlight the dramatic business impacts that can

result from poor security. Companies are finding there are also direct impacts to the bottom line and to shareholder value when security breaches are allowed to undermine confidence in the business web or to shut the door of an e-business through denial of service.

While information security remains a highly interdisciplinary and technically complex challenge, it is an area which can be improved dramatically when addressed with the appropriate business focus. We provide an executive checklist of key security actions to assist in improving the basic understanding of what needs to be done in every enterprise to establish effective protection of e-business value.

Introduction



E-business offers tremendous opportunities for reducing costs and improving revenues. But along with the advantages of conducting business online it also brings new threats and liabilities that leave businesses highly vulnerable to cyber attack and fraud. Business today must not only be concerned with competition for market share in an expanding global marketplace, but also with the impact of e-business on core business

purpose, service availability, customer confidence and privacy. All of these highly volatile elements are critical parts of a firm's reputation and valuation. And although each of these issues is separate and distinct, each is also related to a critical success factor in e-business today: information security. Executives can no longer afford to consider security the "locks on the doors"; instead, they must acknowledge security as an integral

component of a corporate strategy—a component that is necessary to facilitate the creation of systems that respond and adapt to the rapidly changing business environments that characterize the New Economy.

The **net present value (NPV) of information security** is the value that is created when barriers to e-business are removed through mechanisms that ensure business integrity, service availability and customer/consumer confidence and privacy. Information security NPV is realized when appropriate access is facilitated so that businesses can run seamlessly without

interruption. Businesses thus need to discard the outdated view of security as simply an “insurance” plan against fraud; they need to view it as a necessary element for the long-term viability of new markets and to ultimately enable the New Economy to achieve its full potential.

This white paper details the role of security in an overall business strategy, outlines the pitfalls of neglecting security, introduces a means of measuring the information security NPV and provides an executive checklist to ensure that your security efforts are on track.

All Business Will Be E-Business

“All companies will be Internet companies, or they won’t be companies.”

— Andy Grove
CEO, Intel Corporation

The rate of e-business growth has been astounding. According to *InfoWorld* editor-in-chief, Michael Vizard, e-businesses have to cope with a doubling of their trade every three months.¹ Dell Computer is a prime example. Dell filled its first online order in June 1994. Internet sales reached \$1 million per day in 1997, then mushroomed to \$5 million a day in 1998, to \$10 million per day by the beginning of 1999, reaching \$33 million per day by the end of the third quarter 1999.² According to Goldman Sachs, the aggregate value of e-commerce between e-businesses alone is expected to rise to \$1.5 trillion in 2004 from \$114 billion in 1999.³

Despite the growth that has already occurred, the use of the Internet is in its infancy. “Online retail activity in the

fourth quarter of 1999 accounted for less than 0.65 percent of total retail business (\$5.3 billion of \$821.2 billion, according to the [U.S.] Commerce Department),” writes Leon Kappelman of *InformationWeek*; he added that, “We’re not even close to reaching any kind of limit on the growth of e-business.” And these figures are only for North America. When the rest of the world is considered, the potential for growth is vast indeed. According to Kappelman, “About 4.6 percent of the world’s population (275 million of 6 billion) had Internet access as of February 2000, up from 3.3 percent a year earlier. North America has about 5 percent 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 percent and that there will be more than 700 million Internet-connected devices by 2003, up from 200 million last year.”⁴

The reason for this rapid growth, indeed, the magic of the Internet,



comes from its ability to tie people together. Organizations are using the Web in a wide variety of ways to improve their relationships with customers, partners and suppliers. They are using the Web to create efficient, automated supply chains and distribution channels, as well as new types of marketplaces, such as e-business exchanges. Like a stock exchange, such as the NASDAQ, e-business trading exchanges facilitate community as well as buying and selling among trading partners within specific vertical markets, such as

electronic components, chemicals or pharmaceuticals. By leveraging the Web's universal access, e-business exchanges can easily aggregate a large number of sellers and buyers. Bear Stearns forecasts such exchanges will have a valuation of \$228 billion in 2002.⁵ Moreover, new methods of doing business over the Web are emerging every day. One of the most recent trends is wireless web access. A new study by IDC found that by the end of 2002, wireless subscribers with Internet access will outnumber wired Internet users.

The Need to Establish New Ground Rules for E-Business

Whenever human beings congregate for a joint endeavor, they need to establish ground rules and clear expectations about each other's behavior. These rules enable the group to function effectively, and also serve to protect the individual. In business, such ground rules take the form of standard business processes, as well as laws and regulations. When business operations change, these processes and regulations must also be updated. Because the Internet often establishes new business paradigms, businesses have a continual need to develop new processes and ground rules to ensure sound business operations.

The following are a few of the ways that the Internet has altered the way businesses interact with each other.

✎ Most brick-and-mortar business dealings involve a physical interaction and therefore give businesses the means to know exactly whom they're dealing with. For example, a person might come

into a store or at least leave an address or phone number. The Internet makes it far more difficult to know if a person is whom he or she claims to be. Internet users can be located anywhere in the world, and many methods are available to mask their locations and identities, making it much easier to commit fraud.

✎ In the physical world, it is difficult to access large volumes of confidential information. To steal confidential papers stored in a company's files, an industrial spy would need to physically break into the office. With the Internet, a hacker located anywhere in the world can make off with company secrets stored on a server without ever having to come near the physical premises. Downloading the equivalent information volume of several sets of encyclopedias happens in a matter of seconds.

✎ Paper-based business processes leave a margin for error. For



example, a company that pays by check has a float period of five to ten days and knows its check cannot be cashed until the bank processes the transaction. This float period provides time to stop payment on the check if fraud is discovered. With new online settlement systems such as debit cards, however, transactions are completed in real time, leaving

organizations more vulnerable to fraud.

As a result of these and other changes brought about by the Internet, organizations need to develop new business processes that ensure the proper completion of business transactions in order to protect both themselves and their partners.

No Legal Recourse

In a time of rapid change, businesses may be tempted to rely on legal authorities to deal with the fallout from these changes. But such legal recourse is expensive, and results are not guaranteed—even when the company wins its case.

In *DoubleClick versus Henderson*, DoubleClick asked the courts to issue an injunction to prevent former employees from advertising stolen trade secrets for a one-year period. Even though DoubleClick proved that the employees had, in fact, stolen the trade secrets, the court did not grant the relief that DoubleClick requested. Instead, the court issued a six-month injunction, ruling that the “rapidly changing world of Internet advertising” limits the life of trade secrets.

Ford Motor versus Lane represented a similar outcome when Ford proved wrongdoing, but the court did not grant the company the desired redress. In this case, a web site operator had

received stolen trade secrets about designs and future activities that were clearly labeled proprietary and then published the information on the site. The court agreed with Ford that a prior restraining doctrine should have precluded the site from publishing the information. However, the court still ruled that the site could publish the information. Why? The court believed the site’s free speech rights superceded Ford’s right to retain trade secrets

In today’s business world, relying on the legal system for protection or to provide a means of financial recourse doesn’t make good business sense, particularly while the courts remain unclear about how they will rule on such matters. Proactive measures that prevent security breaches and fraud from occurring in the first place will prove more cost-effective and serve business better in the long run.



Security Is a Critical Enabler for E-Business

One way that organizations can adapt to the changes resulting from new e-business technologies is to rethink their views on security. Traditionally,

organizations have regarded security as a kind of insurance policy and have devoted roughly 1 to 3 percent of their IT budgets to security measures. In the

“glass house” paradigm of business computing, such thinking was appropriate. Mainframe systems were, and still are, fairly self-contained, and the threats to them are reasonably well understood. However, because the Internet makes organizations, and their critical information, far more vulnerable to intrusion and attack from outside, organizations need to greatly increase their security measures to enable trusted business dealings in this new environment.

Anyone doubting this assertion need only look at the skyrocketing instances of security breaches. In a recent survey of 273 Computer Security Institute (CSI) member organizations,

the CSI and the San Francisco FBI Computer Intrusion Squad found that nearly 90 percent of respondents detected some form of security breach in 1999—either from inside the organization or from external hackers. Of these attacks, 70 percent were considered serious, including theft of proprietary information, financial fraud, system penetration from outsiders, denial-of-service attacks and sabotage of data or networks. These attacks resulted in substantial financial losses—the \$266 million in losses in 1999 that these member companies reported to CSI was more than twice the average annual total losses of \$120 million reported from 1996 to 1998.

The NPV of Information Security

As a key strategic enabler of new trusted e-business processes, information security becomes a generator of NPV for the organization. Information security protects business reputation, consumer confidence and market valuations, and it delivers a competitive edge by allowing new distribution channels, revenue streams and even business models in an otherwise diluted and overly compromised marketplace. In other words, instead of being viewed solely as a risk-avoidance measure (like a kind of insurance policy that never pays anything back), information security is required both to support and enable e-business.

In today’s e-commerce environment, effective information security can serve to increase business and profits,

not merely to reduce risk. To assure success, therefore, e-businesses need to bring information security to the forefront of strategic thinking. They no longer can view security as an add-on feature relegated to the end of the design process or as a cost center or as solely the purview of the technical staff in an organization. Instead, they must realize that information security is a process that is essential in meeting the legitimate needs of the public. They must also realize that their marketing and public relations departments need to be well versed in the principles of information security so that they can communicate effectively with an anxious public about the measures that safeguard customer privacy and money.



What Information Security Brings to the Table

E-business information security brings the safeguards of traditional business practices to the electronic realm; that is, confidentiality, control, integrity, authenticity and availability.

☞ **Confidentiality** ensures that only authorized persons can see specified information. Unlike the cases described in the previous section, information security enables organizations to maintain trade secrets.

☞ **Control** determines who is authorized to access and possess information. For example, a software vendor may want to control who can access the software it is attempting to sell over the Internet so it can maintain profit margins.

☞ **Authenticity** means that corporate and individual identities can be confirmed—that the information provided has not been tampered with. For example, organizations performing a transaction over the Web will want to be sure that the amount of funds transferred was the correct \$1,000 amount, rather than \$10,000.

☞ **Availability** ensures that information can be accessed over the Internet.

Availability can be compromised through system failures that result from hardware problems or denial of service attacks.

When all parties in e-business transactions have security systems in place to provide these capabilities, they can rest assured that their e-business operations are following solid business practices. However, when one of the parties in a transaction does not follow these policies, that organization can compromise business dealings for all of its trading partners. As Howard Schmidt, Corporate Security Officer of Microsoft notes, “Security is only as good as the weakest link in the chain. If I do business with someone who has a lower level of security than I do, my security is weakened and this affects my business model. For example, if I am basing my business model on the fact that I am doing business with that particular business and I trust them and someone hacks their system, now I’m doing business with someone with whom I do not have a trusted relationship. The hacker could easily submit invoices without authorization.”

How Security Helps Companies Create Value



A survey of some of the biggest players in the on-line space reveals that successfully addressing issues of information protection, system availability and system integrity is a prerequisite to taking advantage of new business opportunity. Enron’s energy exchange, with \$186 billion in annual trades, had to overcome the barriers of safeguarding multimillion dollar transactions while guaranteeing

accurate and instant prices 24X7. The security mechanisms involved in on-line 24X7 availability and confidentiality of transactions were fundamental to enabling Enron to create this new business model.

Charles Schwab looks to create new value propositions for its customers. Today, its online brokerage trades \$25 billion per week, but before it could go

online it had to ensure the reliability of the technology and protection of its customers' assets. Security mechanisms and processes could have been barriers to this new offering and revenue stream for Schwab, but they were successfully addressed and today Schwab runs what many consider to be the largest secure e-commerce site in the world.

With security technology in place, organizations can begin to establish sound practices for conducting business over the Internet. In doing so, they are able to benefit from the potential advantages and new revenue streams the Internet has to offer. When considered in this light, a \$5 million investment in security might enable a new revenue stream that could add \$25 million to the bottom line. The Enron example is one of creating an entirely new business model (the energy exchange) through use of the Internet. Schwab successfully improved its value to customers by adding a new service. Successfully employing security in business strategies adds value in other ways as well such as allowing a firm to:

- ❏ Leverage the value of information
- ❏ Improve customers' experience with the site
- ❏ Create new distribution channels.

LEVERAGE THE VALUE OF INFORMATION

Business forces are driving organizations to make more information available to customers and partners. For example, in supply chain automation applications, a company might decide to open its inventory system to customers to increase the value of that information. Making

inventory information available in real time enables cost savings through just-in-time inventory management. Security is necessary to allow the permissible use of valuable information and to prevent the inappropriate use of or release of proprietary information to unauthorized parties.

Financial service firms often need to improve information management for their customers through information aggregation. This raises the issue of how information from multiple sources is securely collected, transmitted and stored. Those firms that can successfully introduce secure information management to their clients will gain a competitive advantage by enabling services that are viewed as an increased value by their customers without exposing themselves to liability that comes from breaches of customer confidence.

IMPROVE THE CUSTOMER EXPERIENCE

When customers go to an e-commerce site, they have certain expectations. The site should be easy to use and make it easy to find information. It should deliver orders correctly and on time. Expectations of privacy are even more fundamental. Even if a company provides an exemplary customer experience, if a customer's credit card number is stolen because the site was not secure, the best user experience will mean nothing. Recently, for example, an e-commerce software supplier had a vulnerability in its code that allowed hackers to easily key in a string of characters that resulted in the display of the orders customers had purchased at the site.

The e-business marketplace is beginning to realize the critical nature



of building customer relationships that lead to repeat business. Because a victim of a security breach is unlikely to return to a site, such a breach can irrevocably damage the trust and confidence necessary to build long-term relationships.

CREATE NEW DISTRIBUTION CHANNELS

The Web has created the potential for a wide range of partnerships, relationships and connections between companies that can greatly facilitate business operations. For example, organizations are automatically procuring goods and services from their suppliers over the Web; they are using the Web to streamline relationships with their distributors; they are developing business exchanges that allow many buyers in a vertical market to access relevant products from a wide range of suppliers; they are offering online auctions.

And they are coming up with new ways of doing business online every day. One of the more exciting new developments is distributed merchandising. This new distribution channel, which has no counterpart in the brick and mortar world, is extremely convenient. Customers can make purchases by simply clicking on a banner ad served up to them on any site they visit, without having to go to the web site of the company offering the product. This channel is attractive to marketers because they can use it to implement targeted marketing campaigns, then make it easy for customers to make impulse purchases of promoted items.

For these exciting new ways of doing business to achieve their maximum potential, organizations need security that extends to all points of contact. As new channels become available, organizations need to ensure that these channels are appropriately secured as well.

The Impact of Poor Security

While effective security can enable companies to establish the sound practices necessary for trusted business relationships, in the race to bring products, services or sites to the e-marketplace, many organizations continue to rush to market and neglect security. As a large number of high-profile cases have demonstrated, such neglect can be a big mistake. Lack of adequate security is increasingly causing problems that include denial-of-service attacks, breaches of privacy, lawsuits and the erosion of customer trust.

DENIAL OF SERVICE

A number of recent high-profile security breaches have involved denial-of-service attacks. These attacks have caused outages on sites such as Yahoo, buy.com, and eBay. When such attacks occur, availability can drop from 95 to 98 percent to as low as 0 percent, making it impossible for customers to get through to a site.⁶

For companies whose only link to the outside world is their web site, such outages mean lost revenues and lost opportunities, because customers cannot make their intended purchases.



The inconvenience can also damage customer relationships or cause customers to go to competitors that are just a click away in the online world.

The damage from these attacks can even extend to the financial markets. eBay, Yahoo and buy.com stocks all lost significant value immediately following their denial-of-service attacks. Yahoo lost 15 percent, eBay had a 24 percent decline in stock price and buy.com stock lost 44 percent of its value.

BREACHES OF CONSUMER CONFIDENCE

Security breaches can also compromise consumer confidence. Research indicates that wary consumers are choosing not to make purchases online, resulting in revenue losses estimated at \$2.8 billion in 1999. Many e-commerce companies collect information about their customers in order to provide personalized service. This information can also be susceptible to unintended access. Following are a few recent examples of how software breaches on the net reveal consumer account information and credit card numbers:

✎ 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 could 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 was, the file should be encrypted. Initial evaluation suggested that the weakness affected from several

hundred to as many as thousands of e-commerce sites where the software installations were performed improperly.⁷

✎ In another recent case, in December 1999, CD Universe customers were shocked when a Russian hacker calling himself Maxus accessed the CD distribution company’s customer credit-card database. The criminal 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, he 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.⁸

✎ A thief who ran a packet sniffer to capture 100,000 credit card numbers from a dozen on-line commerce sites was arrested in May 1997, when he tried to sell the numbers to the FBI for \$260,000.⁹

✎ In 1998, an employee of a Japanese bank offered to sell detailed customer records to a mailing-list company. Fortunately, that firm immediately contacted the bank, and the scam was stopped.¹⁰

✎ Barclays, one of the UK’s biggest Internet bank services was forced offline for nearly four hours in August 2000, when four customers reported they were able to view other customer’s account details. The bank insisted that despite being able to see these details, it was impossible to carry out transactions using these accounts, and in fact no customer lost money because of the incident. Later in the month Barclay’s suffered another embarrassing incident when it was discovered that after logging out of the online service, an account could



be immediately reaccessed using the “back” button on a web browser. If a customer accessed his Barclays account on a public terminal, the next user could use this method to view the banking details. According to the bank, when customers join the online banking service they are given a booklet that tells them to clear the cache to prevent this from happening. However, that procedure effectively shifts the responsibility for security to the end user.

LOST BUSINESS AND THIRD-PARTY LIABILITY

Lack of security not only has a negative impact on the company whose web site is not adequately protected, it can also affect other companies as well. For example, breaches of security and trust at one company in a market segment can make consumers wary of doing business with any company that operates in that market niche.

More serious are hackers’ denial-of-service attacks in which they take over unprotected PCs at one or more unprotected sites and then use those machines to bombard a targeted site with requests for access. The resulting overload can cause the targeted site to shut down. When such attacks occur, the targeted site pays a price because other sites did not maintain adequate security. Although no lawsuits have been filed so far, it is reasonable to expect that someone will eventually charge organizations operating such unsecured sites with negligence. Indeed, the unprotected site is more likely to be the target of such litigation than the hackers that initiated the attack because such organizations usually have much deeper pockets.

Recent court cases indicate that demonstrating that an organization has in fact created a security policy can furnish some protection from lawsuits. In the Caremark case, hackers broke into the company’s business systems and stole critical information. Publicity regarding the break-in adversely affected stock prices. As a result, claiming that the officers should have employed better protections to safeguard company assets, shareholders attempted to sue Caremark officers and directors individually for fraudulent theft from the company. In this case, the court ruled that because the company had assessed the problem beforehand, set up a security team and prioritized the company’s response—in other words, had set up a due diligence framework for security—the officers should not face personal liability, even though they were unsuccessful in detecting the particular fraud scheme in question. While this case highlighted the issue of personal liability for corporate officers, it also laid out the framework for corporations to avoid this liability by demonstrating that they had exercised due diligence by setting security policies to protect the company’s assets.

LACK OF CONSUMER TRUST

Perhaps the most ominous detrimental effect that poor security has is its impact on consumer confidence. If poor security practices continue after being discovered, they have the potential to substantially dampen prospects for future e-business growth. Survey after survey confirms that key impediments to increased consumer use of online purchasing are fears of losing control over credit card numbers and loss of privacy.



Furthermore, a security breach can reduce the value of a company's brand. According to Alan Greenspan, Chairman of the U.S. Federal Reserve Bank, a company's reputation, or its brand, has become even more important in our information-driven economy: "In today's world, where ideas are increasingly displacing the physical in the production of economic value, competition for reputation becomes a significant driving force—propelling our economy forward. Manufactured goods often can be evaluated before the completion of the transaction. Service providers, on the other hand, usually can offer only their reputations."

In a Rockbridge Associates' study conducted over a two-year period of 1,001 consumers selected at random, most respondents expressed suspicion about the security of online transactions: 58 percent do not consider any financial transaction online to be safe; 67 percent are not confident in conducting business with a company that can only be reached online; 77 percent think it is unsafe to provide a credit card number over the computer; and 87 percent want e-commerce transactions confirmed in writing.¹¹

A December 1999 survey by the e-commerce firm CyberSource of 100 online merchants reported that 75 percent of the respondents rated credit-card fraud as "a concern," but only 59 percent 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.¹²

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 information will be misused or stolen is cited as the main reason 74 percent 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 percent are "very concerned" about the security of databases holding their credit-card information; 57 percent believe that credit card data can be easily used for unauthorized transactions; and 54 percent think their credit card data can be intercepted in transit by hackers.¹³



A Security Checklist

Securing your e-business operations is vital to protecting the value your site already has and to creating additional value for your organization. But, security is only useful if you implement the right measures for your application. It is a common error for a business owner to look to other business models for guidance on security architecture. Doing so often results in wrong assumptions about appropriate implementations of technology to support the security needs for the owner's specific business. For example, an organization may erroneously believe that Secure Sockets Layer (SSL) security, which comes built in on most popular Web browsers, will protect them. SSL security may be adequate for financial services organization where customers send information to the financial services institution, which in turn processes those transactions exclusively using their internal systems, but it can be completely inadequate in applications where business partners exchange information in on-going sessions.

In reality, there are many different security requirements for different types of applications. Therefore, it is important to understand how to properly implement an appropriate security system. The following checklist is useful as a quick e-business security "health screen" before launching into business on the Web.

1. **Policies and Awareness.** Are the policies complete, and do they actually affect employee behavior? In e-business, network connections are made between firms every day as part of the dynamic nature of the "business Web." Who is authorizing those

connections? What is the security of the company at the other end of the link? How do you check? Just as important, is the connection terminated when the business need for it no longer exists?

2. **Organizational Roles and Responsibilities.** Who in the company is responsible for e-commerce security? Shared accountability can be tantamount to *no* accountability unless clear governance structures and defined roles and responsibilities are in place to ensure that every organization understands how it contributes to the overall security posture of a firm.
3. **Audits, Reviews and Periodic Self-Assessments.** Routine health checks are necessary to maintain existing security measures. They also help determine whether the threat or risk level is changing, requiring adjustments in policies and implementation of security controls. How frequently are hardware, software and data controls assessed on existing systems? How are new systems tested before they go online?
4. **Physical Security of E-Systems.** Logical controls can be rendered useless if someone can come in and physically tamper with a machine, causing configuration changes that affect security or, even, worse, outages. Who has access to systems during nonworking hours?
5. **Network and Client/Server Security.** Are guidelines for the appropriate configuration of IT infrastructure components



documented and used throughout the company? A set of baseline controls for implementing information security for all components of information systems should be implemented consistently.

6. **User ID and Authentication.**

Are users assigned strong passwords? As an average, based on AtomicTangerine's research, about 30% of user-chosen passwords are easily cracked, allowing unauthorized and often unlimited use to IT resources. Are your password files secure? Often implementation of file systems allow hackers to export the password file to their own machine without ever breaking into the system. Once the password file is obtained in this fashion, it can be cracked at leisure, and away from the detection of the victim organization. An even better alternative to passwords is the use of one-time secure tokens to replace passwords or biometric techniques such as fingerprint, voice prints and iris scanning.

7. **Backup and Recovery.** If your file system is corrupted, can you recover? Are backups made for all file systems, not just mainframes? Are user data on laptops backed up? Mid-range systems, especially UNIX machines, are frequently updated by administrators with special utilities and patches—is this information documented in case the system has to be rebuilt (which will be required if the system is compromised by a hacker)?

8. **System Development.** Security is best when it is built in, and not an afterthought. Do your design standards for web applications and back-end integration projects include guidance on good security techniques? Does the software development methodology include



appropriate linkages to security design?



Conclusion

Information security is rapidly emerging as critical in protecting company value, and invaluable in creating *new* value for companies. “Institutionalizing” the security practices and techniques in companies can go a long way toward positioning a firm to compete effectively in the Internet marketspace by ensuring business partner and customer confidence, as well as enabling them to move quickly to seize Internet-based

business opportunities. Business strategies now require an “information security point of view” to ensure that opportunities for value creation are not overlooked or assumed to be too risky. Those companies that learn to leverage this new value creation opportunity will find information security can result in a competitive advantage in consumer confidence, trading partner trust and brand value.

Notes

- ¹ Vizard, M. FROM THE EDITOR IN CHIEF: In e-business, as in war, the edge goes to those who have the best technology. *InfoWorld* 22(i11):97 (March 13, 2000)
- ² Lammers, D. Bones and e-commerce. *Electronic Engineering Times*, 26 (September 6, 1999)
- ³ Ledwith, S. Internet crime causes problems for law enforcers. Reuters news wire RTir 9:38 PM GMT (December 7, 1999)
- ⁴ Kappelman, L. A. 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*, 150 (March 20, 2000)
- ⁵ Bear Stearns, “The Internet Business-to-Business Report” (September 1999)
- ⁶ Harrison, A. Cyberassaults hit Buy.com, eBay, CNN and Amazon. *ComputerWorld* (February 9, 2000)
- ⁷ Wilson, J Shopping Software May Be Flawed. Associated Press newswire 06:48 PM ET (April 22, 1999)
- ⁸ Smetannikov, M. and L. Trager. Credit-card fraud hits Web. *Inter@ctive Week* 7(i2):8 (January 17, 2000)
- ⁹ *New York Times* (May 23, 1997)
- ¹⁰ *RISKS FORUM DIGEST* 19(53): <
<http://catless.ncl.ac.uk/Risks/19.53.html#subj3> >
- ¹¹ *E-Commerce Times Online* (June 21, 1999)
- ¹² Dennis, S. Internet Fraud a Growing Concern to Online Merchants. *Newsbytes* (December 6, 1999)
- ¹³ Hamilton, T. Web sales stunted by security fears - survey - 84% of web users worry when personal information goes on-line. *Toronto Globe and Mail* (April 27, 2000).

