December 2001

Security in Today's E-World

Manjari Mehta
University of Houston

Beena George
University of Houston

SECURITY IN TODAY'S E-WORLD

Manjari Mehta
University of Houston
Mcmehta@mail.uh.edu

Beena George
University of Houston
Bgeorge@uh.edu

Abstract

This paper applies an existing security model from IS research to the current e-commerce environment (a) to assess whether the model represents the risk components and (b) to identify the threats in today's e-commerce arena. Using data from a web-survey, this paper compares the changes in threats in the networked environment before 1992, with the current environment. Our findings indicate that (a) no major changes are required to improve the existing model and (b) viruses and system penetration by hackers are perceived to be the two most severe threats to an organization.

Introduction

Security has long been a concern of Information Systems (IS) managers. However, reports of serious security breaches have become more frequent in today's networked environment. In the most recent CSI/FBI (Computer Security Institute/Federal Bureau of Investigation) Computer Crime and Security Survey (Power, 2000), 70% of the respondents from US corporations and government agencies reported that they had experienced unauthorized use of computer systems. The most serious dollar losses involved theft of proprietary information ($66,708,000) and financial fraud ($55,996,000). In February 2000, eBay, Amazon and CNN were attacked – each suffered loss of several million dollars in just the couple of hours their web sites were down. The number of credit card thefts totaled to 809,000 – resulting in losses in excess of a 100 million dollars in year 2000 alone. Denial of service attacks on web sites and modification of information by email viruses have had a direct impact on productivity – and consequently, on the bottomline (Hazari, 2000).

In an economy where an increasing number of business transactions and monetary transfers occur via the Internet, it is imperative that the business environment be safe and conducive to these new forms of transactions. Security management problems stem from the need to balance two conflicting goals: (a) providing information and information services to as many and as fast as possible - the e-commerce goal and (b) ensuring confidentiality, integrity and availability of information and information systems - the goal of security.

The purpose of this paper is to describe a model that provides an overview of the threats to security in today's E-World – the Internet enabled business environment. The next (i.e., second) section examines security models from previous IS research, along with the context in which they were built, in an effort to identify models that provide an overview of today's security threats to IS. The third and fourth sections (a) trace the evolution of e-commerce and (b) explore the current e-commerce environment to determine whether the threats have changed since introduction of the World Wide Web in 1992. The fifth section discusses whether an existing security model can accommodate these changes and presents the results of a web-based survey designed to identify security threats in today's E-World in an effort to recognize the new challenges face those responsible for IS security. The final section discusses the implications of our survey and proposes a possible redesign to combine the existing models covering the aspects of security that have recently developed as a result of e-commerce activities.

Security Models Revisited

Different researchers have examined different aspects of security; some have focused on security breaches, some on their far-reaching consequences, some on security measures and some have provided a comprehensive overview of all these aspects. Articles on IS security appearing in leading IS journals (*MIS Quarterly*, *Information Systems Research* and *Journal of MIS*), and the *Computers & Security* journal in the past fifteen years were reviewed to identify the security models proposed during these years.

Gallegos and Wright (1988) classified threats[1] based on the affected environment (database, CPU, communication links) and the source of the threat (operator, natural disasters, application programmer, terminal user, systems programmer, hacker). Straub and Nance (1990) discussed methods to detect and discipline computer abuse. Goodhue and Straub (1991) studied the perceptions of managers about the security controls installed in their organizations to test hypotheses that a user's concern for security depends on industry risk, company actions and individual awareness; of which the latter two were found to be statistically significant. Straub and Welke (1998) suggest a security action cycle to mitigate systems risk, which involves four sequential activities: deterrence, prevention, detection, and recovery. They postulate the use of a security risk planning model to match security risk with appropriately prioritized security controls.

Wood (1988) stressed the need for the endorsement of security planning by senior management and emphasized that "the inadequate information security models, the reactive and incremental improvement approaches used to address security, the information overload, and insufficient staffing and resources are all symptoms of a most serious problem." Cole (1990) described a security model in the context of open distributed computer systems as proposed by the European Computer Manufacturers Association and recognized "security information as the basis for propagating trust and security knowledge around a distributed system." Ekenberg et al (1995) took an object-oriented approach and presented a model to estimate the costs of risks and losses due to accidental or deliberate disclosure, transfer, delay, modification, or destruction of information. Schwartau (1998) proposed the Time-Based Security Model (TBS) and employed a process methodology to (a) quantifiably test and measure the effectiveness of security in inter-enterprise environments and (b) make informed security budget decisions.

Ryan and Bordoloi (1997) evaluated the security threats in mainframe and client-server environments and suggest that organizations need more preparedness against the threats of viruses, inadequate logon security and backup files, and uncontrolled access. Cohen et al (1997a, 1997b) charted an elaborate set of security attack and defense mechanisms in two separate articles. In the E-commerce environment specifically, Ratnasingham (1997) found that existing Electronic Data Interchange (EDI) security was inadequate in most organizations. Zviran and Haga (1999) addressed the gap in evaluating the characteristics of real-life passwords and investigate the core characteristics of user-generated passwords and associations among those characteristics. Furnell and Warren (1999) studied problems posed by hackers and "cyber terrorists" and the nature of the responses necessary to preserve the future security of society.

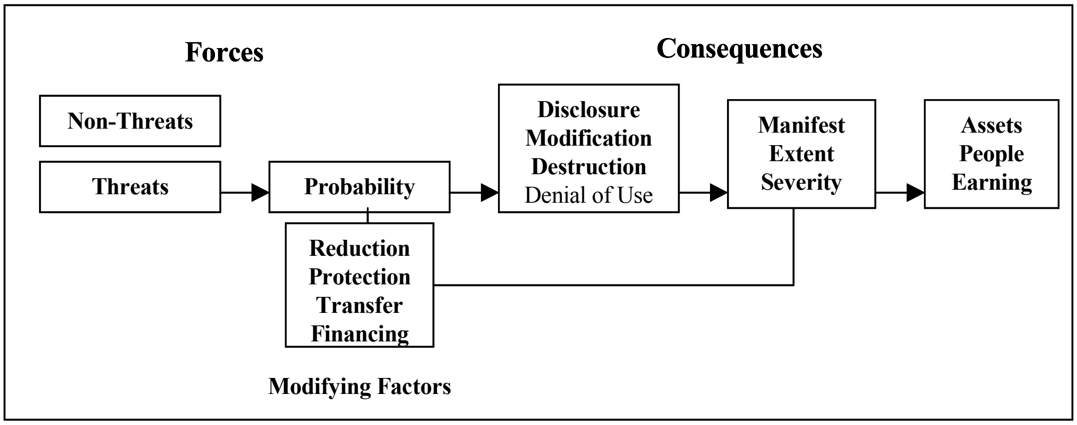

Figure 1. "The Components of Risk" – Model 1 (from Loch et. al, 1992)

Loch et al (1992) build on Crockford's (1980) risk management model and identify security concerns of MIS executives in both standalone and networked environments. These concerns are divided into five major components: forces (threats and non-threats), probability, modifying factors, consequences and resources that are affected due to the manifestations of the threats (see Figure 1). Multiple 'forces' exert influence on an organization; 'threats' constitute a broad range of forces capable of producing adverse consequences. 'Modifying factors' are the internal and external factors that influence the probability of a threat becoming a reality or the severity of the extent of the threat when it does become a reality. 'Transfer' denotes "contractual conditions that require the other party to give indemnity against certain types of liability or loss" whereas 'financing' means "insurance against some categories of risks". Based on Crockford's definitions, 'consequences' are the ways a realized threat impacts resources like the organizations' assets, people or earnings. Loch et al's model (henceforth referred to as **Model 1**) does not consider the possibility of consequences affecting the threats in the form of a return loop to model the situation wherein a

[1] Threat: Any potential event or act that could cause one or more of the following to occur; unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental. (Threats and Risk Assessment Working Guide, Government of Canada).

consequence of today becomes a threat tomorrow. For example, the consequence of telecom eavesdropping today could be feared as a threat tomorrow – and deterrents can be set up in anticipation of the threat of eavesdropping.

Cohen et al (1998) build a framework (henceforth referred to as **Model 2**) that is similar in many aspects to Loch et al's model. This framework represents a breach of security as a process in which actors perpetrate the causes (threats) using mechanisms (attacks) to produce effects (consequences). The main difference between Models 1 and 2 is the notion of attack mechanisms,[2] explicitly considered by Cohen et al. (see figure 2).

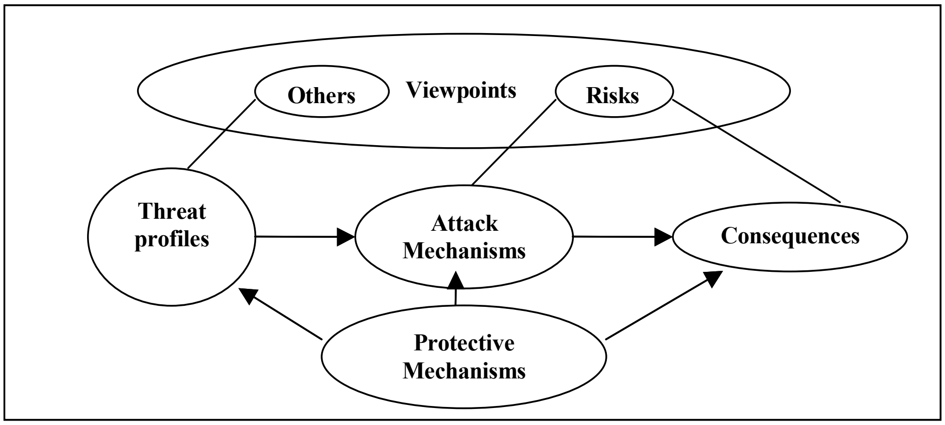

Figure 2. The Cause and Effect Model – Model 2 (from Cohen et al, 1998)

Both Models 1 and 2 clearly depict the following common-sense notion: **if** a set of assets is of high value to an organization **and if** the likelihood of a threat occurring is high **and if** there is vulnerability that can be very easily exploited by the threat **then** the level of risk is high (Ciechanowicz 1997). If the risk is high, then it is likely that threats will manifest themselves in the form of attacks, which in turn will have serious consequences to the assets of the organization. Taken together, these models consider the following aspects of IS security: threats, attack mechanisms, consequences, defense mechanisms and security measures. Thus we believe that these models can help us understand the nature of security threats in an e-commerce context.

Evolution of E-Commerce

During the 1970s the first networks like ARPANet and Usenet were established and banks began to use Electronic Funds Transfer (EFT) over secure private networks (See Figure 3).

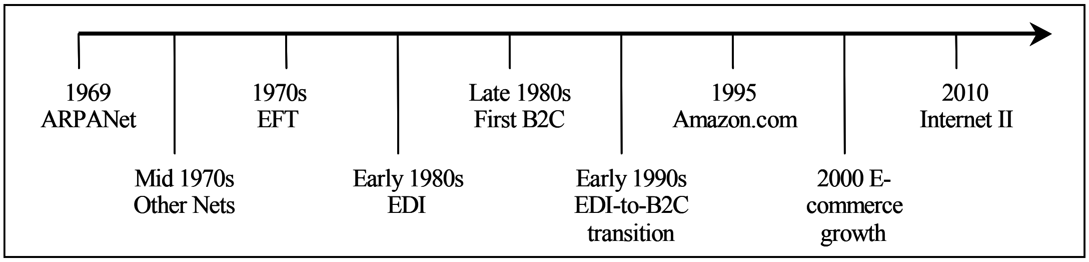

Figure 3. Evolution of E-Commerce

This led to the creation of direct-deposits and debit-cards. With the advent of email and EDI, ANSI proposed standards for EDI and EFT in the early 1980s, other organizations also began to endorse the first generation of e-commerce. "Around the late 1980s, e-commerce became an integral part of organizations, although not over the public Internet" (Trepper, 2000). Then in 1989, the newborn Internet provided new but difficult to use e-commerce technology. At this time, only people who knew the technology could use it. The technological implementation of security controls was also not as sophisticated as it is today. Soon after the World Wide Web arrived in 1992, organizations discovered that graphics-based technology had become easier to use for information publishing and dissemination. Meanwhile, the costs began to steadily decrease, making it easier for small businesses to put their business on the Web. Larger (even international) audiences could now be reached with very little technological investment (Trepper, 2000). It was then that organizations tested the e-commerce concept by putting up electronic storefronts and seriously considering standardization, security and privacy issues for the first time.

[2] An attack mechanism is the means for realization of a threat (Cohen et. al., 1998).

> “The growth from the Internet to Intranets to Extranets has been exponential in the past 5 years. The 3 C’s of first generation e-commerce: Content, Community, and Commerce have now evolved into the 7 C’s of second generation e-commerce: Content (e.g. Yahoo), Community (e.g., Ivillage), Commerce (e.g., Amazon, with a first-mover-advantage), Communication (e.g., Doubleclick), Connectivity (e.g., Cisco), Collaboration (e.g., Mercata), and Customization (e.g., Netperceptions), (Hazari, 2000). Each of these C’s reflects an evolution of features - from those that were characteristic of automated processes to those that extended externally to other consumers as well as business partners.” (Hazari, 2000) "Historically, information security was meant to protect and confine information. Now, the emphasis is on making sure the information is correct, or authentic, and timely” (Burnham, 1999).

Business Models

The first generation of e-commerce tried and tested the B2C (Business to Consumer) models, followed by the second-generation arrival of B2B (Business to Business) and Click-and-Mortar models. “B2B models provide advantages of integration and communication with partners and suppliers and Click-and-Mortar models take advantage of offline and online channels being established in physical store locations but at the same time offering online commerce convenience” (Hazari, 2000). The traditional model of Manufacturer-to-Wholesaler/Distributor-to-Retailer-to-User is being dis-intermediated by the new ‘Dell’ Model directly linking the manufacturer and the end user. Kalakota and Whinston (1996) list four different applications of technology that converge to create the discipline of e-commerce: (a) collaborative work through email and the corporate digital library (b) electronic document exchange using EDI (c) electronic funds transfer and d) marketing and customer support through electronic publishing.

With new business models emerging (e.g., Priceline), companies must balance experimentation with risk-taking to achieve optimum efficiencies. A new way of presenting information to customers over a digital medium has also required companies to re-think ways of keeping customers loyal since competitors are now only one click away. In the 1970s and 1980s, technological development was unable to support the implementation of direct marketing. Gradually database technology became robust enough to help automate specific marketing and management tasks. In the late 1980s and early 1990s, this led to target marketing shops having many custom-made, disparate products. None of these applications shared customer data or corporate data. Only recently have the marketer and manager been able to use different applications and yet readily share the same customer and corporate data (Visionchain). Better still, it is now possible to have enterprise-wide integrated applications that allow sharing of data.

Another strategy for companies that have electronic storefronts and a physical location has been the merging of two models (click-and-mortar), where a customer places an order on a web site and then picks up the product at the store (Hazari, 2000). Only companies successful in leveraging the various opportunities that e-commerce presents will maintain a competitive edge.

As e-commerce evolves more and more channels of delivery will emerge. However, with the increase in these channels of communication, the vulnerability of the communication system has also increased since more points-of-attacks are now possible. For example, when there was no email, there was no possibility of spoofing, wherein emails could be interrupted, scanned for confidential data and information could be modified, destroyed, or stolen. Thus, with every evolving business model, new vulnerability zones arise, and with new technological advances, new ways to realize security threats in forms of attack mechanisms are discovered.

Security Threats and Attacks to the Evolving E-Commerce Activity

This section considers some frequent security problems and maps each to the components of Model 1. These security problems were identified through a survey of last three years’ issues of trade journals like *Computer World* and *Infoworld.* Examples of security threats in today’s E-World appear in Table 1. The impacts of these threats constitute the “consequences” described in Model 1.

To accommodate the changes that have occurred both in the business and the technological environment and to strengthen Model 1, a few suggestions are made. For instance, email harassment or spamming have adverse effects not on the information or information system per se, but on the people in the organizations. The definition of “consequences” in Model 1 should be broadened to include adverse effects not only on information and information systems but also on people. The theft of information (e.g., credit card information) that compromises the confidentiality of information can also be considered a kind of “disclosure” of information – to sell the information to another party or to blackmail the victim organization. Thus, the definition of the term ‘disclosure’ also needs to be extended to explain the theft of information. Similarly, ‘delay’ can be seen as a temporary ‘denial of use’ and could be classified in this category. With respect to the ‘modifying factors’ such as ‘financing’ and ‘transfer’, it is understood that they do *not* modify the probability, manifestation, extent, or severity of any threats directly. They save a firm from potential financial losses but (unlike 'prevention' and 'detection') not from the actualization of threats. Thus, the 'modifying factors' can be redefined to classify 'prevention' and 'detection' differently from 'financing' and 'transfer.'

Table 1. Threats and Consequences in the Current Environment

Examples	Consequences mentioned in the Loch et. al. and Cohen's Security Models
1. A vandal might alter the design of web page. (like the New York Times suffered in Feb, 2001)	1. Modification of information. Potential earnings are lost.
2. A saboteur might erase R&D data or paralyze networks, and an industrial spy might copy trade secrets.	2. Destruction or Denial of Service and disclosure of information.
3. A blackmailer might plant a digital bomb and threaten to trash systems unless payment is made.	3. Destruction of information and information systems.
4. In January '98, in Europe's first case of electronic bank blackmail, the German Verbraucherbank offered a USD5,300 reward for information on a hacker who was blackmailing the bank by releasing the customer account information on the Internet.	4. Disclosure of information.
5. Internal hacking cost UK organizations £1.5 billion in the six years from 1992, with 70% of all hacking incidents being internal (Department of Trade and Industry).	5. Denial of Use, Destruction, Modification or Disclosure of information.
6. Virus: A survey shows that virus incidents have increased by 48% in 1997, despite more anti-virus software in place.	6. Destruction or modification of information.
7. Software piracy	7. Disclosure of information.
8. A customer, a trader, or a hacker may perpetrate credit card abuse. Hackers may intercept or steal information and thereby obtain valid credit card numbers of others.	8. Disclosure of information. Vulnerability: networked environment; casual security; and failure to update security procedures.
9. Innocent users may receive some unpleasant material such as threatening, obscene or hateful email repeatedly.	9. Denial of use (in a way, since the email harassment would interrupt operations)
10. In November 2000, the Swiss Bank accidentally posted prominent clients' information on a public Internet site.	10. Disclosure of information. Threat: Human Error. Channel: web site (E-world channel)

To assess security threats in today's E-World, a web-based survey[3] was conducted of senior IS managers and leaders of 30 large-multinational organizations. The respondents were presented with a list of 16 threats obtained from recent published surveys and other media reports and asked to rank order these threats in terms of the severity of their manifestations and their consequences by assigning each a score from 1 to 100.

Not surprisingly, the results of the survey show that a majority (78%) of the respondents consider security to be a major concern in their organizations. Virus and system penetration by outsiders (e.g., hacking/espionage) were perceived as the most serious threats with mean ratings of 65 and 63 respectively. Natural hazards (33) and repudiation (34) ranked the lowest. An unusual concern not spotted in previous survey results was the perception that fictitious people/impersonators (58) now constitute serious security threats (see Table 2).

Loch et al (1992) also conducted a survey to identify the most serious threats to organizations in mainframe, microcomputer and networked environments. Examining results from the Loch et al survey (1992), the following threats rank the most serious in a network environment: natural disasters, inadequate control over media, weak/ineffective controls, hacking and access to system by competitors (see Table 2). This implies that prior to Loch et al's survey in 1992 (i.e., during the first generation of e-commerce) the threats perceived to be the *most* serious were different from those faced in today's E-World. For instance, in 1992, natural hazards ranked as the most severe threat in both networked and mainframe environments. Today, they are perceived to be of least concern to organizations. It is apparent that organizations have been able to mitigate this threat by establishing mirror sites and stand-by servers at different geographical locations and improving physical security. Also, the respondents from that

[3] Survey available on request from authors.

survey cited weak and ineffective controls as a 'threat.' In fact, lack of effective controls is a vulnerability[4] since it increases the probability of a threat event (like hacking) occurring. Loch et. al.'s (1992) finding that weak and ineffective controls were a threat implies that people *were* aware of security controls in place in their organizations, but thought that they were not sophisticated enough. On the other hand, the results of our survey suggest that such technological sophistication is not lacking today and that most people do not believe that current security controls are ineffective.

Table 2. Perceived Security Threats Comparison: 1992 versus 2001

Most severe threats in a networked environment in 1992 (Loch et. al.)	**Most severe threats in 2001 (Our web-survey results)**
1. Natural Hazards 2. Inadequate control over media 3. Weak and Ineffective Controls 4. Hacking 5. Access to system by competitors	1. Viruses 2. System penetration: Hacking/ Espionage 3. Fictitious people/Perpetrators 4. Denial of Service 5. Insider abuse of net access 6. Unauthorized access by insiders 7. Credit card fraud 8. Human Error 9. Infringement of intellectual property rights 10. Spoofing 11. Implied trust exploitation 12. Active Wiretap 13. Sabotage 14. Telecom Eavesdropping 15. Repudiation 16. Natural Hazards

Our survey results also allow threats to be categorized based on the agreement of the respondents regarding the severity of the threats. Sorting threats based on their standard deviation being higher or lower than the mean of standard deviations allows classification of the threats into the four groups that appear in Table 3. The results suggest that viruses, denial of service, insider abuse of net access, unauthorized access by insiders and human error require a proactive, long-term focus.

Table 3. Agreement on Severity of Threats

Low level of agreement among respondents	Implied Trust Exploitation, Active Wiretap, Sabotage	System Penetration: Hacking/ Espionage, Fictitious People/ Impersonators, Credit Card Fraud, Infringement of Intellectual Property Rights, Spoofing
High level of agreement among respondents	Natural Hazards, Repudiation, Telecom Eavesdropping	Viruses, Denial of Service, Insider abuse of Net Access, Unauthorized access by insiders, Human Error
	Less severe Threats	More Severe Threats

Recent surveys on IS security support our findings. In a survey conducted by CSI/FBI in 2000, respondents listed the following threats resulting in the most serious financial losses: viruses (70%), net abuse (45%), laptop theft (45%), denial of service (21%) and unauthorized access (16%). The consequences of all the above-mentioned threats can be included in the categories identified by Loch et al (1992).

[4] Vulnerability is a quantifiable, threat-independent attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability and/or integrity, or increase the severity of the effects of a threat if it occurs. (Threats and Risk Assessment Working Guide, Government of Canada).

Discussion and Conclusions

This paper demonstrates the applicability of security models from previous IS research in today's E- world. A comparative study has been conducted to identify differences in the perceived severity of threats to IS today versus that of ten years ago. The findings suggest that viruses and system penetration by hackers are perceived to be the two most severe threats to an organization today as compared to natural hazards and weak and ineffective controls ten years ago.

A possible redesign of Model 1 would be to explicitly incorporate the 'attack mechanism' component of Model 2 (see Figure 4, see after the references). In addition, delay of information and harassment of people have been added to the set of 'consequences.' The remainder of the model is the same as that depicted in Figure 1.

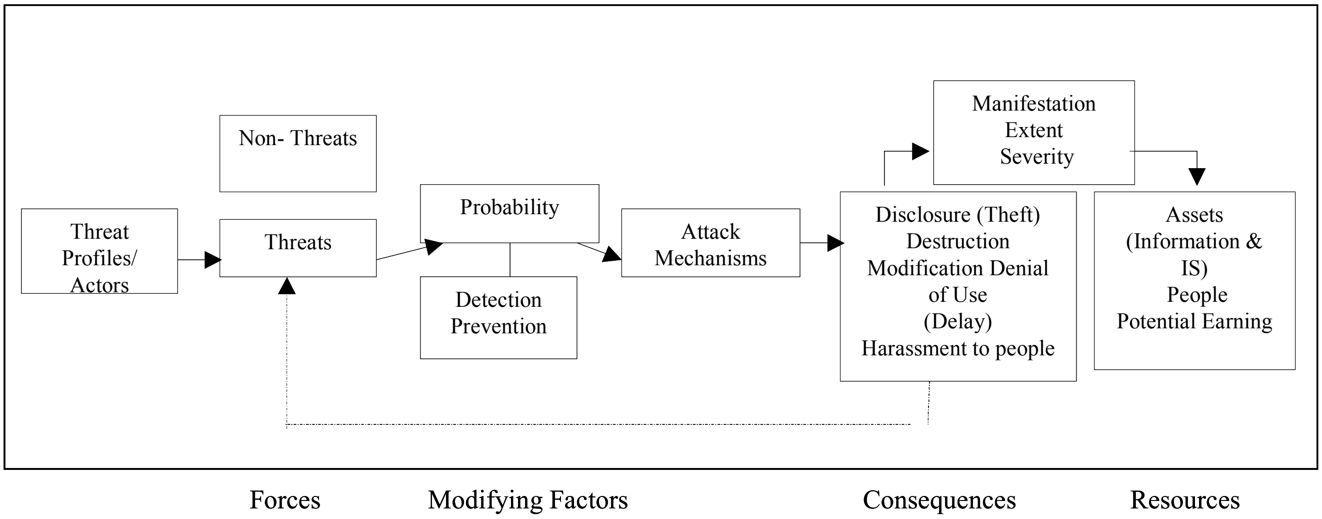

Figure 4. 'Attack Mechanisms'- A Possible Addition to the Loch et al's Model

Threats can only manifest themselves in the form of some attack mechanisms, which is not explicitly mentioned in the Loch et. al. (1992) model. For the examples discussed in Table 1, we find that threats that existed ten years ago are realized in *different ways* today. In fact, it is the attack mechanisms that *have* changed over the past decade, since it is the changing technology that is employed in realizing these attacks. The probability of certain security threats (e.g., credit card fraud) has increased because of changes in technology and eventually because of the way business harnesses technology. Thus, it would be a mistake to consider technology a "black box" - it has a major impact on the way concepts (threats) are realized (via attacks). Again, the examples in Table 1 point to an obvious conclusion – the "*extent*" of the consequences has magnified manifold - the Internet has provided a vast audience for businesses, but made the businesses vulnerable to unprecedented attacks at the same time.

Both Loch et al (1992) and Cohen et al (1998) models allow us to traverse back and reason the threats, attacks, and the perpetrators, given a set of consequences and then determine the right security controls in advance. In addition, it would also be interesting to include in Loch et al's model the possibility of consequences affecting the threats in the form of a return loop, to represent the situation wherein a consequence of today becomes a threat tomorrow.

Together, these two models allow us to study the dimensions of information systems security by reducing the details of a more specific model and describing the exact nature of these dimensions to a reasonable extent. In conclusion, we believe that the models proposed by Loch et al in 1992 and Cohen in 1998 give a comprehensive overview of the issue of security – even in today's E-World.

References

Boncella R, "Web Security for e-commerce", *Communications of the AIS* (4), 2000

Cheng, H.K., Sims, R.R. and Teegen, H. "To purchase or to pirate software: An empirical study," *Journal of Management Information Systems* (13:4), 1997, pp. 49-60.

Cole, R. "A Model for Security in Distributed Systems," *Computers & Security* (9:4), 1990, pp. 319-330.

Ciechanowicz, Z. "Risk analysis: Requirements, conflicts and problems," *Computers & Security* (16:3), 1997, pp. 223-232.

Cohen, F. "Information system attacks: A preliminary classification scheme," *Computers & Security* (16:1), 1997a, pp. 29-46.

Cohen, F. "Information system defenses: A preliminary classification scheme," *Computers & Security* (16:2), 1997b, pp. 94-114.

Cohen, F., Phillips, C., Swiler, L.P., Gaylor, T., Leary P., Rupley F., and Isler R. "A cause and effect model of attacks on Information systems," *Computers & Security* (17:3), 1998, pp. 211-221.

Ekenberg, L., Oberoi, S. and Orci, I. "A cost model for managing information security hazards," *Computers & Security* (14:8), 1995, pp. 707-717.

Furnell, S. M. and Warren, M. J. "Computer hacking and cyber terrorism: The real threats in the new millennium?," *Computers & Security* (18:1), 1999, pp. 28-34.

Gopal, R. D. and Sanders, G. L. "Preventive and deterrent controls for software piracy," *Journal of Management Information Systems* (13:4), 1997, pp. 29-47.

Hazari, S. I. “The evolution of e-commerce in Internet time”, 2000

Lee, J.A.N., Segal, G and Steier, R. "Positive Alternatives: A Report on an ACM Panel on Hacking," *Communications of the ACM*, April 1986, pp. 297-299.

Kalakota, R. and Whinston A. B. “Frontiers of e-commerce”, Addison-Wesley, 1996.

Loch, K.D., Carr, Houston H. and Warkentin, M.E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, June 1992, pp. 173-186.

Loch, K.D. and Conger, S. "Evaluating Ethical Decision Making and Computer Use (1)," *Communications of the ACM* (39:7), 1996, pp. 74-83.

Power, R. "2000 CSI/FBI Computer Crime and Security Survey", *Computers & Security* (26:2), 2000, pp. 33-49.

Ratnasingham, P. "EDI security - Re-evaluation of controls and its implications on the organizations," *Computers & Security* (16:8), 1997, pp. 650-656.

Ryan, S.D. Bordoloi B. "Evaluating Security Threats in Mainframe and Client/Server Environments," *Information & Management*, February 1997, pp. 137-146.

Schwartau, W. "Time-based security explained: Provable security models and formulas for the practitioner and vendor," *Computers & Security* (17:8), 1998, pp. 693-714.

Straub, D.W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), 1990, pp. 255-276.

Straub, D.W. and Nance, W.D. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), 1990, pp. 45-62.

Straub, D.W. and Welke R. J. "Coping with Systems Risk: Security Planning Models for Management Decision-Making," *MIS Quarterly*, 1998, pp. 441-469.

Threats and Risk Assessment Working Guide, Government of Canada, 1999, pp. 116 –129.

Trepper C. “E-commerce strategies”, Microsoft Press, 2000, pp.11-12.

Wood, C. C. "A Context for Information Systems Security Planning," *Computers & Security* (7:5), 1988, pp. 455-465.

Zviran, M. and Haga, W.J. "Password security: An empirical study," *Journal of Management Information Systems* (15:4), 1999, pp. 161-185.

http://sunil.umd.edu/documents/ecomeval.htm

Visionchain, http://www.visionchain.com/sections/evolve.html

Burnham, *UniSci Science*, 1999