Global Information Assurance Certification Paper

The Evolving Rules of *e*-gagement

Mark LaRocca
SANS Institute
GIAC Security Essentials Certification (GSEC) v1.3
Option - c

The Evolving Rules of *e*-gagement

Mark LaRocca
SANS Institute
GIAC Security Essentials Certification (GSEC) v1.3
Option - c

Table of Contents

The Evolving Rules of *e*-gagement

Mark LaRocca
SANS Institute
GIAC Security Essentials Certification (GSEC) v1.3
Option - c

I. Abstract

Due to the recent devastating security breaches in America and worldwide, we in the security industry have been focusing our attention on answering questions and analyzing what was done in the past, what can be done now, and what should be done to prepare for the future. Our past and current business model of security is comprised of two separate entities the first of which is focused on the physical and the building facility while the second is focused on IT and its networks. This separates two very similar skills that could benefit from working together and, more importantly, creates gaps in security. A synergistic approach would merge the separate securities into a more focused security triad: information security, physical security and personnel security.[*] Using tools from each skill, we can gather more information and gain a bigger, more complete picture of our entire business environment and its intricate labyrinth of people and machines. From the front door to the server room, humans are the common denominator, which we try to keep working securely and safely. The common threads of human denominator and mutually common goals are too large and too closely related to keep these dependent talents separate. The Evolving Rules of *e*-gagement is my introduction to the concept of total security, the blending of skills, personnel, and the tools. Either by combining these two security skills or by working closely together with effective communication, we will be stronger, more diverse and better capable of fighting the continued attacks to our networks, co-workers and businesses than we are now.

This paper is intended to initiate evaluation and consideration for comprehensive security in any size business; it is not the total security Bible. One size does not fit all, nor does one security model or method work for everyone. At a time when business spending is limited but security risk is high, security professionals can still tighten our homes, networks, buildings, cities, states and countries. We must all decide to make a personal commitment to secure our domain of influence. Only then can the wave of successful and committed security spread out to other people and businesses around us and "infect" them with the same

[*] Schwartau, Winn. "Security Synergy." Infosecurity Magazine. November – 2001. URL: http://www.infosecuritymag.com/articles/november01/industry_synergy.shtml (04-December-2001)

commitment to total security.

Mark LaRocca
Option - c

The Evolving Rules of *e*-gagement

II. Introduction

September 11th, 2001, continues to be a defining moment in both physical and information security. Six months past the fact I hate to refer to this catalyst but I must. Although many in the security field had already been advocating stricter and tighter security, this event helped bring it to the forefront of everyone's attention. The security that was once a routine and taken for granted is now being evaluated, investigated, argued, scrutinized, tested, and retested. The agreed goal of this effort is better security. How to achieve better security is the debate, and after the finger pointing I am confident positive changes will be made. The most important step in the security evaluation is to have a realistic look at our current and divided model of security. We do not need to re-invent the wheel, but we must redesign the carriage.

III. September 11th – Security's Time to Learn

One problem is that the solution cannot be defined and executed until we understand how the previous security model failed. With September 11th as a backdrop, from an IT security perspective, several failure points can be directly linked to outdated Policies and Procedures and in particular our three pillars of Availability, Confidentiality and Integrity. Integrity was compromised long before that fateful day. Complete identities had been issued or stolen under false pretenses.[1] All hijackers used multiple aliases and birth dates. One hijacker who lived in Virginia had been apprehended for speeding. His credentials were in order and he was therefore released with a ticket. Well, not exactly in order, the address listed on his driver's license did not exist.[2] In another example, a suspect from September 11th who had a warrant issued for his arrest was stopped and subsequently released. The officer said he did not know of the warrant.[2] When we look at several practices designed to protect air travelers, the picture does not get any better. First let us examine the checkpoint or screening area supervised by the Federal Airport Administration (FAA). Agents at the security point allowed

twenty questionable suspects past their scan. Three of the suspects had direct links to Bin Laden's al-Qaida network; another two of them were on the terrorist watch list which had been created during the previous summer.[1] In addition, US intelligence possessed a videotape of one hijacker and a different suspect in the USS Cole attack.[1] Availability and Integrity collapsed due to a denial of data, even though it was unintended denial. The intended function of the U.S Intelligence and FAA databases were clearly missed. Next, the civilian physical security scans with x-ray and metal detectors allowed box cutters and various other weapons to be carried onto the planes, not just by one individual but by multiple suspects. Although I do not have direct knowledge of the screeners' handbook and policies, I would think the lack of detecting weapons is a failure of policy and procedures. Aboard the planes, the terrorists were allowed to carry out their mission effectively because flight personnel have been trained to go along with the demands of highjackers. Probably such training is based on the theory and belief that passengers' lives could thus be saved. Clearly this is an issue of old, outdated policies and procedures not being under constant review and scrutiny to deal with current times. The objective that lost its way in this case is, "know your enemy". This might need to be taped on doors and monitors for all of us to remember.

It has been said that he who holds the information holds everything. In the case of September 11th, the information was there, though separated and departmentalized. Is this a case of only having outdated policies and procedures? Or of not having access to the correct information? Is the sole cause a failure of proper screening at the physical checkpoint? No. It cannot be blamed on one single cause, one skill of security, or one department. Although these are serious problems that deserve attention, I see it as the continued use and repair of an old outdated security model. Why would these seemingly related and dependent skills be separate? Suppose that these separate areas were combined into one cohesive unit, with real-time communication, and a sharing of skills and information. Could such communication or security model have stopped this specific security breach? Who can say for sure, but at the very least, it would have provided a good chance to stop such a series of events. After all, non-computing security is as important a component of IT security as computer based security. The two are dependent upon each other; truly, one cannot exist without the other.

IV. Physical or Non-Computing Security

Non-computing security is defined as, "… safe guards which do not use the hardware, software and firmware of the IT. They include physical security, personnel security, and procedural security."[3] These safe guards of non-computing security could implement the use of but not be limited to "chip cards" (covers smart and memory cards), PIN entry access, cameras, biometrics, design theory and trained personnel to enforce all the various policy and procedures for the

company. Many more options are and will continue to become available as time passes. Some of these options require little more than extra planning, while others have hard costs and provide many other options.

Physical Security-Hardware

Biometrics (scan recognition of fingerprints, facial features, hands, eyes, body, etc.) has the attention and admiration of many, even if it might not be a reasonable security option for them currently. Biometrics also has its share of doubters who raise some important issues. One such issue is the safety and storage of the database that the actual biometric hardware will access. Plenty of personal information will be stored on these databases. What if they could also be accessed, copied, stolen and sold to the highest bidder? From what we have learned about database management under government and private authority already, we can conclude this is a valid concern. Given current conditions, could we really assume that Availability, Integrity and Confidentiality of these databases would be any better? For anyone who opts for this security method, the storage and protection of the biometric database should be as important as the information databases the biometric scanning is protecting. This is in part why the privacy policy was created and can be of good use to those companies without biometrics.[4] Even with the most conservative estimate concerning false positives from biometrics, at 1% this may not yet be a reasonable answer to security for some high volume facilities. As a research scientist explained recently in the Wall Street Journal, if a facility like a large airport were scanning with a 1% false positive rate, that would mean they would be "flagging" 700 people during a regular daily flow. This is probably too large a number to be effective in both the return on investment (ROI) and the practicality of implementing.[5] In spite of these facts, biometric vendors have found an insatiable business consumer market for their goods recently. And with the interest in their goods, the cost of purchasing and using some of the lower end interfaces has been reduced through economies of scale. Though still not economical for a "mom and pop" organization, these systems can easily be a required necessity in the businesses of banking and financing, travel, medical, insurance, and energy. An easy formula to calculate if a security option is justifiable is to compare the cost of what you need to protect against the cost of the protection method chosen.

Chip cards provide a tight security model at a more economical cost than biometrics. They allow strict authentication for building and network access and, in the chip card model, can store user private keys for public-key infrastructure (PKI) applications. Some important and promising advantages with this security option are the acceptance by vendors, manufacturers, and programmers of following the International Organization for Standardization (ISO) 7816 protocol standard. [6] Such acceptance makes the current and future use and manipulation of smart cards easy and manageable across different security platforms. Two

important groups are the Personal Computer/Smart Card Workgroup (PC/SC) and the Open Card Framework (OCF). The use of a multi-platform system to control and monitor building and specific sensitive department access can provide a highly controlled environment and, if warranted, an opportunity to gather an increased amount of information for investigation. Access control vendors have models that have an accessible and readable transaction log, read either by hooking the card reader up to a serial port or by specific software.[7] Viewing these logs on a regular basis can make specific habits and alterations in an employee's behavior more easily recognized and defined than they are now. We could pull logs of building access and compare them against network log-in and access to see if the user or someone else is abusing user accounts or accessing non-cleared resources. Many of the new security management packages being developed and sold today are software based so that in a security room, staff can point and click their way through the facility, open and close doors, generate and print custom reports. [7] Physical security and its tools are as high tech as IT security and would benefit from knowledgeable users who in turn can manipulate and tweak the software for tighter total security.

Another product allowing for real-time monitoring and providing a recordable archive is Closed Circuit Television (CCTV). Advances in this field now include such features as on-screen programming, sequential switching (for automatic multi camera/multi scene switching), auto detection (movement), and video encryption. The encryption stops unauthorized interception of the CCTV broadcast and can automatically detect different video signals like Phase Alternate Line (PAL), Syetm Equential Couler A Memoire (SECAM) and National Television Systems Committee (NTSC).[8] Advanced chips are marketed for cameras that make three-dimensional viewing on screens a reality, which makes it possible for a single guard to tour his entire facility by the movement of a mouse or joystick from his office or easy chair via the Internet. Additional technology will make it possible to use the same cameras to capture a snapshot of individuals and instantly compare their irises against a database of those of known felons, terrorists, and other criminals or against a company employee database.[7]

Physical Security – Design Implementation

A fairly new approach that coincides with the awareness perspective and incorporates the environment is a design approach to security called Crime Prevention Through Environmental Design (CPTED). CPTED, in its organization's web site, states that "The proper design and effective use of the environment can lead to a reduction in the fear and incidence of crime, and an improvement of the quality of life."[9] CPTED uses four strategies that I will summarize from the cpted-watch web site. This technique should be considered and discussed while at the total security-planning table while considering the security concepts of Prevention-Detection-Response and Risk Analysis.

1) Natural Surveillance – a concept of design helping maintain and maximize the visibility of people, wherever they may be.
2) Territorial Reinforcement – properly defining public and private areas either by "natural" (hedges, tree lines, and boulders) fences, barricades or manmade barriers. This strategy focuses on territorial control. Users or inhabitants develop the sense of control while trespasses and possible offenders do not.
3) Natural Access Control – design element that promotes safety while increasing the separation of public and private areas. Either denying access to the crime target areas or making them appear too risky for the criminal is the goal.
4) Target Hardening - this is what we all know about physically securing the doors and windows of our homes and offices.[10]

Physical Security – Personal

While options like the telephone, videoconferencing and other web based interactive communications (WebEx)[11] are excellent tools to help in reducing travel for companies and their employees, nothing replaces face-to-face business. Hard as it is to define where our company's intranet and network stops, business and new customers dictate the expansion of our business borders as well. That is where personal protection steps in. The human element to security has also seen an increase in interest. Not only has the need for security consultants increased, but the kind and depth of coverage needed has risen as well. Top business executives in high profile jobs and those executives who travel to high-risk areas are requesting more services and a more visible intimidating persona (Secret Service types) to carry out that protection. It should come as no surprise that these total security companies have learned to adapt to both the changing times and their customers' evolving needs. What we want to perceive and what we want the world to perceive is changing. In the case of executives wanting a more obvious stereotypical protection, both perceptions can lead to a safer reality.

It is easy to become intimidated when you hear about physical security and its hardware components. Cost and/or training of these security options can break a lot of businesses. And, honestly, not every business needs biometric access to its network or building. The entertainment industry loves to stereotype security personnel into one of two categories. One is a clean-cut, strong build business suit person with dark sunglasses and an earpiece. The second is the burly bar bouncer who uses intimidation stemming from sheer size and mean attitude. These may or may not be very effective models of security for certain businesses. But what we can implement from the physical side is the keen awareness, the street smarts and gumshoe techniques.

Physical Security - Awareness

Too little importance is placed on other less technical skills. Observation, intuition, awareness, and a keen sense that something just isn't right seem to be lost in this technical explosion. These skills are not designated or restricted only to trained personnel. They may only need to be awakened and stirred into becoming instinctive to some, just like knowing the IRQ assignments when troubleshooting a conflict. We were not born with the knowledge we use on a daily basis in our jobs; we learned it. But from an early stage in man's development and our own we have been able to use instinctive sublime intuition, gut feelings, perceptions, and hunches. These intuitive and natural feelings need to be used and sharpened just as much as our network security skills. Because of their training, security and military personnel have grown to not only sharpen these skills but to count on them. Perhaps this is a good reason why ex-military men and women are used for all types of security purposes in their civilian lives. In conjunction, military and government organizations have teams of specialized investigators who are equally comfortable investigating a range of crime scenes, be it a murder scene or PC forensics. Mike Curry, an executive with the "total security" business SACAN in France and Canada, agrees that crime has changed and so should the business of deterring. He continued, "In order to attract business and in fact be successful in today's market, it is essential that security companies remain capable of providing traditional type (physical security, guards, protection) services as well as technical (electronic internet type specialization) services. We have that capability with specialists available for whatever the customer requires."[12] Be it for customers or for employers, this mentality of total security is taking solid ground and should be implemented into the learning and blending of security duties. In and out of business, today's crime is evolved and much more sophisticated than it used to be.

IT Security - Threats and Trends

Because of the growing trends in crime against business and people, these companies used their foresight to know that the criminals today and the crimes they commit are requiring that investigations have both physical and technical investigative techniques. What are these negative trends? The CSI Computer Crime and Security Survey 2001 crunched the numbers from their survey and these are the trends on the rise, according to their respondents[13]:

- Theft of proprietary Info
- Sabotage
- System penetration
- Insider Abuse of Net Access
- Financial Fraud
- Denial of Service
- Virus infections
- Active Wiretap and Telecom Eavesdropping
-

Numbers and studies vary and all have their supporters and their cynics, but the facts and the trends are clear and distinguishable. Both the attack method and the attacker knowledge broaden. Because business will continue to edge competitors and attempt to gain more customers, these attacks will increase in number and frequency. Add to that the number of businesses, governments, and civilian users who continue to access the web and you quickly understand there is no reason to believe the trends will change. Given the circumstances, IT security has no alternative but to accept its growing role and incorporate the many changes being dictated.

Government has taken a step towards enforcing that businesses will put IT security at the top of its priorities. Government and business alliances are encouraged to build better cooperation between the two. The objectives of this new alliance are not new. Best practices have been encouraged for some time, but what is encouraging about the focus is that all business and government departments are sharing. One product of the meetings leaving the boardrooms and government committees is the direction for a uniform guide on best practices.

Best Practices - Foundation for Total Security

A sign of the times, best practices has become a goal for many different businesses and industries. For IT security, the best practice stronghold is leading to uniformity and acceptance. There is agreement that creating policies and their structure should be number one in the process. Organizational flows for these policies are abundant, but the fundamentals of content and purpose are central. Research attention led me to agree with a particular model, explained by Fredrick Avolio in his Best Practices in Network Security white paper.[14]

Key to developing the policies is to include members from all departments of an organization. The security planning committee should involve all departments of IT, physical security as well as interested people from other non-IT departments. They can be key in helping define who needs access to what data and how to access it. Is Internet mail and access to it relied on for business? Are there remote users? Do they need access to client data? Do clients need access to their data? Buy-in by the organization affected and having executive buy-in is imperative to establishing the importance and seriousness of the policies. Employee buy-in is achieved by participation of the key members from the departments. They have a vested interest in and first hand knowledge of the policies by assisting in policymaking. But more importantly, being educated about their purpose will carry a lot of weight.

With the knowledge of input from the total organization, the security teams can now go about analyzing the threats and vulnerabilities and can perform risk assessment. Because we incorporate both physical and network security in this

analysis, the building structure, its surroundings, employee safety, network and data, the human aspect and natural occurrences can have equal assessment. Central to this analysis, planning and scenario playing is to be truthful and realistic. Assessing possible over probable, probable over remote, and prioritizing the threats and risk will all help ensure realistic goals and put top priority issues at the top of everyone's list.

There are as many models for the policies and their structure as there are reasons for implementing them. The important thing is to make sure the policies are easily available, simple to understand and utilize. After going through the daunting task of research, writing them and putting them into place, we do not want them to get lost on the Intranet or be too complicated to understand. Specific actions will require implicit reactions. The policies and reactions should be explained in their entirety and leave no room for misunderstanding. The root policy model is one that gives concise rules on acceptable behavior for the entire network, such as data access and by whom, what activities are acceptable, what are not, and the controls that will monitor and regulate these standards. The root policy is the top of the tier. Except where noted for RBAC (Role-Based Access Control), the bulleted points below are a snapshot of Mr. Avolio's Root Policy model and the individual policies that will govern the specifics and business of the network and use.[14]

- Security Architecture Guidelines - This will define the actual structure of the network in terms of physical structure, topology, communication and protocols used. If encryption will be necessary for client files, their data, or employee information, then this policy will dictate the how and when. If it is determined during the security planning that not only should this information have PIN access and a firewall, the Security Architecture Guide will place it and decide how to audit and manage it. This is prime policy to incorporate both physical and network security
- Incident Response Procedure - Defines the Who, What, When, and Where of an incident. This is useful for when an incident occurs so there is not a lot of panic and "headless chicken" activity. You do not want to overreact and call in the Marines but you want to react adequately to the issue. One important item to cover in this policy is whom to call and when.
- Acceptable Use Policies – End-users are the direct focal point, which makes this a good focus for both securities. Web and mail use are items to be covered, addressing the acceptable versus the unacceptable and its consequences. Should proprietary data be copied to floppies and taken home? Though all sub-policies are directly related to the Root Policy, this will elaborate issues concerning employee behavior at work and on the network. Enforcement of these policies should be the joint effort of network and physical security.

- System Policies and System Administration Procedures – This includes software

specifics such as what software is allowed and which updates, patches, and service packs will be installed by whom and when. The backup schedule and procedures will be included.

- Other Management Procedure - Helps detail data handling, viewing and types of information that may be classified for certain personnel. An excellent way to help restrict access is to keep focused to the rule of least access. We can keep user rights and permissions to the minimum through department, user group, or Role-Based Access Control (RBAC) assignments. RBAC takes Microsoft NT user groups to another level. Roles are based on the specific company and its operations. Users have specific roles in any organization; with RBAC each role is first established and then defined through hierarchies, roles and relationships. These roles are regulated, controlled, and updated either statically or dynamically. A user cannot be included in more than one role in the department or organization, though some of the duties may be similar. For example, one employee may count and deposit the money, but another, who cannot perform deposits, can perform error corrections to the deposit transaction.[15] Policing and enforcement of "other management procedures" can also be regulated with the assistance of physical security through our working together and using access control devices to more critical departments, i.e. server room, accounting, Research and Development.[15]

With the support of senior management and the users, the process of eliminating what the security teams and policies have pointed out will be easier. Our objective is to achieve a more secure environment at the end of the day than when we started. Priorities with the highest ranking are taken care of first, followed by the next serious. We are engaged in electronic guerrilla warfare; the enemy hits and retreats. The enemy hits the weak points and then search for another one. Whether the enemy is hiding in the masses or infiltrating our own camps, the use of physical and network security skills and tools is our best chance in fighting this war. The more we know, the better. The more we share, the stronger we become. Communication, numbers, and support are our allies. It is time we use all these resources and strengths.

VI. Total Security

This new understanding of "total security" is echoed throughout the security industry as the numbers of these complete security companies seem to grow for today's demand. A well-rounded and knowledgeable security director (CSO) and department are the direction of the evolving security model. In fact, pioneers of this model such as Microsoft Corporation and Pemco Services, both out of the Northwest, lead the way with this cohesive model for security. Eduard Telders, Pemco Corporate Security Manager expressed it this way: "All companies have…abuses of systems and other [human resources] problems. Computers have just become one of the tools to commit [electronic] indiscretions."[16]

I have mentioned the action of blending the security skills. How this can be done is dependent upon the organization, its type of work and security goals. In one scenario, it may be most effective to combine the offices and employ effective personnel who can achieve the goals of both skills. We know that government agencies have these people, as do some state and city enforcement offices. The total security companies like SACAN have the people and capabilities, "for whatever the customer requires." Whether a company utilizes the CSO model where the two security offices report to the CSO or combine the offices and employ those specialists, which can cover both skill sets is not important. The important issue is to keep in mind that the skills of both IT and physical security need to be practiced. Patrice Rapalus, Director of CSI, agrees that to combat the bombardment of human driven attacks, stealing, and snooping, an all-inclusive plan of defense including policy, firewalls, encryption, training and funding should be organized and implemented. Rapalus goes on to say, "Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions." [17]

An example of how blending the two skills could be of benefit could be one of a tenured model employee who has shown up for work at the same time every day. There has been no apparent net abuse except for daily access to the same two IP address. Through network tools you know they are Teddy bear trading and auction sites. The employee's boss is a financial executive who relies on her help to do almost everything for his daily routine. For the last month, her behavior has changed. She has shown up early, before her boss, and has used his log-in account before he has arrived. Tight password management requires secrecy as well! To add to this suspicious net use behavior, she has altered from the same two IP addresses to a few vacation sites and one travel agency. Maybe her vacation is coming, maybe not. But by having access to both the physical and information techniques you also could use these flags as an incentive to gather more information or alert the proper company personnel. Is this too much of a "big brother" scenario or does this suggest that individuals are losing their privacy in the work place? It is possible. Certainly there are important concerns to these issues. Open dialogue, learning from our mistakes, and an understanding that both sides of the security picture have valid concerns will warrant flexibility by al involved. Also essential is the need to educate the people who will help facilitate this secure environment. The training of our security people is imperative.

VII. Conclusion

Additional information on our enemy is crucial. Projects such as the

"Honey Net Project" and the focus on sharing of information will help us not only understand what threats are being utilized and how to combat them but will also prepare us for the next generation of threats. Not only is the number of threats increasing but the severity of the threat is growing as well. These threats are coming in on all sides and in all forms. No one tool or one skill set can detect everything. For the network, it can be the profiled hacker: the male in his early twenties who is a loner with low self esteem and who has problems establishing and keeping relations, possibly a student or IT professional who attacks from his home and though boredom takes out a company web site by sheer luck. A possible threat to the physical network, business and employees is a disgruntled employee who might either be stealing client data and selling it to a business rival or snapping and bringing the company and employees to a quick and alarming realization that security was an afterthought. Let us not omit the possibility of corporate or government espionage. The truth is that we cannot stop everything. Perfect security is unattainable. One thing we can learn from the past is that security is everyone's job. We are only as strong as our weakest link. But if we continue to be aware, stay in tune with our physical and electronic surroundings, educate management and users, also continue honing network security skills through workshops and classes while continuing to share information and keep a responsibility to security, we will continue to keep an edge and eventually expand that edge. "We've been through a lot of crises, and they have a natural cycle. When it is over, people relax, and relaxation brings new vulnerabilities."[18] We cannot afford to relax.

Cited References

1. "The hijack suspects." BBC News. 28-September-2001 URL: http://news.bbc.co.uk/hi/english/world/americas/newsid_1567000/1567815.stm (28-March-2002).
2. "Hijacker 'pulled over by police'." BBC News 9-January-2002 URL: http://news.bbc.co.uk/hi/english/world/americas/newsid_1750000/1750938.stm (28-March-2002).
3. Stoneburner, Gary. "Underlying Technical Models for Information Technology Security." Recommendations of the National Institute of Standards and Technology. December 2001 URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf (15 Jan. 2002): 21.
4. Verton, Dan. "IT shops balance security, privacy." Employee privacy key in cyberattack defense. 25-February 2002 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO68593,00.html (06-Mar. 2002)
5. Berman, Denise K. "…against Future Threats." Workplace Security - Wall Street Journal 11-March-2002: R10.
6. Di Giogio, Rinaldo. "Smart Cards: A primer." December-1997 URL: http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev_p.html (03-April-2002)
7. Marketplace. URL: http://www.securitymanagement.com/library/000355.html (11-January-2002)
8. "The Basics of CCTV" URL: http://www.pidallas.com/abc_cctv.htm (12-March-2002)
9.Draper, Rick. "CPTED Crime Prevention though Environmental Design." URL: http://www.cpted.org/ (15-March-2002)
10. Howe, Dorinda R. http://www.cpted-watch.com/ (12-March-2002)
11. http://webex.com/home/default.htm
12. (Mike Curry, personal e-mail communication, 15-October-2001)
13. Power, Richard. Computer Security Issues & Trends Vol. VII, NO.1 – 2001 CSI/FBI Computer Crime and Security Survey. Spring 2001.
14. Avolio, Frederick M. "Best Practices in Network Security." 20 March 2000 URL: http://www.networkcomputing.com/1105/1105f2.html (10-March-2002)

15. Ferraiolo, David. "An Introduction To Role-Based Access Control." 18 July 2000 URL:http://csrc.nist.gov/publications/nistbul/csl95-12.txt (10-March-2002)
16. Radcliff, Deborah. "The Guardian." 09 July 2001 URL: http://www.computerworld.com/itresources/rcstory/0,4167,STO61984_KEY73,00.html (08 Oct. 2001).
17. Power, Richard. Computer Security Issues & Trends Vol. VII, NO.1 – 2001 CSI/FBI Computer Crime and Security Survey: 2, Spring 2001.
18. Hymowitz, Carol. "Business's New Agenda." Workplace Security - Wall Street Journal 11- March-2002: R6

Other References

Rash, Wayne. "Evolution comes to security" 13 Nov. 2001 URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2824295,00.html (05 Jan. 2002)

Phillips, Andrew. Provided by Gartner "Planning for smart cards" 29 Jan. 2002 URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2843255,00.html (15 Feb. 2002)

Millman, Howard. Provided by CNET Enterprises "Prepare for your greatest security risk: An inside attack" 01 Aug. 2001 URL: http://www.techrepublic.com/article_guest.jhtml?id=r00220010801cnt01.htm (08 Oct. 2001).

Crume, Jeff. Inside Internet Security - What hackers Don't Want You To Know. London: Pearson Education Limited, 2000.