Adopting Security from an ROI Perspective

Views Emerging from a CommerceNet Invitational Workshop

Cupertino, California September 11, 2001

Dr. J. Craig Mudge, workshop leader

October 9, 2001 *www.commerce.net*

Participants: Mig Hofmann, CommerceNet
Henry Lichstein, former Citibank executive
Scott Loftesness, Glenbrook Partners
Phil Mellinger, First Data Corporation
John Meyer, CommerceNet
Craig Mudge, Pacific Challenge
Alan Norquist, Ponte
Dick Sites, Adobe
Joe Tardo, Broadcom
Mike Watters, network security investor/entrepreneur
John Weinschenk, VeriSign

Table of Contents

Introduction

Computer and network security products, services, and projects are often sold using scare tactics. By describing the business consequences of potential security breaches, in terms of fraud, loss of reputation, loss of company data, interruption to operations, and exposure of consumer information that a company might sustain if a particular security measure is not adopted, vendors and security managers attempt to convince organizations to purchase or implement their wares.

While the attraction of such a sales technique is obvious, there are other techniques that might facilitate more rapid adoption of security and, consequently, increase confidence in electronic commerce. CommerceNet sponsored an invitational workshop on September 11, 2001 to explore these other approaches.

We paid particular attention to the financial analysis technique of return on investment (ROI) in the adoption of security measures for the Internet and e-commerce. We also proposed potential security projects that CommerceNet could pursue to advance technology and business practices in this important area.

Participants were drawn equally from three communities: users, researchers, and vendors. [1]

[1] **Historical footnote:** On September 11, 2001, the United States and, indeed, the entire world suffered a terrible tragedy. Four commercial aircraft were hijacked and turned into weapons. Two of the aircraft purposely crashed into and destroyed the twin towers of the World Trade Center in New York City, one aircraft hurtled into the outer wall of the Pentagon in Washington, D.C., and the remaining aircraft plunged into the ground outside Pittsburgh, Pennsylvania. Thousands of lives were lost in these horrendous acts of terrorism.

Ironically, the CommerceNet Invitational Security Workshop was held on this fateful day. As these tragic events raise security to the forefront of people's consciousness around the world, so companies globally should be asking the same questions: How good is our security today? What level of security do we need? How much are we willing to pay for that security? What risks are we willing to take? These questions are difficult to answer at any time, but are particularly relevant in the wake of the disaster experienced in New York, Washington D.C., and Pennsylvania.

While horrified by the tragedy experienced on the day of the workshop, participants reaffirmed that security is a pertinent and timely topic of discussion.

Context of the Workshop

Workshop participants agreed that cost-effective security is a critical component of electronic commerce (e-commerce). Because security incurs a cost in terms of both infrastructure and inconvenience, it is typically met with resistance at budget time and is often disabled by users when possible. However, as e-commerce systems become more sophisticated, security requirements become more complex and the implications of corresponding security solutions are harder to comprehend.

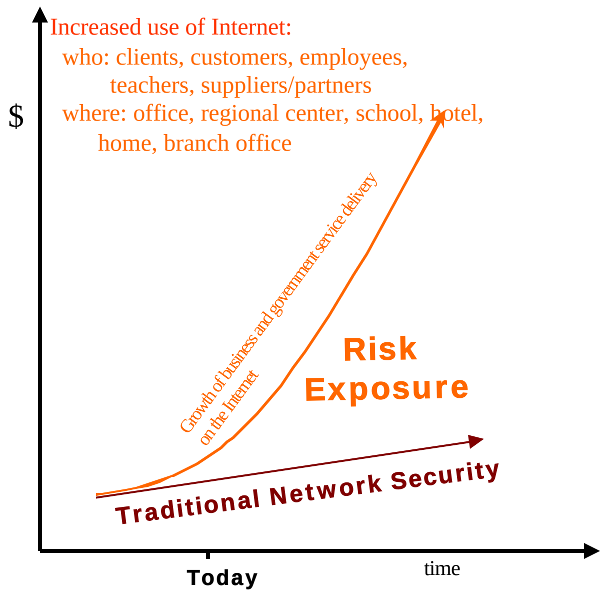
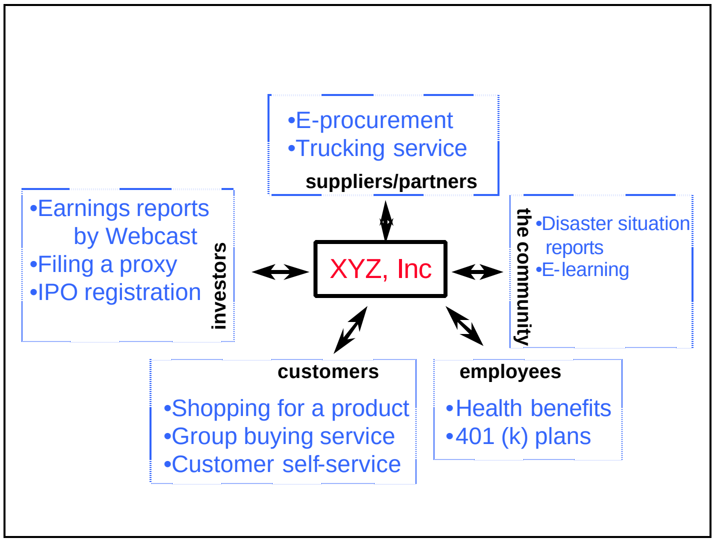


Figure 1: Widening Gap between Internet Growth and Traditional Network Security

As business and government functions migrate to the Internet and web delivery of information becomes standard practice, the gap between vulnerabilities and security solutions continue to widen as indicated in Figure 1. Moreover, there are increasing concerns about the privacy of personal information as people transact more business on the Internet.

Privacy of customer data is a concern not only in transit, but also while data resides in systems and databases that can be penetrated by hackers.

The following diagram showing Internet support of five of a firm's relationships (with suppliers, employees, investors, customers, and the community) reminds us of the vast extent of today's information environments.



Today's operating systems and application software are not only increasingly complex, they are often of poor quality and sometimes released with little regard for security issues. This complexity and quality are both sources of vulnerability.[2]

[2] In almost all recent security assessments, Microsoft's IIS (Internet Information Server) web server is found to be particularly vulnerable. Use of IIS requires constant vigilance for security alerts, continual application of security patches from Microsoft, and measures to quickly detect vulnerabilities and attacks against its numerous security holes.

Security from an ROI Perspective

When costs and benefits are easily measured, ROI is used to aid business decision-making. The MBA-qualified person has several tools in her tool box -- Payback Analysis, Net Present Value (NPV), portfolio theory, IRR (internal rate of return), and risk management to name a few in an ROI collection. These tools are used to compare different investment projects or different solutions to business problems. For example, projects are approved if their ROI exceeds an internal "hurdle rate". Financial benefits (decreased costs and increased revenues) and other parameters, such as discount rate, are measured, or estimated, and fed into "ROI calculators". When soft or intangible costs or benefits are included, the analysis has less confidence.

In our current poor economic climate, ROI analysis is being used more frequently to make IT spending decisions. In a July 2001 survey of 200 IT managers by *InformationWeek*, 80% say the importance of measuring ROI has increased since a year ago. In such analysis, each cost element (software licenses, consulting, staff salaries, outsourced hosting, hardware, management, etc.) is taken into account. Again, intangible benefits, such as improved customer access, or satisfaction, are generally left out.

One of the attractions of outsourcing a function is that the costs of that function become a lot clearer. In security, the term ROI is also being used to (loosely) describe a "build-vs-buy" analysis to decide whether to outsource intrusion detection. Ignored again are the costs that stem from damage to reputation, strategic setbacks, lost data, eavesdropping on customer data, or lost days of trading.

Workshop participants presented several examples of projects significantly affected by ROI analyses:

1. A highly respected software company, with revenues over a billion dollars, initially determined that continuing using 40-bit encryption would be significantly cheaper than 128-bit because there was no additional development or export license required. Eventually, due to security concerns, 128-bit security was added to the product and properly licensed. Interestingly, using quantitative ROI, this same company migrated its finance and human resource organizations to electronic systems. The company has daily visibility into its financial status and has been able to considerably improve predictability of revenue.

2. A network performance monitoring company developed a product using an RMON (Remote Monitoring) probe. It believed it could justify product cost based on increased network uptime yielding dramatic productivity improvements; however, because the initial and ongoing costs were so high and the benefits were not clear to the customers the product failed. A product using similar technology, however, was successful when used to benchmark Internet performance. While the product was just as expensive, the benefits were clear and measurable as Internet clients could now track their dial up infrastructure, monitor the end-to-end experience of their users, and locate problems in the network. When used as an Internet benchmarking tool, the benefits were quantifiable and the product became an industry standard.

3. Evaluating PKI and its attributes, a bank invested in pilot projects to assess the viability of the technology for the provision of personalization in its Internet offerings. Although it enhanced the consumer experience, reduced internal fraud and demonstrated the ROI required for the bank's financial model, PKI required additional investment in supporting technologies such as smart-card readers,

secure directories and application API's. The bank determined that the potential benefits would not be achievable until these other technologies became readily available.

4. A government project (pre-web) analyzed the use of hardware packet encryptors to segregate classification levels in an agency's network. Although there was a large cost reduction utilizing the packet encryptors, other issues such as non-standard host interfaces and the limitations on throughput capacities caused the project to be rejected.

5. On-line travel reservations were initially rejected even though they delivered lower transaction costs than when conventional travel agents were intermediaries. There were several reasons for this, including possible loss of control by the airlines or large buyers, the danger to long-standing relationships, and doubts about service levels. In the early days of e-commerce, similar rejections occurred in the auto retailing and software distribution industries because of uncertain channel conflicts.

6. In a customer service project for a Regional Bell Operating Company (RBOC), a business introduced the concept of client server computing and indicated the qualitative benefit was improved customer service because of the increased speed with which the application could respond. The RBOC was concerned about the cost of the increased memory in each PC and did not approve the project until quantitative measurement proved the average call time dropped significantly with the upgraded PC's.

7. A six-year-old company with 2,500 employees has implemented a web-based employee travel procedure, which links travel authorization, its travel agency, and its expense reimbursement workflow. The decision to implement this security-enabled system was based on an analysis of cost savings.

As demonstrated by these examples, ROI is affected by a number of factors. In many cases, management is most interested in numbers such as reduced costs or accelerated revenues. Decreasing costs may include something as straightforward as staff reductions or implementing services that are less expensive. Revenue increases are more difficult to project, but are still considered quantifiable.

Qualitative factors are often much more elusive. Calculating benefits and measuring the effectiveness of a solution are often very complicated tasks. For example, a company may view security as a way to avoid down time, increasing system availability and productivity, but how can it accurately project the anticipated increase in up time that a security solution will provide? If a company mandates privacy and authentication requirements, how much will its liabilities decrease? What might be the potential savings to a company's reputation that otherwise might be damaged by a security breach which becomes publicized?

ROI often comes down to determining the level of acceptable risk and the true cost of the insurance required to avoid that risk. If a security risk has been identified and a plan has been created to address that risk, it may be turned down today because the potential increased security does not appear to be worth the cost. However, if that same company experiences or sees tangible evidence that other businesses have suffered a security breach, previously suggested projects are resubmitted and quickly approved.

There are many ROI calculators available today for analyzing security projects, particularly from virtual private network (VPN) and password management vendors. These calculators attempt to demonstrate the cost savings of moving from one infrastructure to another, often using very imprecise estimates.[3] Thus, it is not surprising that only 8% of Fortune 500 CIO's believe vendor ROI claims.

Generally, workshop participants concluded that ROI was not an effective approach for analyzing security projects due to the lack of calculable metrics and the difficulty in quantifying the benefits. ROI did appear to have some limited applicability to projects such as migrating to VPN, but was not thought to be the most salient technique for the majority of security products or projects.

[3] One workshop participant mischievously noted that he did not know of an ROI calculator that would return a result recommending against the purchase of that vendor's solution.

Security as an Integral Part of Business

Rather than adopting security solely on the basis of ROI, workshop participants addressed alternate ways of presenting security. Many different perspectives emerged on approaching security creatively, including some that helped security become integrated into the very core of business.

Security as a "disruptive technology" enabler

One suggestion included viewing security as a "disruptive technology", offering a new or better way to do things. In the case of virtual private networks (VPN's), security is facilitating migration from high-priced leased line networks to low-cost encrypted VPN's. The ability to provide secure communications across public networks allows firms to move from dial-up remote access servers to secure remote access, thereby making telecommuting available to any employee. Subsequently, telecommuting assists companies in meeting federal and state regulatory requirements as well as reducing infrastructure costs such as office space and electricity. Viewing security in this way makes the cost justification very simple and straightforward.

In another instance of security as disruptive technology enabler, using authenticated and encrypted links has permitted organizations to offer personnel services over the web (i.e., benefits enrollment, tax forms) in a more convenient and accessible manner. This type of secure link improves personnel services delivery while decreasing the number of personnel required to process forms. While the company incurs cost by investing in the required servers, the overall cost is lower than retaining the staff necessary to provide personnel services.

Security and the associated disruptive technologies may also enable new business opportunities. VPN's make collaborative business ventures possible and may also facilitate location-independent storage. Secure Socket Layer (SSL) communications capabilities built-in to today's web browsers enables electronic commerce, which includes outsourcing capabilities and access to secure electronic documents. It is also interesting to note that, in some cases, security departments have been able to transform security projects into profitable products that other companies are willing to purchase.

Security as unobtrusive as electricity

Security should be as unobtrusive as electricity. Whether at work or at home, electricity is constantly available at a consistent service level, omnipresent and coursing through the walls; however, electricity is not intrusive or even noticeable. Typically, electricity is a critical component of any infrastructure constructed for business or personal use. Building codes provide strict standards on how electricity will be incorporated into the structure. If security migrated to a model similar to electricity, security processes would automatically be embedded in business infrastructures and consistent standards would be established such that security could be accurately measured and rated.

Security as consistent as financial controls

In many ways, security can be compared to financial control processes established by a company. While companies may experience peaks and valleys in applying measures of fiscal responsibility, businesses usually employ a very consistent approach to financial controls. If implemented similarly, security would become a daily process ingrained in the fabric of the business.

Security as comprehensive as fire prevention

One of the characteristics of importance in the fire prevention area is the requirement forced upon companies to act responsibly (because of fire codes, insurance requirements, etc). Unfortunately, network security is a young industry and the basics of certain minimum levels of standards (which companies must follow) simply haven't emerged.

When comparing potential security violations to fire prevention, as shown in Figure 3, it is clear that the security industry today has significant gaps in the products or services required to provide a comprehensive security solution. Additionally, some companies today aren't willing to pay for security. Similar to fire prevention, companies must determine how much risk they are willing to take and at what cost. In the case of security, companies are often "self-insured" and avoid active inspection or tests of their security systems because they don't want to know the results.

Factor	Fire Prevention	Network Security
Risk Management	Insurance, off-site storage	Periodic backups
Prevention	Building codes, inspections, fire drills	Firewalls, encryption, PKI
Detection	Smoke alarms	Anti-virus software, Intrusion Detection Systems
Reaction	Sprinklers, fire escapes, professional fire departments	Full-service security firms; ???

Figure 3: Network Security Compared with Fire Prevention

However, if companies addressed security in the same manner fire prevention is approached, companies would attempt to minimize their risk, pay for the appropriate and customary preventative measures, and engage professionals to detect and react to security violations.

Security as integral as sanitation

Sanitation is an integral component of a restaurant's business. Partially, sanitation is forced by inspection and regulation; however, restaurants that choose not to implement appropriate sanitation measures lose customers and may eventually go out of business. Likewise, security should be an integral part of doing business on the Internet and the cost of poor security is mistrust, potential lost sales and the loss of customers who find other providers that better meet their security needs.

There were interesting suggestions from the workshop for other ways to analyze security spending. One alternate method is spending as much or more than your competitors. This approach will not assist a company in determining how the security budget should be spent, but at least provides a general guideline. A few companies require that a specific percentage of every project budget be spent on security. These companies view security as an investment in next generation technology that will increase their competitive advantage.

In summary, proving ROI for security projects is a complex task; however, shifting the security paradigm and positioning security as an enabler can often be a very effective approach. When improving security fosters technology advancement and enhances business opportunities, chances of project approval increase dramatically.

The Quality Movement as an Analogy

Security practitioners face a problem akin to that faced by the quality movement in its early stages in the 1970s and 1980s and this is impeding the adoption of widespread trusted e-commerce. Quality has had a profound effect on business, but was at first rejected on the basis of cost. Today, paying attention to quality at each stage in a product's life is accepted as a standard business practice. However, in the early days, there was a lot of resistance. Gradually, as product developers measured costs over the entire life cycle of a product they could see that if quality was designed into a product and quality was controlled at each step in manufacturing then lower costs of rework, and reduced field-support costs, justified the original investment. The return was seen and gradually became accepted.

As a result of some of the workshop participants sharing their personal experiences with the quality movement we can suggest some useful parallels.

a. Both movements are enabled by technology and require a process mentality.
b. By establishing stretch goals, these movements force process development and new technologies.
c. Both the quality and security movements require in-depth education and significant culture change.
d. Resistance is typically encountered when measures are forced from outside and security is implemented best when it is a natural by-product of the company's evolution.

With education, experience and culture modifications, security can follow in the footsteps of the quality movement and change from an explicit to implicit practice; move from being a strategic advantage to becoming a competitive necessity; and transform from a conscious, forced process to a fundamental expectation. Once this occurs, corporate policies, procedures and budgets will reflect security becoming "part of the woodwork".

Observations on the Security Industry

As the workshop progressed, a common thread emerged: application and network security is a relatively immature industry. Internet applications and infrastructure have yet to develop the security and quality control mechanisms that were developed by telephone and telecommunications companies over decades. Telecommunications carriers are highly regulated and forced to provide security and certain service levels for their customers. However, this type of regulation has been avoided by the Internet community due to fears that regulation would drastically slow technology development and the associated growth of the Internet.

Some of our observations relate to the security industry, and some to security technologies.

Industry

- There are no standards by which to measure security in the electronic commerce industry.
- From a CIO perspective, one does not feel as if one has done enough, has spent enough on security, whereas in the building industry, there are building codes to help give a baseline.
- There are very few security regulations in the industry
- Monitoring and controlling a security infrastructure are expensive because both practices are people intensive and error prone.
- As in many technology battles, the best technical solution is not necessarily the one that wins (for example, SET vs. SSL).
- Organizations often attempt to address perceived as opposed to real security risks.
- Managed security service providers (outsourcing provi ders) offer no guarantees, just best efforts.
- Software licenses offer no guarantees. “The market doesn’t reward security.”
- There are no Service Level Agreements for security as can be found in the telecommunications industry.
- Hackers and attackers gain notoriety and scare both consumers and businesses.
- Since security is not yet “part of the woodwork” it can be an excuse to sit out the Internet revolution.
- Many consumers see identity theft as a major concern and believe that using electronic commerce makes personal information too easy to access.
- Commerce in information goods often reaches a business balance between trust and ‘leakage’. For example, Stephen King offered his novella “Riding the Bullet” over the Internet. When people pointed out that anyone buying the book electronically could just give it away to their family and friends, Stephen King responded that he made $400,000 more than he would have made otherwise.

Security technologies

- There is no cost-effective infrastructure to support authentication for both sides of a consumer transaction. No entity appears able to provide authentication on the scale required for consumer use, which leaves us with sub-optimal solution of user id and password.
- There is no support for multiple identities in the event the consumer desires to interface with businesses on different levels.
- As companies implement their own security products or procedures, a "bunch of islands" are being created and little attention is given to interoperability or how to connect with open interfaces.
- Consumers are concerned over how companies recover from security "glitches" and what impact that has on the delivery of goods.
- Legacy content requires a different approach from new content.
- Businesses are concerned about how to manage numerous business partners and meet their security requirements.
- Businesses are concerned over the privacy of their partners' data as well as their own internal data.
- Authentication and encryption is perceived as too expensive and too complex for many businesses and consumers.
- Passwords aren't strong enough but digital signatures are too complicated to implement.

Projects for CommerceNet

Workshop participants approached this part of the day in an unusual way. As we have said, the security industry is not yet a mature one. As a result, we compared the industry with a teenager. Participants considered ways to quickly progress through the awkward, emotional teenage years to adult-like maturity without stunting the growth of the physical body. Thus, the question changed from "What projects or initiatives could improve the adoption of security?" to "In what ways could the adoption of security be accelerated without impeding the growth of electronic commerce?"

Participants agreed that there were a variety of projects that could address these requirements, as follows:

1. An Underwriters Lab for security
Institute an organization similar to UL (Underwriters Laboratories Inc., an independent, not-for-profit product safety testing and certification organization) that would define security standards and test compliance. Perhaps a certification program similar to ISO 9000 would be a starting point.

2. An information and educational source
Establish an unbiased forum that promotes consensus among diverse security stakeholders while collecting and disseminating best practices and benchmarks in security. Provide examples of good security practices and good communication of security practices[4]

3. Secure directories

[4] Visa has published a list of 15 requirements for keeping credit card numbers and transaction data secure. It is a simple but very powerful list aimed at helping owners of e-commerce web sites that hold large numbers of credit card numbers. Because it is also a good example of the power of simple presentation, we reproduce it here in its entirety (from https://www.visa.com/nt/gds/pdf/AcctInfoSecStandardsManual.pdf

1. Establish a hiring policy for staff and contractors
2. Restrict access to data on a "need to know" basis
3. Assign each person a unique ID to be validated when accessing data.
4. Track access to data, including read access, by each person
5. Install and maintain a network firewall, if data can be accessed via the Internet
6. Encrypt data maintained on databases or files accessible from the Internet
7. Encrypt data sent across networks
8. Protect systems and data from viruses
9. Keep security patches for software up-to-date
10. Don't use vendor-supplied defaults for system passwords and other security parameters
11. Don't leave papers/diskettes/computers with data unsecured
12. Securely destroy data when it's no longer needed for business reasons
13. Regularly test security systems and procedures
14. Immediately investigate and report to Visa any suspected loss of Account or Transaction information
15. Use only service providers that meet these security standards

Recognizing the importance of directories (of trading partners, of services, of products, and so on), and the development of UDDI[5], define a secure directories project, most probably within the web services framework.

4. Payer authentication pilot
Sponsor a payer authentication pilot that examines the technology fit and effectiveness of existing solutions, matched to a spectrum of risk.

5. Web check
Produce a one-time check that could be emailed as payment method. Consider making the FSTC electronic check patents available at no cost to companies wanting to commercialize the technology.

6. State of Ipv6 adoption
Determine the current state of IPv6 adoption by supporting a pilot with Identrus using an IPv6 backbone.

7. Actuarial data
Encourage the collection of reliable and comprehensive actuarial data, so that security-insurance can be structured as a business.

8. An authenticated email service
Provide a service for email authentication and privacy, potentially using LDAP and PKI. This could initially be a free service to encourage adoption.

9. Source tagging
Encourage development of a mechanism, often referred to as source tagging, in the Internet world that is similar to caller ID in the telephone system. By embedding this capability into the infrastructure, Internet source addresses would always have a unique identifier. [6]

The last two projects would be more effective if they were pushed down into the network infrastructure, one which was trusted. Moreover, authenticated source addresses would dramatically reduce spamming and a Source tag would reduce Distributed Denial of Service (DDOS) attacks. Of course, the idea of handling these functions within the network is at variance with the end-to-end design principle of the Internet.

[5] The Universal Description, Discovery and Integration (UDDI) project aims to create a platform-independent, open framework for describing services, discovering businesses, and integrating business services using the Internet.

[6] The idea is to harden the Internet infrastructure so that it is much more difficult to use false IP addresses, or return addresses different from the true sender address. Routers would then reject packets with such IP addresses. The development of fax machines provides an analogy. The requirement that fax machines generate and include in each fax the correct originating phone number cut down substantially on spam and false faxes. It also allowed building fax machines that reject or ignore faxes with a blank field for the originator, and enabled fax machines that reject faxes whose caller-ID phone number does not match a fax's claimed originating phone number.

Although some of these projects do not match CommerceNet's mission or resources, the consortium could play a role in promoting these projects and finding the right homes for them, since they would all hasten the arrival of trusted ubiquitous e-commerce. Not just through adoption but through network effects.

Summary

Security practitioners face many challenges today that impede the adoption of widespread trusted electronic commerce. Just as quality initiatives in industry were initially rejected due to the costs and inconvenience involved, companies today are often unwilling to invest in security measures that are viewed purely as a cost item.

CommerceNet sponsored this invitational workshop to suggest methods by which security projects could be better aligned with business objectives and practices instead of sold entirely on fear.

After much discussion on ROI, it was determined that it is not as useful a tool as previously felt. There are several reasons for this, including difficulties with quantifying benefits such as preservation of reputation and estimating the size of revenues that might be lost when operations are interrupted. Moreover, as the term ROI is often loosely used in sales situations, and as biased ROI calculators abound, the term has lost some credibility.

In addition to using ROI, security managers can reposition security as an enabler, looking for ways to transform an organization's culture and perspective on security. Companies need to view security as an integral part of doing business. When this is done, security measures are likely to be adopted more readily and become as pervasive and unobtrusive as electricity running through the walls of an office. And viewed as consistent as financial controls, as comprehensive as fire prevention and as integral as sanitation for a restaurant.

Because of the relative youth of the security industry, there are few standards and very little benchmark information available to help CIOs and other executives responsible for security. The workshop examined ways to accelerate the maturity of the security industry without impeding the growth of electronic commerce.

Several projects were suggested for CommerceNet – in authentication, payments, education, and raising awareness. Some of them involved pushing security functions down into the network infrastructure. Not all of the projects proposed will match CommerceNet's charter or resources, but we recommend that CommerceNet take a proactive role in finding homes for those projects it chooses not to mount itself.

As the catastrophic events of September 11, 2001 illustrate, nations and businesses need to pay more attention to security vulnerabilities. In the future, not only will security technologies be more effectively applied to reduce the likelihood of breaches of *physical* security, but the vulnerability of critical information infrastructures will also receive more attention.

By viewing security as a *movement*, practitioners, businesses, governments and citizens can take a more comprehensive approach and so discern the various components that are needed, such as education, benchmarks, certification, standards, and solutions that are easier to use.