Creating Business Through Virtual Trust:
How to Gain and Sustain a Competitive Advantage Using Information Security

July 4, 2006

Kenneth F. Belva, CISSP

Credit Industrial et Commercial,
New York

Manager, Information Security Risk Management Program

Sam H. DeKay, PhD.

The Bank of New York

AVP, Information Security Policies and Procedures

Disclaimer
This paper offers the opinions of its authors. They alone assume responsibility for the ideas contained herein.

Your Comments

The authors welcome your comments concerning the contents of this paper. Please submit all comments at the following site: http://bbs.ftusecurity.com

Part I

An Overview of Virtual Trust

Introduction

This interview dialog was created for an information security television segment that was not aired. The authors felt it serves as an introduction to and summary of Virtual Trust and other concepts described in more extensive detail within the paper. Part II of this document contains the full text of the paper.

The Interview

Interviewer [To Ken]: Welcome Ken**,** nice to have you with us today.
Ken [TO Interviewer]: It is a pleasure to be here.

Interviewer [To Camera]:
Ken is currently employed at Credit Industrial et Commercial (New York) where he manages the Information Technology Risk Management Program. He reports directly to the Senior Vice President and Deputy General Manager. He is currently on the Board of Directors for the New York Metro Chapter of the Information Systems Security Association. He authored the contrarian paper: "How it's Difficult to Ruin a Good Name: An Analysis of Reputation Risk." He has presented on topics such as patch management as well as moderated a panel discussion on corporate governance. He taught as an Adjunct Professor in the Business Computer Systems Department at the State University of New York at Farmingdale. Mr. Belva is credited by Microsoft and IBM for discovering vulnerabilities in their software. He is the author of the chapter, "Encryption in XML" in the "Hackproofing XML" document, published by Syngress. Mr. Belva holds these certifications: Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Information Security Manager (CISM). In addition, to his professional responsibilities, he currently sits on the Board of Directors for Franklin and Marshall College's Regional Alumni Council for the New York Metro Area.

Interviewer: Today we will be discussing the document you wrote and co-authored called *Creating Business through Virtual Trust: How to Gain and Sustain a Competitive Advantage Using Information Security*. But, before we begin, can you give us a little background information on your co-author, Sam H. DeKay, PhD., and tell us what inspired both of you to write about this particular subject.

Ken: [Responds to Interviewer] Sam has worked in the field of information security for more than 20 years. Dr. DeKay is currently responsible for developing information security policies and standards at The Bank of New York. Prior to this, he served as

Manager of Information Security at Empire Blue Cross/Blue Shield and at ABN Bank (now known as ABN AMRO) in New York. In 2003, Sam was designated a Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association. In this capacity, he has written and edited study materials intended for security professionals planning to take the CISM exam. Dr. DeKay has also been appointed a member of the Generally Accepted Information Security Principles (GAISP) Project, under sponsorship of the Information Systems Security Association. In addition to holding memberships in the Information Systems Audit and Control Association and the Information Systems Security Association, he is also an active participant of the Technology Managers Forum. He holds PhD degrees from Columbia University and Fordham University.

Interviewer [Question 1]: How do you see the Information Security industry today and how is your paper relevant?

Ken [Answer.] If we use some auditing language, we have various types of controls: detective, corrective and preventative. The information security field generally comes in two primary flavors: detective and preventative, leaving corrective for the procedural action to be taken. First, we have the detective side which strengthens the controls in both technology and business processes. By technology I mean strengthening the security controls in the software or OS itself. Blackhat took place recently and we can see people detecting security issues that are latent. By business process I mean those controls that help safeguard business. The second flavor is preventative: it is the attack/counterattack arms race. Examples of this are Anti-Spam solutions and IPS devices. We use these controls to prevent damages from occurring.

I think that this paper is relevant because we rarely discuss using security as a way to enable business to do things. Attacks, fraud, threats – these grab the headlines these days. We do not think of security as an enabler. However, without security we cannot conduct e-commerce.

Interviewer [Question 2]: What is Virtual Trust and what are Traditional and Virtual Guarantors of Trust?

Ken [Answer.] Traditional trust and traditional guarantors of trust are non-electronic means of establishing trust: signatures, notarizations, contracts, etc. Virtual Guarantors of trust are electronic and function by means of software—for example, digital certificates and digital signatures. These are mechanisms by which we can create electronic representations of real relationships. Virtual trust is a type of trust created between two parties though virtual guarantors of trust, basically through bits and bytes.

Interviewer [Question 3]: How does security enablement work?

Ken [Answer.] Security enablement requires authentication of a user or customer, although other means are possible too. Authentication allows us to know it is really us that is behind what we are doing, such a logging into our online banking website.

Through authentication we can create data flow streams that will connect businesses and facilitate transactions. We can also create new data flow streams as new technology is enabled with security mechanisms. Security enablement also involves encryption and digital rights management, which I will speak about later.

Interviewer [Question 4]: This all sounds well and good, but what if I'm a skeptic? Why is it not the technology first and security second?

Ken [Answer.] That's a great question and by far the most challenging to answer. I also think that the answer to this helps illuminate why we have not historically spoken about security an as enabler, rather only in terms of prevention of loss.

Commercial transactions are based on trust, real or imagined. We often confuse reliability with the security mechanisms that are needed to protect information. We tend to settle to a level of trust that is bearable, not absolute. RFID is not well secured, but it is believed to be secured enough that people use it. One way of determining the pragmatic level of security is based on the likelihood of fraud. The same protocol in one situation may not be correct for another. Both EZPass and e-passports use RFID, but it can be argued that the security needed in the case of EZPass is much less than for e-passports.

Often when we develop a new technology, protocol or process, we have a certain level of trust in the technology or process that is unfounded. This makes sense to us, as customers, because we tend to trust others as human beings. We take this trust for granted before the proper amount of trust is developed into the mechanism or product.

Historically this was the case with Windows, but Microsoft is really making tremendous strides to build an OS that is really secure from the ground up. They know that the trust needs to be in their product; otherwise, the product will lack credibility with customers. While this sounds like loss prevention, it's really not. Once they straighten out their reputation, they are then going to say, "Look at all the amazing things you can *do* with Windows that you just cannot *do* elsewhere." It's getting the security model correct so they can move forward and enable business do to things they could not do in the past. The goal is doing and that doing is based on trust and enablement more so than loss prevention.

Interviewer [Question 5]: What does this mean for Trustworthy Computing, lets say from Microsoft and Apple?

Ken [Answer.] It means being able to do things that were not possible before because the security mechanisms are now in place to enable business. Just consider the case of Apple. People were trading .mp3 on P2P networks and there did not seem an electronic solution to purchase music over the web. Apple instituted digital rights management and convinced the major players in the music industry to trust Apple to sell their songs digitally. Security mechanisms enabled Apple to create a new product and it allowed businesses to trust Apple that their intellectual property would not be stolen. This

effectively created a new revenue stream for Apple. This is an example of the concept of Virtual Trust.

I think we will find more of these examples in the future. We are generating so much information via blogs, social networking websites and other electronic means that we will need security mechanisms to begin to create new products and services where the end user must be known and identified.

Interviewer [Question 6]: So, where does one gain and sustain a competitive advantage using information security as an enabler of business?

Ken [Answer.] One gains a competitive advantage though security by creating new revenue streams or cutting existing operating expenses. A new revenue stream may be selling a new product, such as in the case of Apple, or reducing expenses through VPN or VoIP. This is only limited by one's imagination and current technology/security mechanisms.

Interviewer [Question 7]: What specifically can businesses do when thinking about security as an enabler?

Ken [Answer.] Business can look for possible places to enable and create cash through existing business relationships any time messages (IM, Email, etc.) and electronic products, such as music or books, are transmitted.

Interviewer [Question 8]: Do we have any specific examples of this? What about in the future?

Ken [Answer.] I've mentioned Apple's digital rights management. Other examples include SWIFT messaging for financial transactions, VPN connectivity between business entities and VoIP implementations.

Interviewer [Question 9]: Why might Virtual Trust become the dominant paradigm, as mentioned in your paper?

Ken [Answer.] It may become dominant because it is more business oriented than the insurance or loss prevention model of information security. The virtual trust model seeks to establish new commercial possibilities and to create cash flows. Businesses exist to obtain returns on investments, not merely to prevent losses. Virtual trust is intended to obtain these returns.

In addition, the big compliance push is dwindling. The Gartner Group recently noted that IT security budgets could be scaled back for corporations that have already put the proper infrastructure in place to address issues related to regulatory compliance . Granted, there will always be a necessary amount of spending to retain compliance, but these sums will begin to decrease because security is being put into the SDLC, maintenance of existing

technological infrastructure and into verification of controls around corporate policy and procedures.

Interviewer [Question 10]: Your paper mentions the "insurance model" in contrast to the Virtual Trust model. Are these two perspectives incompatible?

Ken [Answer.] No, they are in fact very compatible and consistent. As mentioned previously, corporations will still need to audit for various compliance regulations. It's just now that we'll begin to see security as the foundation of a business's data transactions (just as a legal contract is the basis of trust for certain kinds of business transactions) instead of just an expense.

Interviewer [Question 11]: Where can a viewer find more information about Virtual Trust?

Ken [Answer.] You can visit my website at www.ftusecurity.com and there is a bulletin board set up regarding this paper at http://bbs.ftusecurity.com .

Sam and I are interested in all comments and suggestions regarding the paper and fundamental concepts of Virtual Trust.

[CLOSE]

Interviewer

Ken, thanks so much for joining me here today.

Part II

Creating Business Through Virtual Trust:
How to Gain and Sustain a Competitive Advantage Using Information Security

Abstract

Cash. Profit. Margins. Productivity. This is the language of businesses. At this time, it is not the language of information security. Business is concerned with the creation of new entities and assets that generate cash. Information security, by contrast, is traditionally concerned with protecting these entities and assets. In this paper we examine a perspective which currently exists but is largely dormant in the information security field. We maintain that information security can be actively involved in the creation of business and that the skills required to create commercial activity must be added to the information security professional's intellectual tool set. We also present evidence to demonstrate that the capability of security to create business, which we designate by the term "virtual trust", may become a dominant paradigm for how to think about information security.

I. A Tale of Two Paradigms: The "Insurance Model" and "Virtual Trust"

The CIO of a major bank in Australia, speaking before a gathering of his peers from other financial institutions, recently announced that they "should use the tactics of Fear, Uncertainty, and Doubt to convince senior management to invest in security" [18]. "While senior management may be aware of the risks to their information infrastructures," he advised, "they often do not fully understand the damage that a breach in security can cause a business. Fear, Uncertainty, and Doubt can also motivate board members to take direct action to mitigate risks" [18].

The Australian CIO did not originate the term "Fear, Uncertainty, and Doubt." In fact, these three words are so familiar to many information security professionals that they have become abbreviated as an unappealing acronym, FUD. Originally invented to describe the sales tactics of major hard- and software manufacturers, FUD has now become associated with a persuasive means of convincing corporate managers that human and financial resources should be allocated to the information security function. A prominent American technology professional, quoted in *CIO Magazine*, claims simply: "Fear, uncertainty, and doubt—FUD--has been used to sell security. If you scare them, they will spend" [6]. Information security is the antidote to FUD; its purpose is to introduce controls to dispel fears of losing data, funds, and privacy. As succinctly stated by Shelton Waggener, another American CIO: "Security is really an insurance policy" [13]. Eric Goldman, Director of the High Technology Law Institute at the Santa Clara University School of Law, offers a rephrase of Waggener's sentiment: "There is no real

wealth created by the investments in security, it is just a cost of everything we do in our lives" [8].

This paper offers an altogether different view of the function of information security. We propose that information security is not just a kind of insurance, but a means of actually creating business and generating profit. We suggest that the typically double-negative rationale that justifies the existence of security—preventing loss—no longer accurately describes the full role of information security in banking, commerce, education, health, and law.

Since the 1960s, the dominant paradigm, or understanding, of information security has been the prevention or mitigation of loss. To paraphrase Waggener, the "insurance model" has been accepted as the governing concept by which information security justifies its existence. And this model has, indeed, been successful: in fiscal 2006, the U.S. federal government alone spent $5.1 billion on products, personnel, and services that prevent, or reduce the likelihood of, incidents that may adversely affect the confidentiality, integrity, and availability of data [4].

Within the last ten years, however, information security has commenced to serve a new purpose: establishing trust between people and between businesses and their customers. This new purpose has implications, not only for our understanding of the functions of information security, but also for future legislation, technology, and business opportunities. The function of establishing trust may also transform the traditional approach toward information security—that of a cost center—to a new view of security as a critical enabler of business.

We are not claiming that the "insurance model" must be abandoned and replaced with the new concept of "virtual trust." However, we hope to present evidence demonstrating the emergence of a new role for security as a driver of business. Information security can no longer be characterized as a field and practice that merely prevents or mitigates loss.

For nearly forty years, the "insurance model" has provided a clear and compelling means by which to perceive the essential rationale and function of information security. In October, 1967, the Defense Science Board Task Force on Computer Security was commissioned by the Department of Defense to develop and document effective measures to secure data processed by resource-sharing systems. The Board's published report, released in 1970, was entitled simply: *Security Controls for Computer Systems* [19]. This document describes security as a "problem" that involves preserving the integrity of data and programs.

In 1973, Harry Katzan, Jr. authored *Computer Data Security*, one of the first publications concerning information security in non-government environments. Katzan, quoting an earlier IBM document, succinctly describes the essential function of security: "Data security can be defined as the protection of data from accidental or intentional disclosure by unauthorized persons and from unauthorized modification" [7, p. 4]. Three years later, Donn B. Parker's *Crime by Computer* offered harrowing anecdotes concerning real-life crimes perpetrated via computer. Parker concluded that "'Computer abuse' is broadly defined to be any incident associated with computer technology in which a victim suffered or could have suffered loss" [12, p. 12]. Parker's book was still available in bookstores when John McNeil published *The Consultant*, the first crime

novel featuring computer fraud and a technically-savvy detective [10]; the novel offered a popularized notion of information security as an antidote to criminal activity.

The dual themes of loss and prevention, prevalent in the information security literature of the 1970s, continue to retain their potency today. CobiT, the organized set of IT controls recommended by the Information Systems Audit and Control Association, maintains that the function of systems security is "maintaining the integrity of information and processing infrastructure and minimizing the impact of security vulnerabilities and incidents" [2]. The *FFIEC IT Examination Handbook*, familiar to most security professionals in the U.S. financial services industry, states that "An information security strategy is a plan to mitigate risks while complying with legal, statutory, contractual, and internally developed requirements" [5].

Preventing loss, the major focus of the "insurance model" of information security, is so pervasive that the paradigm has spawned a related effort to justify the expenditures associated with security. This effort is prominently highlighted in the annual *CSI/FBI Computer Crime and Security Survey*, which describes the methods used by participating organizations to quantify the cost/benefit aspects of computer security. The *Survey* cites three metrics traditionally used to provide a rationale for allocating dollars to the information security function: Return On Investment (ROI), Net Present Value (NPV), and Internal Rate of Return (IRR) [14]. Each of these metrics involves the calculation of actual or potential economic loss due to lack of adequate security controls. The "insurance model" has become a means of justifying the increasingly costly resources required to support information security.

Recent federal and state legislation is also driven by the desire to prevent loss—of confidentiality, privacy, or money. The Gramm-Leach-Bliley Act of 1999 (GLBA), for example, seeks to ensure that sensitive customer information, and especially financial data, will be secure both from identity theft and from old-fashioned monetary thievery. HIPAA, the Health Insurance Portability and Accountability Act, focuses upon the confidentiality of health-related information. A proliferation of recent state legislative initiatives, beginning with California's SB1386, is intended to thwart the loss of personal data that could, in unauthorized hands, result in identity theft. Similar laws are currently under consideration on Capitol Hill.

Indeed, from the late 1960s until today, the "insurance model" remains a powerful engine, capable of generating new jobs in the field of information security, new hardware and software intended to secure data, new regulations, and even new kinds of crime.

II. Understanding Traditional Trust and "Virtual Trust" Concepts

The "insurance model" uses a set of concepts which we call Traditional Trust. We contrast this with a new conceptual framework, Virtual Trust. Both models rely on the core concept of *trust*, a necessary component of business.

Definitions of trust vary. For our purposes it is enough to mention some of the qualities and effects of trust. When we trust another person or entity, we have confidence that the outcome we expect to happen will happen because the person or entity recognizes, pursues, and completes the ends they are bound to by their word or deed. In short, if I tell you I will do something, it will be done.

Unfortunately, trusting another entity is more difficult than one might expect. Entities are often motivated by self-interest; they behave in ways that benefit them. Sometimes acting in one's self-interest dictates acting in ways that include breaking existing trust relationships, deceiving those who have trusted us. (The question of ethics is not dealt with in this paper. We are simply describing the real-world mechanics of trust, not the way they should work.)

From an historical perspective, how is such trust between entities established? Entities have used seals, signatures, contracts, deeds, treaties, notarized documents, handshakes and code words, among other methods, to create trust. These non-electronic (and/or physical) tokens of trust may be categorized as *Traditional Guarantors of Trust*, mainly for historical reasons. Often there exists a system -- such as a government or coalition of governments -- to settle disputes should they arise between the parties that made the agreement. In a less abstract context, the U.S. state and federal court systems are examples of independent entities enforcing *Traditional Guarantors of Trust*.

In contrast to Traditional Guarantors of Trust, we categorize electronic, non-physical tokens of trust as *Virtual Guarantors of Trust*. Examples of *Virtual Guarantors of Trust* include digital certificates, digital signatures, user names and passwords, public and private keys, the digital numeric sequence in two-factor authentication tokens, the electronic representation of a biological identifier, checksums and hashes.

Therefore, we make a distinction between *Traditional Trust* (which uses Traditional Guarantors of Trust) and *Virtual Trust* (which relies upon Virtual Guarantors of Trust).

Virtual trust is a reality. We encounter examples of virtual trust on a daily basis, but usually do not recognize or name it as such; it is merely taken for granted. The purpose of this paper is to make clearly visible the existence and value of virtual trust, an electronic means of establishing trust relationships that has largely remained invisible, even to information security professionals. We will provide examples of virtual trust and will demonstrate how virtual trust was used in the past and present and indicate possible ways in which it may be used in the future.

As noted earlier, the field of information security traditionally looks at guaranteeing that the internal controls that support virtual trust are not *destroyed* or *weakened* (by failed internal processes). This guaranteeing is the protection function described in the introduction of this paper. In direct contrast, **we indicate how to *create* virtual trust**. **In effect, we describe how to *create business* using the mechanisms of information security. Additionally, we discuss how to *create and maintain a competitive advantage* using virtual trust.**

III. Creating Business Through Virtual Trust: A Macro Perspective

Professionals in the field of information security are well aware that the "insurance model" is quite capable of creating business; each day, their email in-boxes are laden with offers from vendors or consulting services seeking to promote new and better means of preventing potential loss. It is not likely that the volume of these messages will decrease, because the current regulatory climate, coupled with an increasing reliance upon globally interconnected systems, has also generated new vulnerabilities and threats. Fear, uncertainty, and doubt is not merely a cynical sales

tactic; FUD is often a legitimate response to real problems. Senior managers are anxious to protect critical information assets from potentially destructive or damaging forces; information security, like an insurance policy, is the price paid for ensuring that the destruction or damage is reduced to a minimum.

However, this is not the kind of business created by the "virtual trust" paradigm. Virtual trust is not intended merely to protect information, but to create or enable an asset for the purpose of generating profit. The concept of trust, as mentioned previously, is not focused upon preventing loss. Rather, establishing trust is a precondition for conducting commerce. If trust does not exist between businesses and customers, then commercial transactions will not occur. Profit-making enterprises can thrive only when an assumption of trust is reasonably justified. Without a high degree of virtual trust, certain kinds of business would not be possible: automated teller machines, for example, would not function if their users are not securely identified and authenticated. Similarly, most e-commerce transactions could not occur if remote, unseen vendors cannot be trusted to identify themselves accurately. Virtual trust permits transactions between two parties who are at a distance and yet who can trust one another because they have been mutually authenticated. Because of this trust, business can occur; a flow of cash is made possible.

Robert Metcalfe, creator of Ethernet, is credited with developing a mathematical formula that attributes significance to the growth of communication networks. According to Metcalfe's Law, the "value" or "power" of a network increases in proportion to the square of the number of nodes on the network. The virtual trust model of information security adds a new dimension to this law: the business/commercial "value" or "power" of a network increases in proportion to the square of the number of SECURE notes on the

network. This suggests that, as the number of securely authenticated businesses and customers increases, the volume of commercial transactions and of cash flow also increases exponentially.

A physical metaphor that aptly illustrates the conceptual framework of virtual trust is a bridge. Consider, for example, the great Brooklyn Bridge that first opened for traffic on May 24, 1883. Today, this architectural masterpiece is perhaps best known as an element of a joke: "If you believe that, I have a bridge to sell you." But, when this structure was completed more than a century ago, the bridge itself was conducting the selling: it enabled new commerce, and had a profound impact upon the economies of both cities—New York (now Manhattan) and Brooklyn—connected by the bridge. Persons crossing the bridge never doubted its structural soundness. Its gargantuan stone towers, firmly planted on enormous caissons, and its strong 15-inch suspension cables became symbols of a bold, robust city and nation.

Virtual trust also functions as a bridge and establishes trust in much the same manner. Two entities must be connected for a commercial transaction to occur: the buyer and seller. But, as in the historical example of the Brooklyn Bridge, the electronic connection must also be secure; participating entities are loathe to lose money or critical information. The structural elements of a bridge, its stone superstructure and its steel cables, provide assurance that the edifice will withstand pressure and weather. Similarly, the components of virtual trust—digital certificates, signatures, and other forms of authentication—offer this assurance for buyers and sellers. And, like the Brooklyn Bridge, the "bridge" of virtual trust creates new possibilities for commercial activity and economic growth.

IV. Creating and Maintaining a Competitive Advantage Using Virtual Trust: A Micro Perspective

Now that we understand how business is created through virtual trust via the bridge-building example, we will explore methods of creating and maintaining a competitive business advantage using the mechanisms of information security.

Virtual trust is created mainly by two mechanisms: authentication and non-repudiation. Authentication occurs when one can establish who one is. Entering a user name/password and/or using a biometric device allows a system to identify you to establish your credentials and rights on that system.

Non-repudiation occurs when an individual or entity cannot deny that specific actions have been taken. A digital signature, for example, is intended to establish that it was you, and no one else, who sent a specific message.

For the purposes of this paper, we will assume that the concept of authentication includes non-repudiation, although they are two logically distinct concepts.[1] From this point forward we will mention Authentication only, unless we specifically mention otherwise.

Different methods of authentication yield varying degrees of trust because some mechanisms are stronger than others. Information security professionals, for example, have attained consensus that user names and passwords are not as strong as other forms

1 When one authenticates, one supplies credentials that prove who one is. By contrast, non-repudiation involves the notion that one cannot deny that they were responsible for a specific transaction. We assume that the person who supplies the authentication credentials is also the individual to whom the credentials are assigned. This assumption is required to trust the system; however, the assumption is not entirely justified. For example, one may authenticate via VPN to the corporate network to complete some work. But, as one gets up to make coffee, one's son sits at the computer and surfs the corporate network. Thus, although a legitimate employee has been granted authenticated access , non-repudiation does not exist because the employee's son is operating the keyboard. [FYI: This is just an example. The writer of this example does not drink coffee often or have a son (that he knows of).]

of authentication, such as biometrics. Different authentication mechanisms can provide different kinds of information. For instance, digital certificates tell us about the individual presenting the certificate.

But exactly what can be done with authentication? The answer to this question, in turn, answers how to create and maintain a competitive advantage. We are seeking to perform two activities. First, we want to create or change a cash flow into the business. Second, we are seeking to decrease operating expenses though increased productivity.

Let us turn to the creation and change of cash flow. Digital certificates facilitate SSL encryption which, in combination with user names and passwords, enables business to conduct ecommerce via the Internet. This commerce represents a cash flow. For some businesses, like Amazon.com, the Internet is their only channel. For others, such as retail clothing stores, it is an additional means of communicating with customers. The security mechanisms of digital certificates and user names/passwords create a cash flow and generate opportunities for business.

A primary example of creating business through security is the SWIFT network and application. SWIFT enables a secure messaging system for financial institutions. For the purposes of this paper, it is enough to know that entities that use SWIFT may send and receive payments as well as conduct other forms of business. The encryption used by SWIFT is primarily for purposes of non-repudiation. However, SWIFT will become a PKI over the course of the next two years (2008). In 2005, SWIFT message traffic generated revenues of 346,410,000 Euros, yielding a net profit of 7,790,000 Euros [15, p 34.]. Clearly, secure messaging generates revenue and is profitable. Not only may we say that SWIFT was enabled though secure messaging; it is more accurate to state that the

business *is* secure messaging. Without the security, the message would be worthless and the model would fail.

The creation of a cash flow by incorporating security controls was stated by Microsoft when it suggested that people pay for sending email. People would be issued "Caller IDs" that would identify them as the legitimate sender of the email. The rationale was that by charging for securely authenticated email, the amount of SPAM would be decreased because the SPAMMers' cost would increase. The effect of such a policy would be that providers who charge for a secure email service would generate significant revenue.

Apple's iTunes employed Digital Rights Management (DRM) technologies to create a new product and, hence, a new revenue stream. Over 1 billion songs have been downloaded from iTunes [1]. In the case of iTunes, DRM works by restricting the number of CPUs on which the .mp3 will play. The songs are also stored in a proprietary, encrypted format. These two factors, at minimum, erect a prohibitive barrier and thereby reduce the likelihood that an end user will trade songs.[2] The various security mechanisms used by Apple's iTunes DRM created the Virtual Trust necessary to persuade the music industry that their rights will be protected digitally and be profitable.

ExxonMobil SpeedPass offers another example of cash flow made possible by using information security mechanisms. Before SpeedPass, a customer was presented with two options when paying for gas: cash or credit. SpeedPass is an RFID token that the customer may link with a credit card. When the customer stops at a gas pump which accepts SpeedPass, they are immediately authenticated via RFID and the charge is billed.

---

[2] While not impossible to remove the DRM protection mechanism, it seems prohibitive to perform this removal in bulk quantities while also maintaining the sound quality.

This linking of an arbitrary credit card with the SpeedPass RFID token allows the customer to alter the flow of cash at their discretion.

Citibank is using RFID to create PayPass. In a similar way that ExxonMobil uses SpeedPass, PayPass allows the consumer to swipe an RFID tag at certain locations to immediately debit their account. There are transactional security mechanisms—such as not being able to charge more than a certain dollar amount—built into the process to protect the consumer. This offers an example of the "insurance" and "virtual trust" concepts used in combination. Virtual trust is employed to create a new channel for cash flow and the insurance model ensures that security controls are placed upon this revenue stream.

In the Northeastern United States, EZPass is an RFID system that allows customers to pass through highway tolls and be automatically billed per month. In addition to collecting dollars and cents, RFID / EZPass created a new revenue stream for the states that use it.

Security professionals are aware that RFID is not an overly secure protocol. Research has revealed that RFID transmissions may be captured and burned onto other RFID chips (cloned) or replayed. But we should not dismiss the concepts of virtual trust so quickly. Rightly or wrongly, consumers and corporations are relying on RFID tokens to conduct commercial activity. Research may indicate that the level of trust individuals are placing in this technology is unfounded and that the security protocols employed in RFID must be strengthened. Nonetheless, it is clear that people are trusting the RFID

tokens to conduct transactions. RFID is an example of virtual trust created by the authentication security mechanisms used in the protocol.[3]

Let us turn to the reduction of operating expenses. There is historical precedent for the use of virtual trust to reduce operating expenses; however, the reduction is usually attributed to technology rather than to security.

VPN connectivity is a classic study. Businesses reduce their communication expenses by a secure connection via the Internet. Before VPN technology, business needed to purchase lines for each remote location. However, with VPN, these lines were not necessary and publicly available channels requiring less overhead could be used.

Encryption is strongly used in governmental communication in the field of battle. Without such encryption, the enemy could intercept a message and disrupt military strategy. Current technology encrypts and decrypts traffic in real time, enabling secure communications between base and infield units. Traditionally, using the insurance model of information security, we would say that encryption protects the content of the messages. However, from the perspective of virtual trust, encryption enables communication to occur in the manner intended. Without encryption, the value of these messages—due, for example, to interception—would be worthless.

While it is beyond the scope of this paper, it should be noted that Voice-over-IP (VoIP) appears to be the next technology that will demonstrate cost-efficiency in business environments. As often the case with technology that is implemented for internal use only, VoIP is frequently not deployed in a secure manner; security will be assumed

---

3 As mentioned previously, authentication is the presentation and acceptance of credentials to a system; these processes of presentation and acceptance are not the same as non-repudiation. Research concerning RFID technology demonstrates exactly this point: we cannot necessarily trust that the authentication credentials passed to us are valid because it is possible to steal them. However, virtual trust grounded in strong authentication attempts to incorporate non-repudiation and authentication.

because the internal network traffic is presumed to be trusted. However, as in the case of VPN technology, when VoIP is deployed across the Internet, encryption can be used to create virtual trust.

The most potent counter-argument against the above cases is that the technology, not the security, is the essential business driver. However, this is an inaccurate perception. We feel that, if people are using a specific technology, a certain degree of trust can be assumed when using it. This trust is linked with our belief that the technology is secure enough for whatever use we ascribe to it. Email is a prime example. Most of the time we do not consider encrypting our email; we send it plain text across the Internet. Plain text is secure enough for most email transmissions between entities since we are not really sharing anything of value. However, plain text email is not secure enough to send Social Security numbers, bank account numbers and the password to our online banking account. If I wanted to transmit these pieces of information in a secure manner, I would need to enable my application with the proper control mechanisms. Then the trust would be sufficient to allow me to conduct the necessary transactions. It is precisely this type of assumption that permits our internal network traffic to remain unencrypted, yet also allows us to feel secure about the corporate network.

V. Further Virtual Trust Concepts Defined

We have examined virtual trust from both a macro and micro perspective. At this point, it is worthwhile to further distinguish the virtual trust model from the "insurance" model as defined earlier in this paper.

The model of virtual trust incorporates a series of concepts intended to achieve enablement instead of protection. We should note here again that enablement does not displace protection as a valid model. Indeed, the protection mechanisms play an integral role within the enablement process. But the enablement model represents a significant change in mindset.

The concepts that comprise enablement, or virtual trust, are derived from both business and from information security. As has been mentioned previously, the security component is often mistakenly identified with the technology within which security controls are embedded. That is, we merely presume that a specific technology—such as a communication network—is trusted in two ways: first, we assume, rightly or wrongly, that security is inherent in the technology (internal networks are a good example of this); second, the things we do with technology are assumed to be secure to the extent that we can use them and they are useful. In reality, however, security controls—such as encryption—are separable from the technology over which controls have been established. Virtual trust is not merely an accidental byproduct of implementing technology; it is the result of a convergence between specific technologies that perform security functions (e.g., encryption, digital certificates) and technologies that transmit or store data (e.g., VPN, VoIP).

The insurance paradigm has adopted a triad of concepts as its central mission--securing the confidentiality, integrity and availability (CIA) of data. At the root of these concepts is the notion of protection: we must protect the data from being viewed by an individual who is not authorized; we must protect the data from being changed when it

should not; and we must protect our resource so that when an authorized individual needs access to the data they may be able to do so.

Our core virtual trust concept is cash flow. Essentially, cash flow is a revenue stream for a business; it's how a business makes money through invoicing. We will not examine this concept in detail, as we have discussed it earlier.

The next concept, reducing operating expense, will also be treated lightly because it, too, has been considered previously. Basically, the reduction of operating expense—viewed from the perspective of information technology—usually consists of automating a process to reduce overhead.

Productivity is our next term. We may define productivity as "increasing cash flow while reducing operating expense." Traditionally, productivity is associated with technology; however, with the proper security, we can also increase productivity. BlackBerry devices are an example of enhancing productivity via secure transmission of information to end points.

One may object and say that we have insecure BlackBerry configurations and this is just as productive, if not greater, than secured BlackBerries. This response, however, is not satisfactory because it does not account for the risks being taken in terms of trust and asset value. As mentioned earlier, the proper response to this objection is that we run at a trust level—rightly or wrongly—associated with the perceived risks associated with using a specific technology. We don't use the devices without security; rather, we use them at a security level consistent with our perception of the benefits of operating the device by comparison with our perception of a particular level of risk.

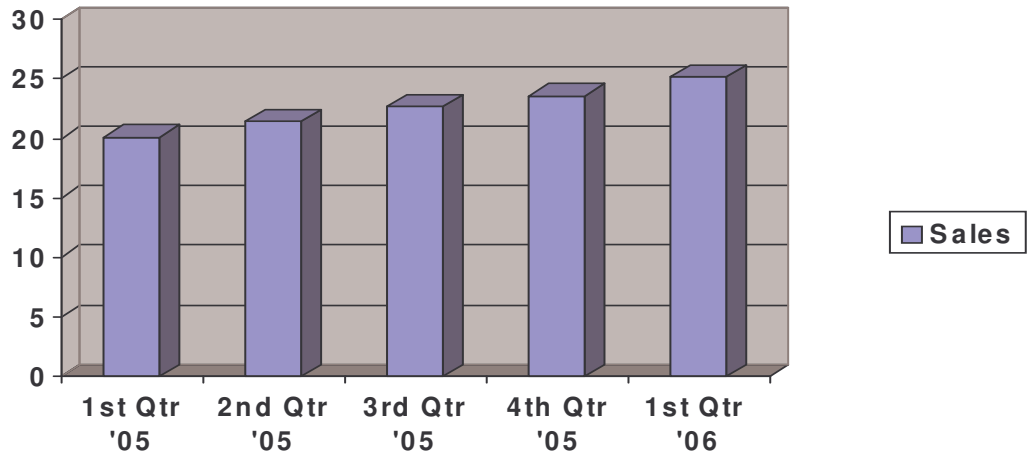
Transparency is another relevant concept. To end users, the enabling security must not be overly visible because security mechanisms are often viewed as obstacles to efficiency. The end user must be able to take for granted that the system they are using is secure. This transparency is dependent upon trust. Transparency allows for seamless transactions between various parties using, for example, digital certificates as the authentication mechanism. This transparency allows for an increase in productivity from an internal business perspective. It also enables a greater generation of cash flow because the end user, with, for instance, an RFID token, does not need to think before scanning the token (impulse buying). Also, the transparency of security decreases the effort to purchase items (e.g., coins are not put in soda machine, credit cards receipts do not need to be signed, traffic passes smoothly through toll booths).

Data flow is our final term. Data flow exists at two levels: on a communication network and within an application. At the network level, it represents the passing of data from one end point to another. At the application level, data flow is the moving of information (such as records) from one entity's processing unit to another. Data flow can be considered the equivalent of cash flow. That is, data flow is the business transaction itself and, therefore, is how cash flows are created through technology. Traditionally, we thought that we must protect data as it flows from one end point to another. In our new virtual trust model, we say that we need to create a *secure* data flow from one end point to another. We assume that within this enablement we will protect the data. The purpose of rephrasing is not just rhetorical; the purpose is to show that our goals are, in fact, different.

Cash flow is the goal of commercial enterprise, and as we enable and build trust through authentication, we will not forget that the CIA triad helps to create a reliable environment within which commercial transactions can occur. But it is the secure enablement of virtual trust between parties that will allow for the creation of business through security, rather than using security only as a mechanism to protect our assets. We will, in fact, *create* assets rather than just build walls around them.

VI. The Future of Virtual Trust

Every quarter, the Census Bureau publishes a statistical analysis of the growth, or decrease, of retail sales in the United States. Since at least the first quarter of 2005, the analysis has identified trends related to e-commerce, defined as the placement of orders and the negotiation of terms of sale over an online system [17]. The most recent data indicate that electronic commerce has experienced significant growth during the past five quarters. The following chart illustrates the progressively higher volume of e-commerce, measured in billions of dollars [17].



The report also states that sales attributed to e-commerce transactions have increased an average of 5.66% during each of the measured quarters. By comparison, retail sales not conducted online experienced an average growth of only 1.84% in this time frame. These data suggest that electronic commerce will represent an increasing source of sales activity in the future, despite the warnings of some commentators that consumers' fears of identity theft may stifle online business activity.

"Virtual trust" has made possible a considerable proportion of this sales volume, at least regarding Internet transactions. (At this time, we cannot speculate concerning the extent to which virtual trust enables business occurring via extranets, Electronic Data Interchange networks, or email.) As the cash flow attributed to e-commerce continues to expand and to represent an ever-greater portion of the total value of retail sales, and as this growth is increasingly dependent upon the technical mechanisms that provide trust between businesses and their partners and customers, it is possible to make several predictions concerning the future of virtual trust. This future has implications for developments in electronic commerce and other online transactions, legislation, the evolution of information security, the metrics by which the benefits of information security are measured, and the security software industry.

Developments in electronic commerce

In the not-so-distant past, you used a personal computer to browse the Web and a cell phone to make telephone calls. Now, of course, these distinctions are passé: cells are equipped with browsers, and voice-over-IP enables telephone communications via the PC. This "device convergence"—the tendency to enable many functions from a single computing device—is now a reality, as attested by even a cursory visit to your local

electronics store. And, also verifiable at your store, the bundled functions are increasingly supported by portable devices, such as PDAs, instant messaging equipment, and mobile phones.

These powerful devices are capable of supporting the software required for virtual trust. PDAs and cell phones, for example, can receive and store cookies, exchange digital certificates, and conduct transactions in an encrypted session. The portability of these devices, and the accompanying capability to engage in virtually trusted communication and commerce, have eliminated many of the traditional barriers to the conduct of business. Websites can communicate with customers on a global basis, and at any time. eBay, for example, will accept bids from cell phones on a 24x7 basis. Music can be downloaded to a cell phone whenever desired by the consumer. Retail banks can notify customers, via mobile phone text messages, concerning authorized—and potentially unauthorized—transactions. Radio Frequency Identification, RFID, permits orders from vending machines—even at 3:00am. Time and geography are not necessarily obstacles within this worldwide marketplace. And the "virtual trust" paradigm of information security has, to a considerable extent, helped create the marketplace.

The ultimate objective of electronic commerce is to enable ***any transaction, anywhere, and at anytime***. Obviously, there are limits to the feasibility of this objective: you may have your RFID device, but the vending machine is nowhere in sight. However, the bundling of functions within portable devices, the expansion of communications networks, and the increased reliance upon virtual trust are making e-commerce a ubiquitous reality. The major remaining obstacles are, it seems, cultural rather than technical. Language barriers, for example, may inhibit some web-based transactions.

Mechanisms to bridge these cultural divides must be devised before customers are able to conduct any transaction, anywhere, and at any time.

Legislation

The Federal Deposit Insurance Corporation has required national banks within the United States to implement "strong authentication" for electronic banking transactions. Use of an ID and a password or PIN is no longer sufficient to access an account from the Internet. The FDIC mandate is, it seems, based upon several assumptions: (1) electronic banking will represent an increasing volume of retail activity; (2) a high degree of virtual trust between banks and their customers is required in order to transact business remotely; and (3) so-called "dual authentication"—consisting traditionally of a user ID and password—does not provide sufficient trust.

If these assumptions are valid, it is likely that the concept of "strong authentication" will be applied to ever-expanding array of online transactions, especially those involving sensitive information. It seems probable, for example, that the transmission of medical data may require a greater degree of virtual trust than is currently required. Similarly, email messages that represent the conduct of financial or legal transactions will require strong authentication between sending and receiving parties. It is anticipated that legislation requiring the implementation of this authentication will occur, possibly at both the state and federal levels.

Revisiting the "Insurance Model"

The virtual trust paradigm of information security is essentially concerned with the issue of authentication. A digital certificate, for example, is issued in order to assure a customer that he or she is, in fact, conducting business with a specific organization.

However, virtual trust also usually involves the encryption of data and may require customer information derived from a cookie stored on the client's PC or other device. Thus, the elements of encryption and identification, important components of the "insurance model" paradigm, are also incorporated into "virtual trust."

The practice of information security, developed during the past four decades, has created additional tools and concepts that may usefully be incorporated into the virtual trust model. For example, the logging and monitoring of security-related events is a significant and necessary effort; auditors currently expect, as a matter of due diligence, that information security staff will capture and retain electronic or hardcopy evidence of events occurring within networks and systems. Logging and monitoring tools could perform similarly valuable services for the virtual trust function. For example, customers would be able to review reports describing recent online transactions or receive automated alerts concerning possible unauthorized activity. Current reporting mechanisms are usually implemented on an *ad hoc* basis only—businesses voluntarily determine that transactions will be confirmed via email. Similarly, customers are not automatically notified if a transmitted digital certificate has expired; a conscious effort to discover this information must be made. However, increasing reliance upon virtual trust seems to require that logging and monitoring tools must be more accessible and meaningful to customers. Buyers need not beware that their money has been spent and that records of the transaction are nonexistent.

"Layered security" is another concept that may beneficially be borrowed from the "insurance model" paradigm. The idea of "layering" refers to the process of implementing numerous security controls, some of which perform seemingly redundant

functions, in order to prevent unauthorized access. "Layered security" is frequently applied to networks, especially those that connect internal applications and systems to the untrusted Internet. Properly configured routers, firewalls, and intrusion detection and prevention systems are all integral elements of a layered approach to network security. This form of security is expensive, because of the many software purchases involved, and it is time-consuming to test, implement, and monitor. However, it is deemed necessary in order to prevent unauthorized intrusions into a network that provides access to important data. "Layered security" does not, unfortunately, offer a seamless and centralized means to protect network resources; it is often a rather messy patchwork of unconnected software.

The virtual trust paradigm of information security will, in the not-distant future, confront the problem of whether or not to adopt a layered approach to its promise of delivering trusted transactions. It is tempting, for example, to envision handheld computing devices that embed security controls capable of automating the processes of connectivity, identification, authentication, authorization, and encryption. The user simply accesses an e-commerce site via the browser, the customer and the business are mutually authenticated, and transactions can occur with no further ado. Similarly, it is an appealing prospect to imagine a universal connectivity standard that eliminates the need for storing multiple cookies, or receiving numerous digital certificates, or the remembering of innumerable passwords.

As mentioned previously, several retail banks have, in fact, recently implemented a form of virtual trust that authenticates user transactions in an efficient, seamless manner. The customer simply holds his or her bank card to a point-of-sale terminal and,

when read by an RFID device, the customer's account is debited and a purchase made. The messiness of "layering" has been tidily cleared: there is no password to remember, no PIN to enter, no signature to write or authenticate. "Virtual trust" has become very simple indeed.

However, has the process of authentication become so simple that trust is eroded? Is the mere act of holding a card that is read electronically equivalent to virtual trust? Banks that adopt this system are clearly aware that the card may be "held" by an unauthorized person; perhaps a decision has been made that the benefits associated with ease-of-use outweigh the costs associated with fraud. At any rate, these banks have chosen to implement virtual trust without layered security.

Electronic commerce transacted via the Web often represents an attempt to incorporate virtual trust into a layered security environment. Digital certificates provide authentication, the web site usually requires identification and further authorization of the user, cookies supply certain details concerning customer preferences, and an SSL session offers an encrypted session. Several components, some of which are apparently redundant, comprise the totality of virtual trust. These components are analogous—if perhaps less messy—than the elements comprising traditional "layered" network security. However, in the Web-based context, layering is intended to ensure that a high level of trust is present before money is exchanged and goods purchased.

Does the layered approach adopted by most major websites truly guarantee a high level of trust? Or is the point-of-sale bank card, absent of multiple security controls, a good-enough method of authentication? If, as mentioned previously, legislation will increasingly focus upon the need for strong authentication when funds are transferred

electronically, it seems that "layered security" may emerge as a required element of the virtual trust paradigm. However, as exemplified by easy point-of-sale authentication based upon RFID technology, businesses may be reluctant to encumber customers with security controls. It seems that the "trust" element of "virtual trust" will be subject to increasing scrutiny and possible redefinition.

Beyond the Metrics of Loss Prevention

Economists have proposed three major methods for measuring the dollar value of benefits derived from implementing security controls. As summarized in the annual *CSI/FBI Computer Crime and Security Survey*, these methods include Return on Investment (ROI), Net Present Value (NPR), and Internal Rate of Return (IRR) [16, 9]. These metrics essentially consist of comparing the costs associated with information security—especially salaries, software licensing fees, hardware purchases—to the estimated value of money saved by preventing loss. Proponents of these metrics acknowledge that assigning dollar amounts to potential losses is an highly subjective matter—how, for example, is preventing loss due to damage of corporate reputation assigned a monetary value? [11]. However, the metrics of loss prevention remain our only means of conducting cost/benefit analysis for the information security function.

The virtual trust paradigm introduces a new perspective from which to view metrics. Because virtual trust creates the possibility of commerce conducted from remote locations, and because this trust is established for the explicit purpose of generating cash flow, it may be possible to develop metrics that recognize information security as an enabler of business. Such measures would, assumedly, involve a comparison of relevant costs—such as expenses associated with the purchase of digital certificates and the

support of additional identification and authentication systems—to the value of commerce generated by virtual trust. Although this value is subject to the same subjective interpretation as the metrics involved with loss prevention, quantitative research has been conducted concerning the likelihood of customers to patronize online sites that provide a high degree of trust [3]. For example, the online brokerage firm E*TRADE has estimated that the implementation of strong authentication has increased its trading volume by 30% [14].

As the volume of electronic commerce continues to expand, and as this expansion is increasingly dependent upon virtual trust, it seems that metrics intended to quantify the economic value of information security cannot ignore the income generated as a result of establishing trust.

"Virtual Trust" as an Over-the-Counter Product

Less than ten years ago, many businesses seeking to engage in electronic commerce hired specialists to design, develop, implement, and maintain websites. The specialists frequently included HTML and Java programmers, graphic designers, and network professionals. these developers comprised the burgeoning "dot com" industry. However, as websites proliferated and became increasingly central to Internet communication and to e-commerce, the tools required to develop these sites emerged as over-the-counter products. Computer stores in local malls now invite would-be online merchants to purchase software that greatly simplifies the web development effort. With a bit of ingenuity and patience, anyone wishing to establish an electronic storefront can create their own e-business presence.

Based on this democratization of web design, it seems reasonable to assume that "virtual trust" is likely to experience a similar destiny as an over-the-counter product intended to empower amateurs. Currently, the issuance of digital certificates largely remains the business of private "authorities." Similarly, the enabling of SSL sessions and the design and transmission of cookies have remained the responsibility of technical specialists. However, as virtual trust becomes an increasingly critical component of the e-commerce arena, the elements that comprise this trust will be more readily available to the buying public. Indeed, this trend has already begun: Windows XP includes a feature to permit digital certificates, or electronic signatures, to accompany email transmissions; eBay has now entered the business of selling digital certificates to its participating merchants. However, there are no technical or legal obstacles to the packaging of virtual trust as a readily purchased software product. Aspiring e-commerce entrepreneurs will be provided the tools required to use digital certificates and signatures, to design and transmit cookies, and to provide encrypted sessions.

The Future of "Virtual Trust": Opportunities to Grasp and Lessons to Learn

If the present expansion of electronic commerce continues at its current rate, the role of virtual trust will assume even greater centrality. New products and services—such as virtual keys for automobiles and the notarizing of legal documents via electronic signatures—will, doubtless, emerge. However, this future is not necessarily limitless; serious obstacles remain that will, and should, serve to constrain the reliance upon virtual trust as a critical enabler of business. As mentioned previously, cultural barriers—including diverse languages and privacy regulations—cannot be ignored as potential brakes upon the momentum currently experienced by the virtual trust paradigm.

Similarly, the paradigm must confront the issue of "layered security" and determine if weak authentication alone is sufficient to guarantee consumer trust, or if additional security controls must be borrowed from the tools currently associated with the "insurance model."

VII. Enabling trust may become the dominant paradigm of information security

We believe that the new virtual trust model may become the dominant paradigm of information security. Businesses exist in order to generate revenue and, ultimately, profit. Protection of assets is simply a cost of doing business, and commercial enterprises wish to decrease expenses whenever possible. However, virtual trust focuses upon the enablement of business to generate more cash and, hence, increased profit; the objective of protecting assets, while an integral component, is not the primary goal of virtual trust. It seems that profit-oriented enterprises, while seeking to gain and maintain a competitive advantage, will increasingly adopt and measure the benefits of information security as presented from the perspective of virtual trust. This perspective asserts that some security controls—such as digital certificates and signatures—actually create the possibility of doing business. A visit to any major e-commerce website quickly reveals that information security is no longer concerned merely with protecting assets and providing insurance against loss. FUD has become an obsolete rationale for the existence of information security.

There are additional reasons to anticipate the increasing dominance of the virtual trust model. First, as mentioned previously, the continued expansion of commerce conducted remotely—an expansion encouraged by the ubiquity of multi-functional

mobile devices—is dependent upon the establishment of trust. Second, the vested interests of businesses and information security professionals will promote the significance of virtual trust. Commercial enterprises will seek new methods to provide secure, yet also efficient, relationships between themselves and their customers; information security professionals will strive to develop these methods. Third, as a result of the demand for processes and products that establish trust, new employment possibilities will be created since security will be pushed out into a new space. Finally, information security professionals will have a more positive and more important role within the organization; they will be viewed as creators of cash flow, revenue, and profit.

The enabling trust function will promote information security as a critical driver of business, not merely a system of controls that pleases auditors, satisfies regulators, and prevents loss. The virtual trust model of information security is not based upon selling fear; it envisions security as a creator and driver of business.

References

1. Apple – iTunes – 1 Billion Songs (nd). http://www.apple.com/itunes/1billion/

2. *CobiT Online* (4th edition). (2006, January 1). Information Systems Audit and Control Association.

3. E-commerce, trust, and SSL. (nd). http://www.verisign.com/ssl/ssss-information-center/commerce-trust-ssl/index.html.

4. Fed's IT spending to reach $6.3 B. (2006, July 10). *Washington Business Journal*.

5. *FFIEC IT examination handbook*. (2003, September 11). ABC Corp.

6. Finally, a real return on security spending. (2002, February 15). *CIO Magazine*.

7. Katzan, H., Jr. (1973). *Computer data security*. New York: Van Nostrand Reinhold.

8. Lemos, R. (2006, July 14). Daily flaws ratchet up disclosure debate. http://www.securityfocus.com/print/news/11400.

9. Lucas, K. (nd). Economic evaluation of a company's information security expenditure. http://www.infosecwriters.com/text_resources/pdf/Economic_Evaluation.pdf.

10. McNeil, J. (1978). *The consultant*. New York: Ballantine Books.

11. Mercuri, R.T. (2003). Security watch: Analyzing security costs. *Communications of the ACM* 46(6).

12. Parker, D.B. (1976). *Crime by computer*. New York: Charles Scribner's Sons.

13. Security survivor all-stars. (2006, June). *Information Security Magazine*.

14. Stiennon, R. (2006, June 1). Speech at Trend Micro executive briefing in New York City.

15. SWIFT Annual Report 2005 (2006). *SWIFT Annual Report 2005: Raising ambitions* http://www.swift.com/index.cfm?item_id=59684

16. *Tenth annual CSI/FBI computer crime and security survey*. (2005). Computer Security Institute.

17. U.S. Census Bureau. (Last revised: May 18, 2006). http://www.census.gov/mrts/www/data/html/06Q1table1.html.

18. Use FUD to talk risk and security. (2005, August 1). *ZDNetAustralia*.

19. Ware, W.H. (ed.). (Reissued October, 1979; originally published 1970). *Security controls for computer systems.* Washington, D.C.: Office of the Secretary of Defense.

Biographies

Kenneth F. Belva, CISSP

is currently employed at Credit Industriel et Commercial (New York) where he manages the Information Technology Risk Management Program. He reports directly to the Senior Vice President and Deputy General Manager. He is currently on the Board of Directors for the New York Metro Chapter of the Information Systems Security Association. He authored the contrarian paper: "How It's Difficult to Ruin A Good Name: An Analysis of Reputation Risk." He has presented on topics such a patch management as well as moderated a panel discussion on corporate governance. He taught as an Adjunct Professor in the Business Computer Systems Department at the State University of New York at Farmingdale. Mr. Belva is credited by Microsoft and IBM for discovering vulnerabilities in their software. He is the author of the chapter "Encryption in XML" in Hackproofing XML published by Syngress. Mr. Belva holds the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) certifications and has passed the Certified Information Security Manager (CISM) exam. In addition to his professional responsibilities, he currently sits on the Board of Directors for Franklin and Marshall College's Regional Alumni Council for the New York Metro area.

Sam H. DeKay, PhD.

has worked in field of information security for more than twenty years. Dr. DeKay is currently responsible for developing information security policies and standards at The Bank of New York. Prior to this, he served as Manager of Information Security at Empire Blue Cross/Blue Shield and at ABN Bank (now ABN AMRO), New York. In 2003, he was designated a Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association. In this capacity, he has written and

edited study materials intended for security professionals planning to take the examination leading to CISM certification. Dr. DeKay has also been appointed a member of the Generally Accepted Information Security Principles (GAISP) Project, under sponsorship of the Information Systems Security Association. In addition to holding memberships in the Information Systems Audit and Control Association and the Information Systems Security Association, he is also an active participant of the Technology Managers Forum. He holds PhD degrees from Columbia University and Fordham University.