Cutter IT Journal

The Journal of Information Technology Management

Vol. 19, No. 5
May 2006

"This month we turn from overall strategic considerations to more utilitarian issues, as we go from asking whether we need to do something different to asking what, specifically, we should do."

— Larry Clinton, Guest Editor

Securing Cyberspace: What Exactly Should We Be Doing?

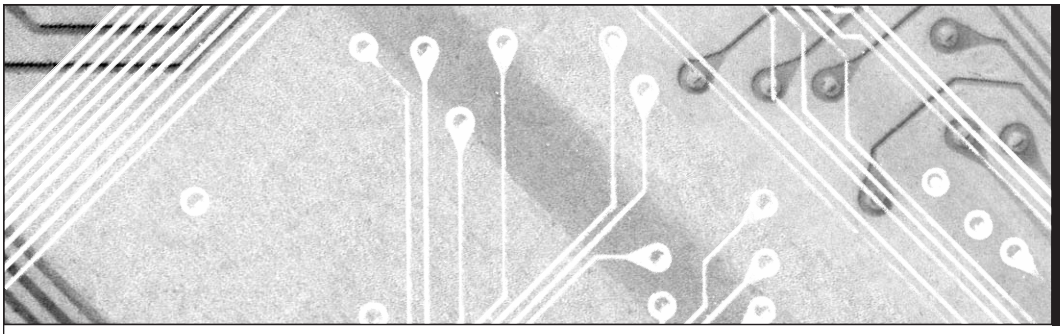
Start Rewriting

Current cyber security strategies are like putting Band-Aids on a cancer. Unless we do the R&D necessary to rewrite the core protocols the Internet is based on, such as TCP/IP, we are headed for economic — and possibly physical — disasters.

Get It in Writing

Responsible corporations already have the best possible tool to expand the perimeter of true Internet security, but many are failing to use it. Properly drafted commercial agreements can do more to expand good security practices than any SOX-like legislation.

CUTTER CONSORTIUM



Cutter IT Journal

About Cutter IT Journal

Part of Cutter Consortium's mission is to foster the debate of, and dialogue on, the business technology issues challenging enterprises today, to help organizations leverage IT for competitive advantage and business success. Cutter's philosophy is that most of the issues that managers face are complex enough to merit examination that goes beyond simple pronouncements. Founded in 1987 as *American Programmer* by Cutter Fellow Ed Yourdon, *Cutter IT Journal* is one of Cutter's key venues for debate.

The monthly *Cutter IT Journal* and its weekly companion *Cutter IT E-Mail Advisor* offer a variety of perspectives on the issues you're dealing with today. Armed with opinion, data, and advice, you'll be able to make the best decisions, employ the best practices, and choose the right strategies for your organization.

Unlike academic journals, *Cutter IT Journal* doesn't water down or delay its coverage of timely issues with lengthy peer reviews. Each month, our expert Guest Editor delivers articles by internationally known IT practitioners that include case studies, research findings, and experience-based opinion on the IT topics enterprises face today — not issues you were dealing with six months ago, or those that are so esoteric you might not ever need to learn from others' experiences. No other journal brings together so many cutting-edge thinkers or lets them speak so bluntly on issues such as:

- Proving the value of IT ROI
- The give and take of offshore outsourcing
- The value of high-quality data
- The evolution of agile project management
- When and how to kill a dying project

Cutter IT Journal subscribers consider the Journal a "consultancy in print" and liken each month's five or six articles exploring a single topic to the debates they participate in at the end of a day at a conference — with every participant in the conversation forcefully expressing his or her viewpoint, backing it up with data and real-life experience.

Every facet of IT — application integration, security, portfolio management, and testing, to name a few — plays a role in the success or failure of your organization's IT efforts. Only *Cutter IT Journal* and the *Cutter IT E-Mail Advisor* deliver a comprehensive treatment of these critical issues and help you make informed decisions about the strategies that can improve IT's performance.

Cutter IT Journal is unique in that it is written by IT professionals — people like you who face the same challenges and are under the same pressures to get the job done. The *Journal* brings you frank, honest accounts of what works, what doesn't, and why.

Competition remains intense in the high-tech world. Budget cutbacks and short deadlines have become the norm. You need advice and experience you can rely on. Put your IT concerns in a business context. Discover the best ways to pitch new ideas to executive management. Ensure the success of your IT organization in an economy that encourages outsourcing and intense international competition. Avoid the common pitfalls and work smarter while under tighter constraints. You'll learn how to do all this and more when you subscribe to *Cutter IT Journal*.

Cutter IT Journal®

Cutter IT Journal® (ISSN 1522-7383) is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700 or, within North America, +1 800 964 5118; Fax: +1 781 648 1950 or, within North America, +1 800 888 1816; E-mail: citjeditorial@cutter.com; Web site: www.cutter.com).

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Information LLC. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.

Opening Statement

by Larry Clinton

FROM STRATEGY TO PRACTICE

Like this edition, January's *Cutter IT Journal* was focused on cyber security. The organizing question for that installment was, "Is it time to rethink our strategy?" Much to the chagrin of those who look to these pages for vigorous debate, there was broad consensus: "Yes. Absolutely. Are you kidding?"

This month we turn from overall strategic considerations to more utilitarian issues, as we go from asking whether we need to do something different to asking what, specifically, we should do. And while the last cyber security issue was populated primarily with "outsiders" from government, academia, and think tanks, the current issue calls on the real-world experience of industry practitioners, who address "next steps" from both macro and micro perspectives.

Among those who should find advice about practical next steps in their own work are:

- C-level executives (CEOs, CIOs, CSOs, COOs)
- IT, business, and risk managers
- Internal and external auditors and accountants
- Internal and consulting attorneys
- Business development specialists
- Technical standard setters, researchers
- Teams that work with these individuals

BOTTOM-UP, TOP-DOWN, OR BOTH?

Our first two articles both address macro-level cyber issues but take substantially different approaches. Bill Hancock of SecureInfo Corporation looks at the core technical problems that underlie cyber insecurity and argues for rebuilding the foundation of the Internet from the bottom up. Debra van Opstal of the Council on Competitiveness takes a decidedly top-down approach, as she argues that the entire issue of corporate security needs to be recast at senior levels in order to fully appreciate the business benefits that improved resilience will yield.

There can be a no more fundamental approach to addressing cyber security issues than to focus on the core protocols upon which the Internet is built. Hancock argues that the problems we are currently seeing in cyber security are about to get much worse (a theme echoed in virtually all the articles in not only this edition but the January one as well) because we continue to deploy base technologies that were developed almost 30 years ago, when security was not an issue. According to Hancock, we need to:

1. Fix TCP/IP
2. Secure growing wireless communications methods
3. Address identity management issues

Hancock views TCP/IP as a highly useful protocol, which rightfully will be used in all future networks, but one that "never had any security methods built into it." He then offers a series of technical steps that need to be undertaken in the next 10 years to address these issues.

The problems of wireless cyber security start with the handsets themselves, none of which, according to Hancock, has reasonable operating system self-protection from viruses, worms, and other attack profiles. Compounding the growing problem of wireless insecurity are those pesky users. Hancock predicts that users of the future will demand ubiquitous wireless access but will be reluctant to set up the security offered for their devices simply because of the technical effort required.

Next, opting for understatement, Hancock characterizes identity management as a "massive problem" that will require R&D and "a lot of it." He concludes by discussing the thorny questions of who should be doing the needed R&D to address these problems and who should pay for it. TCP/IP was created by the US federal government, while most of the recent technological innovations have come from startups or grassroots groups. There is substantial doubt that the latter groups can, or should, be the mechanisms for addressing the larger emerging problems we face.

As I have argued in these pages previously, the only mechanism dynamic enough to address cyber security issues on a sustainable basis is the profit motive. As a result, we must continue to pursue the development of a business case for security. Into this breach steps van Opstal, who suggests we need to move beyond security — which many infer is a government concern focused on stopping terrorism — and consider these problems as part of a "resilience imperative" for business.

Instead of addressing the IT managers, R&D scientists, and industry standard setters to whom Hancock is speaking, van Opstal redirects our thinking to the upper levels of corporate management, which, she says, must become more fully engaged. Van Opstal reports on a study the Council recently conducted to determine whether a business case can be made for investment in security and resilience. The conclusion is that although the business case for antiterrorism is weak, there is a compelling case for security. It will, however, require "transformational thinking … about security, risk, and resilience." Perhaps most importantly, the market must understand how to value these investments.

Although the Council's study initially focused primarily on addressing physical security needs, the Internet Security Alliance has recently agreed to partner with the Council to assure that cyber issues are likewise addressed. The partnership is cemented by the similar approaches the two organizations take to the issues, the most central of which is a shared focus on the need for change *in* the private sector *by* the private sector.

The Council's study found that "most companies don't think of security as a core value driver. Organizationally, the security function is often decoupled from risk management, business continuity, and strategic planning, and that limits the ability to create business benefits from security. The resulting 'risk silos' have the perverse effect of increasing the overall risk profile."

What needs to happen? First, we have to agree on a consistent definition of security. The roles of CIOs and CSOs must become well understood within the corporation. Organizations must develop and adopt metrics for success and implement regular security training. According to the Council, adopting these measures could lead to substantial corporate benefits, such as productivity gains, streamlined workflow, lower insurance costs, new revenue opportunities, and reduction in legal and regulatory risks.

USING CONTRACTS, INSURANCE, AND COALITIONS TO ASSURE SECURITY

While our first two articles address issues primarily of concern to the "generals" charged with designing core protocols and determining corporate structure, the next three articles address the needs of the field officers and foot soldiers who focus on planning and implementing the day-to-day activities of business. Each of them describes a case of industry leadership worthy of emulation.

Jeffrey Ritter begins by observing that the modern "extended enterprise" often requires the management of a portfolio of relationships among multiple business parties (suppliers, customers, outsourced service providers, etc.) and that managing these relationships effectively is proving difficult. Among the most challenging aspects of these relationships is the need to adequately define the required functions or services in order to enter into a contract for their performance by others. Often there are few integrated descriptions of what needs to be done, and those that do exist (e.g., operations manuals) rarely contain enough detail to sufficiently specify the needed functions in a service contract. As a result, the service agreement can become a battlefield for the parties either before or, worse, after the deal has been initiated.

One of the critical factors often overlooked in these agreements is the need to manage information security, even though it is now essential to do so. This need has become even more apparent as enterprises become ever more global, engaging service providers operating in different countries, under different legal systems, and

with different controls for protecting electronic information. Unfortunately, there have been very few resources to help IT professionals, information security officers, auditors, and attorneys understand how to structure the relevant contract provisions — until now.

Contracting for Information Security in Commercial Transactions — An Introductory Guide is a resource Ritter helped develop that provides guidance for parties in addressing information security issues when negotiating commercial agreements. Such negotiations should take account of staffing, system infrastructure, regulatory exposure, funding requirements, and allocations of liability, all or any of which could impact, or even disrupt, the business case for the agreement.

Even if businesses actively adopt and agree to extensive security measures to protect against system breaches, they cannot eliminate every possible loss. The inevitability of attacks, at least some of which will be successful, is the most obvious reason to include insurance in the corporate arsenal of security and resilience measures. Ty Sagalow, AIG's president of product development, general insurance, argues that a comprehensive approach to risk management typically includes the purchase of insurance. In the physical world, we buy insurance for a wide variety of threats, including fire, earthquake, flood, and legal liability of various kinds. Sagalow argues that the value of insurance applies with equal force to the cyber world.

Sagalow points out that insurance has been recognized as a core element of the United States' *National Strategy to Secure Cyberspace*, issued in February 2003. Not only can cyber insurance mitigate against a potentially devastating attack, but the use of insurance can be one of the clearest market drivers for improved security practices within corporations, thus strengthening overall defense. Just as the use of auto insurance discounts has led to safer driving, so too can cyber insurance discounts lead companies to improve their security posture. Thus, greater use of cyber insurance is a win-win proposition from both industry and public policy perspectives.

Yet a different example of industry leadership is described in the article by Steve Ruwe of Visa. Ruwe observes that while fraud was once "chiefly committed locally, one victim at a time, the greatest threats today come from highly sophisticated crime syndicates throughout the world that seek to steal data from thousands of consumers at a time." Several years ago, Visa developed its Cardholder Information Security Program to provide incentives for merchant banks to adopt best practices for securing cardholder data. In 2004, the congressionally appointed Corporate Information Security Working Group (CISWG) recognized that program as the best of its kind.

However, realizing that cyber security must inherently be a cooperative project, Visa worked with its sister companies in the payments industry to develop a new industry standard. By essentially forming a "neighborhood watch" program for the payments industry, Visa has assisted in fortifying the environment even further. Ruwe's article not only outlines the basics of these collaborative programs, but also lays out an agenda for the industry to move forward with the help of both consumer organizations and government.

BACK WHERE WE STARTED

Finally, Greg Garcia from the Information Technology Association of America (ITAA) brings our discussion full circle. Just as Bob Stephan, Assistant Secretary for Infrastructure Protection at the US Department of Homeland Security, began our January edition on cyber security by calling for an industry-government partnership, so too does Garcia.

Garcia lays out an extensive programmatic list of public policy "to do" items for various players, including the US Congress, international bodies, and private industry. He warns that if industry does not seize the initiative, Congress will step into the breach and begin to regulate. While Garcia's warning may once have seemed a chilling prospect, the dire security picture painted by the numerous articles in these two issues suggests that government intervention and cyber security regulation may be the least of our worries.

Larry Clinton is the COO of the Internet Security Alliance (ISAlliance), a leader in advocating market-based systems for improving information security. Mr. Clinton served as cochair of the US congressionally appointed Corporate Information Security Working Group (CISWG) on market incentives, which developed recommendations to encourage better corporate security without federal mandates. Mr. Clinton testified before Congress on this program in April 2005. He also sits on the board of the National Cyber Security Partnership (NCSP), the Internet Education Foundation, and the US Congressional Internet Caucus Advisory Committee, and chairs the NCSP Committee on Incentives for Improved Corporate Security. In addition to publishing and testifying on cyber issues, Mr. Clinton has appeared on C-SPAN, MSNBC, and CNBC to discuss information security. Prior to joining ISAlliance, Mr. Clinton was with the US Telecom Association (USTA) for 12 years, including the last six as a VP. Before joining USTA, Mr. Clinton was a Legislative Director in the House of Representatives and consulted for a variety of industries. He can be reached at ISAlliance, 2500 Wilson Blvd., Arlington, VA 22201, USA; E-mail: lclinton@isalliance.org.

How to Stop Talking About — and Start Fixing — Cyber Security Problems

by Bill Hancock

Why are viruses so successful in killing systems? The answer is simple: operating systems do not protect themselves. I know this to be true. Many years ago, I was an OS developer at a very large computer company. I crafted a product that would check all programs, when they were asked to run, for anomalies and other infestations. To ensure a running system, applications were inoculated at system installation time before the system had a chance to be infected in any manner. In this way, a system "blueprint" of a clean system could be made, cryptographically stored, and used to control any malware introduced into the file system. If infested, the modified program was not allowed to run. Viruses disappeared from that OS, which is still in use today in large, complex computing environments where reliability is a major requirement. It's funny how other vendors did not seem to learn that lesson.

As a security "graybeard," I spend a great deal of time in meetings with companies, developers, government agencies, international consortia, and other assorted groups of people who continually want to do something about cyber security. Yet they never get to the heart of the problem: fixing the issues that cause the security problems to happen.

The problems we see in cyber security — breaches, viruses, worms, data theft, system corruption, network scanning, packet grabbing, and any number of related issues — are about to get much worse. This is mostly because we continue to deploy base technologies that were developed almost 30 years ago, when security was not an issue and we could trust that computers on a network would not try to subvert the operations of others on the network. We continue to write software with programming models of yore, and yet we do not instill good security programming principles (such as the Systems Security Engineering — Capability Maturity Model [SSE-CMM]) in those who write code. We continue to deploy systems and networks in insecure ways for the sake of getting things to market quicker and making money faster, at the risk of compromising customer privacy data and increasing the occurrence of identity theft. At the same time, we strive to make these flawed programming methods and insecure protocols and tools more easily available via wireless technologies in order to make network connectivity ubiquitous. We even extend them to areas where such technology has not previously been a factor: home appliances, automobiles — even clothing.

Consequently, we perpetuate the cycle of poor cyber security and, indeed, make the situation worse as we become more dependent on technological innovations that inherit technical security flaws from the underlying infrastructure and methods used to create them. We both need to create the security components we lack (e.g., cryptographic key management) and better apply the security components we have (e.g., installation of wireless security controls). Without some serious changes in the way we apply security science to the base technologies used to construct the technologies of the future, we are a long way from achieving cyber security.

CYBER SECURITY'S TRIPLE PLAY

So what needs to be done? The technologies of the next 10 years are going to revolve around three basic areas:

1. The TCP/IP protocol
2. Wireless communications methods
3. Identity management

Addressing these three basic areas will go a long way toward making real security possible and breaking the interminable cycle of doom-and-gloom meetings we all seem to be stuck in these days.

Fixing TCP/IP

TCP/IP is a formidable protocol and highly useful for base networking. The problem is that it never had any security methods built into it to ensure that even base security controls (authorized user access, protocol

header verification controls, protocol filter lists, session verification, etc.) were included. As companies look to save money by merging data networking, video, and voice methods into more manageable network infrastructures, the push is on to replace traditional telco methods with TCP/IP networks. Unfortunately, TCP/IP networks do not have the luxury of being private in nature, like SS7, or singular in technical use, like a traditional videoconferencing network.

IP spoofing attacks are possible with TCP/IP because the protocol does not do source address cryptographic verification — an omission that allows DDoS (distributed denial-of-service) spoofing attacks and all sorts of false address infiltration. Basic companion applications such as DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name Server) are sorely lacking in basic security controls, which prevent infiltration of the applications, improper modifications of application data pools and databases, and infiltration of the applications themselves (in which they may be co-opted to help in a cyber attack). The TCP/IP v6 (IPv6) protocol suite does not solve the problem, for a number of reasons:

- It has no strong source authentication.
- It continues to allow the use of many of the same companion protocols as IPv4.
- It does not provide for fine-level controls over packets and transmissions to ensure that only authorized and properly identified packets are allowed on a network.

TCP/IP will be used extensively in all future networks and rightfully so. In its current incarnation, however, it lacks basic security controls and methods to properly protect the network itself, not filtering traffic that is supposed to be on the network and not authenticating and authorizing applications, users, and packets to access network resources when they are supposed to. This leads to scenarios in which the "bad guys" can get on components and the "good guys" cannot stop them. Worse, there are situations in which the good guys do not have the basic access or security controls needed to stop the bad guys, and yet they must deal with the aftermath of bad guy access.

TCP/IP is rapidly becoming a security liability. If we are to reverse this ominous trend, protocol and networking experts need to do serious research to formulate all the proper controls, methods, and technologies to ensure that future ubiquity of the TCP/IP protocol provides for reliability, security, and control over traffic. To improve security within the TCP/IP "stack," vendors of network technologies need to work on the areas outlined below.

Security Programming

Too much critical infrastructure is based upon the TCP/IP protocol in its current state. Emergency reaction networks, critical financial transaction networks, the power grid, process control, water processing, and all manner of critical network infrastructure are using networking as a means to interoperate — without using basic, solid security programming practices and methods. Using an uncontrolled network protocol environment without proper security engineering of applications is a recipe for a security disaster that will affect critical infrastructures throughout the technical universe. Security programming needs apply to the vendor-supplied TCP/IP protocol stacks themselves, base creation protocols (such as ASN.1 and its related compilers), router/switch kernels, secondary supporting protocols (such as ICMP, DNS, DHCP, and others), and all kinds of applications that use the TCP/IP stack to interoperate over a network.

TCP/IP is rapidly becoming a security liability.

Preconfiguration of Network Applications for Proper Security Operations

A lot of network programs that use the TCP/IP stack for interoperation have some (and in some cases, a lot of) security controls and methods within them. Many times, these controls are intentionally disabled or not engaged, as they require the system integrator or sysadmin to selectively turn on/off the controls as needed. These actions often cause application outages and tech support calls. To reduce vendor costs and headaches, the security controls are disabled to allow easier installation of networked applications, leaving the network door wide open for malfeasance. Vendors of networked applications need to enable security controls out of the box and deal with the support issues that come along with good security practices in order to keep networked applications from becoming network targets at inception of use.

Reengineering of Base Protocols to Address "New" Networked Realities

When TCP/IP was invented in the 1970s, its inventors did not foresee how widely the protocol would come to be used. I know — I have personally spoken to the authors many times over the years about protocol

security and related subjects. They have always been quite candid about the lack of security controls in the protocol stack. I am also acutely aware that TCP/IP's initial mission was not to control power grids, critical financial networks, and the other vital infrastructure (such as 911 networks) that TCP/IP currently provisions. All these vitally important uses represent the "new" networked environment, where a weak implementation of security all the way to the base protocol levels results in repetitive and continued attacks on critical infrastructures, which in turn damage components of internetworks.

The user of the future will be wireless and will require ubiquitous access.

TCP/IP stacks are now being used in some very critical locations, yet they lack modern protocol controls that would solve a great many security problems. For instance, a cryptographically sound device identification field in the IP protocol header could be used to identify an incoming packet stream back to an exact creation point that could not be spoofed or faked. If a firewall were to have a method by which to authenticate the header to a device authentication database as part of the initial connectivity "handshake," this would virtually eliminate packet-level DoS and DDoS attacks — whether the session were encrypted or not. Routers could use such a feature to properly establish route paths and network data flows to deal with quality of service (QoS) and route data management.

Routing update attacks would be nonexistent as well, since routers would know exactly which specific routers are allowed to update route paths and which ones are not. Upgrade of transaction handshakes within a protocol session at random times could ensure that the source of a connection is still the original source and that it has not been hijacked mid-session via some third party. These and many other improvements are needed to create a secure protocol suite that can be used freely in critical infrastructures as part of the new network reality.

Engineering for "What's Next" in Security Controls

It is not enough to correct a problem simply for the issues that are currently being experienced. Good engineering means looking ahead and dealing with "what's next" in security controls. A reengineering effort will require a hard look at what types of network challenges and application shifts we will face over the next 10-20 years to ensure that security processes and methods are engineered to handle future network uses. Security controls for bio-implants (e.g., a wireless pacemaker that uses network protocols to adjust settings) are one possible use for future networks. Anything from subcutaneous communications implants to automated transportation systems (e.g., self-driven automobiles) will require a safe and secure networked environment to ensure that they function not only correctly, but securely, to safeguard life.

Securing Wireless Communications

Another major area that will need a lot of work is wireless access. This would include the traditional wireless data networking types (such as Wi-Fi [802.11] or WiMAX [802.16]) but also traditional cellular protocols, which are rapidly being moved into a voice and data mix (CDMA, TDMA, GSM, GPRS, 3G). The big issue here is mostly on the handset side of the equation. Over time, the most popular and ubiquitous access to server technologies will be via wireless handsets, which will be the "super PDAs" of the very near future. Technologies such as VoIP will merge with handset voice methods and will continue to evolve on data access methodologies (as opposed to the current split of data and voice telecom networks).

Children currently in middle school and high school will enter the workplace fully equipped to use handset technologies, having started with text messaging, IM, Internet chat technologies, e-mail, and other applications on wireless handsets provided to them by their parents. They will demand that their wireless handsets provide access to traditional customer relationship management (CRM), corporate expense and payroll, e-mail, and other kinds of corporate communications. They will adopt faster data rate technologies, such as 802.16, and will use wireless networking to access home equipment and family communications. They will not want various handsets for corporate voice, personal voice, home voice, and other voice uses. They will use the handsets as a replacement for credit and smart cards, preferring to "beam" credit and debit card information to point-of-sale kiosks and vending machines. They will exchange personal business card and medical information by beaming it to other parties, doctor's offices, hospital emergency rooms, and police officers (should the occasion arise). Wireless will involve wide area wireless, local wireless, and "piconets" such as Bluetooth, all

from the same handset and "talking" to all manner of server applications. The user of the future will be wireless and will require ubiquitous access.

The problems of wireless cyber security start with the handset itself. Most are based on Symbian, Pocket/Windows Mobile, or Palm OS, none of which has reasonable operating system self-protection from infestations such as viruses, worms, Trojan horses, and other attack profiles. Applications written for these systems are usually *not* secure in form or composition and do not have application security controls that provide for cryptographic privacy measures or protection of personal data (e.g., credit/debit card information) on the handset itself. Handsets typically do not have traditional encrypted VPN services, SSL, or other cryptographic channel connection capabilities. In other words, handsets used in wireless applications are wide open to infiltration, data theft, and DoS attacks.

Wireless transmission is typically in the clear, which makes it easy to grab data via simple tools. Wireless systems have come a long way, especially Wi-Fi and WiMAX, in terms of node authentication (via WPA2). Access methods to the wireless network even exceed traditional wired technologies such as Ethernet 802.3 — provided they are implemented, that is. Unfortunately, users don't implement most wireless security controls because it is typically nontrivial to turn them on and coordinate all the security methods and management involved.

Standards committees (such as IEEE 802 series) have to do a lot of work to simplify the setup and management of wireless security before wireless security methods on networks realistically become more secure. This includes automating the setup of IEEE 802.11x management protocols and security methods, such as the use of WPA2. Key management of encrypted session protocols (such as IPsec tunnels) also needs to be automated and manual setup reduced so that these protocols will be widely adopted as the norm instead of being the setup nightmare they currently are (especially when dissimilar vendor products are used on either end of an IPsec connection topology). In most situations, especially with Wi-Fi networks, setting up the wireless component is a simple matter — most vendors have automated the majority of the access point technology setup. However, the security setup for the same vendors' equipment is onerous at best — to the point that most customers don't even bother to set up security for the Wi-Fi access points because of the technical effort and time involved.

Achieving Identity Management

Identity management is the third major area in which work needs to be done to solve cyber security issues. Identity can be broken down into devices, programs, and humans. Identity management is the matrix of permissions and access controls that would interact with these three basic IDs to allow/disallow access to a myriad of items that exist on networks and systems. For instance, if a device on a network possessed cryptographically sound credentials, it could use them in an upgraded TCP/IP connection request where a firewall would capture the credentials and use an identity management system to verify whether the device requesting connectivity to a network is allowed to connect. Once verified, the device would be allowed to access the network. At the very minimum, this type of rudimentary authentication would shut down a wide variety of DoS and DDoS attack types commonly seen on networks today, which also have a debilitating effect on e-commerce.

Identity management is a massive problem. Use of different authentication methods and styles, incompatible software applications, lack of proper use of ID technologies in base connectivity technologies, lack of standards, and a host of other issues make identity management one of the more difficult issues to deal with. But it is also one of the most important issues to deal with, as it is core to many security access methods and controls, both currently in existence or to be created. Identity management is critical to:

- Traceback after attacks
- Proper protection of vast data repositories
- Safeguarding personal information on devices such as wireless handsets

It is a difficult problem that will require a lot of research and a lot of work before a solution set can be created, and this means R&D — a lot of it.

For example, one problem that most IT managers will be dealing with very soon is two-factor authentication: the use of two pieces of information to identify an entity, exactly, to another entity. The two pieces are typically a bit of information about who you *are* and a bit of information about what you *know*, presented in a cryptographically sound fashion. The "who you are" component is rapidly evolving to biometrics or cryptographic identification of one flavor or another. The "what you know" component, traditionally a passphrase of some sort, is evolving to more complex

forms of identification, which include soft tokens (cryptographically strong authentication "files" that are preplaced on a system to identify the system or user), hard tokens (physical devices, which may include biometrics, time-synchronized keys, one-time pads, or other independently generated authentication information), and all manner of exotic identifiers (voice print recognition, facial thermography, etc.). In all situations, users present such identification credentials to the system(s) for access.

Of course, there is always the issue of who should be doing the R&D and who should be paying for it.

This becomes somewhat difficult to manage when various systems use different types of credentials for two-factor authentication. In such cases, the user is forced to physically retain multiple credential provisioning technologies (e.g., multiple biometric devices) to access multiple systems or technical entities — something most users will not tolerate. The system administration of two-factor authentication across multiple entities is a tedious, time-consuming effort even if all the credential types are the same for all systems. When they vary — and they do vary — then the problems creep into the users' intolerant hands, and they simply do not want multiple credentials for multiple systems.

Enter the concept of federated identity management. This is the idea that a trusted third party becomes the "credential broker" for the dissimilar types of credentials used for two-factor authentication between systems. Getting complex yet? Wait until you include devices that are autonomous and ubiquitous, such as home networking hubs, power meters, and the various kinds of sensor equipment that are becoming automated and accessible online.

Current identity management methods are crude and very difficult to manage. Protocols currently in use do not support even these authentication methods, and it will require R&D to properly upgrade the protocols to deal with the new identification realities.

LET'S GET THIS PARTY STARTED

As I've said, all three of these main issues will require collaborative and extensive R&D to solve. There is no one solution and no one method that will function in all situations. Still, if we don't start the work now, we won't have the technical tools we need to solve basic security issues coming up very quickly in almost every system and networking situation.

Of course, there is always the issue of who should be doing the R&D and who should be paying for it. TCP/IP exists because the US government had a need, funded the research, and created a federal standard for operations of the protocol in its initial uses. Over time, the Internet Engineering Task Force (IETF) has become the "owner" of the protocol suite, but the IETF has become somewhat mired in politics and distracted by numerous other issues that keep it from doing a thorough housecleaning of the protocol environment in use. Plus, unlike the Advanced Research Projects Agency (now the Defense Advanced Research Projects Agency [DARPA]), which created the initial suite of TCP/IP protocols, the IETF is not funded to do basic, original research.

Most of the technological innovations in internetworking over the last few years have come instead from startups or small communities that had a need and, via the grass roots, created the protocols in wide use today. This method will not work for the massive undertaking of reworking the base protocol of most internetworks. A major effort by a credible and influential organization will be needed to get the R&D accomplished to properly solve TCP/IP protocol suite security issues, especially at the base protocol levels. This may start with original academic research and trials, but to become operational, it will need to involve network carriers and large networking product vendors and suppliers. It's going to be a group effort unlike anything previously done due to the enormity and complexity of the work needed and the broad effect it will have on the community of network consumers, which continues to grow exponentially.

Other important issues that need to be resolved include such seemingly trivial items as common logging formats for security products. Think it's not an issue? Name two products from two separate security vendors that have the same event log format. To properly analyze security events, all event traffic from all security sensors and products needs to be consolidated and analyzed by autocorrelation technology to identify issues and problems. Doing this manually is a long and laborious process. It often is not done at all due to the overall difficulty involved.

Good security methodology requires that log files, events, and security information be continually analyzed for anomalous behavior and patterns of poor

behavior, and operating patterns of normality must be created against which potential poor operating patterns may be scanned. Scan results can then be used to identify a security situation. R&D needs to happen to properly address the problems of commonality of logging and autocorrelation of events so that meaningful security incidents do not get lost in the infinite mire of logged events.

The point of all of this is that if real security problems are to be addressed, we need to do the technical work. An infinite array of meetings, opinions, and articles will not solve the basics of security, and we will continue to deploy technologies that do not have base security controls implemented within them. In time, as we continue to merge technologies with poor security underpinnings, the problems of security will get worse, and the threats and risks to businesses and individuals will increase.

Bill Hancock is the Executive VP and CTO/CSO for SecureInfo Corporation, where he is responsible for global strategy of professional security services, managed security services, and compliance product sets. He is a well-known network and security consultant, designer, and engineer with thousands of network designs and hundreds of hacker/cracker trackdowns to his credit. He is often seen on CNN, ABC, BBC, CBC, NBC, FOX, and other networks as an expert on security, networking, and the Internet. Dr. Hancock has done extensive research on cyber warfare and has consulted and lectured on the subject to industry and governments around the world.

Dr. Hancock has written 31 books on computer networking and security, currently writes a regular column in Network Security*, and is a columnist for* Computers and Security *as well as* BusinessWeek*. He is a US network expert to the ISO and chairman of the Federal Communications Commission's (FCC) NRIC Homeland Security focus group on cyber security. Dr. Hancock also serves on the FCC Technological Advisory Committee, an elite group of technologists who advise the government on networking and telecom technology issues. He is a founding member and immediate past chairman of the Internet Security Alliance. Dr. Hancock can be reached at SecureInfo Corporation, 211 N. Loop 1604, Suite 200, San Antonio, TX 78232, USA; Tel: +1 210 403 5600; E-mail: bill.hancock@secureinfo.com.*

Moving Beyond Security: The Resilience Imperative

by Debra van Opstal

THE BUSINESS CASE FOR SECURITY

In the wake of 9/11, the United States' attention turned inward, toward its long and porous borders, the pervasiveness of vulnerable IT systems, and critical interdependencies among and between IT, electric power, telecommunications, and virtually every other sector. As Tom Ridge, then director of the Office of Homeland Security, noted at the Council on Competitiveness's first *National Symposium on Competitiveness and Security*, "We're a target-rich environment — and the private sector owns most of the targets."

Perhaps for the first time in US history, its domestic business assets, workers, and critical infrastructure were on the front lines of a battlefield — key targets and possibly pathways for attack. The growing dependence on IT systems and embedded software increased the potential that cyber attacks would affect millions of Americans. The possible diversion of commercially available feedstocks of radiological, chemical, or biological materials fueled concerns about weapons of mass destruction.

Even as the risks were growing, global competition left less margin for business to justify investments to safeguard against low-probability but high-consequence events. There is no question that homeland security is a private-sector concern. It is widely estimated that 80% of the economic infrastructure in the US is owned or operated by the private sector. And fully 100% of America's economic enterprise depends on the safety, soundness, and security of that infrastructure.

A few years ago, the Council on Competitiveness launched a new initiative to look at the balance between competitiveness and security in five industry sectors — chemical, electric power, financial services, oil and gas, and pharmaceutical. In the studies,[1] we posed two key questions:

1. Is it inevitable that security be a drain on productivity and corporate profitability?
2. Can a business case be made for investment in security and resilience?

Two committees were formed to examine these issues. The expert Advisory Committee, cochaired by Catherine Allen, CEO of BITS, and Robert Moore, director of global security for Merck & Co., identified the cross-cutting findings from the sector studies. A CEO Steering Committee, cochaired by Charles Holliday, chairman and CEO of DuPont, and Jared Cohon, president of Carnegie Mellon University, brought unique leadership perspectives on the risk-benefit calculations for security.

The conclusion? Although the business case for anti-terrorism is weak, there is a compelling case for security. We can make our economic enterprise more competitive *and* more secure. However, this will require transformational thinking by America's business, university, labor, and government leadership about security, risk, and resilience. Security must be linked to enterprise-wide risk management with new organizational structures, new metrics, and new technological options to capitalize on the economic value that can flow from these investments. The markets must understand how to value these investments. The imperative is for a new private-sector paradigm — one that can deal with all of the new forms of market, technology, regulatory, and external risk.

STUFF HAPPENS

So let's take a pop quiz. Which of the following poses the greatest risk?

1. Leaking water
2. Overgrown trees

[1]Although the impetus for the Council's studies was ensuring US homeland security, our focus on the risks of business disruption from technological, market, or financial trends is not limited to US corporations and citizens. The resilience imperative is relevant to all countries and companies, as globalization and the growing dependence on IT and the Internet creates new risks for business sectors and consumers around the world.

3. Tailgating

4. Computer viruses

5. All of the above

If you answered "All of the above," you would be right. Water leaking into a chemical containment vessel led to the chemical disaster in Bhopal, India, which left 200,000 people injured and 10,000 dead. Failure to trim back trees was the proximate cause of an international power blackout in August 2003 that affected 50 million people in the US and Canada and resulted in $6 billion in economic losses. In 2001, American Airlines Flight 587 was caught in wave turbulence after following too closely behind a jumbo jet and crashed in Belle Harbor, New York, killing 265 people and incurring nearly a billion dollars in legal fees and successful claims. The 2000 "I LOVE YOU" bug attacked 45 million computers and resulted in $6-$10 billion in damage and losses.

The point is that despite best security practices, careful engineering, and operational controls, things can go wrong. And whether it's accidental or malicious, the effects may be pretty much the same. Ironically, while the US remains hyperfocused on the potential for terrorist attack, market, financial, and technological trends may pose an even greater risk (certainly a higher-probability risk) than terrorism. Our studies indicate that the globalization of supply chains, IT interdependencies and technological complexity, political instability, and concentration of sources of supply have increased the potential for disruption in every sector (see sidebar below).

The challenge is not just protection; it is *resilience*. Following the lead of management consultants Holland & Davis LLC [1], we define the resilient firm as:

- Elastic and adaptive enough to stay on track
- Capable of retaining or resuming its position
- Capable of recovering rapidly from adverse conditions
- Capable of taking advantage of opportunities when everyone else is dodging bullets

Resilience mitigates business risks (to employees, supply chains, intellectual property, IT systems, and plant and equipment), secures the economic enterprise, protects shareholder value, and reduces the impact of terrorist attacks as well.

COMPANY PERSPECTIVES ON SECURITY

Historically, businesses have viewed security, whether physical or IT, as a sunk cost — an expense to be minimized. As one executive at a small chemical company noted, "Security is just a level of inconvenience. Added security leads to more inconvenience."

After 9/11, some companies are transforming the way they think about — and manage — security and risk. Security is "baked into" every process and decision,

THE RISK ENVIRONMENT

In every sector we studied, industry trends over the past decade have rendered companies more vulnerable to a variety of disruptions, irrespective of the events of 9/11 and the threat of global terrorism. Among them are:

Electric power. Deregulation (which resulted in major restructuring and vertical disintegration in the industry) has increased the number of interfaces among and between the utilities and transmission companies and created more potential failure nodes. Advances in technology have increased the interdependencies between the energy, information, and communications sectors. Embedded IT control systems have increased reliance in every sector on secure and continuous electric power. Emerging technologies like VoIP make communications more critically dependent on electric power.

Financial services. Although the sector is driven by a set of stringent regulations and guidelines, technology continues to create new security risks. Fraud, software vulnerabilities, patch management, and the proliferation of viruses and botnets are among the new challenges the industry faces. Strong interdependencies with other critical infrastructures — particularly communications and power — complicate the industry's own business continuity and crisis management planning.

Pharmaceutical. Cost pressures are impacting product and supply chain resilience by reducing the redundancies, resulting in a decreased capacity to respond to emergencies ranging from pandemics to biological attacks. The shift to digitization of intellectual property and manufacturing control systems creates new layers of IT vulnerability. And the globalization of product networks creates an interdependency between the prescription drug supply and continuous operation of transportation networks.

not bolted on with fences and firewalls. As a financial services executive remarked:

> It took us a good long time to convince our CEO that the world has changed. In the past, the regulators looked at results. In the old days, (if the results were good), you could assume that we were managing the hell out of risk. Today they say, "Show me your risk management processes." If you cannot document how your structure produced those results, they assume it could be luck and you are not managing risk.

If quality and safety can become competitiveness drivers, why shouldn't we be thinking about innovative ways to realize business benefits from security?

It is instructive to remember that 20 years ago, America's business leaders thought that quality was simply an expensive luxury — until the Japanese proved its value as a productivity driver and competitiveness enabler (and cleaned US clocks on the global markets). In response, the integrated quality management movement took off in the US. Today, quality is a table stake in the global marketplace.

In the same way, the chemical industry met the disaster at Bhopal with a new framework for integrated safety management. Companies found that the focus on safety yielded benefits across the organization, far beyond saving the direct costs of accidents. Today, the industry calculates the direct costs of injuries at about $70 billion, including medical expenses, wage indemnity, and administration costs. But that is just the tip of the iceberg; the real costs are estimated to be five times greater in lost production, process interruptions, equipment replacement, and litigation, as well as damage to employee confidence, customer relations, and public image. The drive toward zero accidents was not just the right thing to do — it was good business practice.

If quality and safety can become competitiveness drivers, why shouldn't we be thinking about innovative ways to realize business benefits from security?

WHY THE PRIVATE SECTOR IS LESS RESILIENT THAN IT COULD OR SHOULD BE

What makes the Council's sector studies distinctive is their focus on the need for change *in* the private sector *by* the private sector. The fact is that most companies don't think of security as a core value driver. Organizationally, the security function is often decoupled from risk management, business continuity, and strategic planning, and that limits any ability to create business benefits from security. The resulting "risk silos" have the perverse effect of increasing the overall risk profile [2].

A study by Deloitte Research, *Disarming the Value Killers*, notes that most companies are exposed to more than one type of risk — from poor financial controls and product problems to supply chain issues, employee fraud, terrorism, and competition [2]. Many, however, fail to recognize and manage the relationship among different types of risk. Furthermore, actions taken to address one type of risk have the potential to increase exposure in other areas.

The study found that from 1994 to 2003, almost half of the 1,000 largest global companies suffered declines in market value of more than 20% in a one-month period because of gaps in their risk management systems — and these value losses were often long-standing. For roughly one-quarter of the companies, it took more than a year for their share prices to recover. By the end of 2003, share prices for another one-quarter of the companies had still not recovered to their original levels [2].

Although the concept of enterprise-wide risk management systems is very much in vogue, it often ignores the security function as an integral part of risk management and mitigation. As an executive at one oil company noted:

> Our operating systems were never built for digital security. There have been specific cases in which hackers got all the way into the digital process controls. As we've moved into higher levels of digital integration — integrated with inventory and financial controls — more of our systems are no longer isolated. Automating oil field production has increased the level of exposure as well. And, cyber vulnerabilities create physical security problems; all locking mechanisms are now IT-controlled. Security has become a strategic risk management issue.

The sector studies also identified other major gaps that hinder transformational change. Such change will require:

- A consistent definition of security
- Well-understood roles and responsibilities for chief security and chief information security officers
- Metrics for demonstrating success
- Regular security training programs
- A new leadership vision and strategy for resilience

Waiting for Webster to Weigh In

Security means different things in different companies. In some, security is siloed between physical and IT assets. Others add in supply chain security, IP protection, or different combinations of these assets. Even within a single company, senior executives had different views about the role and scope of security.

Do definitions really matter? Absolutely. The practical consequences of the lack of definition are that it's harder for companies within a sector to agree on best practices. Between sectors, the effort to reduce the risks that stem from infrastructure interdependencies gets bogged down in different organizational silos. Lack of a common lingo makes it harder to partner effectively with each other and federal, state, and local governments — even to demonstrate due diligence to Congress and the American public.

Company Cops or Global Risk Managers?

The roles and responsibilities of CSOs and CISOs, unlike other senior corporate positions, are not clearly defined. They can range from company cop (viewed with suspicion) to global risk manager (where no decision is made without the security signoff). In addition, the way security managers are positioned within the organization — their accountability and reporting chains — affects their ability to implement innovative and enterprise-wide solutions that strengthen corporate resilience and risk management.

MIA: Metrics for Demonstrating Success

It is difficult, if not impossible, to manage for resilience when the metrics for determining success are unavailable, anecdotal, or inconsistent. What is clear is that the range of potential benefits from the security program extends well beyond the cost of terrorist disruptions. The lack of a framework to capture efficiency gains, reduce theft or fraud, enhance productivity, or capture new markets is a critical barrier. The inability to measure benefits reinforces the conventional perception that security is a sunk cost rather than a core business enabler. The lack of good metrics impedes the ability to:

- Demonstrate to CEOs and boards of directors that the returns on investment outweigh the costs
- Develop market-based standards for security that can be implemented through market mechanisms, such as insurance
- Demonstrate to government that business has taken a proactive approach to resilience that reduces the need for top-down prescriptive regulations

Workers as the First Line of Defense

As the chemical industry proved with integrated safety management, employee commitment and training are critical to embedding a new concept across the operation. Like safety, resilience is a process, not a program. It should engage every worker as part of the first line of defense in protecting the company's assets and restoring business continuity when protection fails.

On the IT side, investments in firewalls and virus protection are often wasted if not accompanied by an investment in continual employee training. Many employees place information at risk on a daily basis — through careless security practices or installing unauthorized software that can corrupt systems.

But many companies lack the training programs that would achieve the requisite level of employee awareness. Some leading companies increasingly offer detailed and role-specific training. It is automated, occurs at regular intervals, and is tied to codes of conduct. Unfortunately, such training is the exception, not the rule.

Investments in firewalls and virus protection are often wasted if not accompanied by an investment in continual employee training.

The Leadership Imperative

Perhaps the most important thing we learned from the sector studies is that a new vision for resilience cannot be achieved through a bottom-up approach. It requires strong management vision and determination, clearly articulated goals, and processes that engage the entire workforce.

At a minimum, CEOs should be asking the following questions:

- Are we strategically integrating security in our global operation in the same way that we integrate other functions, such as finance, legal, or risk management?

- Do we understand the overall risk profile of the company's assets, the relationships between those risks, and the mitigation paths?
- Is the security function able to provide financial information that enables an assessment of its costs, benefits, and performance?
- Can security processes and procedures be improved in a way that will yield other benefits back to the company?

Why should CEOs care? Beyond the business benefits of protecting shareholder value (the "carrot") are the "sticks": the threat of reactive regulation and the requirements of the US Sarbanes-Oxley Act. There is little question that industry could face reactive regulation in the event of another terrorist attack. To date, efforts to regulate security have been incremental and sector-specific. However, in an attack scenario, regulatory incrementalism could become a regulatory tsunami if the private sector cannot demonstrate due diligence. Moreover, given the integration between IT control systems and physical security, Sarbanes-Oxley likely mandates a more rigorous assessment of security procedures and systems than is currently in place. Because the security function is not always at the table in risk management discussions, security risk is often not adequately conveyed to senior management and not completely aligned with business strategy.

There is little question that industry could face reactive regulation in the event of another terrorist attack.

THE UPSIDE OF SECURITY

When a business goes down, the costs are enormous. The average cost of business disruption is nearly $8 million for brokerage firms, $3 million for energy firms, $2 million for telecommunications firms, and $1.1 million for retail firms — *per hour* [3]. The business case doesn't just rest, however, on the avoided costs of business interruptions. The Council's case studies show there are also potential positives to investments in security.

Because there are no consistent metrics, it is difficult to capture these benefits — and few companies do. Nevertheless, some of them include:

- **Productivity gains from streamlined workflow, lower insurance costs, as well as reductions in losses.** IT-based identification, tracking, and verification systems in container cargo, for example, should not only increase security of shipments, but also reduce the $12 billion per year in losses from theft. In the pharmaceutical industry, better electronic locking and tracking systems could reduce the problem of counterfeit prescription drugs in the supply chain — a major drain on corporate revenues. Mobile intruder-detection technologies serve the dual purpose of security and inventory management; the robot detectors read bar codes even as they make the rounds. Biometric access control systems do double duty in granting access only to authorized personnel while also monitoring contractor and employee hours without the use of time sheets.
- **New revenue opportunities from consulting and proprietary solutions as well as innovative new technologies.** In the financial sector, a handful of companies have patented authentication and verification software and are marketing services based on their own security processes. In the chemical industry, one company has developed a security information management system, linked to the personnel access control system, that it plans to market to users in both the public and private sectors.
- **Reduction in regulatory and legal risk through enhanced capability for compliance, reduced media scrutiny, and effective two-way communications between the public and private sectors.** Seen through a resilience lens, investments in security preserve shareholder value, customer value, and employee confidence, as well as the firm's reputation and community standing — all of which serve to improve competitiveness.

The bottom line is that the view of security as static, defensive (guards, gates, and guns), and compliance-driven needs to be relegated to the "old thinking" heap. The Council for Competitiveness is reaching out to companies and industry associations in partnership, such as the cooperative understanding recently established with the Internet Security Alliance, to begin this process of transformational change. In a world in which risks of every kind are growing, we need to move together toward a strategy that embeds security as a core business value and strategic opportunity.

REFERENCES

1. Holland & Davis LLC. "Business Resilience ... for Changing Times," January/February 1999 (www.hdinc.com/hotTopics/hot_topic_2-99.html).

2. Kambil, Ajit, and Vikram Mahidhar. *Disarming the Value Killers*. Deloitte Research, February 2005 (www.deloitte.com/dtt/cda/doc/content/DTT_DR_VKillers_Feb05.pdf).

3. Kostman, J.T. "Security ROI: Measuring the Benefits of Investments in Security." Presentation to the Council on Competitiveness Advisory Committee on Competitiveness and Security. Washington, DC, March 2006.

Debra van Opstal is Senior VP for Policy and Programs at the Council on Competitiveness, where she is responsible for new program development and oversees work in the organization's national, regional, and global programs. She also directs the Council's Competitiveness and Security program. Ms. van Opstal joined the Council as VP in April 1996 to manage its ongoing work in innovation policy and national competitiveness. She has edited the twin volumes Going Global: The New Shape of American Innovation *and* The New Challenge to American Prosperity: Findings from the Innovation Index*, and she coauthored, with Michael Porter of the Harvard Business School, the Council's* 2001 Competitiveness Index.

Prior to joining the Council, Ms. van Opstal was a Fellow in Science and Technology (S&T) and Deputy Director of the S&T program at the Center for Strategic and International Studies in Washington, DC. Her publications include Global Innovation/National Challenges, Integrating Civilian and Military Technologies: An Agenda for Change, View from the Decisionmakers, Combating Terrorism: A Matter of Leverage, *and* Meeting the Mavericks.

Ms. van Opstal currently chairs the judging panel for the Gerald R. Ford national security journalism award. She holds a bachelor's degree from Pitzer College and a master's degree from the Fletcher School of Law and Diplomacy. Ms. van Opstal can be reached at DvanOpstal@compete.org.

Contracting for Information Security in Commercial Transactions: A New Tool for Managing Risk

by Jeffrey B. Ritter

Information technology has enabled a remarkable transformation in the way companies define the perimeters of their enterprise. The capability for any business to communicate information between and among its suppliers, customers, developers, and service providers has introduced new views on how third-party operations are considered to be part of the central business. The "extended enterprise" now requires the management of a portfolio of relationships that are intended to deliver agility, efficiency, and improved profitability. But that management task has proven challenging to implement, and many of the early promises regarding the potential for outsourcing, distributed services, Web-based data processing, and the even newer innovations of grid computing and service-oriented architectures (SOA) are not being realized.

DEFINING SERVICES, NEGOTIATING TERMS

One of the surprising realities involved in extending the enterprise is the self-assessment required to do so. As companies began to execute on senior management mandates to outsource specific functions or services, they realized that one of the most challenging aspects is the need to define the elements of those existing functions or services, in order to then enter into a contract to require their performance by others. The process has often proved difficult to accomplish effectively. Most businesses have evolved and grown their various functions organically; much of what gets done within a specific business unit is learned and transferred from generation to generation through formal training, on-the-job training, and the informal evolution of uniform practices. When the outsourcing or similar transaction must be completed, there are often very few integrated descriptions of how a business unit actually works. Those that may exist (as operations manuals, for example) are rarely authored with the detail needed to effectively express in a contract or service agreement the requirements to be met by the new service provider.

As a consequence, the proposed deal (whether an outsourcing, shared services, SOA transaction, or similar vehicle) quickly evolves into two separate exercises. The first step requires a business to develop a suitable description of its operations; the second step is to negotiate with the proposed service provider an effective agreement under which those operations will be performed. The synergy between these exercises is obvious — the obligations of the service provider who is asked to be part of the customer's extended enterprise will only be as good as the customer's description of its business operations. Short-changing the description will result in a contract that leaves both the customer and the service provider uncertain as to the actual services to be provided. Providing excessive detail will often provoke the service provider to reevaluate the pricing, since a more detailed job description empowers the customer to be more demanding of the service provider, which in turn requires the service provider to perhaps deploy more resources to support the specific engagement under negotiation.

The service agreement for the overall transaction can become a battlefield for the parties. For the customer, there is often pressure before a draft agreement is prepared to move expeditiously in seeking vendors, proposals, and options for replacing the current internal services. But that pressure gives the customer an appetite for brevity, particularly in defining the relevant service descriptions for the vendors. From the vendor's perspective, there is a natural desire to minimize the investment in securing a customer (including the time required to conduct an effective due diligence on the description of services that may be included, for example, in an RFP) until the customer has made a preliminary, favorable selection of that vendor. As a consequence, when a vendor's preliminary bid has been selected and the customer and service vendor begin to craft the definitive contract, a troubling disconnect appears between how the services were described for the purposes of the RFP and what is required for the contract.

Experience suggests that, in the long run, greater definition and clarity are always to the mutual benefit of the parties, even if the level of detail required for an effective definition of the services causes the parties to invest time and effort in rethinking the original description and, at the same time, the terms on which the service provider is prepared to perform the service. The customer hopes to keep the service provider committed to its original bid, while increasing the detail and granularity of the service description. The service provider, however, will often use each new detail added to a service description as an opportunity to renegotiate the price and related terms. In doing so, the service provider hopes to better ensure that assuming responsibility for the more detailed services will not diminish the profit margin embedded within the original proposal.

IMPORTANT AFTERTHOUGHTS: DEPENDENCIES, INFORMATION SECURITY

At this point in the negotiation process, unfortunately, one of the most difficult components comes into play. In defining the essential services that are the subject of the transaction, the business unit executive will often overlook the need to consider the degree to which the specific services are supported by larger infrastructure resources that serve the entire company. In addition, that manager will often fail to factor in the oversight, supervision, and quality control functions performed for the benefit of the entire business that are indivisible from the business unit itself. These functions will include, for example, accounting, facility security, human resources management, and insurance coverage cost allocations. When these omissions become apparent, the negotiations are often thrown into chaos.

Another critical factor that is frequently overlooked is the need to define and manage information security as part of the services that are within the scope of the transaction. Incorporating and extending a company's information security controls into any service transaction has become essential to ensuring that the most important output from that service — the business information assets that are returned to the customer for use within other business activities — has integrity, reliability, and value. If the information returned by a service provider lacks those essential attributes, then the overall efficacy of the transaction is at risk, even if the service provider is otherwise performing the services efficiently.

The need to address information security has presented a new challenge to the executives negotiating these commercial agreements, as well as the attorneys and the information security professionals that team up to put the final transactions together. The situation has become even more challenging as companies expand their extended enterprise on a global basis, engaging service providers that operate in different countries, under different legal systems, and with different controls for protecting the security of electronic information.

Unfortunately, very few resources exist to help companies — including their IT professionals, information security officers, auditors, and attorneys — understand how to structure the relevant contract provisions. There are even fewer resources that provide functional examples of the terms and conditions needed to properly express the requirements for achieving and maintaining information security as an integral part of the relationship being established by a commercial agreement. The absence of these resources adds significant cost and expense to such transactions.

Another critical factor that is frequently overlooked is the need to define and manage information security as part of the services that are within the scope of the transaction.

As unfortunate as this lack of resources is, there is a worse (and perhaps more common) scenario: that the prospective customer simply fails to recognize the information security issues prior to finalizing the commercial agreement. In this situation, the risk exposure magnifies itself. The customer will eventually discover that the information security topic needs attention (most often as a result of an internal audit or governmental examination), but at that point in time, the service vendor has significant leverage. In addition to the cost of actually negotiating the requirements, the additional services the customer requires will justify the service vendor's demands for additional compensation.

COMPANIES FACE MYRIAD SECURITY CHALLENGES

The security challenges large corporations and their business partners face are complex and difficult to address:

- Companies must develop and maintain the security of their information assets within a globally competitive environment that often places two different business values into conflict: the need for strong corporate security and the value of achieving cost-effective services, particularly involving the processing and management of electronic information.
- When electronic data is involved, virtually every business both receives and transmits information. As a result, the rules of engagement involving information security are often different than in many other business relationships. Information security procedures must be uniform and consistent and must generally work equally for all parties involved in a transaction. In addition, traditional contract remedies (e.g., breach of contract lawsuits) are often not practical in the information security context because of the need for the parties to work cooperatively and respond to problems with urgency.
- The consequences of information security incidents have become the topic of news headlines. As a result, companies must pay closer attention to their risk exposure in this area, with a greater awareness that those issues may affect brand value and customer loyalty.
- Government regulation of business information systems is extending to include attention to the terms and conditions of the contracts under which data processing and other critical services are delivered. Scrutiny is being given to general issues involving the security of personal information, but also complex subjects such as authentication controls, risk transfer, records archiving, forensic imaging, and the security of mobile devices.
- Information security attacks have become more sophisticated. New strategies and tactics by malicious actors continue to test the integrity of corporate information systems with increasing momentum and complexity. Companies dependent on data processing services must be capable of mounting collaborative defenses with their business partners and information sources to protect the ongoing functional capability of their networks and services, discharge fiduciary obligations, and remain competitive.

A GUIDE TO MANAGING INFORMATION SECURITY RISK

Indeed, in order for firms doing business involving the exchange of data (i.e., virtually all modern businesses) to successfully traverse the legal mine field presented by the Internet, they need a guide to this murky and potentially hazardous landscape. Any such guide must fulfill a variety of missions. It will need to introduce an architecture, vocabulary, and contract structures through which information security can be accomplished across modern commercial relationships. The guide must serve as a resource for use by professionals responsible for negotiating and drafting the information security aspects of service agreements and other contracts. It must offer a standardized approach to dealing with information security issues as part of the overall transaction, in order to eliminate the add-on costs often incurred when information security issues are considered late in the negotiations process.

As part of the mission of the Internet Security Alliance (ISAlliance), its members commissioned and participated in the Model Contract Project, an ongoing program that will work to:

- Better define the challenges of contracting for information security
- Promote nonregulatory solutions to problems shared throughout the business community
- Provide contracting tools and resources that complement the ongoing dynamic evolution of technology defenses and strategies

This project has produced *Contracting for Information Security in Commercial Transactions — An Introductory Guide*,[1] a new tool that is intended to provide a starting point for professionals who are asked to develop and negotiate terms and conditions addressing information security in sophisticated commercial business relationships. While a variety of approaches were considered, the guide provides three important "building blocks":

1. An overview
2. A glossary of terms
3. Model terms for privacy management

[1]In the interest of full disclosure, I should state that on behalf of the ISAlliance, I largely wrote the guide in question, and my erstwhile law firm, Kirkpatrick & Lockhart Nicholson Graham LLP (K&LNG), conducted the legal research for the guide and reviewed ISAlliance members' submissions of model clauses. The guide embodies the views and input of ISAlliance members, not necessarily my own or those of K&LNG.

Overview

Information security is a professional discipline requiring significant training and, for some, certification in specific fields. While the overview is not intended to provide a summary of the entire field of information security, it introduces the range of topics to be considered in drafting information security terms and conditions in a commercial agreement. Those familiar with information security will recognize that many of the overview topics are also topics referenced in prevailing standards on information security, such as BS7799 or ISO17799. These standards provide useful business method frameworks for managing information security across complex corporate information systems.

Glossary of Defined Terms

Robust commercial agreements are characterized by detailed definitions of specific terms used within the agreements. Information security is like any other important subject within a contract — meanings matter, particular when the terms are highly technical in nature. The defined terms in the glossary are the building blocks from which the remaining substantive terms can be addressed.

The glossary terms are associated with many, but not all, of the topics included in the overview. The definitions illustrate, by example, the challenge of migrating technical terms and concepts into contractually functional language. Taken together, the defined terms provide a vocabulary with which the more detailed and substantive terms and conditions can be constructed.

Model Terms for Privacy Management

The final component of the guide is a representative set of contractual terms under which a company that collects and *processes* personal information might regulate the management and use of that information by a service provider. While future work of the Model Contract Project may address other substantive areas, the strong public awareness of the need for protecting personal information made this topic a priority.

The model terms have evolved out of a series of commercial transactions involving extensive negotiations among the participants. While intended only as an example set of provisions — addressing many topics from the overview and using definitions set forth in the glossary — the model terms help illustrate what is required for practical information security controls to be implemented in a commercial agreement.

Sample Scenario

The guide was prepared with the recognition that nearly every commercial transaction is unique; however, to show how the various elements described above can work together in a specific transaction, it also presents a sample scenario in which all of the various topics, issues, and terms become relevant. The scenario involves a customer that is seeking a service provider to process account records and other sensitive personal information relating to the customer's clients. In addition, the service provider will have access to employee-related information and be responsible for developing specific software applications to be installed in the customer's systems in order to facilitate the desired services. This scenario requires a focus on those deliverables and triggers consideration of a significant number of network-based information security risks that must be addressed in the commercial agreement.

Information security is like any other important subject within a contract — meanings matter.

Additional Resources

Finally, in support of the preceding elements, the guide includes an "Annex of Selected Information Security Resources," a list of various resources available on the Internet to which executives, managers, and their lawyers can refer in order to gain further information regarding information security, applicable regulations, and related topics.

HOW — AND WHOM — THE GUIDE CAN HELP

The guide is intended to empower various teams within corporate environments to better perform their roles in structuring and managing commercial transactions. For example:

- **Internal corporate teams.** Business managers, information security officers, internal auditors, and attorneys can discuss how the topics presented in the overview impact potential functions and services for which information security controls may be appropriate. The dialogue can also be used to focus on variables that could impact — and potentially disrupt — the business case for the transaction under

consideration, such as staffing, system infrastructure (computers, applications, security controls), regulatory exposure, funding requirements, and allocations of liability.

- **Negotiation teams.** The business teams directly negotiating the contracts or agreements can use the guide for similar discussions between the parties. As noted earlier, many of the topics that relate to information security are not properly addressed early in the lifecycle of structuring and drafting commercial agreements. The guide (and similar materials, such as those identified in the "Annex of Selected Information Security Resources") can stimulate an attention to those topics.
- **Attorneys.** Attorneys responsible for drafting and negotiating the information security provisions of commercial agreements can employ the guide to help structure and audit their own due diligence efforts to determine the scope of the contract and, of course, draft and negotiate appropriate terms and conditions. In addition, the guide helps focus counsel on the practical elements that must be considered in order to implement "reasonable" and "suitable" information security controls in commercial contractual relationships.

The guide also provides direct value to the information security professional. These professionals often have less experience than other team members in focusing on the types of commercial agreements involved. They will be able to use the guide's building blocks to:

- Enable dialogues with internal business teams that are evaluating outsourcing, data sharing, or similar deals that focus on the key topics of information security
- Provide starting points for determining the contract terms — particularly the definitions — needed to express information security controls
- Enable targeted focus on the specific language of requirements needed to meet various regulatory obligations

The ISAlliance's Model Contract Project is a work in progress. The project team hopes that the publication will encourage discussion on how to better address information security within commercial relationships. Comments or questions concerning the guide can be directed to modelcomments@isalliance.org.

Jeffrey B. Ritter has most recently been a partner at Kirkpatrick & Lockhart Nicholson Graham LLP, resident in their Washington, DC, office. His legal practice has emphasized information technology for nearly 20 years, with a special focus on information security, privacy, and global system governance. During his career, Mr. Ritter made significant contributions to United Nations projects to enable the development of a global legal framework for electronic commercial practices. In 2004, the American Bar Association recognized him for his substantial contributions to developing the law of cyberspace. Mr. Ritter may be reached at jeffrey.ritter@comcast.net.

The Role of Cyber Insurance in Fighting the War on Terror

by Ty R. Sagalow

REMOVING UNCERTAINTY FROM THE EQUATION

The campaign against terrorism is being fought on many fronts — and this extends all the way to cyberspace. In this most unconventional battle, attackers can be expected to use every tool available to them — including the Internet — to breed fear and chaos, to threaten the national interest, and to breach our borders, both on land and online.[1] Yet the enemy's fear-based campaign can be blunted to the extent that we remain one step ahead and remove uncertainty from the equation.

For several years, government, business, and individuals have made substantial efforts to defend the nation's cyber borders more rigorously and to create a widespread awareness of the need to do so. The government and private sector have joined forces to communicate the universal need to leverage more effective information security risk management technologies and practices, including cyber insurance, to prevent and mitigate the potential damage of cyber attacks.

THE INTERNET ADDS A VIRTUAL DIMENSION TO THE BATTLEFIELD

Ironically, the Internet was developed in the 1960s under the leadership of the US Department of Defense as a decentralized military communications network that could withstand a cataclysmic attack [2]. It has since evolved into a vast global network of interconnected computers that individuals and businesses use to exchange information and conduct business transactions. The connectivity that was once a military advantage now adds a new, virtual dimension to the battlefield, offering attackers limitless entry points and causing a staggering sum of damage to date.

The pace of innovation in network technology has not been met — and probably can never be met — by the standardization necessary to ensure 100% reliability in end-to-end network and systems security. Indeed, cyber threats are ever changing, and as soon as a security solution is introduced, increasingly sophisticated perpetrators take on the task of working around it.

The fact is, gaping security holes exist within the public and private global network infrastructure, and a litany of attacks has borne this out. Widespread viruses that may shut down entire companies are no longer headline news due to the unfortunate frequency of their occurrence.

In December 2005, Russian hackers broke into the Rhode Island government site and stole credit card information on as many as 53,000 transactions [10], illustrating not only the global nature of the threat, but also that government sites may be as vulnerable as any others. Perhaps more disturbing is the saga of Joseph Konopka, alias "Dr. Chaos," who in December 2005 was sentenced to seven years in federal prison for hacking into computers and causing 28 power outages in Wisconsin before he was apprehended [4].

Cyber terrorists also have exploited systems' vulnerabilities by stealing information such as individual identities. The US Federal Trade Commission cites identity theft as the leading consumer complaint [5], a growing problem with grave consequences. Using stolen identities, terrorists can fund their operations and damage US interests. In June 2002, a chilling case of online identity theft was revealed in which an individual's credit card information was used through confidential online transaction broker ccNow to buy a Russian-made night-vision rifle and a range finder, which calculates the distance to an intended target. The cardholder discovered

[1]While this article focuses on the US, the basic issues and the realities of risk apply in equal force to any country with an economy that depends, in a significant manner, on interconnected computers or networks.

the fraudulent charges, which were reversed, but not before the weapons had been shipped to an unidentified criminal in Saudi Arabia [9].

In a disturbing piece of research, the Identity Theft Resource Center reported in September 2005 that of the criminals who stole identities, 66% used the information to open new credit card accounts; 28% used the information to purchase a cell phone; and countless counterfeit driver's licenses are believed to have been issued based on this stolen information [6]. It is not difficult to imagine the value of untraceable funding and false identities to terrorists.

The urgent need to manage cyber risk more responsibly stems from the fact that security breaches can target not only information but also the nation's critical infrastructure.

THE NEED FOR RISK MANAGEMENT TAKES ON ADDED URGENCY

The US government is redoubling its efforts to address vulnerabilities in the national information infrastructure. The task force formed initially as the President's Critical Infrastructure Protection Board (PCIPB) — now known as the National Infrastructure Advisory Council (NIAC) — issued a draft proposal in September 2002.[2] This was later issued as President Bush's *National Strategy to Secure Cyberspace* in February 2003, supplementing *The National Strategy for Homeland Security* as well as *The National Security Strategy of the United States*. The PCIPB strategy strongly called for a risk management approach. It noted that "the tools of destruction are broadly available, and the vulnerabilities of the nation's systems are many and well-known. These factors mean that no strategy can completely eliminate risk, but the nation can and must act to manage risk responsibly" [8].

The urgent need to manage cyber risk more responsibly stems from the fact that security breaches can target not only information but also the nation's critical infrastructure (utilities, transportation, water, and financial services, etc.), which is also inextricably tied to and dependent upon information technology. The drafters of the National Strategy observed, "Cyberspace security is not about 'good ones and zeroes attacking bad one and zeroes.' It is about whether when one throws the switch, the electricity comes on, or whether the money Americans have invested and deposited is there, and whether this country is secure" [8].

With the June 2003 creation of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS), it became apparent the US government takes this threat seriously and continues to urge businesses and individuals to do likewise. In February 2006, Andy Purdy, acting director of NCSD, oversaw the first large-scale mock cyber attack, aimed at gauging the nation's readiness to handle computer threats to critical infrastructure. Results of the week-long exercise, dubbed "Cyber Storm," will be public by late summer [11].

EFFECTIVE DEFENSE RELIES ON PUBLIC AWARENESS

The war on cyber terror has benefited from increasing coverage in the media, as the public begins to recognize the scope and severity of the threats that may exist. Nevertheless, the challenge of combating an invisible foe with (so far) no major attack for the media to point to means that there is little sense of immediate urgency in the public at large. As a result, "netizens" may feel a misleading sense of security online. Government and business leaders must present a coordinated effort to educate the public and private sectors about the new threats and solutions available to combat them. By mobilizing citizens at all levels of society, there is a greater potential for success in thwarting cyber terrorists.

At the moment, too many individuals and companies continue to weaken the broader effort against cyber attackers by failing to take reasonable safeguards. For instance, individuals who neglect to implement personal firewalls and antivirus security software on their home computers may suffer financial losses, such as having their personal information stolen or their computers damaged. Without proper safeguards, an individual may spread a virus to countless other users, exponentially increasing the damage. Worse yet, stolen identity information may fall into the wrong hands, to the benefit of cyber criminals and even terrorists.

ASSESSING RISK IS A VITAL STEP

Government and business agree on specific measures that individuals and businesses can adopt to slow or

[2]At the time of this writing, this proposal has not yet been issued in final form. The content of the final report may vary from that described herein.

perhaps reverse the growth of cyber crime. Balancing technology investment, human controls, and financial protection produces a blended risk management approach that may prove successful. Individuals and businesses should assess what security technologies, procedures, and human controls they have in place and address vulnerabilities by implementing appropriate safeguards. For example, firewalls and antivirus solutions will do little good if an organization's employees are not properly educated about security risks. Likewise, a thoroughly educated employee population will not be able to compensate for poorly designed security safeguards.

After a risk assessment, individuals and businesses should take the necessary steps to prevent and mitigate the potential impact of cyber attacks, using a combination of technology, procedures, and human resources. Taken together, the following five tools represent a complete approach to risk management:

1. **Risk assessment** — analyzing the potential likelihood and the potential impact (financial and nonfinancial) of cyber attacks
2. **Risk prevention** — taking preventive measures to the extent economically reasonable to reduce the likelihood of a successful attack
3. **Risk mitigation** — reducing the potential financial loss arising from a successful cyber attack that cannot be, or is not, prevented
4. **Risk transfer** — transferring to others the financial loss that remains after steps have been taken to assess, prevent, and mitigate risk, typically through insurance supplemented by contractual "hold harmless" indemnification provisions
5. **Risk retention** — retaining the net financial loss that remains after risk prevention, risk mitigation, and risk transfer strategies are successfully implemented

THE ROLE OF INSURANCE IN MANAGING CYBER RISK

A comprehensive approach to risk management typically includes the purchase of insurance. In the physical world, insurance is purchased against a wide variety of threats, including fire, earthquake, flood, and legal liability of various sorts. In addition to financial reimbursement in cases of covered incidents, insurance companies may help individuals and companies identify, assess, mitigate, and manage risk.

The value of insurance applies with equal force to the cyber world, where insurance companies can help assess and value the extent of a person's or company's cyber risk and then assist in recovering from the financial loss arising from cyber crimes and covered security breaches. Thus, individuals and businesses can use cyber insurance as a financial risk management and risk transfer tool, enabling them to better withstand the financial consequences of attacks that breach the security measures they have in place.

The *National Strategy* acknowledged the key role insurance could play in combating cyber terrorism and the need to "work with the insurance industry on ways to expand the availability and utilization of cyber security insurance" [8]. Likewise, the widely referenced 2002 CSI/FBI Computer Security survey of international security experts noted that companies for which e-business exposure is particularly high should consider e-business insurance [3].

Both the banking and financial sectors as well as the insurance sector concurred in their recommendations to the *National Strategy* that "companies whose products or services directly or indirectly impact the economy or the health, welfare, and/or safety of the public should be encouraged to purchase specific cyber risk insurance programs from financially strong insurers" [8].

HOW GOVERNMENT CAN PROMOTE CYBER INSURANCE

The use of insurance in the physical world is often said to be a "public good," as it helps the victims of a financial loss, such as a flood, to get back on their feet more quickly and rewards best risk management behavior (such as the use of antitheft devices in automobiles) with lower premiums. However, a full understanding that these basic risk management principles apply in equal force to the cyber world has not yet occurred. Achieving this goal requires both a public that understands the need as well as an insurance industry ready and willing to take on this new risk. Agreement on how to accomplish this lags behind agreement that "something must be done."

There are specific and practical courses of action that the public sector could adopt. Initially, education is crucial. For example, the US Department of the Treasury has indicated an interest in sponsoring education on the role of cyber insurance in managing the risk of cyber attack, and the Federal Deposit Insurance Corporation

(FDIC) is already holding cyber risk seminars. Congressional hearings seem a logical next step [1].

To encourage insurers to enter this market, government may need to consider providing a financial backstop for the insurance industry in cases of massive cyber attack. Yet another step would be for the public sector to recognize that incentives to encourage businesses to address their vulnerabilities may be critical to winning this battle. One means of doing this would be the creation of safe harbor legislation similar to the SAFETY Act,[3] which would reward best practices for cyber security with specified safe harbor liability reduction rewards, combined with a requirement to purchase insurance [7].

Incentives offer numerous advantages over regulation. Most obviously, the international nature of cyber security issues cannot be adequately addressed by national legislation in any one country. In addition, government regulation of technology may stifle innovation, paradoxically resulting in reduced readiness and security. Finally, the rapid and continuing change inherent in Internet hardware and software demands flexible solutions that can be quickly adapted to new circumstances. This is unlikely to occur in an environment burdened with overwrought regulation [7].

CONSUMER IDENTITY THEFT INSURANCE

Home users wishing to protect their online exposure can purchase cyber insurance to guard against the growing incidents and costs of online identity theft. According to the Identity Theft Resource Center's September 2005 findings, it now costs an individual an average of 330 hours to mitigate the damage caused by this crime [6].

Insurance provides individuals with reimbursement of certain losses arising from identity theft, payment of lost wages for time spent away from work to rectify credit records, and payment of legal fees to defend suits or remove civil judgments brought as a result of identity theft. Given that most cyber criminals perpetrate identity theft to commit other crimes, such as sabotaging or stealing data, this last component of coverage is particularly valuable. A policy may also provide personal coverage against computer viruses, cash value for computer or operating system damage, or repair costs to an individual's personal computer. Individuals can obtain coverage directly or through the employee payroll deduction plans of a company that has purchased coverage on behalf of its employees.

COMPREHENSIVE RISK MANAGEMENT PROGRAM STRENGTHENS DEFENSIVE LINE

A complete security risk management program incorporates preventive, management, and recovery measures — integrating a mix of technology, procedures, and financial risk management tools, such as cyber insurance. However, cyber insurance does more than simply protect national interests by providing financial relief for the beneficiaries of coverage in the case of a successful cyber attack. It also helps fortify the defensive line against online invaders by rewarding cyber protective best practices through lower insurance premiums, similar to offering insurance discounts to those aforementioned automobile owners who install antitheft devices in their cars.

The value of cyber insurance is not yet fully understood. Carriers must help educate government agencies, businesses, and the public about the growing perils online and recommended risk management best practices, including insurance. The benefits of insurance include the creation of an efficient funding mechanism to pay for financial losses arising from cyber events, spreading financial risk so that the individual impact of an attack may be broadly absorbed among all policyholders. In addition, cyber insurance creates incentives for individuals and businesses to remain vigilant and deploy the most effective security solutions within their means, because carriers may offer premium discounts to insureds who actively address their network vulnerabilities.

[3]The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) was passed as part of the legislation creating the Department of Homeland Security. To encourage the development and deployment of antiterrorism technologies, the Act protects people or businesses that sell or provide those technologies from punitive damages and other excessive noneconomic claims of liability in terrorism cases. Equally important, to provide some relief to the victims of terrorist attacks, the Act requires the purchase of "Safety Act Liability Insurance" to be used to compensate the terrorist victims with the amount of legal liability being capped at the amount of insurance. This was Congress's method of balancing the interests of the technology sector with the desire not to leave victims without any type of financial relief. The Act provides that the victims of a terrorist attack have no other avenue for relief in the case of a SAFETY Act technology failure than to go after the manufacturer/seller to the extent of the Act.

THE INTERNET: A SHARED UTILITY THAT BRINGS SHARED RESPONSIBILITIES

While businesses are actively adopting security measures to protect against a breach of their systems — such as personal user IDs and passwords, encryption, access monitoring, firewalls, and virus protection — they cannot eliminate or anticipate every possible loss. Managing that loss requires a comprehensive risk management approach. Without insurance, a successful attack on an individual, small business, or large enterprise can have a potentially devastating ripple effect. For example, if a business network is disabled and the company suffers shareholder lawsuits, the damage caused by the attack can have more far-reaching consequences, affecting employees and business partners alike. Thus, financial risk management benefits individuals and businesses, and its benefits accrue to the public at large as an essential means of mitigating some of the harm of hostile attempts to disable the nation's critical infrastructure.

The US government has substantially increased security among its own agencies and raised awareness within the private and public sectors to protect the nation's cyber borders. In 2002, the federal government recognized the importance of this insurance coverage by explicitly covering cyber terrorism and e-business interruption under the US Terrorism Risk Insurance Act of 2002 (TRIA), which ensures federal assistance as a backstop to the private insurance industry. In 2006, DHS and the Department of Justice produced the first "National Computer Security Survey." Among the survey questions was "Did [the surveyed] company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?" The presence of this question in the survey, together with the explicit reference to cyber insurance in TRIA, demonstrates the federal government's position that cyber insurance can and should play a significant role in strengthening the nation's cyber security.

However, the government cannot succeed alone. Individuals and businesses must do their part as well by not only taking every measure available to manage the risk more effectively — making cyber insurance more available and less costly — but also to better hear the voice of the government in incorporating insurance into their overall risk management scheme.

By taking all the actions described in this article, the public and private sectors can more effectively use every means available to fortify the nation's critical infrastructure. Ultimately, the war on terror cannot be won without winning the battle online.

REFERENCES

1. AIG. "Public Policy Issues: AIG Cyber-Risk Insurance Options," 17 January 2004.

2. Brand, Stewart. "Founding Father." *Wired*, No. 9.03, March 2001.

3. Computer Security Institute (CSI). *2002 CSI/FBI Computer Crime and Security Survey*. CSI, 2002.

4. "Dr. Chaos Goes to Prison for Hacking." Associated Press, 1 December 2005.

5. Federal Trade Commission (FTC). "Identity Theft Heads the FTC's Top 10 Consumer Fraud Complaints of 2001." Press release. FTC, 23 January 2002.

6. Identity Theft Resource Center (ITRC). *Identity Theft: The Aftermath 2004*. ITRC, September 2005 (www.idtheftcenter.org/aftermath2004.pdf).

7. National Cyber Security Partnership. "Incentive Working Group Report." Wye II Retreat, Annapolis, Maryland, USA, 21-23 September 2005.

8. The President's Critical Infrastructure Protection Board (PCIPB). *The National Strategy to Secure Cyberspace*. PCIPB, September 2002 (www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

9. Richey, Warren. "Our Man Ordered Waffles, But Paid for Tools of War." *Christian Science Monitor*, 5 June 2002.

10. Rosencrance, Linda. "US State Website Hacked." *Computerworld*, 6 February 2006.

11. Thomas, Benjamin D. "'Cyber Storm' Tests US Defenses." LinuxSecurity.com, 13 February 2006.

Ty R. Sagalow is President, AIG Product Development, General Insurance, where he leads global efforts to research, develop, and launch new insurance and risk management products serving the needs of individuals and businesses worldwide. He formerly served as COO and Executive VP at AIG eBusiness Risk Solutions and is renowned for his knowledge of Internet risk insurance and risk management. He has written several works on the subject and has addressed numerous professional and technical forums on e-commerce insurance product development. He has spoken on the topic at the White House and has given testimony before the US Senate on the threat of cyber terrorism. Mr. Sagalow can be reached at tysagalow@yahoo.com.

The views and policy interpretations expressed in this article are the author's own and do not necessarily represent those of AIG or any of its subsidiaries, business units, or affiliates.

Payments System Security: No Longer Just a "Company Issue"

by Steve Ruwe

The new Electronic Payments Age has heralded unprecedented opportunities. Blink-of-an-eye transaction technology has been the driving force behind the economy's strength and continued growth. Consumers and merchants have embraced the speed and convenience of using payment cards for their purchases, greatly displacing cash and check usage. Unfortunately, criminals have also recognized the possibilities presented by the new technology and have ushered in a new era in the annals of fraud. Where once fraud was chiefly committed locally, one victim at a time, the greatest threats today come from highly sophisticated crime syndicates throughout the world that seek to steal data from thousands of consumers at a time.

ALL TOGETHER NOW

Staying ahead of criminals in today's environment will require a new corporate mindset. The payments system has evolved into an elaborate system involving many players. In such an environment, fraud can no longer be regarded as an internal company issue. A culture of security and shared responsibility must replace such outmoded thinking. With customers' trust and the integrity of the payment card purchasing system at stake, the industry simply cannot move too fast to address concerns about securing payments.

Visa takes this challenge seriously. Our approach has been based on our belief that there will never be a magic silver bullet that will stop fraud once and for all. For that reason, we have sought to stay ahead of the criminals by adopting a "layers of security" philosophy. We are constantly adding new security protections and looking to improve the ones that we already have. The multilayered approach to security has proven its effectiveness. Despite significant challenges, the fraud rate within the Visa system has remained steady.

But innovation in technology can only go so far, and staying ahead of today's fraud threats is no longer enough. The payments system that merchants, financial institutions, and consumers have come to rely upon is a tremendously successful yet complex system. It encompasses millions of interconnections between card issuers, merchant banks, independent sales organizations, merchants, and the payments networks themselves, all of which must be secured. The payments chain will only be as strong as the weakest link. The reality is that criminals will always be with us and will continually be probing, in real time, to find its points of greatest vulnerability.

Despite our successful track record in protecting cardholder data, we at Visa recognize that no single player controls all of the aspects of the network. The time for cross-industry collaboration on issues of cardholder security has arrived. Working together as a whole, the payments industry can accomplish more than participating companies can do on an individual basis. As participants in the payments industry, we must all recognize that security is a shared responsibility, and all of us at Visa, along with our member financial institutions, merchants, government, law enforcement, and even cardholders themselves, have a role to play in stopping fraud.

GETTING CARDHOLDER DATA OUT OF STORAGE

Moving forward, we believe a holistic approach is needed to address security issues across industries. The inappropriate storage of sensitive cardholder data is an example of one concern we are working to address on many levels. Because it can dramatically increase system risk, the storage of such data has long been against Visa's data security rules. Some companies, however, don't fully recognize or appreciate that their practices are out of compliance with the mandatory Payment Card Industry (PCI) Data Security Standard, which applies to any entity entrusted with cardholder data. When criminals hack into systems, this is the data they most want to steal.

Recent data security compromises serve as instructive examples. Incidents that place consumers at risk can destroy trust in a company and can erode confidence in the payments industry as a whole. Visa and Javelin Research released a report in October 2005 that shows that 55% of consumers believe that the problem of payments fraud will get worse over the next six months. Roughly 35% of consumers have a low level of confidence in their ability to avoid payments fraud [1].

Preserving consumer trust means ensuring that each participant in the payments system is living up to its responsibilities. To eliminate the storage of sensitive cardholder data, Visa has been working to better educate merchants about this requirement both through Visa member banks (those financial institutions that have the relationships with merchants) and through direct outreach efforts such as our 2005/2006 merchant security tour in partnership with the US Chamber of Commerce. In some cases, merchants are unaware that their software is storing this data. That's why Visa has reached out to the software industry with our Payment Application Best Practices. This effort will help ensure that software manufacturers create applications that do not retain track data, thus not creating unintended vulnerabilities for end users. (More information on both the best practices and compliance validation can be found at www.visa.com/cisp.)

THE PCI DATA SECURITY STANDARD

When it comes to mutual security issues, none of us can or should go it alone. In fact, our industry has already demonstrated that it can collaborate on this important area of security. In December 2004, Visa, MasterCard, American Express, and the other payment brands announced the PCI Data Security Standard. The 12 basic PCI requirements are:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

The PCI requirements significantly reduce the risk of hackers gaining access to propriety data. This alignment of existing data security standards, which has been adopted throughout the industry, allows for more efficient compliance by entities entrusted with cardholder data. (More information on PCI can be found online at www.visa.com/cisp.)

In some cases, merchants are unaware that their software is storing sensitive cardholder data.

VIEW FROM THE SUMMIT

Visa took another step toward closer collaboration by hosting a first-of-its-kind payments industry security summit in October 2005. It brought together all the key players, including various financial institutions, merchants, card processors, law enforcement, consumer protection organizations, and government to address our common security concerns and to establish a foundation that will lead to important work together.

Visa took the opportunity to propose several specific goals that the industry could work together to accomplish, including:

- Tougher penalties to make sure that the criminals behind these attacks think twice before attempting to compromise payments systems
- An international treaty that bans trafficking in stolen card data and clears the way for the prosecution of those who engage in it
- A consistent, national approach to data security regulation
- A consistent approach to reporting fraud

Additionally, Visa announced that it will explore other security initiatives, including:

- Creating greater incentives for businesses to enhance their data security practices

- Encouraging the creation of an objective, standalone entity to manage data security issues for the industry, reporting on emerging risk and fraud issues as well as promoting, validating, and strengthening data security compliance

TO BOLDLY GO ...

We cannot pretend to have all the answers, but we do understand that we are all in an arms race with today's sophisticated and unpredictable criminals. Time, therefore, is of essence. All players in the global payments system must be unified and resolute in protecting cardholder information. We must be willing to commit to bold steps, and we have to do so both individually and collectively as an industry.

By forming a neighborhood watch program for the payments industry, we are hardening our environment even further. Our businesses absolutely depend on maintaining customer trust, and by working together to protect consumers, we are also protecting ourselves.

REFERENCE

1. Javelin Strategy & Research. *Consumer Confidence Overshadows Fraud Concerns*. Javelin, October 2005.

Steve Ruwe is Executive VP, Operations and Risk Management, at Visa U.S.A., where he is responsible for membership, operating regulations, and arbitration and compliance. Mr. Ruwe is also responsible for Visa U.S.A. risk management activities, including fraud control, corporate and member program risk, and regulatory compliance.

Mr. Ruwe began his career in the payment card industry in 1977. Prior to joining Visa, he held senior management positions at Barclays Bank, Household Credit Services, and Gary-Wheaton Bank. He currently serves on the board of the Economic Crime Institute and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. He is a past board member of the National White Collar Crime Center and has represented the industry in Washington, DC, on numerous occasions. Mr. Ruwe can be reached at askvisa@visa.com.

Forging a Public-Private Partnership: The "Wonk-Free" Approach to Cyber Security

by Greg Garcia

In an IT-reliant society like the US,[1] there is no real physical or economic security without information security. This reality is becoming more apparent every day, as the nation's information infrastructure — and the physical infrastructure it supports — comes under attack from hackers and cyber criminals. Given this reality, companies in the private sector have a choice: adopt a proactive, self-regulatory stance that scales with the nature of the risk and evolves with the changing nature of the threat, or wait for the federal government to step in and legislate the necessary protections.

Approaches to information security engineered by policy wonks in Washington, DC, are apt to cost big bucks and deliver few benefits. Private industry owns and operates an estimated 80%-85% of the United States' information infrastructure. These stakeholders clearly understand the strengths and weaknesses of their systems, software, and networks better than do lawmakers, lawyers, and bureaucrats. Owners need to drive security policy development.

Even so, national security concerns and common sense suggest that government cannot just look the other way on this issue or simply assume that all is well. To protect the nation's cyber assets, the public sector and the private sector must find the common ground necessary to secure critical infrastructure.

This crafting of a workable public-private partnership is not easy, in part because government has so far failed to lead by example. Although the federal government, as one of the nation's largest IT consumers, has gotten more serious about information security, federal agencies still receive poor marks from Congress on their own information security practices.

In both the public and private sectors, information security challenges must be met with a combination of elements; namely, people, processes, and technology. Individuals must be vigilant in maintaining the security processes laid out by their organizations; organizations must craft, implement, institutionalize, and enforce security processes and procedures; and businesses and government must use multiple layers of security technology to deter threats. All three components are necessary to minimize risk.

Having said this, public policy options for forcing all of these dynamic components together are limited, because technology is ever-changing; business models and processes — and the information systems that support them — are widely varied; and human interaction with the technologies and processes that provide security is complex and subject to error. Given these challenges and limitations, what type of public-private partnership does make sense? A partnership that is light on government mandates and remains focused on industry self-regulation. Concerted attention to cyber security is needed in the form of investment, awareness and training, research, information sharing, and other activities. Solutions developed collaboratively by industry and public policy makers can help minimize the threat of attack and ensure that systems and electronic property remain protected.

A ROLE FOR EVERYONE: PUBLIC-PRIVATE PARTNERSHIP

To this end, the Information Technology Association of America (ITAA) recommends a number of high-level actions that all stakeholders — Congress, government

[1]The issues discussed in this article are seen mostly from a US perspective, but as the IT sector is a global industry and one that is constantly focused on innovation in a dynamic marketplace, many of the issues and concerns are similar in countries around the world. Some of the specific policy prescriptions may not apply in some countries, given differing legal frameworks, but readers are encouraged to consider appropriate policy recommendations that are founded on the universal principle of innovation as a linchpin of robust security.

agencies, and large and small enterprises — can take to contribute to this partnership.

Congress

Congress plays an important role in funding research, law enforcement, and government programs in cyber security, evaluating national progress against cyber security challenges, and considering ways to nudge the marketplace forward. Specific congressional actions should include increasing appropriations for cyber security research, including funding for the Cyber Security Research and Development Act of 2002. As technology constantly changes, so do the complexities and vulnerabilities of information systems and the supervisory control and data acquisition (SCADA) systems that control critical infrastructures and manufacturing processes. More research is needed to improve these systems and to identify and reduce their vulnerabilities.

Ratification of the Council of Europe Convention on Cybercrime would minimize obstacles to international cooperation that currently impede US investigations and prosecutions of computer-related crimes.

Congress should also authorize and appropriate funding increases for the National Institute of Standards and Technology (NIST) to support its Computer Security Division, a critical resource in the development of computer security standards and best practices for the private sector and government agencies. Likewise, more funds are needed to hire and train officers in computer crime and forensics and to create a national cyber investigations and forensics training academy and a national center of excellence on cyber forensics.

In addition, Congress needs to ratify the Council of Europe Convention on Cybercrime. This treaty establishes a solid framework for all countries around the world to fight cyber crime, harmonizing national laws that define offenses, defining investigative and prosecutorial procedures to cope with global networks, and establishing a rapid and effective system of international cooperation. Ratification of the convention would minimize obstacles to international cooperation that currently impede US investigations and prosecutions of computer-related crimes. Specific reservations and declarations would ensure that the treaty is consistent with the US Constitution and federal law.

Other useful measures would:

- Increase criminal penalties for convicted hackers
- Create tougher penalties for online identity theft
- Set a national standard on breach notification (thus preempting the potential enactment of 50 state laws), including incentives for companies to adopt information security best practices
- Fund information security education and awareness programs for schools, small businesses, and other users
- Explore, through hearings, economic incentives for information security technology investment and implementation

Congress recently elevated to the level of Assistant Secretary the head of the National Cyber Security Division (NCSD) of the Department of Homeland Security. This was an important action that allows the federal government to better integrate cyber security and physical security policy and implementation and improve the department's private-sector outreach.

As a legislative body, however, Congress should remain circumspect about its ability to mandate technological solutions to the problem, as innovation and the business models that support it change faster than the ability of legislation to be relevant and constructive.

The Federal Government

The US federal government, as a major customer and user of information networks — whether for civil, national security, intelligence, or defense purposes — is a vital partner with the private sector in the detection, prevention, mitigation, and analysis of cyber security vulnerabilities and attacks and in ongoing information sharing and programmatic cooperation. The government is also a major educator of the general public, and it should both lead by example and use its bully pulpit to push for improved cyber security technology and practices.

Accordingly, relevant government agencies should:

- Adhere to and implement requirements under the Federal Information Security Management Act of 2002 (FISMA), using the Best Security Practices methodology piloted by the Federal CIO Council.
- Aggressively implement a requirement that agencies include information security strategic objectives in their information technology procurement decision making. This requirement emerged from an

amendment to the Clinger-Cohen Act of 1996 and was enacted in the 2004 Intelligence Reform bill.

- Access and implement the NIST Security Configuration Checklist repository, which brings together vendors and customers in a voluntary process that matches users' security requirements with configuration settings recommended by vendors.
- Diligently implement and enforce the Federal Acquisitions Streamlining Act of 1994 (FASA), which requires that agencies plan for and acquire commercial goods or services to meet their needs rather than develop them if the commercial sector can provide those goods or services. Many government agencies need to recognize that the best and most cost-effective solution may come from a commercial company rather than from developing solutions internally.
- Partner with private-sector groups to identify and recognize consensus-based, market-driven metrics and best practices across sectors as references for improved cyber security.
- Fund training of government systems administrators in security practices.
- Clarify and enhance working relationships among the cyber security leads of various federal agencies, including the NCSD; NIST; National Security Agency (NSA); Office of Management and Budget (OMB); General Services Administration (GSA); Federal Bureau of Investigation (FBI), Federal CIO Council, and others.
- Treat the private sector as a full and equal operational partner in planning, two-way information sharing, training, and executing solutions, particularly in the current efforts to engage the private sector in the National Infrastructure Protection Plan (NIPP) and the National Response Plan (NRP). Given the importance of the security of IT infrastructure to the operations of other major critical infrastructures (water, oil and gas, financial services, telecommunications, etc.), the IT Information Sharing and Analysis Center is an essential partner with the government and other sectors in monitoring and protecting the security of our cyber infrastructure.
- Continue cross-jurisdictional and international coordination in law enforcement activities.
- Aggressively promote expansion of NSA Centers of Academic Excellence.
- Revive the annual *National Information Systems Security Conference (NISSC)*, which had been held every year from 1977 to 2000. This conference provided a definitive opportunity for government and industry to come together in discussion and information sharing.

US government and industry must recognize that cyber crime seeks to penetrate the vulnerabilities of a global economy and, therefore, has a very large international dimension.

International Organizations

US government and industry must also recognize that cyber crime seeks to penetrate the vulnerabilities of a global economy and, therefore, has a very large international dimension. Indeed, the Internet and e-commerce are international by their very nature and so depend on the growth of free and open networks to achieve their fullest potential. Similarly, nations beyond the US share this country's dependence on information technology for efficient deployment and operation of critical infrastructure systems and services. Attacks on information technology strike not only the technology itself but the large-scale and often mission-critical systems it supports. In this way, nations sharing common values, borders, trade, treaties, and investment have a common interest in the safe and efficient operation of critical infrastructure.

Just as the character, variety, and richness of the Internet and e-commerce gain through international adoption and use, so do these resources suffer as cyber criminals use the "borderless" nature of the Internet to game the legal system through venue hopping for lax enforcement, to launch cross-border attacks on systems or infrastructure, and to share "best practice" information on attack tools and vulnerabilities. In this manner, cyber crime becomes the malicious practice of individual hackers and troublemakers, criminal syndicates, terrorists and other nonstate agents, and even governments interested in espionage or attacks on critical infrastructure in concert with physical attacks. Government and industry in the US must therefore reach out to international counterparts to ensure that there are no "safe harbors" for cyber criminals and no easy targets among the international Internet community.

The good news is that multinational organizations in Europe, Asia, and elsewhere share the commitment to international cooperation for a stronger common cyber defense. The Organisation for Economic Co-operation and Development (OECD), for instance, has published guidelines urging government and industry cooperation on an international framework for information systems security. OECD has also published a checklist providing business executives with guidance on information security governance.

The Asia-Pacific Economic Cooperation (APEC) forum has developed the APEC Cybersecurity Strategy, which provides several cyber security measures intended to harden systems and increase public confidence in e-commerce systems. Key public infrastructure guidelines are an example of an initiative designed to assist cross-jurisdictional e-commerce.

Beyond guidelines and best practices, the need for improved information sharing looms large in addressing information security from an international perspective. Countries share the common strengths and weaknesses of the Internet; if national boundaries prevent responsible parties from sharing vulnerability information, the entire online community stands to be disrupted.

In addressing the Year 2000 date conversion, a computer vulnerability that confronted all technology-reliant economies, governments worked together to share information of common importance. A similar approach could be adapted for the multinational information security challenge. An international information security coordination center could perform meaningful work in such areas as incidence reporting and coordination, inter- and intra-industry information sharing, and public education. Such a center could open doors of communication and cooperation between governments and industries. The center would encourage peer-to-peer relationships and build greater common information security knowledge in particular application domains. It could also help foster a more trusted relationship between government and industry.

Industry

Technology can be both the problem and the solution, the target of attack and the defense against security intrusions — but not exclusively so. With exponentially increasing numbers of nodes and devices interconnected across the Internet and private networks, the possibility for exploitable vulnerabilities rises with every connection. The cyber security industry has been innovating furiously in the technology arms race against those who innovate to exploit, but the battle will continue as long as there is innovation — on both sides. It is therefore incumbent on the industry to organize itself around fundamental principles of secure development and implementation and thus stay at least one step ahead of the cyber criminal. With this objective, industry must meet its partnership obligations by:

- Making security a top priority and putting security concerns at the heart of the design process, using government, industry, and international standards where possible.
- Working with home users, small businesses, and large enterprises (including government agencies and educational institutions) in a continual process of improving the security, maintenance, and reliability of products that maximize users' productivity.
- Continuing to improve the engineering, development, testing, and training processes and methods that reduce defects in systems specification, design, implementation, and remediation (patching). Industry should also partner with government and academia to develop automated tools for evaluating software quality and security.
- Creating a software and systems security accreditation and certification program for increasing security in software and systems development.
- Identifying, adopting, training, and deploying information security best practices with clearly assigned cyber security roles and responsibilities for all employees and organizational leadership, such as the CEO, CIO, CISO, and board of directors.

Training Is Key

Effective cyber security is only as strong as the weakest link. In order for technology solutions to be effective, organizations need a well-trained workforce that observes systematic policies and procedures. Technology tools will always require some human interface and judgment. With this principle in mind, organizations that have not yet put systemic information security systems in place should refer to existing enterprise models that:

- Designate a qualified CISO and establish a clear career path with a training and certification framework for information security professionals within the organization
- Dedicate the necessary financial and human resources to protecting systems

- Identify, adopt, teach, and deploy information security best practices with clearly assigned cyber security roles and responsibilities for all employees and organizational leadership, such as the CEO, CIO, CISO, and board of directors
- Promote an environment of competition on security and assurance by articulating their security needs and expecting vendors to compete to meet those requirements

TAKE THE BALL AND RUN WITH IT

Adopting these measures in a national public-private partnership will move the ball far down the field. If progress stalls, however, Congress has demonstrated its willingness to intercede with legislation that substitutes penalties and costly overhead for patience and persuasion. It is not easy to get information security policy right; it is a complex discipline with many moving parts, and there are many different legitimate definitions of what is the "right amount" of security. If we move too quickly in the interest of "doing something about it," we run the risk of doing something to make it worse. While the information security–related provisions of some laws — such as SOX (which governs all publicly traded companies), HIPAA (which governs health services entities), and Gramm-Leach-Bliley (which governs financial institutions) — have all raised awareness of the need for information security, it isn't clear whether additional legislative requirements are needed to strengthen the nation's information security posture. Industry cannot legislate stiffer penalties for cyber crooks or more resources for cyber forensics; it can, however, move with all deliberate speed to adopt information security best practices and raise the bar very high for those intent on electronic breaking and entering.

In 2005, the information technology industry took a big step in this positive direction by launching the IT Sector Coordinating Council (IT SCC). The IT SCC will serve as the focal point for collaboration and information sharing on critical infrastructure protection within the sector, with the federal government, and with other sectors. The IT SCC joins other critical infrastructure sectors that have organized themselves for maximum effectiveness in responding to national emergencies that could have damaging impacts on the nation's health, safety, and economic well-being.

Working together to establish best practices, share information, identify risks, and build protective barriers, the public-private partnership can become a powerful deterrent in the fight against cyber crime.

Greg Garcia is currently VP for Information Security Programs and Policy with the Information Technology Association of America. In this role, he manages all programmatic and public policy aspects of information security, with a view to strengthening our national cyber readiness among the user and vendor communities.

Before joining ITAA, Mr. Garcia served on the staff of the Science Committee of the US House of Representatives, where he was responsible for industry outreach and legislative issues related to information technology and cyber security. In particular, he played an active role, under the leadership of Chairman Sherwood Boehlert, in the drafting and enactment of the Cyber Security R&D Act of 2002. Mr. Garcia came to Capitol Hill after serving as the head of 3Com Corporation's government relations office in Washington, DC. There he was responsible for all aspects of the company's strategic public policy formulation and advocacy.

From 1998 to 1999, Mr. Garcia was Coalition Manager for Americans for Computer Privacy, a high-profile grassroots policy advocacy campaign that, in just one year, succeeded in overturning US export and domestic use regulation of encryption technology. Mr. Garcia is a graduate of San Jose State University. He can be reached at ggarcia@itaa.org.

About Cutter Consortium

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you Access to the Experts. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts, experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including content via online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products and training/consulting services, you get the solutions you need, while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Cutter Business Technology Council

The Cutter Business Technology Council was established by Cutter Consortium to help spot emerging trends in IT, digital technology, and the marketplace. Its members are IT specialists whose ideas have become important building blocks of today's wide-band, digitally connected, global economy. This brain trust includes:

- Rob Austin
- Tom DeMarco
- Christine Davis
- Lynne Ellyn
- Jim Highsmith
- Tim Lister
- Lou Mazzucchelli
- Ken Orr
- Ed Yourdon