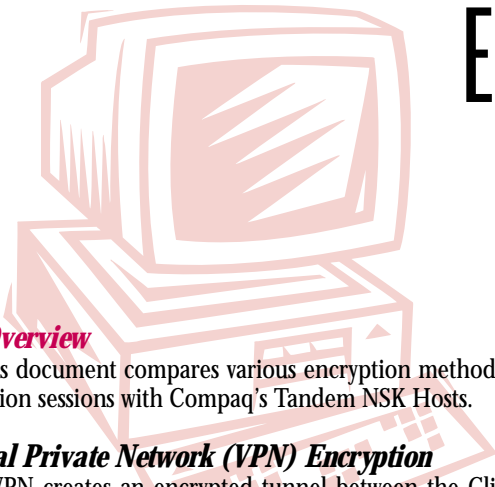


*"The only Password you should share."*



## Encryption Method Comparison for Terminal Emulation

By Scott Uroff • [scott\\_u@xypro.com](mailto:scott_u@xypro.com)

### 1. Overview

This document compares various encryption methods for terminal emulation sessions with Compaq's Tandem NSK Hosts.

#### **Virtual Private Network (VPN) Encryption**

A VPN creates an encrypted tunnel between the Client PC and a VPN server. The VPN Server sits between the Client PC and the NSK, but external to the NSK system. Cryptographic mechanisms located in the Client PC and the VPN Server perform encryption and decryption functions. The VPN server sends and receives unencrypted data to and from the NSK Host.

#### **Secure Socket Layer (SSL) Encryption**

SSL creates an encrypted tunnel between the Client PC and a Telnet Proxy Server. The Proxy Server sits within the NSK environment between the TCP/IP Process and the standard Telnet Server. Cryptographic mechanisms located in the Client PC and the Proxy Server software perform encryption and decryption functions. The Proxy Server sends and receives unencrypted data to and from the Telnet Server within the NSK Host.

#### **Application Layer (End-to-End) Encryption**

Application Layer Encryption creates an encrypted tunnel between the Client PC and a Virtual Terminal Process (VTP) within the NSK environment. The VTP sits between the Telnet Server and the Application (TACL in this example). Cryptographic mechanisms located in the Client PC and VTP perform encryption and decryption functions. The VTP sends and receives unencrypted data to and from the NSK Host Application.

### 2. Your Risks with No Encryption

In an unencrypted environment, data flows between a Client PC and an application running on the NSK Host. Such data flow includes your Userids and passwords as well as critical and confidential business information and transactions. In large environments, in addition to the external Internet, there are likely to be thousands of Client PCs and multiple intranets as well as multiple Host systems running multiple Host applications.

There are at least three points in the transmission path where unencrypted data can be viewed; these points are targets for internal and external intruders to attack your system and capture your data using common, readily available technologies:

A Network Sniffer can see data as it traverses a Network Cloud, whether external (the Internet) or internal (Intranets). Sniffer technologies are readily available; they can be downloaded at no cost from the Internet. They make your data vulnerable to both external and internal intruder attacks.

A Host-initiated SCF Line Trace can see data in transit between the LAN Controller and the TCP/IP Process. SCF Line Traces are commonly used as diagnostic tools, but also can be deployed for attack purposes. They make your data vulnerable to internal intruders which, according to surveys by Ernst & Young and the FBI, account for 80% of security breaches.

A Host-initiated SCF Process Trace can see data traversing between the TCP/IP Process and the Telnet Server as well as between the Telnet Server and the TACL Process. Like the Line Trace, SCF Process Traces were initially intended as diagnostic tools but can be exploited for attack purposes making your data vulnerable to internal intruders which account for 80% of security breaches (per Ernst & Young and FBI surveys).

### 3. Secure Communications Comparison VPN Encryption

In a VPN environment, data is encrypted only between the Client PC and the VPN Server. Data flow between the VPN Server and the Host  
*Continued on page 4.*

#### INSIDE THIS ISSUE

ENCRYPTION METHOD COMPARISON FOR TERMINAL EMULATION .....	1
PRESIDENT'S LETTER .....	2
GREENIDEA UPDATE .....	5
BOARD PROFILE .....	6
INDUSTRY CALENDAR .....	7
CHAPTERS .....	8
INFORMATION SECURITY AND ELECTRONIC BANKING SYSTEMS .....	9
ISSA CHAPTER LISTING .....	11

# PRESIDENT'S LETTER



Dear Fellow Members,

Well the annual meeting has come and gone. Welcome to the new board members and welcome back the members that continue to serve the organization. The Joint Computer Security Conference (JCSC) was well attended and we are looking forward to the fall JCSC.

It was a true pleasure for me to present this year's awards. To recognize the key contributors in our field is an important aspect of our profession. Congratulations to the recipients and thanks for your dedication to the field. Here are the winners of this years awards:

### Hall of Fame

Donn Parker, CISSP  
Harold F. Tipton, CISSP  
William H. Murray, CISSP  
Scott Charney  
Sandra Lambert, CISSP, CDP, CISA

### ISSA Honor Roll

Donald L. Evans, CISSP, FLMI  
Gerald L. Kovacich, CISSP, CFE, ISO, CPP  
Harold F. Tipton, CISSP  
William H. Murray, CISSP  
Richard W. Owen Jr., CISSP  
James Duffy, CISSP

### Chapter of the Year: Capitol of Texas

Ronald E. Helsley, President

### Website of the Year: New York Metro

Wilfred Camillieri, Webmaster  
Ron Petrucci, Website Chairperson

### President's Award of Excellence:

Richard Mosher  
Ed Norris

### Security Professional of the Year

Nena Young, CRP, CBCP

### Outstanding Organization of the Year

Ernst & Young

I also was pleased to present gavels to some of the newest chapters:

Alamo  
The Carolinas  
Connecticut  
Phoenix  
Detroit  
Puget Sound (Pacific NW)  
Silicon Valley  
South Florida

By the time you read this, the Vancouver BC chapter and the Milwaukee chapters will have had their first meetings. Thanks to Laura Stoner and Michael Rasmussen for their leadership in getting these chapters started. We also have been working with folks from Italy, the UK and Finland on getting chapters started in those countries as well. Great work by all of our members on spreading the word and helping us grow.

While I was writing this column, many of us were plagued by "Love Letter" viruses. From the initial feedback I have received it seems that, although it has hit many people hard, we have been better prepared to do the clean up than in the past. We have had some tough issues to deal with this year, but we have learned from them and have improved our processes to deal with them. ISSA members have been out in front on how to deal with security issues and we continue to be a great resource from which the whole profession can learn.

Sincerely,

Howard A. Schmidt  
ISSA President

## ISSA 2000-01

### Officers & Directors

#### President

Howard A. Schmidt  
Microsoft Corporation  
howards@microsoft.com

#### Vice President

Bill Betts, CISSP, CPP  
CompuSec  
billbetts@home.com

#### Treasurer

Rebecca DeWeese  
Columbia University  
rd171@columbia.edu

#### Director of Operations

Richard Mosher, CISSP, CBCP  
Ernst & Young  
Richard.Mosher@ey.com

#### Director of Membership/Chapter Relations

Edward Norris, CISSP  
GTE Laboratories  
enorris@gte.com

#### Director of Communications

David Cullinane, CISSP, CPP  
nCipher, Inc.  
dcullinane@us.ncipher.com

#### Director of Marketing/Public Relations

Kurt Young, CISA  
American Century Investments  
kurt\_young@americancentury.com

#### Director of Education

Deb Peinert  
Charles Schwab & Co.  
Deb.Peinert@Schwab.com

#### Chairperson of the Board

Pat Gilmore, CISSP  
Charles Schwab & Co.  
Pat.Gilmore@Schwab.com

#### Executive Director

Mary Krukowski  
mbrmktg@issa.org

### The ISSA PASSWORD

#### Publisher

Information Systems Security Association  
7044 South 13th St.  
Oak Creek, WI 53154  
Phone: (800) 370-ISSA or (414) 768-8000  
Fax (414) 768-8001  
www.issa.org

Board of Directors e-mail:  
Issa@issa.org

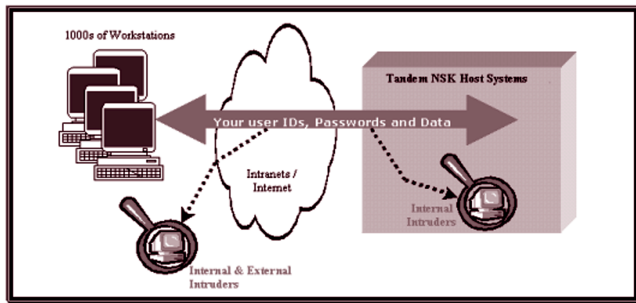
#### Editor

Meta L. Levin  
LevinM@GTE.net

#### Managing Editor

David Cullinane, CISSP, CPP  
dcullinane@us.ncipher.com

Graphic Designer  
Matthew Jossart  
graphics@nasp.a.net



is unencrypted and unprotected as it traverses the Network Cloud to and from the Host. This method leaves your data vulnerable to intruder attack by Network Sniffer, SCF Line Trace and SCF Process Trace.

There are additional disadvantages to VPN-based encryption. This method doubles the traffic on the Network Cloud, which can create congestion and delays. Some implementations place the VPN Server on the Network Cloud, but move the Host to a private network between the VPN Server and the Host. This approach does reduce the traffic overhead problem and the number of target points where a Network Sniffer can be successfully deployed to capture data. However, security can still be compromised on private networks (Intranets), which deploy a Network Sniffer to capture data.

### SSL Encryption

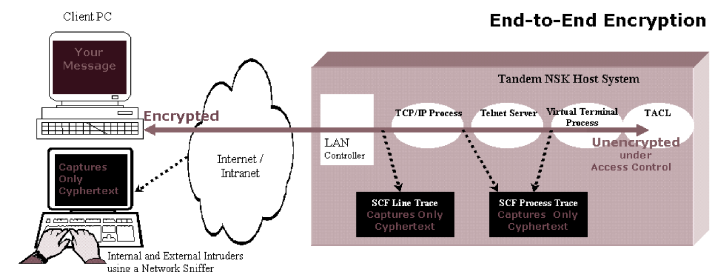
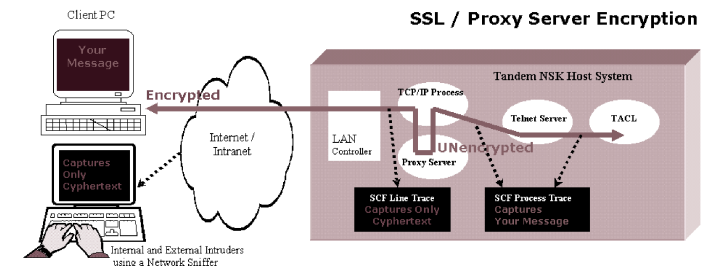
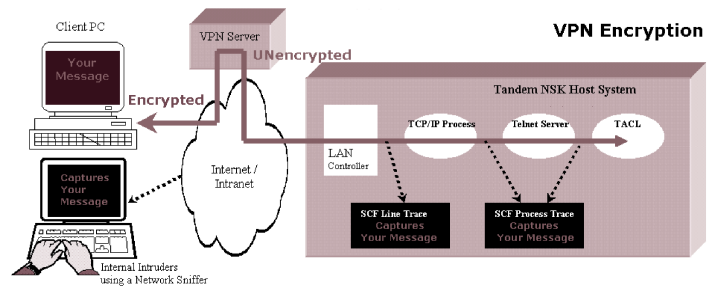
Using an SSL-based approach, data is encrypted only between the Client PC and the Proxy Server software. Data flow is unencrypted and unprotected as it travels between the Proxy Server and the Host Application (TACL). This method prevents the Network Sniffer and SCF Line Trace (between the LAN Controller and TCP/IP Process) from compromising security. However, SCF Process Traces between the TCP/IP Process and the Telnet Server and between the Telnet Server and the TACL Process are still easy targets for internal intruders with super group Userids or aliases. Typically SSL solutions use a fixed public key hardcoded in the client software or require manual management and distribution of encryption keys. Manual key management consumes considerable people time on the host side, with little benefit to Clients in terms of security.

Besides the security risks, there are several performance problems associated with SSL-based encryption. This method doubles the traffic through the TCP/IP Process on the Host, which is likely to result in bottlenecks and delays, especially as transaction volumes increase. Furthermore, normally all cryptographic functions (encryption, decryption and key exchange) on the Host are handled by one Proxy Server Process. This can create another bottleneck as the number of users accessing the Host increases. While it is possible to increase the number of Proxy Servers to spread the load across multiple CPUs, this solution is not necessarily transparent to the end-user. Either each user must select and connect to a specific Proxy Server, or centralized Configuration Management must implement and handle ongoing load balancing as transaction volumes fluctuate and increase. Neither approach ensures against bottlenecks and delays.

Another disadvantage of the Proxy Server is that applications on the Host can no longer obtain the IP address of the Client because all of the clients appear to the applications as if they have the same IP address as the Host. Companies accustomed to using individual IP addresses for configuration management purposes, security, etc. can do so no longer if they use SSL.

### End-to-End Encryption

With the End-to-End method, data is encrypted between the Client PC and a Virtual Terminal Process positioned within the NSK host,



between the Telnet Server and the Application (TACL). This method prevents all three methods of capturing unencrypted data: Network Sniffer, SCF Line Trace and SCF Process Trace as well as supplying Access Control mechanisms for TACL.

Encryption is deployed at the Application Layer rather than the Secure Socket Layer or via VPN. In addition to encryption functions, the Virtual Terminal Process also supplies Access Control mechanisms for TACL. Because each session has its own unique, randomly generated key, End-to-End encryption provides "perfect backward and forward security" too. This means that if one key is compromised, only that session's data is threatened. All data from past ("backward") sessions and future ("forward") sessions remains secure. With VPN and SSL, one compromised key may be used to decrypt not only one session, but captured data from all past and future sessions that use the compromised key.

In addition to being more secure, End-to-End Encryption offers additional advantages in terms of performance. First, there is only one trip through the Network Cloud (instead of doubling the network traffic as required for the VPN approach) and only one trip through the TCP/IP stack (instead of doubling this traffic as SSL does). And because there is one Virtual Terminal Process per user session, the (encryption, decryption and key exchange) load can be spread across all CPUs by whatever load balancing tools or procedures are already in use on the NSK Host system. Load testing demonstrates that current versions of the NSK Operating System easily handle thousands of processes per system, including End-to-End encryption, efficiently and with quite acceptable performance. As transaction volumes fluctuate and increase, the NSK host system adjusts the load spread dynamically and transparently to maintain consistently high performance levels.

### 4. Relevant Security Concepts

At least three key Security Principles apply to evaluating encryption methods.

## Your Security is Only as Strong as its Weakest Link

At home, if you lock your doors but leave the windows open, you are still vulnerable to break-ins. Unencrypted or partially encrypted communications between Client PCs and their Compaq / Tandem NSK hosts are weak links in the security chain, providing "windows" of opportunity for information theft. Compared to physically breaking into your car or home, computer break-ins present extremely low risk of detection or danger to intruders. The combination of low risk, easy information access and very profitable returns has turned computer-based theft into a growth industry.

## Your Selection of Security Mechanisms Should Consider the Value of Your Assets

Business-critical information and transactions involving large dollar amounts require robust, end-to-end encryption mechanisms to mitigate vulnerabilities and protect against break-ins. Just as it would be illogical to put a \$50 security system on a \$1million home, the value of your information assets can be used to determine appropriate information security mechanisms. This applies not only to the method of encryption, but the "strength" of encryption.

For instance, a 168-bit Triple DES encryption is virtually impossible to crack because it is one trillion times stronger than a 128-bit DES. In cryptographic terms, 128-bit DES uses two 64-bit keys and 8 bits of each 64 are associated with validation checking, leaving 56 bits for key "strength". So an "apples-to-apples" comparison would be: 2 x 56 or 112-bit DES encryption by SSL compared to 3 x 56 or 168-bit DES End-to-End encryption. Mathematically, 168-bit DES is seventy quadrillion times stronger than 112-bit DES.

## Security Mechanisms Must be Easy to Use


If your security is cumbersome, people will avoid using it, no matter how strong it is. Such avoidance itself may be well-intended, aimed at

meeting a deadline or getting expediting work, but the results leave your information assets vulnerable to intruders for whose actions your company is likely to be held accountable.

## 5. Conclusions

All three approaches to encryption, VPN, SSL and End-to-End improve the security of sensitive eBusiness communications. However, there are significant differences between the approaches in regards to the quality and scope of security provided. Critical differences also exist in the ability to perform efficiently in highly scaled data processing environments.

Early implementations to improve systems security have utilized VPN or SSL. However, these approaches fail to adequately protect against internal intruders, which account for 80% of security breaches. Because they increase traffic on (network or TCP/IP) technologies that bog down with congestion, VPN and SSL implementations are also subject to delays. As the limitations and deficiencies of these approaches are demonstrated, products in these categories are becoming a source of increasing concern when valuable information assets are involved.

For an integrated security solution, using more advanced technology, End-to-End Encryption is recognized as a superior strategy for eBusiness communications, for both security and performance reasons. 

*Scott Uroff has more than 21 years experience in the areas of Tandem system management, security and performance tuning, as well as design and programming in Tandem, LAN and PC environments. Uroff is product manager for the XYGATE suite of Tandem platform security modules and cross-platform encryption mechanisms.*

## The World's Best Telephone Scanner Just Got a Whole Lot Better!

### Announcing PhoneSweep™ 2.0 Telephone Scanner

- \* Enhanced ODBC-compliant SQL database
- \* Enhanced reports featuring graphics and differential analysis
- \* PPP and RAS password testing
- \* Controls 1-8 modems, up to 1000 calls/hour
- \* Runs on Windows 95/98/NT
- \* In use world-wide
- \* Prices start at \$980

Now Identifies 250 remote access systems, including **pcANYWHERE, ReachOut, CarbonCopy, Cisco, Annex, Citrix WinFrame, Windows NT RAS, UNIX (48 versions!), Bay Networks, BLAST, Audix, VAX/VMS** and 191 more.

**Sandstorm Enterprises, Inc.**  
www.sandstorm.net  
+1 617-426-5056  
PO Box 381548  
Cambridge, MA 02238-1548

Ask us about PhoneSweep Enterprise, with 48 modems / 6000 calls per hour capacity!

All product names referenced herein are trademarks of their respective companies.

## GreenIdea Update

GreenIdea, Inc., which offers Security Awareness software at a special discount to ISSA members, recently added new animation to its screen savers. Called "Visible Statement," the software uses animated graphics on its screen savers to remind users to practice good computing habits. The new additions highlight nine different security issues. In addition to the new animation offered by the company, customers now have the option of ordering custom animation to complement the original package, and users can automatically update and refresh the content.

New customers include The U.S. Census Bureau, Unocal, 3M, PG&E, and Kaiser Permanente. ISSA members can receive a free, full working evaluation copy of the Visible Statement program from GreenIdea by contacting Russ Mumford (415) 863-2157 or e-mail [mumford@greenidea.com](mailto:mumford@greenidea.com). More information is available on the company's web site <http://www.greenidea.com> or through the ISSA web site at <http://www.issa.org/greenidea.htm>.

# BOARD PROFILE

## **Deb Peinert** Director of Education

For new ISSA Director of Education Deb Peinert, it was a case of being at the right place at the right time. If Farmers Insurance in Los Angeles had not had a computer security job open, she might never have found the career. By the same token, if she had never gone to work for Charles Schwab in San Francisco and met former ISSA President Pat Gilmore, she would never have run for a board position.



*"It sounded interesting. . .  
It was technical, but still  
working with people -  
helping people."*

Peinert, a native of Cleveland, Ohio, graduated about 13 years ago from Bowling Green State University in Ohio with a degree in education, specializing in computer science with a minor in mathematics. All her life her parents had talked about moving to California. So, armed with her new degree she headed for San Diego and began looking for teaching jobs. She found none.

Peinert switched gears and began interviewing for computer science jobs. While talking to someone from Farmers Insurance in Los Angeles, she was told there were two job openings. One was data security.

"It sounded interesting," she said. "It was technical, but still working with people - helping people."

She found it fit her personality well. She likes a challenge and finds it "fun to learn new things."

"I don't like to sit around and do the same thing over and over again," she said.

Over the years she has watched her field and her job change, from everything on a mainframe and typewriters in the office, to a terminal on every desk. When she left Farmers Insurance in 1990, there were two PCs in a 10 person department.

From Farmers, she went to Glendale Federal Bank, where she stayed for two years before landing at Paramount Pictures as manager of information security for a two person department. In the five years she spent there she wrote policy, conducted security reviews, and worked on protection for e-mail, the network, the firewall, and Unix - all things that were never a part of her first InfoSec job.

"It was fun and I got to learn new things," she said.

In October, 1997, she came to Schwab in San Francisco as a senior manager. She has been promoted to managing director of enterprise security access and control, and has watched her department grow from 10 or eleven people to the current 22.

It wasn't until she was in a managerial position that she began attending ISSA chapter meetings regularly. After the moving to Schwab she admits that she didn't get there as often as she would have liked, just because of a heavy work load.

In the intervening years her whole family has moved to California. First Peinert and her brother, then her parents and grandparents. With


Peinert in San Francisco and everyone else in San Diego, she only gets to see them on holidays and for special events. Last year she and her brother joined her parents for a week in London to celebrate their 40th wedding anniversary. She also took a U.K. solar eclipse cruise that started in Dover and went to France, Dublin, two places in Norway, Scotland and Amsterdam. She also took advantage of the opportunity to spend some time in Paris and Canterbury.

An avid skier, she regularly downhill skis with friends in Colorado, especially in Vail and Steamboat Springs, her favorites. This year she joined a skiing club out of Lake Tahoe, eventually becoming part of the downhill racing team. For three months, every other weekend, she was on the slopes, competing in races.

"I enjoyed it very much," she said. "I like speed."

In the nicer weather she can be found bicycling and or on in-line skates.

Peinert also enjoys the travel she does, both for business and pleasure. Wherever she goes, she tries to explore historical points of interest. Even while in the U.K., she had a sort of busman's holiday - checking out the area near London where the famous World War II cryptography was centered and the Enigma code cracked.

As ISSA Director of Education, Peinert has several goals. Topping the list is working toward continual improvement of conference offerings, as well as a speakers data base, which would be open to chapters. She wants to work with chapters to offer them as much help as possible in planning and improving programs. In addition, she wants to explore current training needs and interests. 

## A note from Jeff Stelmach

(Author of Information Security and Electronic Banking Systems, elsewhere in this issue)

If you've never been able to convince management about the need for adequate information security, Ira Winkler's book, *Corporate Espionage* (Prima Publishing, Rocklin, CA, 1997) would make a great addition to someone's summer reading list.

## ISSA Membership Update Form

Name \_\_\_\_\_

Member # \_\_\_\_\_ Chapter \_\_\_\_\_

Address \_\_\_\_\_

City, State, ZIP \_\_\_\_\_

Country \_\_\_\_\_

Email \_\_\_\_\_

Phone \_\_\_\_\_

FAX \_\_\_\_\_

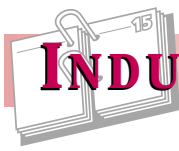
Please send to:

### ISSA Headquarters

7044 South 13 St.  
Oak Creek WI 53154

FAX to (414) 768-8001 or  
[www.issa.org/members](http://www.issa.org/members)

and follow the Member Update link



# INDUSTRY CALENDAR

## *Computer Security Institute*

June 12-14, 2000

**NetSec 2000 - Technical Dimensions in Network Security**

*Location: San Francisco, CA*

October 31-November 1, 2000

**Introduction to Computer and Network Security**

*Location: Gaithersburg, MD*

November 11-12, 2000

**Introduction to Computer and Network Security**

*Location: Chicago, IL*

September 20-21, 2000

**How to Become an Effective Information Security Professional**

*Location: San Antonio, TX*

September 18-19, 2000

**A Practical Guide to Encryption and Certificate Authorities**

*Location: San Antonio, TX*

November 2-3, 2000

**A Practical Guide to Encryption and Certificate Authorities**

*Location: Gaithersburg, MD*

June 15-16, 2000

**How to Develop Information Security Policies and Procedures**

*Location: San Francisco, CA*

August 1-2, 2000

**How to Develop Information Security Policies and Procedures**

*Location: Gaithersburg, MD*

November 11-12, 2000

**Facilitated Risk Analysis for Business and Security**

*Location: Chicago, IL*

August 17-18, 2000

**Securing E-Business: A Technical Guide to Implementing PKI**

*Location: Ottawa, Canada*

November 11-12, 2000

**Securing E-Business: A Technical Guide to Implementing PKI**

*Location: Chicago, IL*

June 10-11, 2000

**Windows NT Security: Assess, Penetrate and Secure**

*Location: San Francisco, CA*

November 11-12, 2000

**Windows NT Security: Assess, Penetrate and Secure**

*Location: Chicago, IL*

June 15-16, 2000

**Secure Migration to Windows 2000**

*Location: San Francisco, CA*

September 20-21, 2000

**Secure Migration to Windows 2000**

*Location: San Antonio, TX*

November 16-17, 2000

**Secure Migration to Windows 2000**

*Location: Chicago, IL*

June 15-16, 2000

**Intrusion Techniques and Countermeasures**

*Location: San Francisco, CA*

October 2-3, 2000

**Intrusion Techniques and Countermeasures**

*Location: San Francisco, CA*

November 16-17, 2000

**Intrusion Techniques and Countermeasures**

*Location: Chicago, IL*

June 15-16, 2000

**Advanced Network Security**

*Location: San Francisco, CA*

June 10-11, 2000

**How to Conduct a Network Vulnerability Assessment**

*Location: San Francisco, CA*

August 15-16, 2000

**How to Conduct a Network Vulnerability Assessment**

*Location: Ottawa, Canada*

September 18-19, 2000

**How to Conduct a Network Vulnerability Assessment**

*Location: San Antonio, TX*

November 16-17, 2000

**How to Conduct a Network Vulnerability Assessment**

*Location: Chicago, IL*

June 15-16, 2000

**How to Develop a Winning Security Architecture**

*Location: San Francisco, CA*

September 20-21, 2000

**How to Develop a Winning Security Architecture**

*Location: San Antonio, TX*

November 16-17, 2000

**How to Develop a Winning Security Architecture**

*Location: Chicago, IL*

October 4-5, 2000

**Firewalls and Internet Security**

*Location: San Francisco, CA*

November 16-17, 2000

**Firewalls and Internet Security**

*Location: Chicago, IL*

September 18-19, 2000

**Forensic Investigation: Tools and Techniques**

*Location: San Antonio, TX*

June 15-16, 2000

**Comprehensive Intrusion Management**

*Location: San Francisco, CA*

August 3-4, 2000

**Comprehensive Intrusion Management**

*Location: Gaithersburg, MD*

November 11-12, 2000

**Comprehensive Intrusion Management**

*Location: Chicago, IL*

June 10-11, 2000

**Essential Skills for the Computer Incident Response Team**

*Location: San Francisco, CA*

November 16-17, 2000

**Essential Skills for the Computer Incident Response Team**

*Location: Chicago, IL*

**Information: [www.gocsicom.com](http://www.gocsicom.com); [csi@mfi.com](mailto:csi@mfi.com);  
(415) 905-2626; Fax (415) 905-2218**

## *Vanguard*

May 14-19

**14th Annual Vanguard Security Expo 2000**

*Location: Atlanta, GA*

*Information: (888) 547-EXPO; Fax*

*(714) 939-0273; [www.vipexpo.com](http://www.vipexpo.com);*

*180 S. Anita Dr., Orange, CA 92868*

## *New York Metro Chapter*

May 23 - 24, 2000

**Computer Security for the 21st Century**

*Location: New York, NY*

*Information: George Dolicker,*

*[gipd@lucent.com](mailto:gipd@lucent.com) or (914) 232-2373*



## Minnesota Chapter

Just 10 years old, the Minnesota Chapter is going strong and growing. There were about 30 members when it started in the fall of 1990. Prior to that a group of InfoSec professionals had been meeting more informally. Now there are more than 100 members, with a mailing list closer to 200, and between 60 to 80 people who regularly attend meetings.

President Jayne Logan has served on the board since 1997. Recently the chapter decided to restructure its five member governing board, eliminating the corresponding secretary position and adding three directors, all of whom will be appointed to one year terms to handle programs communications and membership. Eliminating the corresponding secretary's job is an indication of how things have changed both in Minnesota and around the country. The job's primary responsibility was mailing or faxing meeting notices. Two years ago the chapter began communicating with members almost exclusively through e-mail and its web site. Logan noticed an almost immediate jump in meeting attendance.

"It's been a godsend to be able to communicate with our members that way," Logan said. "Now with e-mail, members can forward the notices on to other people in their companies who might be interested. We noticed participation (in meetings) was much higher after we started."

The chapter meets every other month, and tries to post topics on its web site at least a month ahead. With this came the realization that the

chapter needed a more coordinated approach to long range meeting planning - hence the new program director position. Speakers come from a variety of sources, including vendors, who are asked to make their presentations non-product specific, but then are given an opportunity to talk about their particular goods at the end of the meeting.

Two special interest groups meet regularly: the Health Insurance Portability and Accounting Act group, which deals with issues of privacy raised in implementing this legislation; and the Security Awareness group. Both post meeting notices and minutes on the web site and use the chapter's mailing list to help attract new members. The people who run the special interest groups are invited to participate in board meetings.

Every two years the Minnesota Chapter hosts a local conference. The next one is scheduled for May 2001. It attracts about 200 people, and includes timely topics and good speakers, as well as a vendor show. The chapter tries to keep costs down so as to make it accessible to independent contractors and those who work for small companies, as well as people who are employed by larger organizations.

"Our aim is to break even," Logan said. "We are not out to make money, so we keep the cost reasonable."

In the last two years the chapter also has worked with two local companies to sponsor CISSP training and testing. The locations of the eight training classes are divided between the two companies, and CISSP certified chapter members volunteer to proctor the test. The classes have attracted about 30 people each time.

Logan is excited about all activities in the chapter and is looking for ways to encourage more InfoSec professionals to get involved - the more the better.

## Letter to the Editor

To the editor:

I read the article by Robert Johnston in the January/February edition of *PASSWORD* with great interest. I have a few observations and comments to make.

First some history. The international Information Technology Security community has been working on these types of documents and guidelines for more than ten years. This work has culminated in a multi-part ISO document 13335, "Guidelines for the Management of IT Security (GMITS)." One of the important lessons the group learned early on in developing this series of documents, was that in order to make the document truly internationally useful, one had to avoid aspects related to culture and the legal regime of any particular nation. The document had to be neutral in this regard. This had the effect of limiting the level of detail and the depth of guidance that could be provided. Many times the development group attempted to add greater detail, and on each occasion had to pull back, due to problems in this area. This is largely why so much material at this level is so general in nature.

Many Nations have developed their own national level guidance documentation, including Australia, Canada, France, Germany, the UK, and the US, to name a few. Many of these documents are based on other originals, which have been suitably adjusted to reflect national cultural and legal environments and impacts.

The impact and influence of national cultural and legal aspects can be obvious and overt, but they are also very subtle and pervasive. They need to be given considerable importance if the resulting document is to be both useful and helpful to their intended audience. It is a fallacy to think that one can simply take guidance documentation of this

nature from one culture and legal jurisdiction, and use it in another without change. Conflicts and problems are inevitable.

This situation is not particularly helpful to the large multinational corporations, who in many cases are seeking a single basis for guidance documentation. Perhaps the best approach is to use the international guidance documentation GMITS as the basis, and then in each national area layer on the national level guidance documentation appropriate to the nation of concern. In this manner policies and guidance will be obtained that is both consistent and sensitive to the culture and jurisdiction addressed.

With regard to BS 7799 specifically, with which I am very familiar, this is the second time it has been entered to ISO as a candidate for standardization. On the first occasion it failed largely because of cultural and jurisdiction issues. The latest version has had much of the most obvious cultural and legal references removed, leaving the more subtle influences. Therefore the fundamental problem is not addressed only concealed. BS 7799 is an excellent document containing much useful material. However, in my opinion, this current version is less useful to the British because of this material was removed. Whether or not BS 7799 will become an international standard is hard to guess. In my opinion it should not. That is not to suggest that other countries should not adopt it as a national standard, with or without changes. Again in my opinion it would make an excellent starting point for developing or enhancing national level guidance documentation for IT Security management.

Sincerely,  
John Hopkinson

*Continued on page 12.*

# INFORMATION SECURITY AND ELECTRONIC BANKING SYSTEMS

By Jeff Stelmach • [lstel@chevron.com](mailto:lstel@chevron.com)

Poorly configured or incorrectly used electronic banking (EB) or enterprise resource planning (ERP) systems can result in catastrophic losses to a company. Configured and used properly, EB and ERP can add significant value. Problems often stem from a lack of information in the marketplace about fraudulent activity on these systems, making our jobs as information security professionals more difficult. Investigators and law enforcement may direct companies to withhold information about fraudulent electronic funds transfers (EFT), but that also means that expertise regarding payment security remains cloistered within the walls of finance oriented businesses. In business environments where decentralizing—or even outsourcing—payment initiation is occurring, this is a signal for information security professionals to learn more about payment activity. Security professionals need to understand some of the ramifications when payment instructions are not secure and systems are not operational.

Browser-based banking is the hot topic of bank service delivery discussions these days, and legacy EFT systems, once the backbone of banking activity, are coming to the end of their life expectancy. Browser based products promise to allow payment activity to be further decentralized, but will require more security professionals to be involved in providing the environment necessary to protect financial assets. We also need to keep our finger on the pulse of current discussions in the business world about open security standards for network architecture.

## ***The Truth is Out There***

A number of years ago, Jim Mooney, then the manager of Chevron Corporation's Bank Relations and Cash Management Division in the Treasury Department, told me about a speech he heard at a treasury management symposium, given by a high-ranking treasury manager from a large corporation. Opening his comments with the news that his company had been the victim of a wire transfer fraud, he said it would be taking a \$10 million loss. It turned out to be not true and a way to capture his audience's attention. According to Jim, who is now the President of Chevron Federal Credit Union, it worked well: "There was a remarkable silence in the room as [the speaker] described the supposed incident—no doubt, everyone was thinking about whether they could find themselves in a similar spot someday. I suspect in the days that followed the conference, most of the attendees returned to their organizations and gave some renewed thoughts to payment security." But in the days that followed, there were no actual examples of highly publicized fraud cases to keep those concerns heightened. Of course, there have been high profile cases of wire transfer fraud in the past. In 1994 a major New York financial center bank announced that it had participated with the FBI in a sting operation to catch someone who had been pilfering its wire transfer system designed for use by other financial institutions. While the bank was criticized for not having adequate controls to prevent this incident, it took aggressive actions to help catch the thief and recover most of the stolen funds. Afterwards the bank made significant changes to its access controls, which no longer allow static passwords to be used when logging into its real time wire payment systems.

As security professionals, we are well versed in the need for traditional methods of providing physical and logical security of confidential data. Whether data is stored on a mainframe, server or PC, access control remains a crucial element. The Y2K exercise made us all more conscious of the need to have effective contingency recovery plans for critical systems that could suffer catastrophic failure. And the recent D-o-S attacks highlighted the need to authenticate those who are accessing our networks, systems and applications.

## ***A Little History***

Among the cornerstones of a financial transaction is authenticating those involved in the transaction and confidence in the value of the payment. Looking back at the evolution of payments, the use of cash required an assurance that the person receiving payment was the rightful beneficiary of funds and the belief that currency had value. Soon drafts and checks came along to create a new environment. In order to establish and maintain strong confidence in checks, we adopted strict rules to govern the way checks would be formatted and written, as well as rules defining who would be responsible for counterfeit, altered and stolen checks. Not surprisingly, banks have had a strong hand in revisions to the Uniform Commercial Code (UCC), minimizing their exposure to check fraud losses. Even with changes to UCC, according to the National Check Fraud Center's web site (<http://www.ckfraud.org/>), annual losses are estimated at \$10 billion and growing.

After checks, electronic transfers emerged as an acceptable method for conveying funds from one party to another. Initially, manual instructions would be delivered to a financial institution providing instructions to debit an account and credit the account of a third party. At that time, the banks relied on signatures much like they did on checks. This caught on. Eventually, customers wanted, and banks offered, the ability to access EB systems directly in order to initiate transfers. The result was that use of such systems grew rapidly, but once again we had to establish confidence, as well as new rules. A new section to UCC, UCC-4A, dealing with exposures arising out of these types of transactions, was written and ratified.

Historically, institutions have authenticated electronic transaction users through user IDs and static passwords. But as that major bank learned earlier, static passwords pose a significant risk when used for payment security. New technologies, employing either tokens that produce dynamic passwords (either in combination with a static PIN or with a challenge/response mechanism) or smart cards (with chips embedded in a card to be inserted into a special reader), should alleviate some of the concerns information security professionals have about user authentication. If the user doesn't have the token, the card or PIN, there is less risk of loss from a financial payment application. We are seeing the emergence of digital certificates to provide user authentication for some of the browser-based banking applications.

*Continued on page 10.*

Regardless of whether you employ any of these new technologies, you need a policy outlining safe computing behaviors. Use written policies and guidelines to enforce effective internal controls over the disbursement of corporate funds. They should cover every aspect of an EB system: configuration, operator profiles, minimum standards for approvals, segregation of duties, password standards, periodic audit and maintenance (i.e., deleting old users). Without appropriate guidelines, payment processes can be compromised and the safeguards inherent to a system could fail.

In the past, information technologists have breached a basic security protocol by asking users for passwords in order to gain access to systems to debug problems. In EB systems, that philosophy is unacceptable. Users should be instructed never to reveal their passwords to anyone: no bank representative, no fellow employee, no company manager from the CEO down.

Other means of control can be used when these new user authentication technologies are not available. Electronic payments are basically structured in two parts: the debit party and the credit party. No matter what proprietary application is used, payment instructions can be established in advance and securely stored for future use. These previously established payment instructions (referred to as pre-defines, line codes, templates, pre-formats, or setups) can reduce exposure by preventing input errors for repetitive payments or, worse, unauthorized changes made to payment instructions. If payments are initiated in ERP systems, access to databases containing bank account information should be tightly restricted. Ensure that system configurations do not actually weaken the intended access controls. Perform audits of changes to tables containing bank account information regularly.

Here are some issues information security professionals can use to drive home the importance of information protection when dealing with payment initiation.

### **Data Integrity**

It can be difficult to recover funds transferred into the wrong bank account. Timeliness is imperative. Different rules for recovery apply, depending on the type of mechanism used to transfer the funds (i.e., Fedwire versus ACH). If the bank has already processed a file or payment, it may take much more than a telephone call to have the mistake repaired.

A Fedwire (through the Federal Reserve system) is considered settled when the funds reach the beneficiary account provided in the payment instructions. Fedwire recalls must be requested through formal banking channels, but under UCC regulations the bank of deposit cannot release those funds without the express consent of the account holder. If the account holder is not available to authorize the release of funds—or worse yet, refuses to allow the release of the funds—this process can be protracted.

An ACH, on the other hand, is not considered settled immediately. In the event of an error, the reversal of a corporate ACH can be issued anywhere from as little as 24 hours up to the maximum of midnight of the fifth business day following the transaction's value date. Most of us receive our pay through direct deposit, which operates under NACHA (National Automated Clearing House Association) rules. NACHA rules allow an ACH to be recalled by following specific guidelines. This means that your employer has the right to reverse a payment made to you in error. Reversals are not guaranteed because whether the payment was initiated as a Fedwire or ACH, the risk is that if the funds have been removed from the credit account—or forwarded to another account—recovery is improbable. In one case, cited by an ACH payment specialist, the reversal of a duplicate tax payment to a state revenue agency was denied and the payment would be applied against future tax liabilities.

### **Availability of Service**

The importance of contingency recovery becomes critical when it comes to making certain types of payments, especially when they must be made on time. Significant losses can occur if payments fail to reach another party, such as non-performance of contractual obligations or fees and penalties assessed for late payments. The IRS has been capable of receiving electronic payment of various taxes for some time. Many state revenue authorities now require that periodic tax payments be made electronically. However, any failure to deliver appropriate payments on time can result in sizeable penalties. A 10 percent penalty could easily wipe out the savings realized by not buying backup systems or utilities.

### **Authentication of Users**

Financial institutions rely on the authenticity of users initiating electronic payments. Provisions of UCC-4A and certain bank agreement language may specifically require that a customer indemnify that bank against losses resulting from the bank's (non-negligent) action when acting on the reliance of a person identified as authorized to transmit payment instructions. If an EB system has been installed at your company, the EB system becomes the authority on which the bank acts. If the bank receives instructions initiated on that system, it will act on those instructions, but suffer no losses for errors or fraud if the customer has allowed unauthorized use or poorly monitored access to the system.

### **Preparing for the Future**

It will not be long before the major banks no longer offer traditional mainframe or PC-based EB systems. The costs for maintaining the PC-based systems are enormous: site visits to install and upgrade software and support for customers on various versions of the single product are but a few. A switch to browser-based applications can ameliorate these costs. In addition, we all have browsers on our desktops and we are all connected to the Internet, Extranets or VPNs in one form or another.

Without doubt, the banks will provide appropriate security and access to browser-based products which will offer a safe means to disburse corporate funds. While the banks may recommend the use of various tools to mitigate losses, they most likely will not mandate their use. Individual companies will need to ensure that the end-to-end processes of EB or ERP systems are fully secured when implemented. And just maybe it will be time for UCC-4B to be written that will establish new rules dealing with Internet-era technology.

Information security professionals will need to work closely with treasury or finance staffs to ensure that the applications selected provide adequate controls and security. The one thing to avoid is having a high-ranking treasury manager from your company getting up to speak at a conference and announce that your company will be taking a loss of \$10 million due to fraudulent use of an electronic banking product.

---

*Jeff Stelmach is a Bank Security Analyst for Chevron Corporation, a post he has held since 1993. He has worked for Chevron for 15 years. He is responsible for ensuring that proper controls exist for paper and electronic distribution of Chevron funds. He is responsible for managing the installation and administration of PC-based banking systems globally. Mr. Stelmach coordinates security and controls over batch file delivery processes in North America and West Africa. He has cooperated with law enforcement officials investigating counterfeit check schemes.*



# ISSA CHAPTERS

## ALAMO

Contact: William Tompkins, CISSP, CRP, CBCP  
210-567-2308 • tompkins@uthscsa.edu

## ATLANTA

Contact: Jeff Phillips  
707-754-5777 • jeff.phillips@whittman-hart.com

## BALTIMORE

Contact: John Walsh  
410-244-4631 • john.p.walsh@allfirst.com

## CAPITAL OF TEXAS

Contact: Mike Hamilton, CISSP  
512-463-7178 • mike.hamilton@re.state.tx.us

## CAROLINAS

Contact: Mark Hughes  
704-379-1970 • mark\_hughes@ins.com

## CENTRAL OHIO

Contact: Mark Douglas  
614-249-0825 • douglam1@nationwide.com

## CENTRAL PLAINS

Contact: Craig Schiller  
316-946-7314 • CRAIG.SCHILLER@LEARJET.COM

## CHICAGO

Contact: Steve Hunt  
847-685-6154 • steve.hunt@issa-chicago.org

## COLORADO SPRINGS

Contact: George Proeller  
719-567-8022 • George.proeller@jntf.osd.mil

## CONNECTICUT

Contact: Peter Vogt  
203-431-4037 • peter.vogt@protegrity.com

## DELAWARE VALLEY

Contact: Brent Frampton  
610-669-0684 • Brent\_Frampton@vanguard.com

## DENVER

Contact: Jeffrey Ott  
303-454-6784 • Jeffrey.ott@ey.com

## GREATER CINCINNATI

Contact: Lynne Arrasmith  
513-763-4205 • larrasmith@provident-bank.com

## HAWAII

Contact: Frank B. Lohman  
808-948-5611 • Frank\_Lohman@hmsa.com

## INDIANAPOLIS

Contact: Mark Acton, CISSP  
317-276-6222 • maa@lilly.com

## KANSAS CITY

Contact: JoAnn Fisher  
816-459-5016 • jafisher@farmland.com

## LATIN AMERICA

Contact: Antonio Quiones  
Hitachi Data Systems • 011-525-662-8799

## LAS VEGAS

Contact: Michael McKinzie  
877-516-7401 • mmckinzie@miragersorts.com

## LOS ANGELES

Contact: Steve Haydostian  
818-368-1280 • haydoinc@aol.com

## MILWAUKEE

Contact: Mike Rasmussen  
847-291-7760 • michael@denmac.com

## MINNESOTA

Contact: Jayne Logan  
612-761-3878 • jayne.logan@dhcmail.com

## MOTOR CITY (DETROIT)

Contact: Roger Younglove  
734-269-2684 • roger\_younglove@ins.com

## NASHVILLE

Contact: Brian Tatro  
615-599-8133 • btatro@btatro.com

## NATIONAL CAPITAL AREA

Contact: Bob Giovagnoni  
703-914-5485 • rgiovagnoni@idefense.com

## NEW ENGLAND (BOSTON)

Contact: David Sawin  
401-275-7737 • david\_e\_sawin@fleet.com

## NEW JERSEY

Contact: Bruce L. Murphy, CISSP  
973-236-5440 • bruce.l.murphy@us.pwcglobal.com

## NEW MEXICO

Contact: Nellie L. Ward, CISSP  
505-844-6038 • nlward@sandia.gov

## NEW YORK METRO

Contact: James E. Duffy, CISSP  
203-338-2121 • jeduffy@peoples.com

## NORTH COAST (CLEVELAND)

Contact: Edward Niam Jr.  
216-528-0130 • csi@corpsolutionsinc.com

## NORTH TEXAS

Contact: John McGraw  
972-605-6949 • john.magraw@EDS.com

## ORANGE COUNTY

Contact: Jeff Flynn  
949-551-6398 • jeff@jflynn.com

## OTTAWA

Contact: Ronald D. Chuchryk  
613-727-1448 • rchuch@fox.nstn.ca

## PHOENIX

Contact: Cindy Donaldson  
480-813-9119 • cdonaldson@collinscg.com

## PITTSBURGH

Contact: Richard E. Archer  
412-232-1590 • reacher@kpmg.com

## PUGET SOUND (SEATTLE)

Contact: Frank Simorjay  
425-814-8104 • security@bestnet.com

## SACRAMENTO VALLEY

Contact: Bill Roberts  
916-341-2567 • bill\_roberts@calpers.ca.gov

## SAN DIEGO

Contact: Ted Swisher  
619-725-6831 • swisher\_ted@bah.com

## SAN FRANCISCO BAY

Contact: Anjali Atanacio  
415-995-3877 • anjali.atanacio@pbdir.com

## SILICON VALLEY

Contact: Steve Trolan  
408-358-7653 • steve@trolan.org

## SOUTH FLORIDA

Contact: Dale Peterson  
954-797-9445 • peterson@digitalbond.com

## SOUTH TEXAS (HOUSTON-DOWNTOWN)

Contact: Harvey Nusz  
713-655-8892 • harvey\_nasz@auditforce.com

## ST. LOUIS

Contact: Carolyn Boemler  
314-515-3474 • carolyn.boemler@edwardjones.com

## TAMPA BAY

Contact: Matthew Decker  
813-289-1001, Ext. 362 • prez@tampaissa.org

## TEXAS GULF COAST (HOUSTON-CLEAR LAKE)

Contact: Chris Zinn  
281-283-8136 • chris.zinn@csoonline.com

## TORONTO

Contact: Keith G. Parsons, CISSP  
905-683-9830 • picker@idirect.com

## VANCOUVER

Contact: Laura Stoner  
604-528-5604 • lstoner@ccits.org

For information on upcoming meeting dates for a particular chapter, please call the person listed as the contact for that chapter.

**NOTE:** Please send chapter information to:

ISSA Headquarters  
7044 S. 13th Street • Oak Creek, WI 53154  
(414) 768-8000 • FAX: (414) 768-8001  
E-MAIL: issa@issa.org

SystemExperts

P.U. 03/04 '00, pg. 11

Bob Johnston's response:

International barriers (cultural and legal issues specifically) are a primary impediment to worldwide commerce. We will continue to struggle with these issues while moving towards a world economy. It is these barriers that frequently prevent growing businesses from effectively competing in the world's markets. A common foundation for all aspects of enterprise operations provides the basis and vehicle for smoothly integrating an organization in multiple worldwide geographical locations.

Establishing an international standard for information security will provide that foundation. Having personal experience implementing BS 7799 in foreign cultures and personal knowledge of other successes based upon BS 7799 around the globe I have confidence that it provides the foundation for an ISO standard for information security.

Those who have had the good fortune (or is it misfortune?) to execute information security responsibilities beyond their own national borders are fully cognizant of the multitude of problems introduced as a result of culture, laws and practices. None-the-less, such challenges are being overcome on a daily basis. The very computer that you use is a splendid example in that while its keyboard and electrical connection, along with software (which may be simply the use of another language), are frequently unique, the remainder of the product is standardized. Thus, the manufacturers are meeting these challenges quite readily.

Why then is it such a challenge to adopt a base level set of standards for information technology management? Primarily it is because no one agrees as to the level of detail that belongs in the foundation. Obviously, structural and electrical engineers have gotten over this

hurdle, or else structures and computers would still be on the drawing boards. Information technology must meet the challenge that has already been mastered by so many others within other disciplines.

BS 7799 may be less useful in the United Kingdom as a result of its revisions to make it more acceptable beyond the U.K.'s borders, but it is far more adaptable to the international community. Let us not attack and destroy a well-designed tool for the elements that might not fit within a particular arena. Rather, let us recognize a quality-developed foundation and build upon it as necessary. Once a primary foundation for information security is adopted as an ISO standard, the process for development, implementation and evaluation of information technology relative to the level of control and security will be manifestly enhanced.

## Special Thanks to our ISSA sponsors:

### Gold Sponsors:

ISS

Tumbleweed Communications Corp.

### Silver Sponsors:

ICSA.NET

Vanguard Integrity Professionals

# ISSA®

ISSA Headquarters  
7044 S. 13th Street  
Oak Creek, WI 53154

---

FIRST CLASS  
U.S. POSTAGE  
PAID  
WAUKESHA, WI  
PERMIT NO. 125

---