Identity & Access Management

Sarbanes-Oxley IT Compliance through Intelligent Network Management

The History

The Sarbanes-Oxley Act was the thundering bowshot fired by Congress in reply to the financial debacles that culminated in 2002.

Enron filed for Chapter 11 protection in late 2001, the same year that Fortune magazine rated them the "most innovative company in America," for the sixth time in a row. The WorldCom, Global Crossing, Adelphia Communications and ImClone stock collapses followed Enron in early 2002. The legitimacy of the independent auditing process was called into question and venerable Arthur Andersen subsequently collapsed. As a direct result of the loss of public confidence in corporate financial reporting, Congress enacted the Sarbanes-Oxley Act on July 30th, 2002, approving it in record time.

The Sarbanes-Oxley Act

Much of Sarbanes-Oxley (SOX) is understandably concerned with corporate financial governance. A public company's CEO and CFO are required by signature to guarantee compliance. The penalties are severe. The burden of compliance has fallen on all public corporations, and it is an expensive burden. When the CEO signs off that the corporation is in financial and ethical good shape, it is implied that there are no known "cracks in the foundation" and no looming scandals or disasters that could cause stock price to drop precipitously.

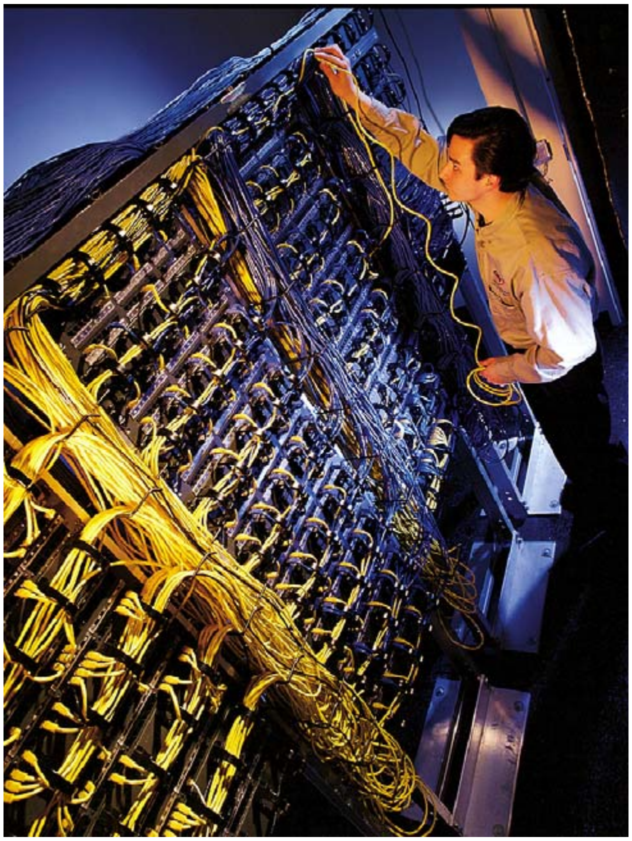


Fig. 1: iTRACS® Enabled Network Cross-connect
A new set of intelligent network management tools help address Sarbanes-Oxley challenges in a manner unique from other systems.

Compliance with Section 404

While it is clearly financial controls that are at the heart of Sarbanes-Oxley requirements, Information Technology (IT) processes and procedures are a big part of the requirements, since IT controls are a critical part of how all businesses maintain their business records, product designs, and customer accounts. It is the IT systems that "keep the books." So how safe is the system if it is poorly documented and insecure? What can be done to prevent internal hacks, impersonation, piggybacking, data manipulation or deletion, scavenging, theft of customer account data, industrial espionage, piracy or sabotage?

Network Process Frailty

Network weaknesses exist and many of them are human weaknesses. Logins and passwords can still be obtained by shoulder surfing (peeking), guesswork, memory aids on post-it notes, social engineering, and password sniffer programs. Every firewall has administration backdoors, and long forgotten or undetected trapdoors exist in every system, and on backup media. Every network can be hacked and spoofed; often undetectably. Control of switches and mainframes can be seized, and crawlspace hideouts created for the storage of large blocks of illegally obtained data, or graphics used for illicit gain. **The 2004 CSI / FBI report concludes half of all data network misuse or abuse is by company personnel, consultants and partners.**[1] The Gartner Group estimates that insiders are responsible for 70% of security incidents that cause monetary loss.[2] Is your network any less vulnerable?

"Threat 5: Lack of effective controls over the IT environment."

"..Section 404 marks the first time that companies have been legally required to evaluate and test their controls in the IT environment in such depth and detail...perhaps for the first time, are uncovering pervasive control issues that may compromise Section 404 compliance."[3]

from "Sarbanes-Oxley Section 404:
10 Threats to Compliance"
by Deloitte & Touche, 2004

Backdoors

With a five minute search on Google, it is easy to find a technical paper describing the twenty most common backdoors into various operating systems. (There are well over 100,000 internet sites dedicated to the exchange of system hacker information. Start with a search for the words "rootshell + hacking".) Backdoors exist in networks and firewalls to allow administrative access. Programmers who work or have previously worked on the system often install their own backdoors for convenience. Backdoors also allow access to hackers. Once a backdoor is identified, the intruder may enter to search for useful files, but is more likely to seek root access. The intruder can set themselves up as a system administrator, and install a sniffer program to seek out additional logins and passwords. The intruder may carve out a crawlspace, labeling it as a "bad sector," for the storage of his programs and stolen files.

With root access, the intruder can erase all evidence of their presence or visits. All of the known methods of checking for presence can be overcome. The intruder may then alter or delete information, or download it, or email it to another location. The intruder may use his crawlspace to run a criminal enterprise, such as the storage and sale of illegal files, from the victim corporation's computer. Yet, while much attention is paid to keeping intruders out, the real threat may actually be inside!

[1] Gordon, Lawrence A., et al, "2004 CSI / FBI Computer Crime and Security Survey," Computer Security Institute, 2004 and at www.GoCSI.com

[2] Gartner IT Security Summit, Presentations, Washington D.C., June 6-9, 2004 and at http://www4.gartner.com/2_events/conferences/attributes/attr_8715_93.pdf

[3] "Sarbanes-Oxley Section 404: 10 Threats to Compliance," Deloitte, 2004 and at http://www.deloitte.com/dtt/cda/doc/content/us_assur_TenThreatsSep2004.pdf

The Insider Advantage

Insider attacks have greater advantage and are typically more financially damaging to the corporation. The average cost of outsider penetration is $56,000. The average cost of an insider attack is $2.7 million.[4] Insiders understand the system, the processes, the culture and the people. They don't have to find ways through exterior firewalls. They have legitimate on-site access. They have many more opportunities for manipulation through "social engineering" to obtain the login and passwords of associates.

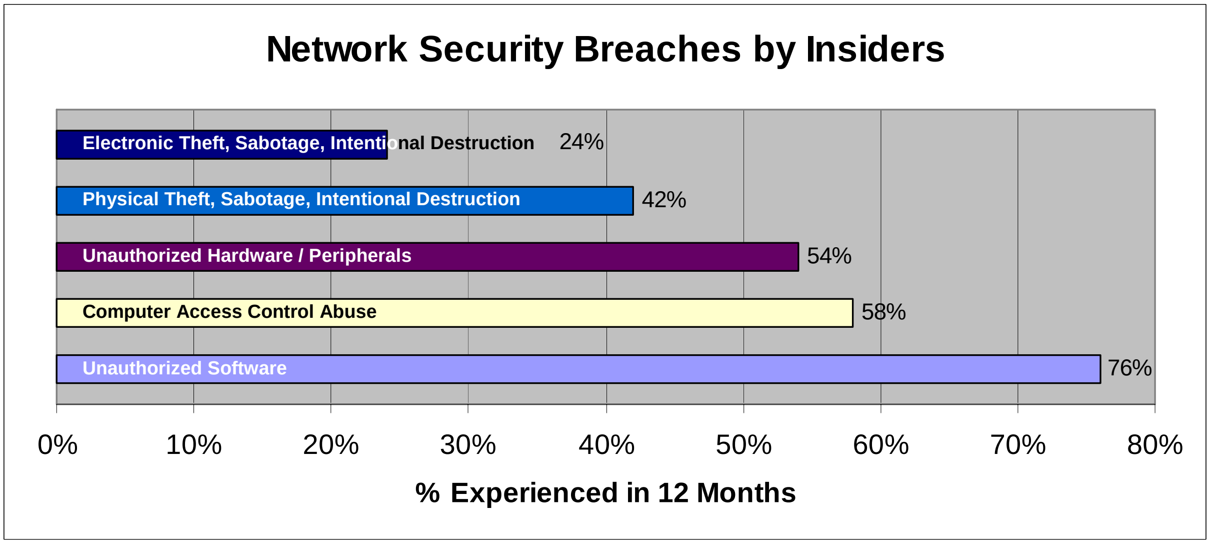


Fig. 2: Information Security Survey 2000[5]

Good Governance is More than Honest Financials

The reader will recall that Sarbanes-Oxley requires rigorous ethics, due diligence and good governance in addition to financial integrity. This also serves to preempt business failures, for reasons other than fraud, and to avoid denial of culpability or knowledge. It serves good purpose to consider all of the possible disasters that might befall an organization, rather than to overlook them and plead ignorance of any weakness in network access or it's documentation. Sarbanes-Oxley requires rigorous controls that are irrefutable, and that provide the protection of non-repudiation.

As a result of the critical nature of information technology networks, those businesses subject to federal government regulatory oversight have additional responsibilities. These industries include banking, finance, insurance, medical, pharmaceutical, telecommunications, transportation and utilities. Applicable IT information security regulations might include those of the Securities & Exchange Commission, the Nuclear Regulatory Commission, and the Food & Drug Administration. Regulation 21 CFR Part 11 is an FDA Federal Regulation regarding IT electronic records associated with the research, manufacture and distribution of pharmaceuticals. The Nuclear Regulatory Commission has numerous, rigorous IT requirements

[4] Shaw, Eric D, PhD et al, "The Insider Threat to Information Systems," Security Awareness Bulletin No. 2-98, Department of Defense Security Institute, September 1998 and at www.dss.mil/search-dir/training/csg/security/Treason/Infosys.htm

[5] Briney, Andy, "Survey 2000: Security Focused, Part 2: Security Breaches" Information Security, September 2000 and at http://infosecuritymag.techtarget.com/pdfs/2000survey.pdf

to protect the records and processes of nuclear facilities and materials. The Health Insurance Portability and Accountability Act (HIPAA) requires the preservation and protection of individual health information. The Gramm-Leach Bliley (GLB) Act requires financial institutions to preserve and protect personal financial information.

The internationally recognized Information Security Management Standard, published by the International Organization for Standardization (www.iso.ch) was first published in 2000 as ISO 17799. It specifies IT asset classification and control, labeling standards, authentication of users, device security, control of network connections, automated terminal identification, access monitoring, business continuity and disaster recovery.

****

Sidebar

Costly Insider Security Breaches

In 1996, Timothy Lloyd was a file system administrator who had worked eleven years for Omega Engineering, a government contractor to NASA and the U.S. Navy. When he learned that he would be let go in a few days, Lloyd inserted six simple lines of DOS code into the mainframe computer and borrowed the backup tapes. A few weeks after leaving the company, Lloyd's program deleted every one of company's mainframe files. The value was estimated at $10-12 million. The company has never recovered. Here, in their simplicity, are the six lines of code.

```
7/30/96
F:
F:\LOGIN\LOGIN 12345
CD\PUBLIC
FIX.EXE  /Y  F: \*.*
PURGE  F:\  /ALL
```

It took the FBI four years to determine what had been done by whom, and build a case against Lloyd. The investigation was longer than his eventual sentence.

◙

Also in 1996, an angry computer operator in Hong Kong brought down Reuters computer network, disrupting financial trading at five banks for 36 hours.

◙

In November 1996, the City of New York brought charges against 29 people, including four former employees of the Department of Finance. They had manipulated the real estate tax records to eliminate billing for any landlord who paid them a 10% commission. $13 million in taxes and $7 million in interest was lost.

◙

In July 1997, Shakuntla Devi Singla, a former employee of the U.S. Coast Guard, used a co-worker's ID to deliberately delete portions of the federal personnel database. The system crashed and the backup tapes were found faulty. One hundred and fifteen employees labored more than 1,800 hours to restore the lost data. Singla was angry that the service had not given serious consideration to her complaints of sexual harassment. Her sentence was five months.

◙

In November 1997, George Mario Parente, a temporary computer technician, broke into the Forbes, Inc. computer system causing $100,000 in damage.

◙

In July 1998, it was reported that Kodak engineer Chung-Yuh Soong had used her email account to send large, confidential data files to her sister at Xerox, a competitor. The plundering was discovered only when she sent a file so large it caused Kodak's server to crash in the days before her resignation in April 1997.

◙

In February 1999, a former computer programmer at the National Library of Medicine, Montgomery Johns Gray III illicitly obtained system administrator passwords and downloaded hundreds of sensitive medical and programming files. He was able to access the system through a backdoor he had created. Child pornography images were found on his computer. He was sentenced to five months in prison before probation.

◙

In October 1999, a former FAA engineer, Thomas Varlotta, was indicted for stealing the only copy of the computer code for the Automated Flight Data Processing System at O'Hare International Airport. Prosecutors said he had previously erased the code from a computer hard drive the day before he quit.

◙

In March 2000, Abdelkader Smires, a database engineer angry at his employer, disabled computers in a three-day cyberattack on Internet Trading Technologies.

◙

In October 2000, the blueprints for Microsoft's most important future projects are stolen.

◙

In February 2005, a security breach at data warehouse ChoicePoint disclosed 145,000 consumer records. Days later, the Bank of America reported the loss of data tapes containing the Visa charge card information of 1.2 million federal employees and members of the U.S. Senate.

◙

Also in February 2005, Hisashi Shimizu, President of Toda America, pleaded guilty to federal wire fraud charges in electronically stealing $7.3 million from his employer. He also left an email note saying "This is revenge on President Toda."

◙

"All the critical services that our society relies on for its everyday functioning are now dependent on computers. And they are interconnected with each other in ways that are so complicated and so vast that even if you just caused one system to crash, that would have cascading effects on other systems in ways that we can only begin to think about."

-Michael Vatis, Director, FBI Computer Crime Task Force[6].

****

How iTRACS® Enterprise Edition™ Solves Many Tough Problems

iTRACS has been a pioneer in infrastructure tracking and asset control systems since 1987. iTRACS products consist of a suite of advanced software applications that detect network devices and document their connectivity end-to-end. They also provide intelligent, automated solutions that instantly update the status changes of interface devices and their connectivity with hardware manufactured by vendor partners. iTRACS is an acronym for **i**ntelligent **T**racking, **R**eporting, **A**sset **C**ontrol **S**olutions.

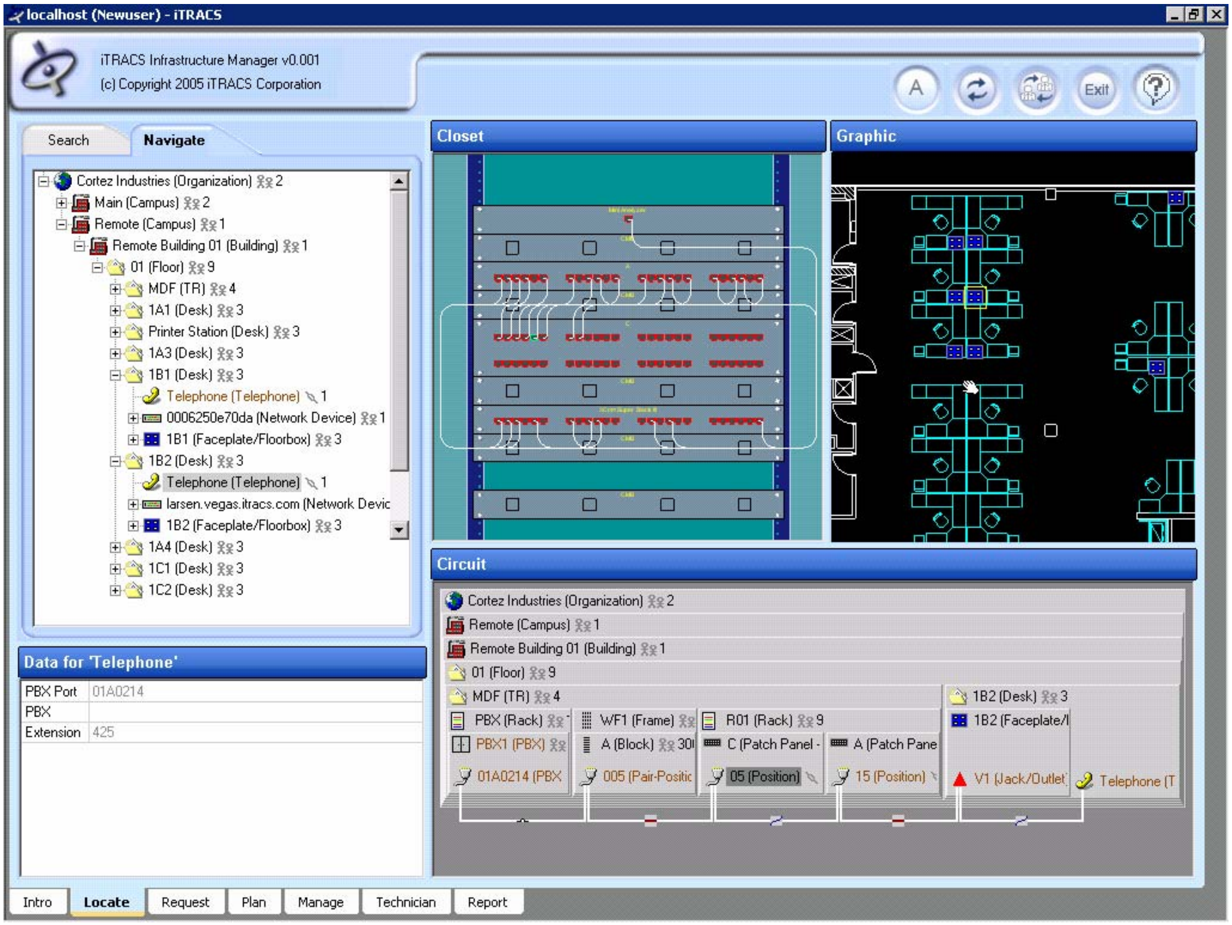
Complete control of IT infrastructure records, network documentation and auditable event logs is provided by iTRACS software, built around a SQL relational database. It maintains the record of relationships and complex data links of any kind. It was originally developed to maintain the cabling connectivity records of British Telecom's corporate clients. The records can be built from spreadsheet files, maps, CAD files, photos, scans and bitmaps. The records are used to tie the data description of the network, and of any device on the network, to maps, floor plans and location overlays. An update to one field in the record updates the relationship to all other linked data in the record. The software maintains and displays extremely complex Enterprise networks in a highly visual - and organized manner.

[6] Bendavid, Naftali, "Computers Spawn a New Criminal Breed, Chicago Tribune, September 6, 1998 and at http://lists.virus.org/isn-9809/msg00032.html

The adjacent illustration, Fig. 3, details a circuit trace and network hierarchy. Connectivity and physical location are graphically illustrated with exact port and outlet locations automatically highlighted on facility CAD drawings. The connectivity data can be organized any number of ways – by location, device type, time, hierarchy, etc.

Control over processes and unauthorized changes, as well as record updates, is provided via iTRACS-Enabled™ hardware, manufactured by partners that include ITT Network Systems, Molex Premise Networks, Ortronics, the Siemon Company and Tyco/Amp Netconnect. Each of these is a recognized leader in physical network infrastructure. The hardware includes "intelligent" cables, iTRACS-Enabled patch panels, patch cords and analyzers that scan for any changes in patch connections. The hardware works with iTRACS software to instantly identify changes within the physical layer of the network and determine if they are scheduled or unscheduled, authorized or unauthorized. The software will automatically update the record, log the event and issue alerts according to predetermined rules and escalation procedures.

Sarbanes-Oxley compliance requires precisely such methods of control over IT processes, change management, event tracking, correlation, auditable logs and reports. They apply similarly to the requirements of HIPAA, Gramm-Leach Bliley, the FDA 21 CFR Part 11 and the ISO 17799 security standard. The means by which iTRACS addresses these convergent issues are enumerated in the lead sentence of each of the following paragraphs.



localhost (Newuser) - iTRACS

iTRACS Infrastructure Manager v0.001
(c) Copyright 2005 iTRACS Corporation

Data for 'Telephone'

PBX Port	01A0214
PBX	
Extension	425

Fig. 3: Screenshot showing circuit trace, connectivity and physical location on a floor plan.

Security against connection or installation of unauthorized devices is provided by iTRACS iDiscover™. It is a software module that auto-discovers active network devices (i.e., PCs, IP phones, data and VoIP switches, servers, network printers, wireless access points). It identifies their type, host name, IP and MAC addresses via SNMP. It determines their physical location on a floor plan – or new location if they are moved. It logs events and activates alarms and can direct switches to disable switch ports or send email alerts to pagers and monitoring systems, or even contact security.

Better business governance, financial cost control and alerts regarding dangerous software on a network PC are provided by iTRACS iCollector™, a new feature of iDiscover. It automatically collects information on the software installed on devices using the network, as well as all hardware and peripherals. It checks software modules, versions and updates, can keep track of license and lease expirations, for comparisons to a list of approved software. It can be configured to send alerts when disallowed or rogue programs are detected. It can verify that machines connected to the network, laptops of visiting consultants for instance, have approved anti-virus protection or requisite security patches. Offending machines can be logically disconnected from the network before they can do any harm, such as introducing a virus or exposing the network to the outside via a backdoor.

The event log entries of each module are independent from system logs, and iTRACS operates as a separate, parallel network. This means that while hackers may manage to evade and erase system log entries, covering their tracks using standard methods, the iTRACS log entries remain secure. Filtering and comparing system and iTRACS event logs can provide clear evidence for forensic analysis.

Phone logs, documentation and accurate records are provided by iTRACS iPBX™. It uses information provided by PBX phone systems and it maintains documentation of system/extension attributes and parameters, detects extension number changes, tracks voice devices and connections, and displays voice device and jack locations on floor plans. This feature has been used to provide E911 emergency services with location information. Telephones behind a PBX, in a ten story corporate headquarters for instance, would not display precise location records other than street address. In many states and municipalities, facilities larger than 40,000 square feet are required by law to provide precise E911 location information to police and fire emergency responders. Employee advocacy groups, such as labor unions and corporate responsibility officers also endorse emergency location provisioning.

Problem	**Solution**
Electronic theft, sabotage, destruction	**iLogin**
Physical theft, sabotage, destruction	**iTRACS-Enabled**
Unauthorized hardware	**iDiscover**
Unauthorized software	**iCollector**
Unauthorized access	**iLogin**
Unauthorized Wireless access	**iDiscover**
Unauthorized connectivity modifications	**iTRACS-Enabled**

Fig. 4: Problem / Solution matrix.

iTRACS iLogin™ can be configured to reconcile the physical location of a login to a domain with the user ID. The log of events is separate from other system logs and is not accessible to manipulation. It provides an invaluable record for real-time detection, or for forensic investigation after an incident. It can also be configured to compare status from security access control devices (i.e., entry card readers) to a display of the physical location of the login. For instance, this process could send an alert if the CFO, who has not entered the building, is apparently logging in from an anomalous location – or if an employee logged into a critical/sensitive network leaves their workstation unattended.

iTRACS tools can also detect wireless access points and even disable unauthorized access points and/or connected devices. This can be used to identify, locate and disconnect "war drivers" who actively seek unauthorized entry to your network from outside your premises, via wireless access points.

Additional security to prevent tampering with critical IT devices can be provided through a product called iTRACS iTRAP™. It consists of a tiny tripwire physically linked to critical connections and equipment. Any physical movement of the protected device will be detected by iTRACS which can trigger an event such as a system alarm, alert or other event, such as snapping and logging a digital photo.

Fig. 5: A few of the security conscious financial clients using the iTRACS system.

Conclusion and Summary

iTRACS software documents complex networks for the world's largest financial institutions, manufacturers, utilities and government agencies. The software helps achieve compliance to Sarbanes-Oxley Section 404, as well as 21 CFR-Part 11, HIPAA, NRC, E911, ISO 17799, and ANSI/TIA/EIA-606-A through methods of control, event tracking, correlation, auditable logs and reports. It offers a new set of tools, unique from other systems, to address Sarbanes-Oxley compliance challenges.

The iTRACS solution is unique in providing a network software/hardware system that can be integrated with other security products and can pinpoint precise ***location-based authentication*** and ***identity & access management*** of devices, persons or related activities on the network. It will trace and illustrate network cable connectivity, locate the connection point on a floor plan of cubicles, identify the machine and the software installed, and can pull up a dictionary of the user identification, complete with ID photo. It can compare the login to physical access control records and it can direct the network switch to disconnect the user if there is an anomaly. It will detect unauthorized devices. It will send an alert and log the event for forensic evaluation. iTRACS is unique in its ability in detecting devices, tracing their physical location and correlating their identification and usage.

Information in detail, live demonstration software, technical specifications and Macromedia movies of many of these products in action can be found at www.itracs.com .

***

About the Authors

Frank Dickman, BSMAE, RCDD, is a widely experienced engineering consultant and former delegate to NEMA, TIA/EIA, ISO, CENELEC and the BICSI Codes & Standards Committees. He is a technical consultant to a number of leading data communications firms and is a recognized expert on U.S. and International physical network standards. He may be reached at frankdickman@yahoo.com

Rick McNees is currently Vice President of Business Development and Marketing for iTRACS. He previously served as the Vice President of Corporate Development for CyberSafe Corporation and Vice President of Strategic Alliances for Platinum Technologies, both highly regarded information security firms. He is the author of numerous articles, a frequent speaker on computer network management and information security and was editor/advisor of the "Practical Intrusion Detection Handbook" and others. He may be reached at RMcNees@itracs.com

About iTRACS Corporation

iTRACS Corporation is the leading provider of intelligent network connectivity management solutions. Their flagship product, iTRACS®, is the world's first automated, intelligent network asset management, tracking and control system. It is used by the world's leading financial institutions, manufacturers, utilities, telecommunication firms, and government agencies, to manage mission critical networks of data, voice, security and other premise wiring and cabling. iTRACS provides users reduced operating costs through improved productivity, greater asset utilization, increased service levels, reduced risk of operational disruptions, enhanced security, and a foundation for ensuring compliance and business continuity. With over two decades of experience, iTRACS has one of the world's largest teams dedicated to this rapidly growing market. iTRACS is headquartered in suburban Chicago. The company has sales and support staff across the U.S.A., United Kingdom and in Singapore; and distribution partners throughout the world. For more information on iTRACS Corporation, call 877-Y-iTRACS (toll free) or 708-486-0147, email sales@itracs.com or visit www.itracs.com .

Bibliography and Sources

Books - Security

Power, Richard, "Tangled Web-Tales of Digital Crime from the Shadows of Cyberspace," Que Corporation (Macmillan), 2000, ISBN 0-7897-2443-X.

Parker, Don B., "Fighting Computer Crime," Charles Scribner's Sons, 1983, ISBN-0-684-17796-X.

Icove, David, Seger, Karl and VonStorch, William, "Computer Crime-A Crimefighter's Handbook, O'Reilly & Associates, 1995, ISBN-1-56592-086-4.

De Angelis, Gina, "Cyber Crimes," Chelsea House, 2000, ISBN-0-7910-4252-9.

Newman, John Q., "Identity Theft-The Cybercrime of the Millennium," Loompanics, 1999, ISBN-1-55950-195-2.

White Papers – Sarbanes-Oxley and Federal Regulations

"Sarbanes-Oxley: What IT Managers Need to Know," Staff Report, TechRepublic, January 18, 2005 and at http://insight.zdnet.co.uk/business/legal/0.39020487,39184539,00.htm

"Sarbanes-Oxley Section 404: 10 Threats to Compliance," Deloitte, 2004 and at http://www.deloitte.com/dtt/cda/doc/content/us_assur_TenThreatsSep2004.pdf

Hurley, Edward, "Security and Sarbanes-Oxley," SearchSecurity.com, September 25, 2003 and at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html

Carlson, Tom, “Information Security Management: Understanding ISO 17799,” Lucent Technologies, September 2001, and at http://www.netbotz.com/library/ISO_17799.pdf

21 CFR Part 11 is an FDA Federal Regulation regarding Pharmaceutical IT Electronic Records www.fda.gov/cder/guidance/5505dft.pdf

The Health Insurance Portability & Accountability Act of 1996 – the HIPAA Statute, and at http://www.cms.hhs.gov/hipaa/

White Papers & Surveys - Security

“Issue of Intrusions into Government Computer Networks,” Congressional Testimony of Ronald Dick, Director National Infrastructure Protection Center, FBI, April 5, 2001 and at www.fbi.gov/congress/congress01/rondick.htm

Shaw, Eric D, PhD et al, “The Insider Threat to Information Systems,” Security Awareness Bulletin No. 2-98, Department of Defense Security Institute, September 1998 and at www.dss.mil/search-dir/training/csg/security/Treason/Infosys.htm

“Global Information Security Survey 2004,” Ernst & Young, 2004, and at http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/$file/2004_Global_Information_Security_Survey_2004.pdf

Winkler, Ira, “Anatomy of an Industrial Espionage Attack,” in “Corporate Espionage,” Prima Publishing, 1997 and at www.dss.mil/search-dir/training/csg/security/V1comput/Case1.htm

Gordon, Lawrence A., et al, “2004 CSI / FBI Computer Crime and Security Survey,” Computer Security Institute, 2004 and at www.GoCSI.com

Briney, Andy, “Survey 2000: Security Focused, Part 2: Security Breaches” Information Security, September 2000 and at http://infosecuritymag.techtarget.com/pdfs/2000survey.pdf

“Traditional and New Strategies in IT Security,” Hewlett Packard Security Team Presentation, HP Hungary, 2003 and at http://www.hp.hu/ise_ticc/english/download/hp_hun_sec_en.pdf

Schindler, Reginal, “Technology Poses New Risk for Health Care Organizations,” Information Risk Group, and at http://www.hospitalconnect.com/aha/fsi/content/schindler.pdf

Palmgren, Keith, “Controlling Internal Abuse Through the Process of Security,” February 7, 2005 and at http://www.securitydocs.com/library/2998

“History of the Hacker Threat” at www.protectedcomputer.com/hackerhistory.htm

Klaus, Christopher, “Backdoors,” August 4, 1997 at ftp.de.freesbie.org/pub/misc/www.rootshell.com/docs/backdoors.txt

Articles – Insider Attacks

McWilliams, Brian, “New York City Victimized by Computer Fraud,” PC World, November 25, 1996 and at http://www.pcworld.com/resource/article.asp?aid=6885

“Ex-Kodak Worker Charged in Theft,” Wired News, July 9, 1998 and at http://www.wired.com/news/politics/0,1283,13581,00.html

Bendavid, Naftali, “Computers Spawn a New Criminal Breed, Chicago Tribune, September 6, 1998 and at http://lists.virus.org/isn-9809/msg00032.html

Simons, John, “How an FBI Cybersleuth Busted a Hacker Ring,” The Wall Street Journal, October 1, 1999 and at http://massis.lcs.mit.edu/telecom-archives/TELECOM_Digest_Online/0418.html

“Former FAA Engineer Indicted in O’Hare Code Theft,” Associated Press, October 21, 1999 and Airport News at http://archives.californiaaviation.org/airport/msg02974.html

Gaudin, Sharon, “The Omega Files,” Network World, June 26, 2000, and at http://www.nwfusion.com/research/2000/0626feat.html

Korecki, Natasha, “Executive Steals $7 M form Schaumburg Firm, Hits Vegas,” Chicago Sun-Times, February 5, 2005 and at www.suntimes.com/output/news/cst-nws-shimizu05.html

“Bank of America Loses Customer Data,” Associated Press, March 1, 2005 and at http://www.msnbc.msn.com/id/7032779/