



Security Assessment Inc.

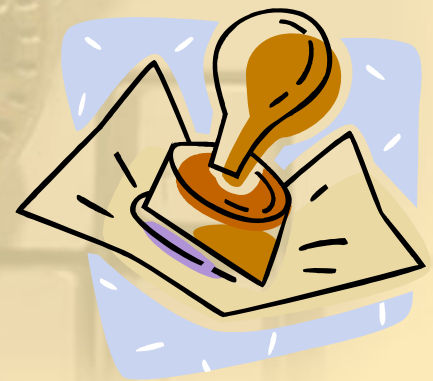
Assuring IT System Security & Compliance

Industry Standards - Regulatory Requirements – Corporate Governance

GEORGE M. ARAUJO, MCSE:Security



Understanding IT Security Risks, Compliance and Frameworks



About The Speaker

George M. Araujo, MCSE: Security

- Principal, Business Development
- Twenty-three years of technology consulting experience in a variety of industries, including Government Agencies, Legal, Medical, Financial and Travel, both locally and overseas
- Skilled in matching business processes to technology with a cost effective and results-oriented approach to business operations and strategic planning
- Implemented Y2K standards for many organizations

Presentation Agenda

- IT SECURITY - What Is It?
- Types of Threats
- In The News
- Actual Incidents
- How To Get Started
- Compliance
- Frameworks
- Impacts/Benefits
- Q & A

What We Do

- We provide independent “third party” services designed to assure IT system security compliance with industry standards, regulatory requirements and corporate governance.
- We offer end-to-end IT security solutions including initial assessment, gap analysis, corrective action planning, implementation and validation.

Our Markets

We serve small to medium sized Canadian companies that use Microsoft or Unix-based IT systems.

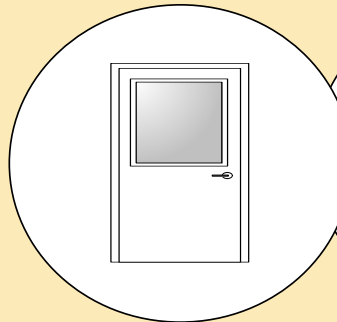
What Is IT SECURITY?

- IT Security means eliminating the disruption of business operations and reducing your exposure to cyber attacks.
- IT Security deals with several different "trust" aspects of information. Another common term is IT Security Assurance.
- IT Security is not just confined to computer systems, it applies to all aspects of protecting information or data, in whatever form. i.e. Physical, People.

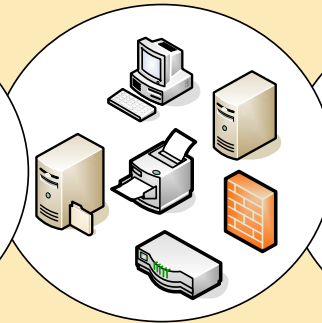
Security Framework

P N S U

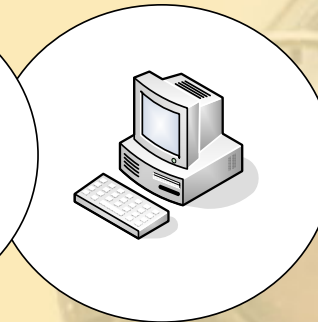
Physical



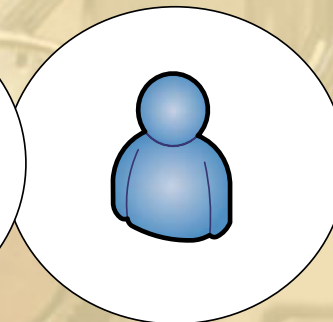
Network



System



User



Just like any chain, your network security chain is only as strong as its' weakest link.

Types of Threats

Hackers

Spam

Phishing

Adware

Viruses

Trojan

Worms

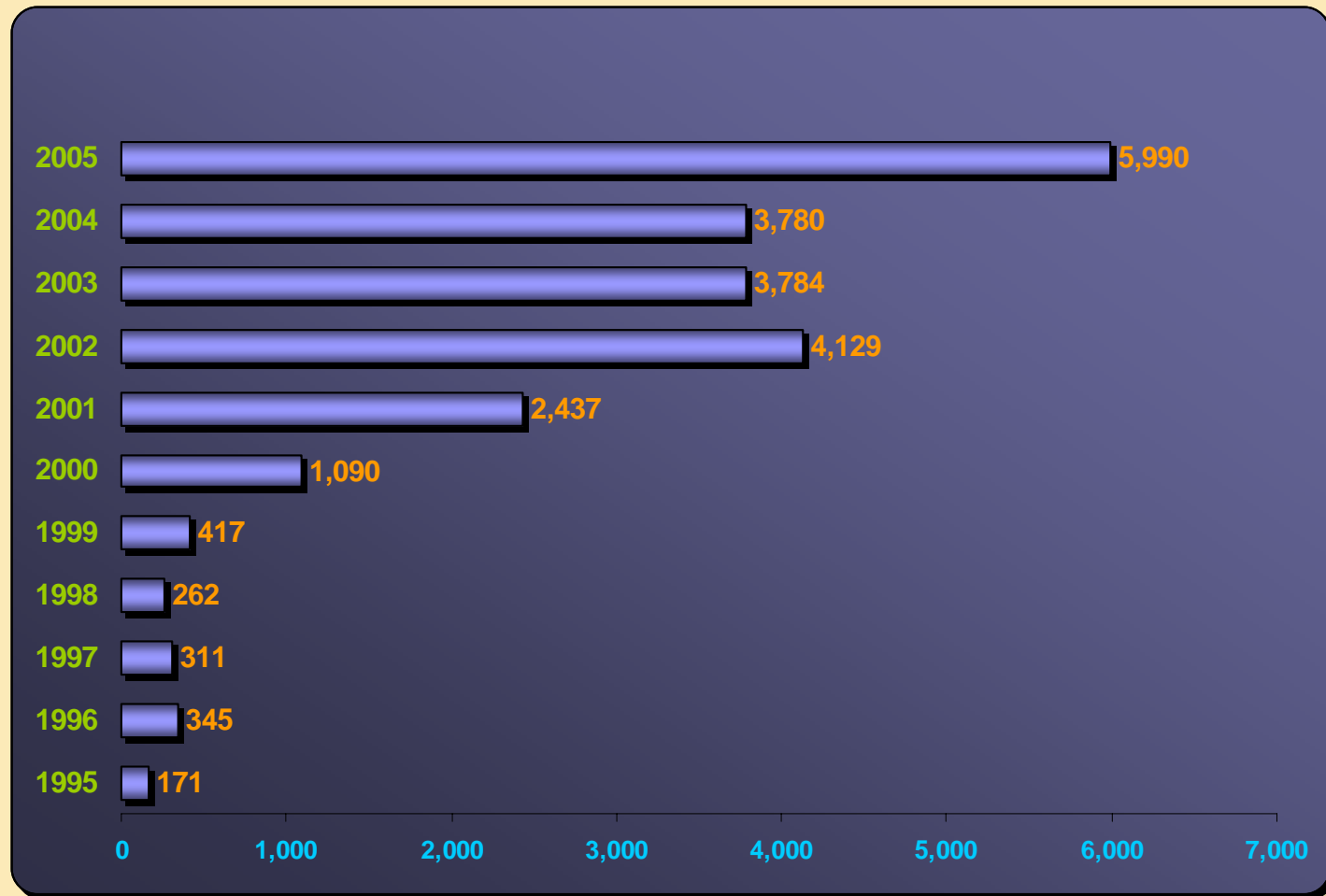
Employee



Identity Theft
Corporate Espionage
Denial-of-Service

VULNERABILITIES REPORTED 1995-2005

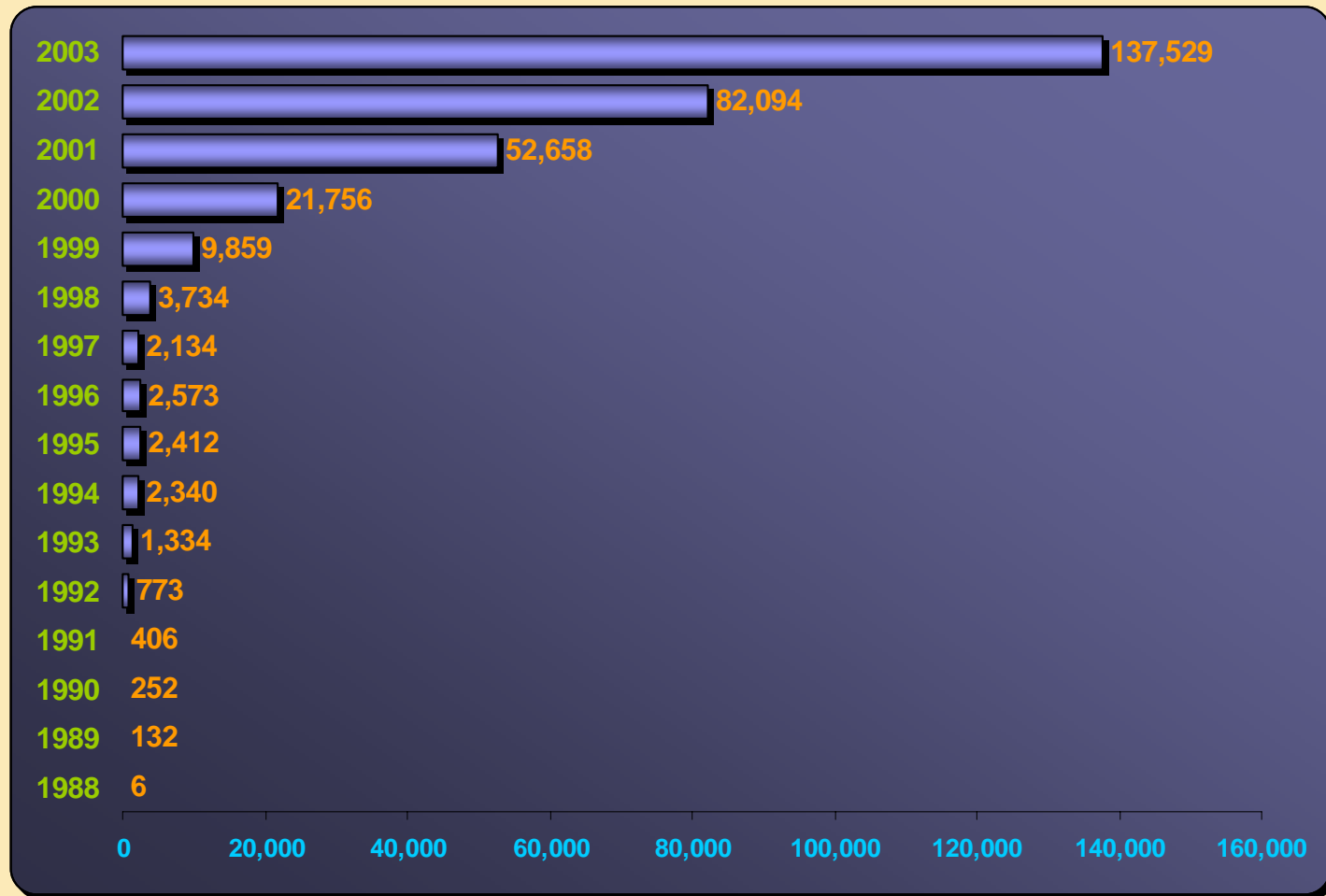
CERT® Coordination Center (CERT/CC)
Carnegie Mellon



Source: www.cert.org/stats

INCIDENTS REPORTED 1998-2003

CERT® Coordination Center (CERT/CC)
Carnegie Mellon



Source: www.cert.org/stats

Data Breaches

- From February 2005 to January 2, 2006 a total of **52,020,632** Persons information have been compromised.
- The data breaches have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security, Account and Driver's License Numbers.

Source Privacy Rights Clearinghouse/UCAN
www.privacyrights.org

Data Breaches Reported Since Feb. 2005

Source Privacy Rights Clearinghouse/UCAN

www.privacyrights.org

Feb. 15, 2005	ChoicePoint	Bogus accounts established by ID thieves	145,000
Feb. 25, 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures	Hacking	100,000
March 10, 2005	LexisNexis	Passwords compromised	32,000
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop	98,400
March 28, 2005	Univ. of Chicago Hospital	Dishonest insider	unknown
April ?, 2005	Georgia DMV	Dishonest insider	465,000

Data Breaches Reported Since Feb. 2005

Source Privacy Rights Clearinghouse/UCAN

www.privacyrights.org

April 12, 2005	LexisNexis	Passwords compromised	Additional 280,000
April 18, 2005	DSW/Retail Ventures	Hacking	Additional 1,300,000
April 20, 2005	Ameritrade	Lost backup tape	200,000
April 21, 2005	Carnegie Mellon Univ.	Hacking	19,000
May 16, 2005	Westborough Bank	Dishonest insider	750
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000

Data Breaches Reported Since Feb. 2005

Source Privacy Rights Clearinghouse/UCAN

www.privacyrights.org

June 16, 2005	CardSystems	Hacking	40,000,000
July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens" exposed
Aug. 22, 2005	Air Force	Hacking	33,300
Sept. 16, 2005	ChoicePoint (2nd notice, see 2/15/05 for 145,000)	ID thieves accessed; also misuse of IDs & passwords	9,903
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800



Data Breaches Reported Since Feb. 2005

Source Privacy Rights Clearinghouse/UCAN

www.privacyrights.org

Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 8, 2005	ChoicePoint	Bogus accounts established by ID thieves	17,000 more
		Total affected now reaches 162,000	
		(See Feb. 15 & Sept. 16)	
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Georgia Tech Ofc. of Enrollment Services	Stolen computer Theft 10/16/05	13,000
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank account info.	161,000



Data Breaches Reported Since Feb. 2005

Source Privacy Rights Clearinghouse/UCAN

www.privacyrights.org

Dec. 16, 2005	Colorado Tech. Univ.	Email erroneously sent containing names, phone, numbers, email addresses, Social Security numbers And class schedules.	1,200
Dec. 22, 2005	Ford Motor Co	Stolen computer. Names and SSNs of current and former employees.	70,000
Dec. 25, 2005	Iowa State Univ.	Hacking. Credit card information and Social Security numbers.	5,500
Jan. 1 2006	University of Pittsburgh Medical Center, Squirrel Hill Family Medicine	6 Stolen computers. Names, Social Security numbers, birthdates	700
Jan. 2 2006	H&R Block	SSNs exposed in 40-digit number string on mailing label	Unknown



Sturke Warns of "Theft"

Tokyo Exchange Executives Take Pay Cuts After Crash

ComputerWeekly – Nov. 18, 2005
The president of the Tokyo Stock Exchange will have his pay cut by 50% for the next six months.

<http://www.computerweekly.com/Articles/Article.aspx?liArticleID=212972&liFla>

FBI Agents Bust
CNN – Nov. 4, 2005
A 20 year old man and
other hackers. The
thought to have made
the **Weapons Division**
California and a

www.cnn.com/2005/TECH/internet

A bot is a program that installs on a computer without the users knowledge and allows a hacker to take control of the infected computer.

[ch.aspx?](#)

[&srch=Hackers+use+bird+flu+emails+to+hijack+computers](#)

IN THE NEWS

BBC NEWS | UK | UK police foil massive bank theft - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://news.bbc.co.uk/1/hi/uk/4356661.stm

bbc.co.uk Home TV Radio Talk Where I Live A-Z Index Search

BBC NEWS WATCH BBC NEWS IN VIDEO

UK version International version About the versions Low graphics Help Contact us

News Front Page World UK England Northern Ireland Scotland Wales Business Politics Health Education Science/Nature Technology Entertainment

Have Your Say Magazine In Pictures Week at a Glance Country Profiles In Depth Programmes

BBC SPORT BBC WEATHER cbbc news BBC ON THIS DAY NEWSWATCH LANGUAGES

Last Updated: Thursday, 17 March, 2005, 13:39 GMT

E-mail this to a friend Printable version

UK police foil massive bank theft

Police in London say they have foiled one of the biggest attempted bank thefts in Britain.



The plan was to steal £220m (\$423m) from the London offices of the Japanese bank Sumitomo Mitsui.

Computer experts are believed to have tried to transfer the money electronically after hacking into the bank's systems.

A man has been arrested by police in Israel after the plot was uncovered by the National Hi-Tech Crime Unit.

Unit members worked closely with Israeli police.

The investigation was started last October after it was discovered that computer hackers had gained access to Sumitomo Mitsui bank's computer system in London.

They managed to infiltrate the system with keylogging software that would have enabled them to track every button

Yeron Bolondi was arrested for money laundering and deception

BBC NEWS:VIDEO AND AUDIO
How the hackers got into the system
VIDEO

SEE ALSO:

- Latest coup for hi-tech crime unit 17 Mar 05 | Technology
- Hi-tech criminals target UK firms 24 Feb 04 | Technology

RELATED INTERNET LINKS:

- National Hi-tech Crime Unit

The BBC is not responsible for the content of external internet sites

TOP UK STORIES NOW

- Ashdown gives Sir Menzies backing
- Tories plan to keep student fees
- Car thief jailed over farmer death
- Twins killed step grandmother

RSS | What is RSS?

IN THE NEWS

EBay tricked by phony e-mail - Computerworld - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail News RSS

Address <http://www.computerworld.com/securitytopics/security/story/0,10801,106798,00.html?source=NLTVWR&nid=106798>

IDG Network: Login Register

  **THE LONG HAUL.** The HP Compaq nx6110 Notebook PC with Intel® Centrino™ Mobile Technology. SMART ADVICE. SMART TECHNOLOGY. SMART SERVICES.

COMPUTERWORLD An IDG company

QuickLink Search Computerworld Advanced Search

Home News Topics **Subscribe** Events White Papers Briefings Webcasts Blogs XML Feeds

Management Careers Security Hardware Software Data Mgmt Networking Government Mobile Development Industry

 **Predictions for 2006** What does the new year hold for IT? Read our Forecast '06 special report.

Home > Browse Topics > Security

EBay tricked by phony e-mail

A phishing attack convinced eBay's own fraud team to endorse it as legitimate, a security consultant says

News Story by Robert McMillan

DECEMBER 05, 2005 (IDG NEWS SERVICE) - A sophisticated phishing attack has proved to be so successful, it has tricked eBay Inc.'s own fraud investigations team into endorsing it as legitimate, according to an independent security consultant who reported the attack to eBay.

In late November, Richi Jennings received a fraudulent e-mail message containing the subject line "Christmas is Coming on ebay.co.uk." Offering him "great tips for successful Christmas selling," the message directed him

Print-friendly E-mail this Feedback Reprints

Related to this topic

- > IT Blogwatch
- > Computerworld blogger: Richi Jennings
- > Unisys snags new \$750M, three-year TSA contract
- > Q&A: Microsoft exec explains the early VMF patch release
- > Three more states add laws on data breaches



IN THE NEWS

Database Breach at Computer Forensics Company Shocks Security Community - Yahoo! News - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail Stop

Address http://news.yahoo.com/s/zd/20051222/tc_zd/168000

Yahoo! My Yahoo! Mail Make Yahoo! your home page

Search the Web Search

YAHOO! NEWS

News Home - Help

News Home U.S. Business World Entertainment Sports Tech Politics Science Health Most Popular Index

Internet Personal Tech. Communications Software Apple/Macintosh Linux/Open Source Tech Tuesday Blogs

Search: All News & Blogs Search Advanced

Database Breach at Computer Forensics Company Shocks Security Community



Lisa Vaas - eWEEK

Thu Dec 22, 3:51 PM ET

Security and law enforcement professionals are appalled that their personal information has been leaked by Guidance Software Inc., a security software and training company they say should have known better than to leave an unencrypted database exposed on the Internet.

ADVERTISEMENT

"I was shocked that a company like Guidance would be this sloppy," said Peter Garza, CEO of EvidentData, a computer forensics and network security firm that counts itself among Guidance's customer base.

"My first response was that I was shocked they would have an unencrypted database that was accessible via the Internet," Garza said. "I would think any vendor that has a system connected to the Internet would be more responsible, but as a security company, [I'd think] they'd be even more



- No One-Stop Shopping to Stop Database Pilferages
- Data Seizure Powers Survive in Patriot Act
- Microsoft Corrects Patch Day Glitch with SUS Update
- Oracle Dons 'Secure Development Lifecycle' in Fortify Deal

PC Magazine

RELATED QUOTES

^IXIC	2305.62	0.00
^IXK	1052.34	0.00
^DJUSS	458.18	+4.99

IN THE NEWS

Analysts Fret as Adware Makers Leverage WMF Flaw - Yahoo! News - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Mail Print

Google Urges Security Fix for CDs Search

Address http://news.yahoo.com/s/zd/20051229/tc_zd/168243

Yahoo! My Yahoo! Mail Make Yahoo! your home page Search the Web Search


YAHOO! NEWS

News Home U.S. Business World Entertainment Sports Tech Politics Science Health Most Popular Index

Internet Personal Tech. Communications Software Apple/Macintosh Linux/Open Source Tech Tuesday Blogs


Search: All News & Blogs Search Advanced

Analysts Fret as Adware Makers Leverage WMF Flaw



David Morgenstern - eWEEK
Thu Dec 29, 2:41 PM ET

Exploits of the WMF (Windows Metafile Format) flaw continued on Thursday as advertising networks took advantage of the vulnerability to spread their "products."




- Another WMF (Windows Major Foul-Up)
- Workaround, Protections Emerge for WMF Exploit
- Critical Impact: Windows Metafile Flaw a 'Zero-Day Exploit'
- Windows Vista: Beware of Metadata Slips

PC Magazine

Several security lists and Weblogs warned that the Exfol adware network was presenting coded WMF images on rotating banner ads.

Researchers said that sites running pop-up advertisements from the network will infect viewers with vulnerable systems.

ADVERTISEMENT



RELATED QUOTES

^XIC	2305.62	+28.75
^XXK	1052.34	+15.81
^DJUSS	458.18	+4.99

Get Quotes

"You don't have to go to a crack site or a porn site," observed a posting on the blog of firewall vendor Sunbelt Software USA, of Clearwater, Fla.

"You go to any site that is using



RIPE Whois Search

you are here: [home](#) -> [Whois Database](#) -> [Whois Search](#)

Whois Database:

```

person: Bold Cornel
address: Aleea Razboieni, Nr. 20 bis.
address: Pitesti, Arges
phone: +40-248646811
fax-no: +40-248646811
e-mail: biff@xnet.ro
nic-hdl: BC469-RIPE
mnt-by: AS8708-MNT

```

Sign In - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail Stop

Address http://81.196.121.135/pages.ebay.com/dl-remove-unpaid-strike&co_partnerId=2&Userid=6&sitek=0&pageType=5pa1=61=6&showgt=6&usingSSL=tru=&sp=5pa2=5 Go Links

10:18 AM **av-confirm@...** Unknown contact

Sign In

[Help](#)

New to eBay? or **Already an eBay user?**

If you want to sign in, you'll need to register first.

Registration is fast and free

[Register >](#)

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot your User ID?](#)

Password

[Forgot your password?](#)

[Sign In Securely >](#)

[Keep me signed in](#) on this computer unless I sign out.

Account protection tips
Be sure the Web site address you see above starts with <https://signin.ebay.com/>

Microsoft Passport users [click here](#).

[About eBay](#) | [Announcements](#) | [Security Center](#) | [Policies](#) | [Site Map](#) | [Help](#)

Copyright © 1995-2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

Internet

```

remarks: +-----+
source: RIPE # Filtered

```

Junk E-mail - Microsoft Outlook

File Edit View Go Tools Actions Help Adobe PDF

New

Open Norton AntiSpam

washingtonpost.com

NEWS | OPINIONS | SPORTS | ARTS & LIVING | Discussions | Photos & Video | City Guide | CLASSIFIEDS | JOBS | CARS | REAL ESTATE

Mail

Favorite Folders

- Inbox
- Unread Mail
- For Follow Up
- Sent Items

All Mail Folders

Personal Folders

- Deleted Items (93)
- Drafts (3)
- Inbox
- Junk E-mail (1)
- Norton AntiSpam Folder
- Outbox
- Sent Items
- Search Folders

Received

Mon 21/11/2005

8:58 PM

FBI Warns of E-Mail About Surveillance

The Associated Press
Monday, November 21, 2005; 4:37 PM

WASHINGTON -- The Federal Bureau of Investigation issued an alert Monday about a scam involving unsolicited e-mails, purportedly sent by the FBI, that tell computer users that their Internet surfing is being monitored by the agency.


The users are told they have visited illegal Web sites and are instructed to open an attachment to answer questions.

The FBI did not send these e-mails and does not send any other unsolicited e-mails to the public, an agency statement said. As many harmful computer viruses are located in e-mail attachments, the FBI said it strongly encourages computer users not to open attachments from unknown recipients.

The FBI is investigating the scam. Recipients of these e-mails are asked to report them by visiting the Internet Crime Complaint Center at <http://www.ic3.gov>.

*** Washington, DC 20535
*** phone: (202) 324-3000

Advertisement



Explore the world of BP's investments in new energy.

Roll over the map to begin.

NetInfo - Whois

File Tools Help

Local Info Connections Ping Trace Lookup Finger Whois Daytime Time Quote HTML Scanner Services E-mail Web Center

Query: online-login-75937.com Start

Response: Trying whois for online-login-75937.com...
Connection established.

GeekTools Whois Proxy v5.0.4 Ready.
Checking access for 205.207.121.232... ok.

Checking server [whois.crsnic.net]

Checking server [whois.easyspace.com]

Results:

Registrant:
mark don
263 Tamarack Court
Blairsden, Ca BLAI RSDEN
US

Domain name: ONLINE-LOGIN-75937.COM

Administrative Contact:
don, mark john_don29@yahoo.com
263 Tamarack Court
Blairsden, Ca BLAI RSDEN
US
+44.8707550009 Fax: +44.1419316401

Technical Contact:
Master, Host hostmaster@easyspace.com
Lister Pavilion
Kelvin Campus
West of Scotland Science Park
Glasgow, Scotland G20 0SP
GB
+44.08707555066 Fax: +44.1419316785

Record last updated on 21-Nov-2005.
Record expires on 21-Nov-2006.
Record created on 21-Nov-2005.

Domain servers in listed order:
NS4.EASYSAPCE.COM 84.22.161.11
NS5.EASYSAPCE.COM 62.128.193.201

How To Get Started

- Have a Security Policy
- Start by checking your physical environment
- Make sure that your systems have all the updates, patches, and hot fixes installed (hardware and software)
- Make sure that your Firewalls and other devices are configured correctly
- Make sure your wireless connections are secure

How To Get Started

- Passwords
 - Do not share your passwords
 - Use complex passwords
 - Change passwords frequently
- Check your logs frequently
- Do not open attachments from unknown sources
- Do not click on links in e-mails or instant messaging (IM) that you are not sure of
- Turn off Outlook message preview
- Educate staff on your Security Policy

How To Get Started

- Web Sites - Are they hosted Internally or Outsourced?
 - If outsourced, do their security practices follow industry standards and does their security policy meet up with your security policy
- Assess your security every 3 months

Compliance Landscape

SOX

Bill 198

21 CFR part 11

PIPEDA

PHIPA

HIPAA



GCP

GMP

GLB

FISMA

BASEL II

SOX & Bill 198

- The sagas of Enron and Tyco International have forced governments and regulators to more closely look at the financial reporting processes of companies in order to enforce corporate governance standards.
- **Sarbanes Oxley Act (SOX) & Bill 198** - An Act to implement Budget measures and other initiatives of the Government
- The law is named after sponsors Senator Paul Sarbanes (D-MD) and Representative Michael G. Oxley (R-OH)
- Business Challenges
 - Both deal with internal controls on financial reporting and hold CEO/CFO liable for financial reporting.

SOX

- Securities regulators in the US and Canada are introducing new rules and regulations to improve investor confidence and stabilize capital markets.
- Transparency, Disclosure and Internal Controls have become top of mind for many organizations.
- The SOX Legislation is a move towards enforcing governance standards and holding CEO/CFO liable for financial reporting.
- Section 103, 104 & 105
 - Audit, procedure and documents must be kept for seven years.
- Section 302
 - CEO, CFO must certify financial report and any changes with accompanying audit process.

SOX

- **Section 404, 409**

- Reports must show controls

- Management is required to include in its annual report a report on the company's internal control over financial reporting. This report should contain:

- A statement of Management's responsibility for establishing and maintaining adequate internal control over financial reporting
 - A statement identifying the framework used by management to evaluate the effectiveness of internal control
 - Management's assessment of the effectiveness of internal control as of the end of the company's most recent fiscal year

- Company's auditors are also required to attest and report on, management's assessment of the effectiveness of the company's internal control over financial reporting.

BILL 198

An Act to implement Budget measures and other initiatives of the Government - Keeping the Promise for a Strong Economy Act (Budget Measures), 2002

PART XXVI - SECURITIES ACT

- The Ontario Government Introduced Bill 198 in October 2002, in response to the reforms taking place in the United States and in order to help restore investor confidence in Ontario's capital market.
- Bill 198 empowers the Ontario Securities Commission to develop similar guidelines to Sarbanes-Oxley.

www.ontla.on.ca/documents/Bills/37_Parliament/Session3/b198ra.pdf

BILL 198

Bill 198 allows Ontario Securities Commission (OSC) to:

- Review information that public companies provide to investors
- Ensure that audit committees play an appropriate role in preparing statements
- Require CEOs and CFOs to certify and evaluate appropriate disclosure controls and procedures.
- Require CEOs and CFOs to certify the accuracy of end-of-year and quarterly financial statements
- Hold CEOs & CFOs accountable for the financial accuracy of those statements

BILL 198

Oct. 30, 2003

The Ernie Eves (C) government announced legislation that, if approved, would make Ontario's system the toughest in Canada.

- The measures include:
 - Penalties to ensure compliance with Ontario's securities laws. Maximum court fines for general offences would increase to \$5 million from \$1 million and maximum prison terms would increase to five years less a day from two years
 - New powers that would give the OSC the authority to impose administrative fines of up to \$1 million for securities law violations and order that offenders give up the profits they have gained from those violations
- Article on the announcement in the Certified General Accountants of Ontario

www.cga-ontario.org/contentfiles/media_relations/releases/archives/02-03/02-2003-49.aspx

<http://www.securityassessment.net>

BILL 198

- In February 2005, the Canadian Securities Administrators (CSA) proposed and released for comment new rules, Multilateral Instrument 52-111 alone with revisions to Multilateral Instrument 52-109
- MI 52-111 - Reporting on Internal Control over Financial Reporting
www.osc.gov.on.ca/Regulation/Rulemaking/Current/Part5/rule_20050204_52-111_ricfr.jsp#N_6_21a
- MI 52-109 - Certification of Disclosure in Issuers' Annual and Interim Filings.
www.osc.gov.on.ca/Regulation/Rulemaking/Current/Part5/rule_20040326_52-109-cert.jsp

BILL 198

- The proposed MI 52-111 and MI 52-109 closely matches the requirements of Sarbanes-Oxley (SOX) Sections 404 and 302.
 - Including: auditor independence; director and audit committee responsibilities and their independence from management.
- CEO and CFO accountability for financial reporting and internal controls; better and faster disclosure to the public; and enhanced penalties for illegal activities.
- The new rules require management to evaluate and test the system of internal control over financial reporting
- Also require company's auditor attestation

BILL 198

- Canadian regulators have created a phased and delayed implementation that gives companies more time to implement the required changes and provide certification.
- Depending on the market capitalization of the organization the new rules will become effective between 2006 and 2009
- Market Capitalization (as at June 30/05) Effective years ending on or after
 - o > \$500 million June 30, 2006
 - o < \$500 million but > \$250 million June 30, 2007
 - o < \$250 million but > \$75 million June 30, 2008
 - o < \$75 million June 30, 2009

BILL 198

October 2003 Ontario Securities Commission (OSC) Case

**“Bill 198 is in force and the OSC’s new rules are under review.
All of this is promising, but it’s only as powerful as we make it.”**

- YBM Magnex - in which a company created by people allegedly connected with the Russian mafia raised millions on the TSE and then disappeared.
- One director had to pay \$250,000 and was barred from serving as an officer or director for five years.
- Two other directors had to pay \$75,000 in costs and were barred for three years

Source: Certified Management Accounts (CMA) Management Magazine

www.managementmag.com/index.cfm/ci_id/1427/la_id/1

PIPEDA

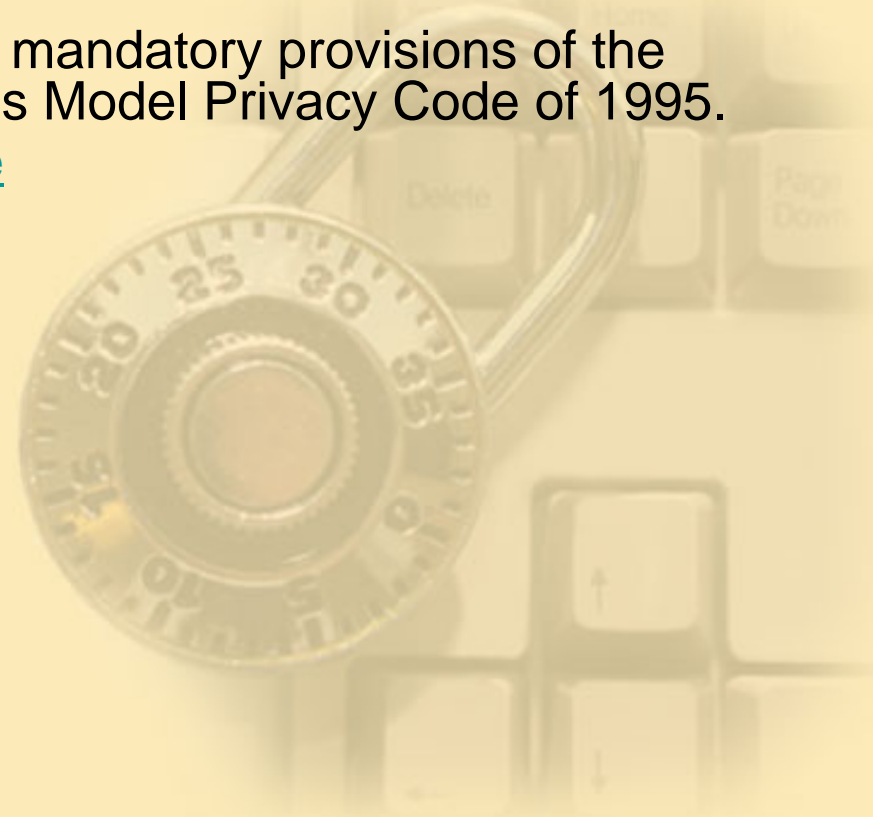
Personal Information Protection and Electronic Documents Act (PIPEDA)

- Canada's federal act governing the collection, use and disclosure of personal information in the course of commercial transactions.
- PIPEDA defines personal information as "information about an identifiable individual". For example:
 - Name, Address, Telephone Number, Gender, Identification numbers, income or blood type, credit records, loan records.
- As of January 1, 2004, all Canadian businesses are required to comply with the privacy principles set out by PIPEDA. The Act covers both traditional, paper-based and on-line businesses.

www.privcom.gc.ca/legislation/02_06_01_01_e.asp

PIPEDA

- The act was created in response to European Union data protection directives that limit trade with nations not providing privacy protection equivalent to the EU directives.
- PIPEDA incorporates and makes mandatory provisions of the Canadian Standards Association's Model Privacy Code of 1995.
www.csa.ca/standards/privacy/code



PHIPA / HIPAA

Personal Health Information Protection Act, 2004 (PHIPA)

- Establishes rules for the collection, use and disclosure of personal health information about individuals, protects the confidentiality of that information and the privacy of individuals.

www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- An act to ensure that customers are able to switch between health insurance providers as smoothly as possible without the unavailability, total loss or loss of integrity within their health data.
- Also address the security and privacy of health data

www.hhs.gov/ocr/hipaa

21 CFR Part 11

21 CFR (Code of Federal Regulations) Part 11 Electronic Records; Electronic Signatures

21 CFR Part 11, the FDA guidelines for trustworthy electronic records

- Requires companies to have in place procedures and controls designed to ensure the authenticity, integrity and, when appropriate, the confidentiality of electronic records.
- To comply, organizations must have documentation on the way their systems have been installed and configured to prove that the IQ (Installation Qualification), OQ (Operations Qualification) and PQ (Performance Qualification) processes were completed.

www.21cfrpart11.com

www.fda.gov/ora/compliance_ref/part11

Frameworks Best Practices Standards



- COSO
- COBIT®

Where Should we be?

- ITIL®
- ISO 17799

How do we get there?

COSO / COBIT

- COSO and COBIT are two control frameworks that have been widely adopted by companies subject to Sarbanes-Oxley Act
- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
- A U.S. private-sector initiative, formed in 1985 and produced the report titled

“Internal Control – An Integrated Framework”
that was released in 1992, commonly known
as the COSO Report

www.coso.org

COSO

- Primary Audience, Management
- COSO is sponsored by five main professional accounting associations and institutes;
 - American Institute of Certified Public Accountants (AICPA)
 - American Accounting Association (AAA)
 - Financial Executives International (FEI)
 - The Institute of Internal Auditors (IIA)
 - The Institute of Management Accountants (IMA)
- COSO focuses on controls for financial processes, and COBIT focuses on IT controls.
- Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence.

COSO

COSO definition of internal control

“Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories”

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

COSO

COSO Internal control consists of five interrelated components

- **Control Environment**

- Control environment factors include the integrity, ethical values, management's operating style, etc.
- It is the foundation for all other components of internal control, providing discipline and structure.

- **Risk Assessment**

- Every business faces a variety of risks from internal and external sources that must be assessed.
- Risk assessment is a prerequisite for determining how the risks should be managed.

- **Control Activities**

- Control activities are the policies and procedures that help ensure management directions are carried out.
- They include activities such as approvals, authorizations, verifications, reconciliations, etc.

COSO

- **Information and Communication**

- Important information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities.
- Effective communication must ensure information flows down, across and up the organization.
- Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.

- **Monitoring**

- Internal control systems need to be monitored--a process that assesses the quality of the system's performance over time.
- Internal control deficiencies detected should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.

COBIT

- COBIT IT controls looks at all the information, not just the financial information,
- Primary Audience, Management, users, information system auditors
- An open standard published by the IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA). It's an IT control framework built in part upon the COSO framework.
- The first edition was published in 1996; the second edition in 1998; the third edition in 2000; the on-line edition in 2003 and the fourth edition in 2005.

COBIT

- COBIT is based on established frameworks, such as the, Carnegie Mellon, Software Engineering Institute's Capability Maturity Model Integration (CMMI), ISO 9000, ITIL and ISO 17799.
- Because COBIT is a control and management framework it does not include process steps and tasks. It focuses on what an organization **needs to do**, not how it needs to do it.
- It provides managers, auditors, and IT users with a set of generally accepted IT control objectives. In its 3rd edition, COBIT has 34 high level objectives that cover 318 control objectives categorized in four domains:
 - Planning and Organization
 - Acquisition and Implementation
 - Delivery and Support
 - Monitoring

COBIT 34 HIGH LEVEL CONTROL OBJECTIVES

Planning and Organization

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Organization and

Relationships

- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage Human Resources
- PO8 Ensure Compliance with External

Requirements

- PO9 Assess Risks
- PO10 Manage Projects
- PO11 Manage Quality

Acquisition and Implementation

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology

Infrastructure

- AI4 Develop and Maintain Procedures
- AI5 Install and Accredite Systems
- AI6 Manage Changes

COBIT 34 HIGH LEVEL CONTROL OBJECTIVES

Delivery and Support

- DS1 Define and Manage Service Levels
- DS2 Manage Third-Party Services
- DS3 Manage Performance and Capacity
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS6 Identify and Allocate Costs
- DS7 Educate and Train Users
- DS8 Assist and Advise Customers
- DS9 Manage the Configuration
- DS10 Manage Problems and Incidents
- DS11 Manage Data
- DS12 Manage Facilities
- DS13 Manage Operations

Monitoring

- M1 Monitor the Processes
- M2 Assess Internal Control Adequacy
- M3 Obtain Independent Assurance
- M4 Provide for Independent Audit

COBIT

- A great benefit of the COBIT best practices is that they are a common approach to good IT control.
- They are implemented by business and IT managers, and assessed on the same basis by auditors.

New COBIT 4.0

- A detailed mapping between COBIT, ITIL, and ISO/IEC 17799
- COBIT 4.0 still has 34 high-level control objectives but they are not the same as the 34 in the 3rd edition. ie The M domain has now become ME, standing for Monitor and Evaluate.
- For more details and to review the changes visit the ISACA web site and read the COBIT 4.0 Frequently Asked Questions section.

ITIL

ITIL stands for the **IT Infrastructure Library**, published by the Office of Government Commerce in Great Britain.

Primary Audience

- IT service providers
 - IT directors and managers
 - CIOs
- The best practices are drawn internationally from the public and private sectors and focus on IT services. IT is often used to complement the COBIT framework.
 - Designed to assist organizations to develop a framework for IT Service Management. It focuses on the people, processes and technology issues that IT organizations face.
 - ITIL covers areas such as Change Management, Configuration Management, Software Control & Distribution and Help Desk

ITIL

- The service management processes are intended to strengthen, but not dictate, the business processes of an organization.
- Unlike the COBIT control objective framework, ITIL defines best practice processes for IT service management and support.
- It focuses on the method and defines a more comprehensive set of processes.
- The best practice processes described in ITIL may be used as a basis for achieving the British Standard for IT Service Management (BS 15000), which is currently being considered for fast-tracking to become an international standard—ISO/IEC 20000.

<http://www.bs15000.org.uk>

ITIL

There are two ITIL publications that describe IT Service Management

Service Support

- Incident management
- Problem management
- Configuration management
- Change management
- Release management
- Service desk function

Service Delivery

- Capacity management
- Availability management
- Financial management for IT services
- Service level management
- IT service continuity management

ISO/IEC 17799

Information technology - Code of practice
for information security management.

- ISO/IEC 17799 is an information security standard published in December 2000 by the ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission)
- ISO/IEC 17799:2002 provides best practice recommendations on information security management.
- Primary Audience - Anyone who is responsible for initiating, implementing or maintaining information security management systems.
- ISO 17799:2002 was revised and re-issued in June 2005 as ISO/IEC 17799:2005
- ISO/IEC 17799:2005 will be renamed to ISO/IEC 27002 in the future.
The 27000 series of standards have been specifically reserved for information security matters.

ISO/IEC 17799

- Information security is defined as the preservation of Confidentiality, Integrity and Availability
- ISO/IEC 17799:2005 has eleven main sections that define the best practices of control objectives and controls:
 - Security Policy
 - Organization of Information Security
 - Asset Management
 - Human Resources Security
 - Physical and Environmental Security
 - Communications and Operations Management
 - Access Control
 - Information Systems Acquisition, Development and Maintenance
 - Information Security Incident Management
 - Business Continuity Management
 - Compliance

ISO/IEC 17799

- Within each section, information security control objectives are specified and a range of controls are outlined as a best practice means of achieving those objectives.
- For each of the controls, implementation guidance is also provided.
- Currently under development
 - ISO/IEC 27799 Health informatics -- Security management in health using ISO/IEC 17799

Impacts

- Erosion of Customer / Investor Confidence
- Loss of Competitive Advantage
- Business Partners Not Trusting Your Systems
- Liability
- Loss of Business

Benefits

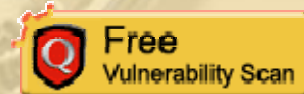
- Customer / Investor Confidence
- Competitive Advantage
- Business Partners Trust
- Confidence & Awareness of Network Infrastructure Strengths & Weaknesses
- Increased Productivity
- Mitigate Liability / Risk



FREE Scan Offer

To Take Advantage of Our FREE
Vulnerability Scan

Visit our Website and click on the icon



5650 Yonge Street, Suite 1500, Toronto, ON M2M 4G3

Phone: 416.245.4589 or 1.866.664.6684

eFax: 416.245.4589

info@securityassessment.net



Q & A

George M. Araujo, MCSE: Security
ga@securityassessment.net

5650 Yonge Street, Suite 1500, Toronto, ON M2M 4G3

Phone: 416.245.4589 or 1.866.664.6684

eFax: 416.245.4589

info@securityassessment.net

END