"7 Steps to Protect Your Business From Hackers, Disasters, and Thieves"

August 9-11, 2005

NEbraskaCERT Conference

Omaha, NE

Debbie Christofferson

Sapphire-Security Services LLC

Debbie Christofferson, CISSP, CISM
Sapphire-Security Services LLC

- **Creating traction and action in your security program based on your bottom line business risk**
- **14 years leading edge security experience, combined with 20 years global Fortune 500 background guarantees the level of knowledge needed for any business in any environment**
- **Certified Information Security Manager and Certified Information Systems Security Professional**

- ***We can support your security strategy, program management, and speaker/trainer needs***
- **Contact us today at 480-988-4194 DebbieChristofferson@earthlink.net**
- **www.sapphire-security.com**
- **Subscribe *now* at no cost to "Security Strategist" for leading edge summaries to help focus your security strategy and results.**

"Got Security?"

- Is security a real consideration and is it supported?
- What is your biggest business concern regarding security?

Are You Leveraging Your $$$?

"Computer security has become the single most important topic in the IT world.

…Security budgets have outpaced overall IT expenditures…"

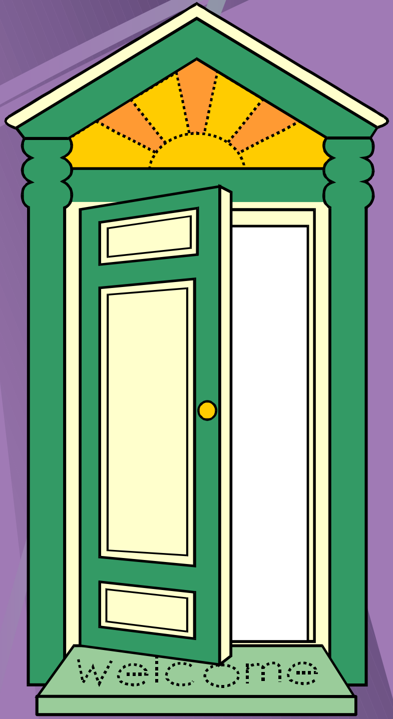
"A Security Plan With Teeth", *CFO-IT Magazine*, Spring 2005

Is Your Spending Making a Difference?

"Gartner says that over the next two years, roughly 80% of all companies will spend about 10% of their security budgets on unnecessary fixes, …"

"Heading Off Hackers", *Computerworld*, January 31, 2005

Contents – 7 Steps

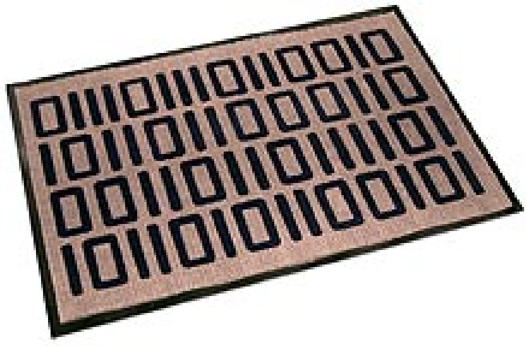


- Identify risks & rewards
- Define strategy
- Pay attention to people
- Execute critical processes
- Deploy technology solutions
- Apply Trends
- Get to the bottom line
- Resources

- Risks & Rewards

www.pl8s.com/coke.htm

Digital Trade Secrets

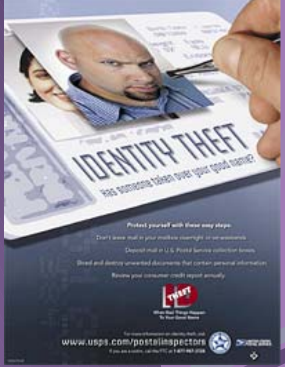


- From 50 to 70 percent of the value of a company today is derived from its proprietary data and trade secrets, and 90 percent of those secrets can be found in digital form.

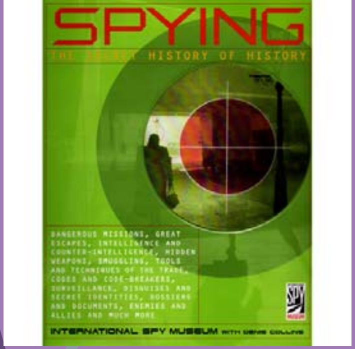
American Society for Industrial Security and

PricewaterhouseCoopers 2000 study

http://www.business2.com/b2/subscribers/articles/print/0,17925,527791,00.html


IDENTITY THEFT
Has someone taken over your good name?
Protect yourself with these easy steps:
www.usps.com/postalinspectors

We’re Under Attack!



- “82% of companies reported virus attacks, even though 99% of them ran anti-virus software.”

  – 2003 CSI/FBI Computer Crime & Security Survey.

- “Symantec Corp. tests indicated an **IM virus** could infect as many as half a million users in as little as 30 to 40 seconds.”

  “Security Wire Perspectives”, 12/6/04, I*nformation Security Magazine*

- “Spyware Will be a top Threat in 2005”,

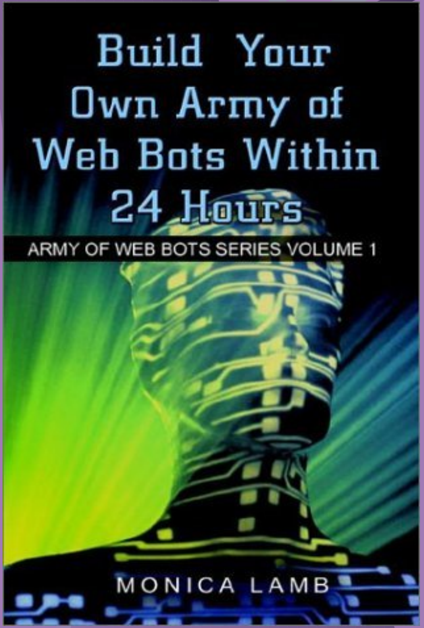
  www.watchguard.com by Marcia Savage, *SC Magazine*

- “Identity Theft Now Costs US Businesses Some $33B a Year” - Peter Krass, *CFO-IT* Spring 2005

- Spam nightmare grows for Small Firms”

  The SC Infosecurity Newswire, 1/28/05 www.scmagazine.com

“Botnets More Menacing Than Ever”



Build Your Own Army of Web Bots Within 24 Hours

ARMY OF WEB BOTS SERIES VOLUME 1

MONICA LAMB

THE ZOMBIE SURVIVAL GUIDE by MAX BROOKS - Microsoft Internet Explorer

http://www.randomhouse.com/crown/zombiesurvivalguide/

THE ZOMBIE SURVIVAL GUIDE

COMPLETE PROTECTION FROM THE LIVING DEAD

BY MAX BROOKS

HOME / LATEST ZOMBIE UPDATES

SELECTIONS

KNOW YOUR ENEMY OUTBREAKS THE VIRUS

ASK THE EXPERT

ZOMBIE LINKS ABOUT THE AUTHOR

GET PROTECTION FROM THE LIVING DEAD!

HOME / LATEST ZOMBIE UPDATES

WHAT IS A ZOMBIE?
How are they created? What are their strengths and weaknesses? What are their needs, their desires? Why are they hostile to humanity? Can you survive an attack? Can you keep your family safe?

THE ZOMBIE SURVIVAL GUIDE is your complete resource for surviving an encounter with the undead.

You'll learn how to recognize your enemy and choose the right weapons to defend yourself. You'll get information on the latest in killing techniques, along with tips on what to do when on the defense, on the run, or on the attack.

Read the selections provided in the left hand menu to learn about zombie attributes, outbreaks, and the virus behind it all.

Contact the author with your zombie questions.

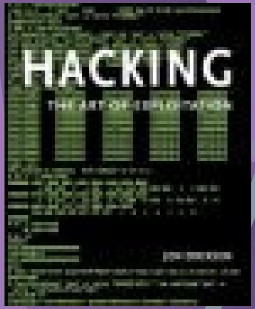
Visit our zombie link directory for the best sites on the web.

To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for...

“...More than a million machines worldwide are bot-infested and under the control of hackers; ... (most) attacks ... monitored last year were designed to covertly steal information or take over computers for criminal purposes.”

By Bill Brenner, News Writer

18-Mar-2005, *SearchSecurity.com*



“…a group of hackers …, learned the practice of "carding"—buying goods online with stolen credit cards.”

“ … among other things, tapped a database of an estimated 50,000 credit cards …”

BY Art Jahnke, CSOOnline Magazine, 010105, “Russian Roulette”, http://www.csoonline.com/read/010105/russian.html

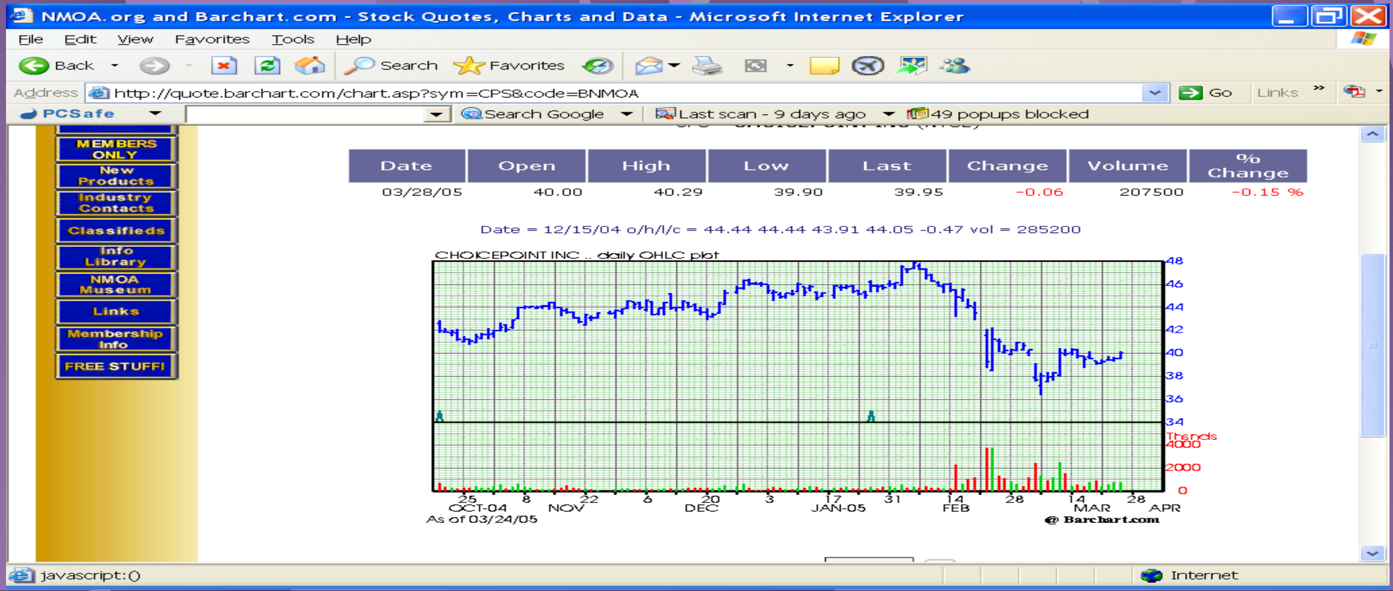
Companies Make it Easy

Thieves snatch documents containing Social Security numbers and other personal data from the mail, steal computers with stored data, hack databases, buy IDs from other thieves, bribe company insiders, fish through the trash, and trick us into providing their user Ids and passwords.

“The New Face of Identity Theft”, *CFO-IT*, Spring 2005

ChoicePoint's stock dropped nearly 10% after announcing that criminals duped it into giving access to its database.

"ChoicePoint Execs Sold Stock Before Leak Revealed"
Harry R. Webber of the Associated Press, *The Arizona Republic*, 2/27/05



NMOA.org and Barchart.com - Stock Quotes, Charts and Data - Microsoft Internet Explorer

Address http://quote.barchart.com/chart.asp?sym=CPS&code=BNMOA

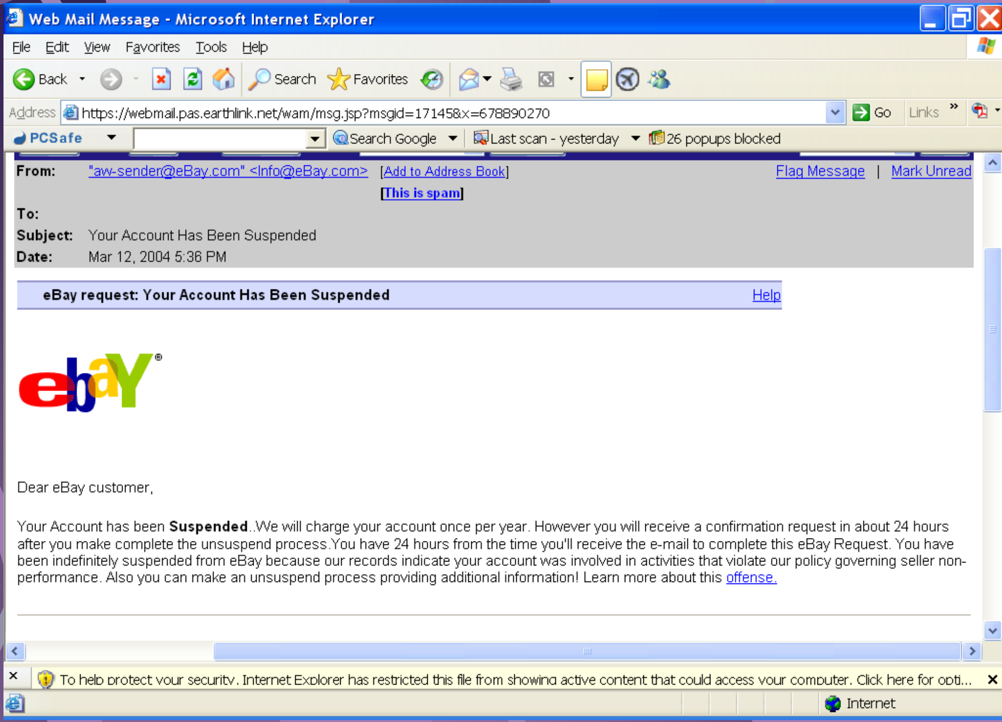
Date	Open	High	Low	Last	Change	Volume	% Change
03/28/05	40.00	40.29	39.90	39.95	-0.06	207500	-0.15 %

Date = 12/15/04 o/h/l/c = 44.44 44.44 43.91 44.05 -0.47 vol = 285200

Phishing

Symantec filters blocking 33M phishing attempts a week in Dec/04, up from 9M a week in Jul/04, ...an increase of ... 366%.

3/21/05 press release at http://ses.symantec.com/content.cfm?ArticleID=5491


Web Mail Message - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Go Links
PCSafe Search Google Last scan - yesterday 26 popups blocked
[Add to Address Book]
[This is spam]
Flag Message | Mark Unread
Help
Internet

Address https://webmail.pas.earthlink.net/wam/msg.jsp?msgid=17145&x=678890270

From: "aw-sender@eBay.com" <Info@eBay.com>
To:
Subject: Your Account Has Been Suspended
Date: Mar 12, 2004 5:36 PM

eBay request: Your Account Has Been Suspended

Dear eBay customer,

Your Account has been **Suspended**. We will charge your account once per year. However you will receive a confirmation request in about 24 hours after you make complete the unsuspend process.You have 24 hours from the time you'll receive the e-mail to complete this eBay Request. You have been indefinitely suspended from eBay because our records indicate your account was involved in activities that violate our policy governing seller non-performance. Also you can make an unsuspend process providing additional information! Learn more about this offense.

To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for opti...

"Thieves Tap Wi-Fi Networks With Ease"

"Connections are being commandeered for child pornography, fraud, death threats and identity and credit-card theft."

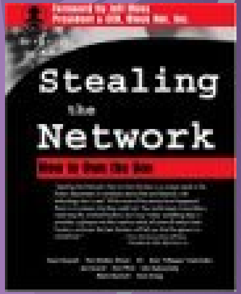
"…Most consumers who spend the $60 to $80 for a wi-fi router are just happy to make it work at all and never turn on encryption."

Wifi Finder detects wireless networks up to 200' away

By Seth Schiesel, *New York Times*

The Arizona Republic, March 20, 2005

"Hacker Breaches T-Mobile Systems, Reads US Secret Service Email"



"A sophisticated computer hacker had access to servers at wireless giant T-Mobile for at least a year, which he used to monitor US Secret Service email, obtain customers' passwords and Social Security numbers, and download candid photos taken by Sidekick users, including Hollywood celebrities, …".

By Kevin Poulsen, *SecurityFocus*, 12-Jan-2005
www.theregister.co.uk/2005/01/12/hacker_penetrates_t-mobile/

“Mobile Phone Virus Found in US”

“The world's first mobile phone virus ‘in the Wild’ has spread to the United States from its birthplace in the Philippines eight months ago, … The virus, called Cabir, has spread slowly into 12 countries and marks the **beginning of the mobile phone virus era**, …”

From MSNBC.com (Topic: Mobile Viruses) Feb 18:((2005)

http://www.businessweek.com/magazine/content/05_09/b3922046_mz011.htm

Creating a Strategy

What are you protecting, and what's the value if it's lost, stolen, altered, or unavailable?

Why Security Matters

Preserve core business and intellectual assets

Avoid financial losses

Keep your business up and running

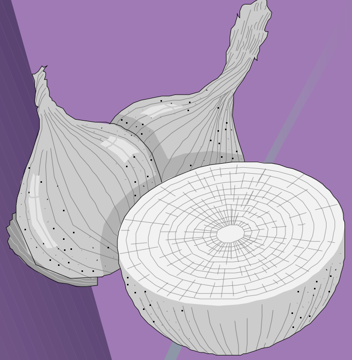
Comply to regulations

Protect customers, shareholders, partners, and communities

Increase productivity and reliability

Enhance reputation and competitive advantage in the market

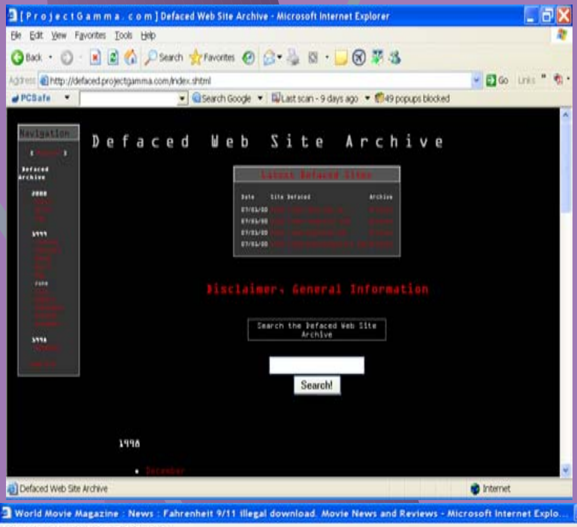
Enable the Business



- How much security is enough?
  - Identify your core business and what absolutely has to be protected
  - Tie strategy to organization’s key objectives
  - Create infrastructure to support your critical business
  - Base it on prioritized risks to core business
  - Engage management

Security Questions

- Can you pass a compliance audit?
- Are your systems used to
  - Spew our forged email?
  - Hack and deface web sites?
  - Serve child pornography?
  - Illegally download music or software?
- What gets posted to your network?
- Do you mean for everything on your web site to be public



[ProjectGamma.com] Defaced Web Site Archive - Microsoft Internet Explorer

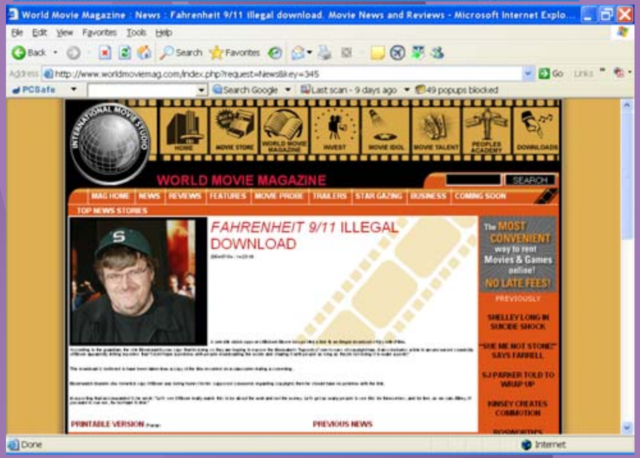
http://defaced.projectgamma.com/index.shtml

Defaced Web Site Archive

Disclaimer, General Information

Search the Defaced Web Site Archive

1998



World Movie Magazine : News : Fahrenheit 9/11 illegal download. Movie News and Reviews - Microsoft Internet Explo...

http://www.worldmoviemag.com/index.php?request=News&key=345

WORLD MOVIE MAGAZINE

TOP NEWS STORIES

FAHRENHEIT 9/11 ILLEGAL DOWNLOAD

The MOST CONVENIENT way to rent Movies & Games online! NO LATE FEES!

PREVIOUSLY

SHELLEY LONG IN SUICIDE SHOCK

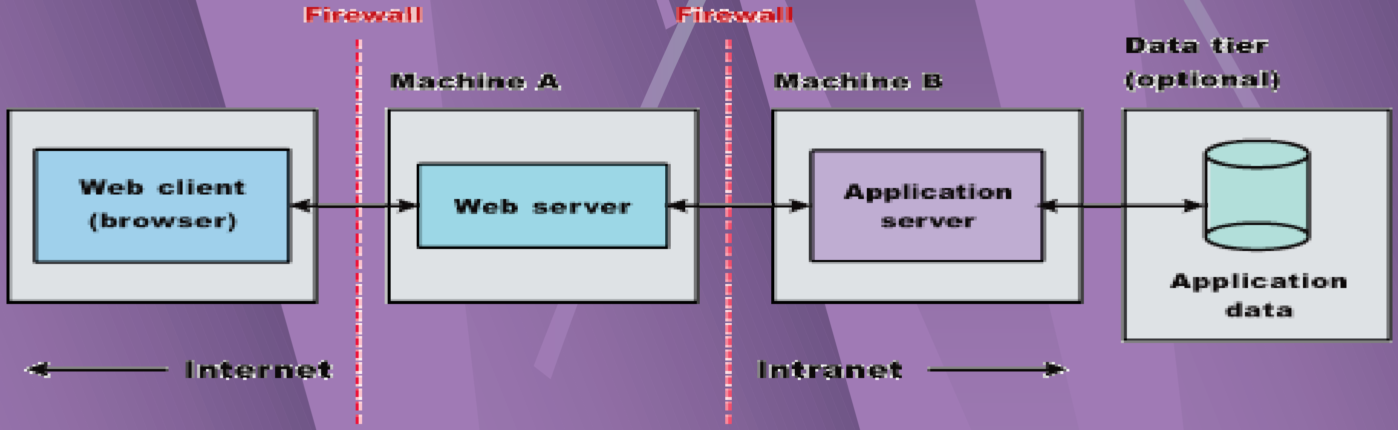
"SUE ME NOT STONE!" SAYS FARRELL

SJ PARKER TOLD TO WRAP UP

KINSEY CREATES COMMOTION

Security Components

- Technology
- People
- Processes



Security Principles

- Treat security as a people problem not a technology solution
- Policy spells out position on protection
- Security exists as a function
- People understand the expectations
- Security is a cost of doing business
- Tie-in to business objectives is critical

Risk Components

- Confidentiality
- Integrity
- Availability
- Accountability
- Priority:

  High, Medium, Low

The Human Element

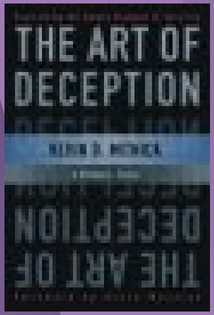
"The Weakest Link!"

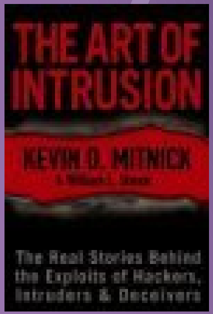
"When I did security audits, I found the fastest path into a secure area was to effectively look for the key under the doormat. People simply don't think about security enough and, without knowing it, will often create exposures … to simplify their jobs. …No platform alone can fully compensate for this."

"What if Microsoft Got it Right?", By Rob Enderle, *TechNewsWorld*, 03/01/04 http://www.technewsworld.com/story/32976.html

“I’ve Seen the Enemy and the Enemy is Me”

“If the exposure is people and people are gullible, then security at a product level might only make you feel more secure. You might not actually be more secure.”




THE ART OF INTRUSION
KEVIN D. MITNICK
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

“What if Microsoft Got it Right?”
By Rob Enderle, *TechNewsWorld*
3/1/05 http://www.technewsworld.com/story/32976.html

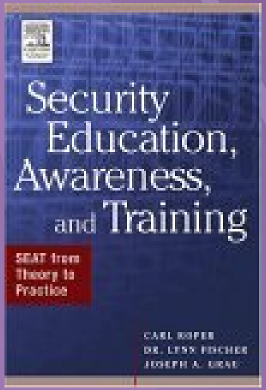
People

- Executive staff
- Managers
- Employees
- Contract & temp staff
- Outsourcers
- Vendors & Suppliers
- Customers
- Visitors

- System Support
  - System & network admins
  - DB admins
  - Web admins
  - Help Desk Admins
  - Programmers & Developers

"…Lack of consumer awareness, if not downright naiveté, allows the war to escalate."   …between hackers and security programmers

***The Arizona Republic*, 12/27/04, "Hackers Hone for Holidays**



"... Home users who aren't updating their antivirus or installing security patches may have to get burned before they understand," - Steve Fallin, director of WatchGuard's rapid response team

"Extroverts More Likely to Open Virus-Laden E-Mail Attachments,", Mark Baard Contributing Writer, *Security Wire Perspective*, 01/24/05, published by *Information Security Magazine*

Processes

Supporting Structure

- Policies & Standards
- Education & Awareness
- Account terminations & changes
- Account management—IDs and access rights
- Incident response
- Business continuity planning

- Change management
- Audits
- Metrics
- Physical access
- Development life cycle
- Media disposal

“Stolen passwords enable ID thieves to roam undetected in computer systems.”

CFO Magazine (CFO-IT), Spring 2005

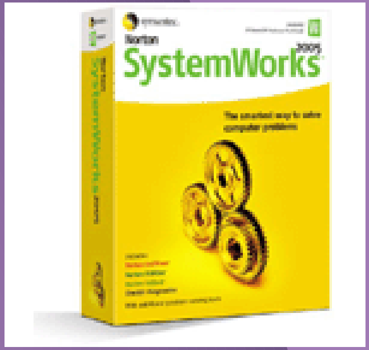
What is Your Favorite Pet's Name?

- T-Mobile.com requires users to answer a "secret question" if they forget their passwords. For Hilton's account, the secret question was "What is your favorite pet's name?" By correctly providing the answer, any internet user could change Hilton's password and freely access her account.

"How Paris Hilton Got Hacked" Feb 22 2005, *Mobile Tracker*, http://www.mobiletracker.net/archives/2005/02/22/paris-hilton-hacked-sidekick-phone-

What are You Throwing Out?

click to enlarge



The Royal House
of Serbia &
Yugoslavia

“Is Your Crown Passable?”

“CEOs running small companies should be realistic about their retirement plans and begin an internal search for a successor well in advance of that date to ensure the individual has the proper training, understands all aspects of the business and is prepared to take the reins.”

R

***BusinessWeek*, by Karen E. Klein, 2/17/05**

Florida's Hurricanes

"Overall return on investment was directly proportional to preparation……Companies that has focused solely on disaster recovery planning—without including plan for full business continuity --were affected more."

"Up and Running", John Medaska,
CSO Magazine, December 2004, P. 22

http://meted.ucar.edu/hurrican/

strike/text/dz_dsc.htm

- Technology

Hype Vs. Reality

- Virus protection at client and server
- Software updates
- Camera phones
- Encryption

- USB Storage devices
- Peer to Peer file sharing
- IDS & IPS
- Network segmentation
- VPN Remote Access
- Firewall
- Penetration testing
- Watermarking

Top Ten Most Critical Web Application Security Vulnerabilities

- Broken Access Control
- Broken Account and Session Management
- Buffer Overflows
- Command Injection Flaws
- Cross-Site Scription (XSS) Flaws
- Error Handling Problems
- Insecure Use of Cryptography
- Remote Administration Flaws
- Unvalidated Parameters
- Web and Application Server Misconfiguration

Source: Open Web Application Security Project (OWASP)

CSO Magazine, February 2005

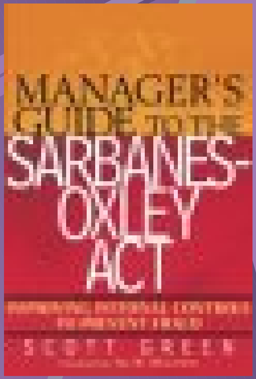
Software Quality

"You really need a revolution in the IT industry, …. If engineers built bridges as software developers build software, there wouldn't be a bridge standing.

Mary Ann Davidson, Oracle CSO, “Security Wire Perspectives”,

Vol. 6, No. 93, December 6, 2004 by *Information Security Magazine*

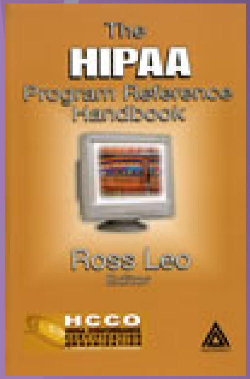
Trends



"Executives International estimates that it will cost corporations an average of $3 million to comply with the rule"

"Sarbanes-Oxley Delay Granted",
Deborah Solomon, *Wall Street Journal*, 3/6/05

Trends



- Converging voice, data, video
- Broadband to power plug
- Wireless and portability
- Increasing regulations
- Outsourcing
- Collaboration
- Mergers & Acquisitions
- Blogging
- PodCasting
- eLearning

Google Desktop Search Download - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://desktop.google.com/
Go Links
Google Desktop

Search your own computer.

- Find your email, files, web history and chats instantly
- View web pages you've seen, even when you're not online
- Search as easily as you do on Google

Google Desktop Search finds:

Outlook / Outlook Express
AOL Instant Messenger
Internet Explorer
Text
Word
Excel
PowerPoint

By downloading, you agree to our Terms & Conditions and Privacy Policy

Agree and Download

FREE and takes seconds to install

*Fast download - about 1 minute on a modem (400K)
*Requires Windows XP or Windows 2000 SP 3+
*Automatically starts when you turn on your computer

About Press & Testimonials Screenshots Help Contact Us

©2004 Google

To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for opt...

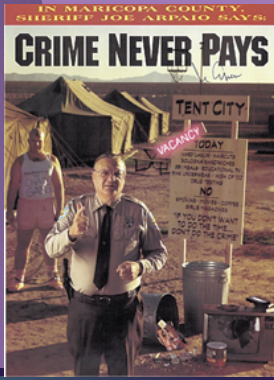
Rising Crime

- "…Sale of bootleg products is estimated at to account for up to 7 percent of global trade…"

  CSO Magazine, Dec/ 2004, "Top Billing: News From Inside the Beltway"

- Rising high-tech theft: Laptops, CPU scams, freight theft

Super-sleuth Sherlock solved crimes with forensic chemistry



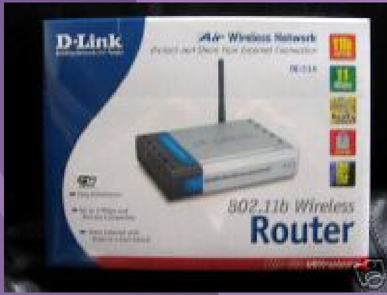
Opportunities

- Update software
- Define & communicate security policy
- Implement standards
- Build security into technology deployments
- Protect data at the source
- Manage accounts
- Audit your program to identify and close gaps
- Hire and manage for skill and retention
- Plan for business continuity

Technology Solutions

www.dw-world.de/
dw/article/
0,,1113690,00.html

- Install firewalls, anti-virus and spyware solutions, VPN remote access
- Segment the network
- Protect data in transit and storage
- Build better software
- Encryption
- Biometrics



Call to Action

"Alexey Ivanov's Advice to CISOs"

1. Do not store information on your network that doesn't have to be there.
2. Don't think that custom software will not be hacked.
3. Pay attention to your entire business infrastructure—IT and otherwise.
4. Make someone responsible for installing all security updates.
5. If you choose to communicate with hackers, do not make promises you can't keep.
   http://www.csoonline.com/read/010105/russian.html

"Companies that manage their information efforts sooner, rather than later, will lower their risks. Those that delay or avoid the issue will suffer through endless cycles of business disruptions, stock price slides and inevitable lawsuits."

"IT security: Something's Gotta Give"

February 10, 2004, by Jon Oltsik

http://news.com.com/2010-7355_3-5156080.html

Conclusion

- Security is not a technology issue
- Layer your approach
- It's not all or nothing: Balance risk and cost to your bottom line

Free US Consumer Credit Report

- www.annualcreditreport.com or
- Call 877-322-8228 toll-free
- Or complete the Annual Credit Report Request Form and mail it to
  - Annual Credit Report Request Service
  - P. O. Box 105281, Atlanta, GA 30348-5281
- Starts in June for Southern states, in September for Eastern states, and already in affect in Western and Northern states.
- Visit www.ftc.gov for more information
- www.myfico.com for credit scores (for a paid fee)

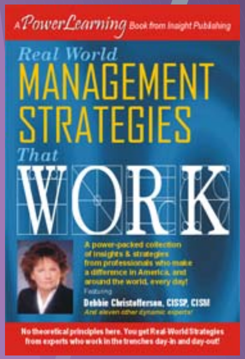
"10 Questions to Keep Outsourcing on the Mark"

- Overseas expansion or global image
- Staff overload
- Tight deadline on critical business objective
- New lines of business
- Areas that don't interact with customers

"Outsourcing Tune-up",
***Computerworld*, 11/2/04**

- Efficiency of operations
- Changes in outsourcing trends
- Changes in talent market
- Vendor performance on benchmarks & pricing
- How well strategic objectives are being met

To Receive Free Reports



A *PowerLearning* Book from Insight Publishing

Real World
MANAGEMENT
STRATEGIES
That
WORK

A power-packed collection of insights & strategies from professionals who make a difference in America, and around the world, every day!

Featuring
Debbie Christofferson, CISSP, CISM
And eleven other dynamic experts!

No theoretical principles here. You get Real-World Strategies from experts who work in the trenches day-in and day-out!

- "*Security Management Strategies That Work for Any Company on Any Budget*"
- "50 Tips to Increase Security Awareness"
- "Tips & Tricks to Pass the CISSP Exam"
- "*The Security Strategist*" Newsletter – Subscribe today by sending email:
- Send email with request in subject line to: DebbieChristofferson@earthlink.net

Debbie Christofferson, CISSP, CISM

- Getting the results you need to protect your bottom line.
- Helping organizations build and manage a successful security strategy based on risks and the bottom line.
- 20 years international Fortune 500 management experience with Intel Corp, across the US, Europe and Greater Asia. Published author.
- *"The Security Strategist"* Newsletter –send email to subscribe *now!*
- Sapphire-Security Services LLC
- DebbieChristofferson@earthlink.net
- www.sapphire-security.com