



“Confronting the Threat Inside the Castle Walls”

Wednesday, August 8, 2006, 2-3:15 PM

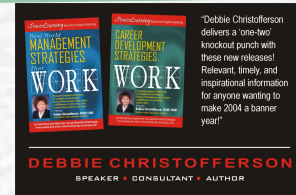
Debbie Christofferson, CISSP, CISM

Sapphire-Security Services LLC



Debbie Christofferson, CISSP, CISM

Sapphire-Security Services LLC



- Debbie knows security from the ground up, based on 20 years first hand Fortune 500 experience across the U.S., Europe, and Asia with Intel Corporation.
- She is President of Sapphire-Security Services LLC
- Debbie is a published author, and writes a column for technology trends and careers.
- She's on the board for Phoenix ISSA, SDSUG, and a member of the ITT Technical Institute's Advisory Board. Debbie is a member of the National Speakers Association, the Arizona Technology Council, ISACA, ATW, Infragard, OWIT.
- Call Debbie to increase the results and effectiveness of security through management consulting, program leadership, workshops or speaking, training or writing.





Session Overview

Statistics show the insider threat rising, up to 50% of security incidents that cause monetary loss. But the number increases when you consider unreported incidents or those that create damage without direct financial loss, such as to branding and reputation, or those related to non-business web-surfing or serving up porn or illegal music download sites. Damage can also occur from malicious behavior or mistakes. Insiders wreak the most damage because of their trusted position. These can include employees, contractors, service providers or vendors--anyone with trusted access to your facilities or computer network. CompTIA's 2005 survey said that mistakes by people were behind four of every five security breaches. This session creates a realistic and cost-effective focus for managing this rising insider risk.



True or False

1. Users are less likely to be caught stealing sensitive information when they can it do offsite.



True or False

2. Most employees will not use instant messaging once a business defines a policy that disallows it.



True or False

3. Securing wireless hotspot usage for your Wi-Fi users includes using a VPN for remote network connectivity, a personal firewall to keep users from connecting to the wireless computer and SSL/TLS for all messaging.



True or False

4. Current employees are the primary source of insider attacks.



True or False

5. More than 50% of insider risk involves conflict of interest.



True or False

6. Ransom demands are made to big business, but not to entrepreneurs and small business owners.



True or False

7. Only ~20% of CFOs are highly satisfied with their security programs.



True or False

8. About 60% of organizations lack a written strategic plan, in spite of large technology investments



True or False?

9. A bank disallows wireless access, but embezzlement of funds occurred from a bank using a rogue wireless access point



True or False

10. Most user accounts are turned off within 3 days of their departure from a company.



True or False

11. The most common UNIX system administrator password is “God”.



True or False

12. If a trusted security staff member who is responsible for incident response is suspended, all their account access can be disabled within 7 days.



True or False

13. In more than 90% of the incidents investigated, revenge was the primary motivator.



True or False

14. The insider attacker is usually a male.



Insider Attacks

15. More than 60% used remote access to carry out the attack.

References – T/F Questions

- Q: 1-5: “Five Common Insider Threats and How to Mitigate Them”, Searchsecurity.com, Kevin Beaver, 1/16/05, http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1158172,00.html?track=NL-20&a
- Q: 6: 2005 E-Crime Watch Survey, CSO Magazine, 3/05
- Q: 7-8: Technology Issues for Financial Executives, 7/13/06 <http://www.csc.com/solutions/managementconsulting/knowledge>
- Q: 13-15: Published 2005 study on insider threats by the United States Secret Service and the Carnegie Mellon Software Engineering Institute’s CERT Coordination Center



“Human error, either alone or in combination with technical malfunction, was to blame for four out of every five security breaches.” ... which is consistent with last year’s results”

CompTIA 2005 survey finding, *Network World Newsletter*, Amy Shurr, 5/31/05, “Organizations Slow to Staunch security Threat”

Insider Threat

- ☞ Benefits
- ☞ People
- ☞ Processes
- ☞ Technology
- ☞ Conclusion & Call to Action



Benefits

- ✓ Mitigate risk
- ✓ Reduce financial loss
- ✓ Increase value of bottom line
- ✓ Improve the bottom line without a huge financial investment

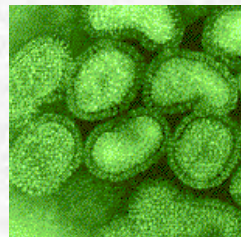


Security

- People
- Processes
- Technology

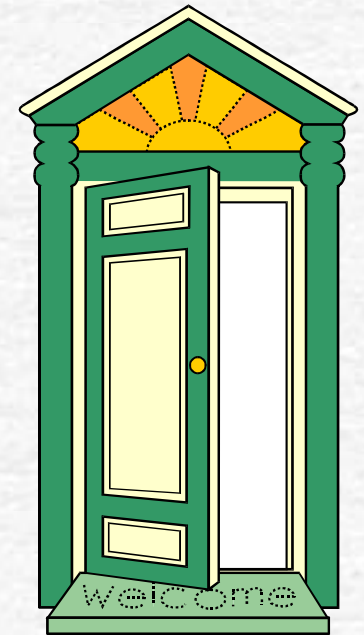
Technology


- Automation
- Perimeter defense, IDS, IPS, Firewalls, network segmentation
- Web facing apps & dbs
- Spyware, anti-virus, spam
- Authentication & Authorization
- Wireless
- Instant Messaging
- Infrastructure
- Collaboration
- Convergence



People

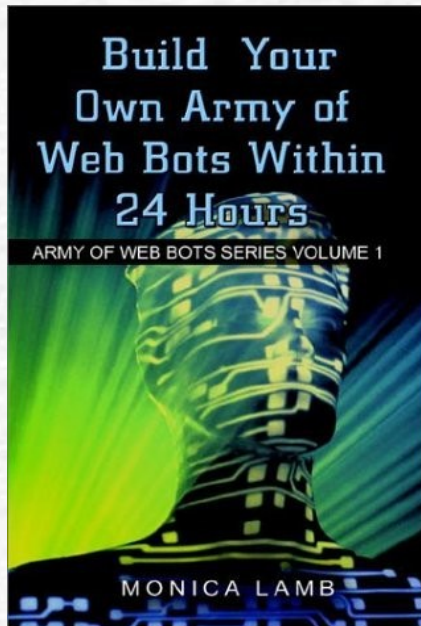
- ✓ Role for security
- ✓ Hire and manage for skill and retention
- ✓ Skills, education and background
- ✓ Orientation & training
- ✓ Tops-down
- ✓ Employees, management, vendors, contractors, service providers, ...
- ✓ Separation of duties



- 
- Companies say IT security is a priority, but few are backing that up with the appropriate level of education and prevention.

CompTIA survey finding this year
Network World Newsletter, Amy Shurr, 5/31/05, “Organizations
Slow to Staunch security Threat”,

Home & Mobile Users



“Bots are often precipitated by unsecured **always-on** broadband connections, ...”

“How to Tell if You Have Bots”, *CSO Magazine*, December, 2005

Credit Card Fraud

“According to the Merchant Risk Council, retailers that don’t manage credit card fraud can have charge-back percentages in the double-digits.”

– CSO Magazine, December, 2005



Fraud, Theft and Errors

- ✓ Vendor transactions
- ✓ Early detection
- ✓ Credit card fraud
- ✓ A/P, Purchasing, Expense Reports
- ✓ Publish outcomes



Processes

- Policy
 - Definition, communication & enforcement
- Education & Awareness
- Incident response
- Audits & assessments
- Baseline of “normal” system
- Logs & review
- Controls to prevent, detect and correct



Processes (continued)

- ☞ Account management
 - Terminated employees
 - Least privilege
 - Accountability
 - Faceless & generic accounts
- ☞ Incident response & investigations
- ☞ Change management including current systems & software
- ☞ Business Continuity plan
 - Key processes, people and systems
- ☞ Employee, consultant, vendor agreements



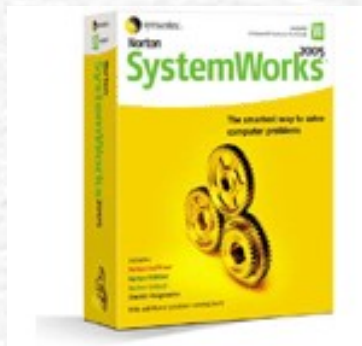
Account Management


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

CFO Magazine (CFO-IT), Spring 2005



What are You Throwing Out?



 click to enlarge



Florida's Hurricanes

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

“Up and Running:, John Medaska, CSO Magazine, Dec-2004



[http://meted.ucar.edu/hurricane/
strike/text/dz_dsc.htm](http://meted.ucar.edu/hurricane/strike/text/dz_dsc.htm)

Rising Crime

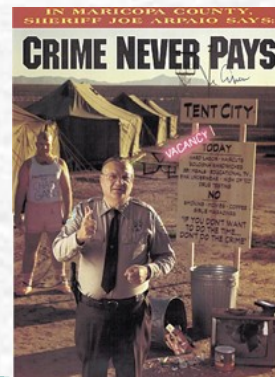
“...Sale of bootleg products is estimated at to account for up to 7 percent of global trade...”

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

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

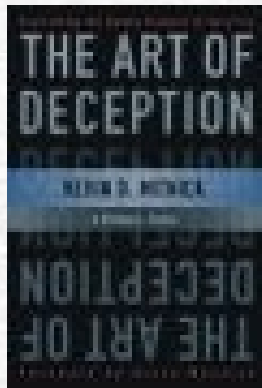


**Super-sleuth
Sherlock solved
crimes with forensic
chemistry**



“The Weakest Link”

“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.”



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

Call to Action

- ☛ Treat security as a people and not a technology issue
- ☛ Balance risk and cost to your bottom line
- ☛ If you need help or a security review, get it done!
- ☛ Join us in monthly security strategy teleseminars!



To Receive Free Reports

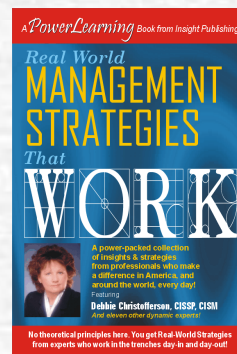
“Security Management Strategies That Work for Any Company on Any Budget”

“50 Tips to Increase Security Awareness”

...Or for other assistance,

Send email with subject to:

DebbieChristofferson@earthlink.net



Sign-up – No Cost to you!

- ☛ Signup for the latest in management security strategy at no charge to you!
- ☛ Security Management Briefings (15 issues/yr)
- ☛ Security Strategy Expert Interview
 - Monthly telephone seminars on leading edge security strategy with leading industry experts.
 - Send email to DebbieChristofferson@earthlink.net, subject: “Security Strategy”
- ☛ Topics you'd like to see?

Request Free Report

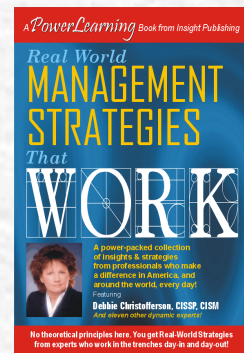
*“Security Management Strategies That Work
for Any Company on Any Budget”*

“50 Tips to Increase Security Awareness”

...Or for other assistance,

Send email with subject to:

DebbieChristofferson@earthlink.net



Free Business Cards

Enter your Text - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Reload Print View Source

Address http://www.vistaprint.com/vp/ns/studio.aspx?cparts=yes&cfs=-1&pf_id=064&combo_id=4298&combo1=904.100.18.11 Go Links

Google free business cards Search 32 blocked Check AutoLink AutoFill Options free business

VistaPrint
BEST PRINTING. BEST PRICE.

[Home](#) [My Account](#) [Sign in Now!](#) [Specials](#) [Shopping Cart](#) [Help](#)

Customize Your FREE Card

Select from 42 Free Business Card Designs!

1. Enter text for Front of document

Company Name

Message

Full Name

Job Title

Address Line 1

Address Line 2

Address Line 3

Phone / Other


Fax / Other

E-mail / Other

Web / Other

2. Select Your Business Card

< 1 2 3 4 5 >



> [See hundreds of other designs - only \\$7.99!](#)

Company Name

Message

Full Name

Job Title

Address Line 1

start Internet 11:00 PM

[Home](#)

- What's New
- Arts & Leisure
- Fashion & Style
- House & Home
- People
- Professional Advice
- Resources
 - Careers/Edu
 - Offers/Shop
 - Organizations
 - Resources
 - Volunteer
- Times of your Life
- About Us
- Search the Site

Career Information for Women in Technology

[Meet Debbie Christofferson](#)
Our experienced expert

[H1B Visas](#)
Lock Out US Technology Workers

[Competitive Intelligence Job Primer](#)
CI offers a variety of lucrative career fields

[Certifications](#)
Increase Your Competitive Advantage

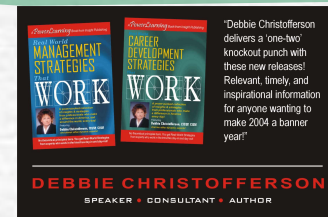
[Re-Careering:](#)
Building Your Field of Dreams

[Investing in Training and Development](#)
Growing Your Career by Debbie Christofferson

[Tech and Career Trends for Women](#)
Introductory Column by Debbie Christofferson



Debbie Christofferson, CISSP, CISM



- Debbie knows security from the ground up, based on 20 years first hand Fortune 500 experience across the U.S., Europe, and Asia with Intel Corporation.
- She currently manages her own business, Sapphire-Security Services LLC, which increase the results and effectiveness of security through management consulting, program leadership, workshops and speaking.
- She's a published author and writes a column for technology trends and careers.
- Debbie is a Board Member for Arizona ISSA & SDSUG, and ITT Technical Institute's IT Advisory Committee.
- She's a member of the National Speakers Association, the Arizona Technology Council, Organization of Women in International Trade, Information Systems Audit and Control Association, Infragard, and the Alliance of Technology and Women.

