Enforcing Security In the Office

Training Supervisors and Managers to Do Their Part

presented at the

FISSEA 2009 Conference

Jane Powanda

March 24, 2009

noblis
For the best of reasons

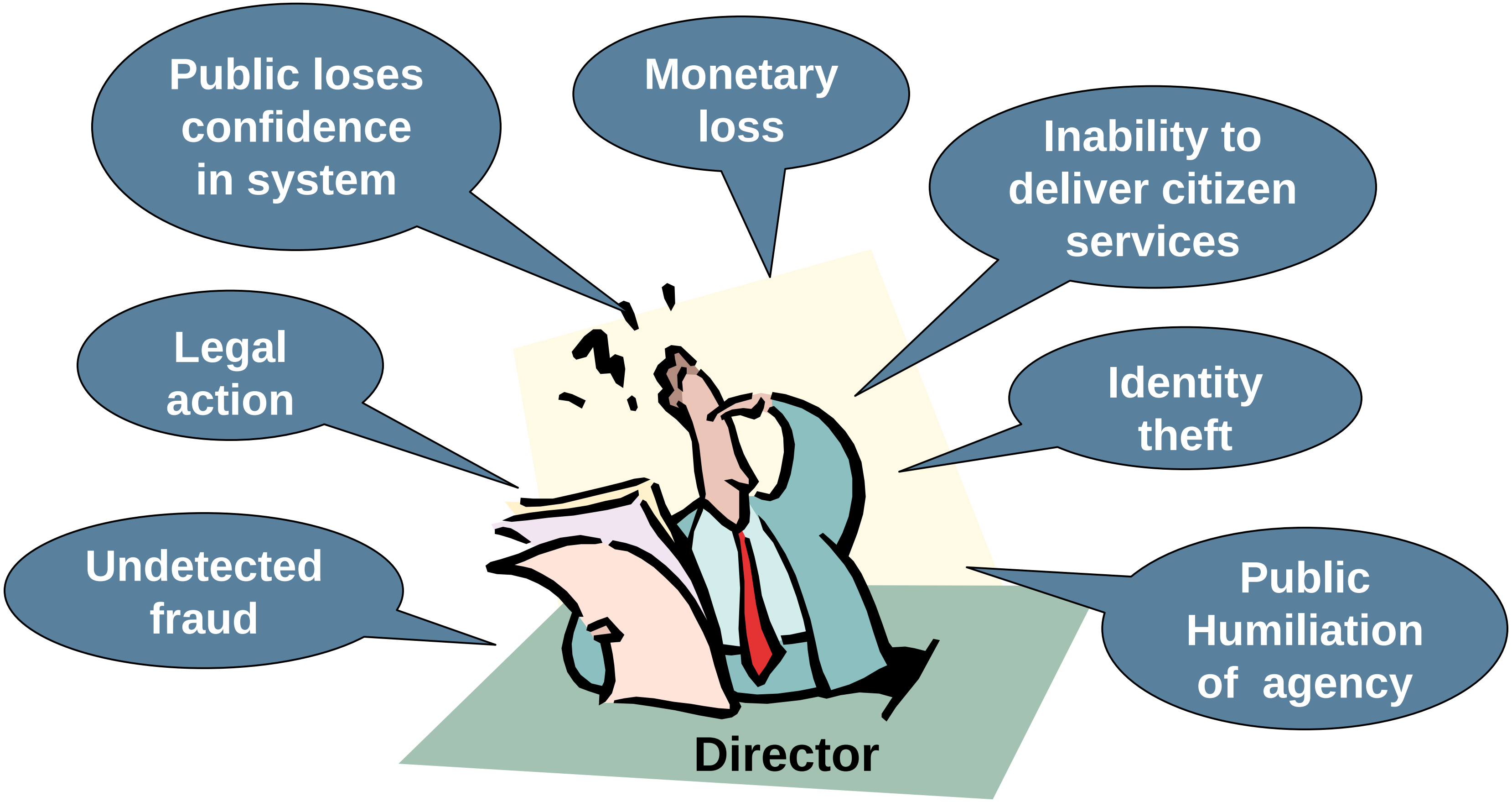
Agenda

- Why Management Needs Security Training
- What Management Needs to Know
- How to Get the Message Across

Why Management Needs Security Training

(Did not Demonstrate Due Diligence)

Security Risks are Business Issues



Public loses confidence in system

Monetary loss

Inability to deliver citizen services

Legal action

Identity theft

Undetected fraud

Public Humiliation of agency

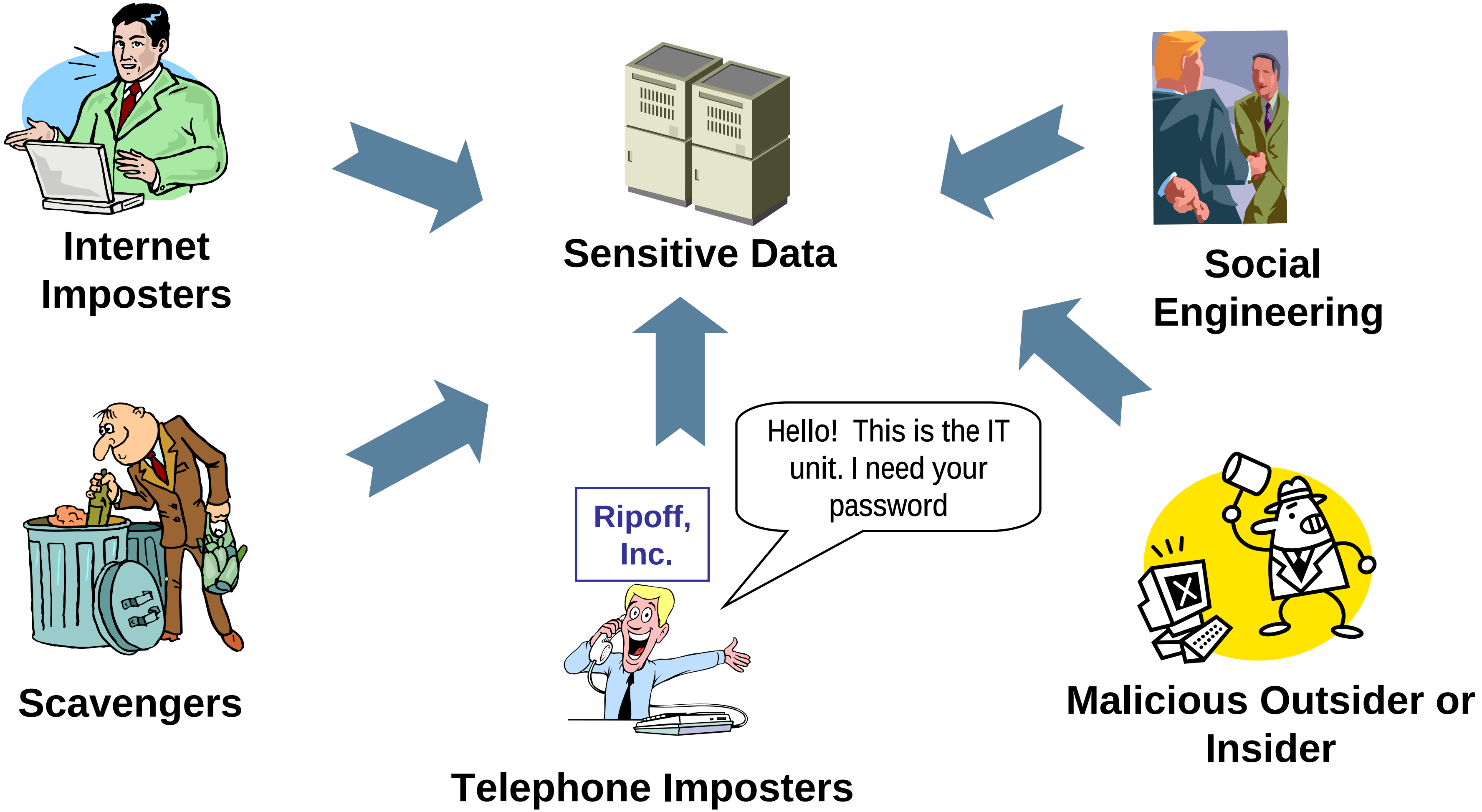
Director

Staff Security Errors Can Contribute to These Risks

Both Staff and Management Actions Contribute to the Risks

- Many staff including supervisors and managers
  - Are not aware of their organization’s security policies
  - Ignore the security policies
  - Bypass security policies to get their jobs done
- Management does not consistently enforce security policies
- Illicit insider activity often goes unnoticed

Many Non Technical Threats Exploit Vulnerabilities in Administrative Procedures



Internet Imposters

Sensitive Data

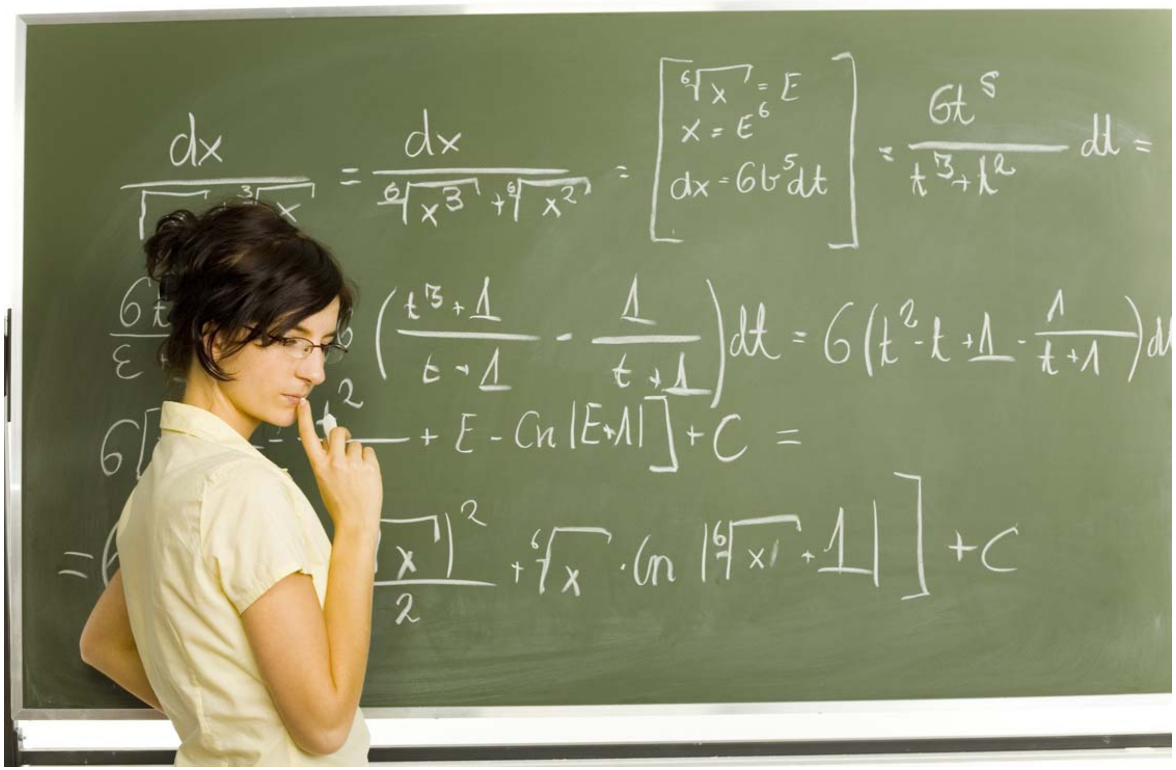
Social Engineering

Scavengers

Telephone Imposters

Malicious Outsider or Insider

What management Needs to Know



This is probably an overkill

OBJECTIVES

At the end of the training, the supervisor or manager will have tools or knowledge to

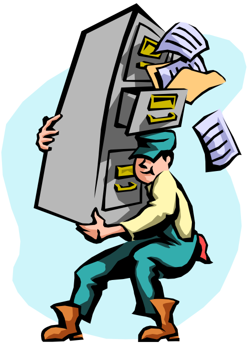
- Mitigate risks to organization due to
  - Lack of security procedures
  - Security policies not being consistently enforced
  - Ineffective security procedures
- Understand organizational security policy “in depth”
- Recognize and respond to insider threats
- Understand options for taking action to ensure that their staff follow security procedures and comply with security policies

Sample Agenda for Security Training

- Business consequences of ignoring security
- Organizational security policy and procedures
- Insider threat and anticipating security breaches
- Monitoring and enforcing security in the workplace
- Laptop security
- Protecting workstation and data assets
- Reviewing and updating administrative procedures to reduce security risk

This assumes that supervisor/manager has already received the same security awareness training as his/her staff

Business Consequences of Ignoring Security
- Recently in the News -



- U.S. Consulate Mistakenly Sells Secret Files in Jerusalem – personal information on US Marines and other sensitive information found in file cabinets auctioned off in Jerusalem.
- EXCEL spreadsheet with personal data on employees e-mailed to healthcare insurance company by company benefits employee
- Bank employee accessed and sold at least 240 bank documents with customer loan information and account numbers
- Flash Drive misplaced or lost exposing personal information for thousands of persons
- Mortgage broker discards consumer tax returns, credit reports and other sensitive personal information in an unsecured dumpster
- Paper manufacturer gets a load of mortgage applications in truckload of paper sent to it to be recycled.
- Benefits enrollment forms stolen from an employee’s car – includes name, address, date of birth and SSN

More Consequences of Non-technical Attacks

- Laptop stolen containing thousands of personal information records – Veteran’s administration is one example
- Delivery driver transporting hundreds of personal records to an archive site never delivers them
- Backup tapes lost in transit because they were not sent either electronically or with a qualified human escort
- Deceased employee continues to use “his” employee account as though he were still living
- Ex-employee accesses system and downloads sensitive information using account that was not disabled
- Employee uses logged in supervisor system to override and change the amount of a tax assessment
- Computer forensic evidence inadmissible in court because manager saved copies of files to another drive so that other users could access them
- Insider uses easily accessible executive secretary’s computer to track executive’s actions

Organizational Security Policy and Procedures

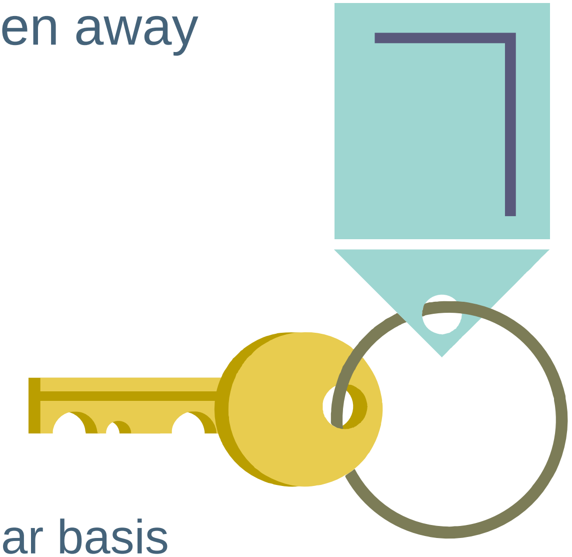
- Which policies are not understood, or often ignored?
- What policies are “missing” and need to be defined?
- What is the intended enforcement mechanism and the penalties for violating the policy?
- Policies often mis-understood or poorly implemented are:
  - Handling Sensitive Information
  - Authorizing and de-authorizing user permissions
  - Mobile device security
  - Incident response – dealing with a possible crime
  - E-mail usage

Handling Sensitive Information

- What information is sensitive
- Rules for use – electronic, verbal, written
- Reporting loss or error
  - Accidentally sending sensitive information in e-mail
  - Sending sensitive information to the wrong person
  - Divulging sensitive information to a suspect party over the telephone
- Victim notification requirements
- Disposal requirements and procedures

Authorizing and De-authorizing Staff Permissions

- Situations where permissions are granted or taken away
  - Transfer to another group
  - Leaving the agency
  - Retiring
  - Death
- Minimizing “authorization creep”
  - Do staff still need existing permissions
  - Review permissions authorized by you on a regular basis
- Physical lock access
  - Physical keys, cipher locks
  - Change when key holder permissions are taken away



Mobile Device Security Issues

- Mobile electronic devices plugged into the USB port can function both as a computer and a storage device
  - Flash drives, USB memory sticks, Cell phones, Palm pilots
  - Gigabytes of data can be stored on a device the size of a thumb
  - Do staff bring these to work?
- Laptops may be authorized for use by some managers and staff
  - Do others bring in their own and plug them into the network?
- Wireless technology enables network connection from outside
  - Do any staff set up their own wireless access points?

SnoopStick™
From CYBERsitter®

Incident Response
- Dealing with a Possible Crime -

- Information on the computer or backup tapes can support the case that an employee has committed fraud
- Information on the computer can support the claim that an employee has violated security rules or performed illegal actions
  - Porn or porn site cookies
  - Personal business or gambling
- Modifying information on the computer or just viewing it by executing commands can contaminate evidence
- Modifying information on the computer can implicate supervisor as party to the crime

Supervisors generally are not permitted to monitor staff calls, rummage through staff belongings, or log onto staff computers without authorization from upper management

Business E-mail Usage

- Lack of privacy
  - Equivalent to sending a postcard
- Inability to ever fully erase
  - Remains in your computer
  - Remains in recipient’s computer
  - Stored in backups that may be around for nearly forever
- Ease of accidental sensitive information compromise
  - Staff erroneously adds the wrong “Mary Smith” to the addressee list
  - Sensitive mail sent to a large group rather that just the intended party
  - Sensitive information accidentally sent by echoing the original e-mail (containing sensitive data) with the reply - implicates you for compromising sensitive information
  - Attachment sent includes lists of customer or employee sensitive information

Insider Threat and Anticipating Security Incidents

- Insiders can bypass physical and technical security measures designed to prevent unauthorized access
- Are aware of vulnerabilities, such as loosely enforced policies and procedures or exploitable technical flaws
- Be aware of employee behavior patterns or traits
  - Social and personal frustrations (family, peer, coworkers)
  - Ethical ‘flexibility’ (if it is not secured, then I can use it)
  - Reduced loyalty (reductions in force, changing allegiances)
  - Entitlement (I’m not getting paid what I should, I don’t get enough recognition for what I do)
  - Lack of empathy (anger at authority)
- Any of these behaviors is NOT an indicator that an employee WILL do harm to the organization, but it may be a warning sign
- Illicit actions could be a result of an acute stressful situation, financial problems, revenge, failure of peers and supervisors to intervene in earlier episodes

Reference - The Insider Threat to Information Systems, Security Awareness Bulletin No. 2-98.

Enforcing Security Policy

- Periodically walk through work area looking for
  - Sensitive information left unattended
  - Sensitive information in wastebasket
  - Passwords left in the open
  - FAX information left on machine
  - Sensitive information left on printer
  - Unattended workstation that is enabled (logged in)
  - Doors propped open
- Enforce policies consistently among employees

Workstation Security

- Logged in **supervisor** or **manager** workstations are more vulnerable than staff workstations
  - Management has more privileges than other staff
- Always enable screen lock when leaving your office or work area
  - You can be implicated in fraud if someone performs transactions on your computer
  - You can be implicated for porn viewing, gambling, etc. if staff or visitors “borrow” your computer
- Also train your executive secretary to lock workstation – (another person with access to privileged information)

Laptop Security

- Never leave the laptop unattended - no place is safe
- Never leave a laptop in you car viewable from the window
- When traveling by air, never take your eye off the laptop while going through the security checkpoint
- Use a non-descript carrying case to carry your laptop
- Use disk encryption
- When possible, keep data on external media
- Don’t tape your password to the laptop
- Transfer collected data to a protected server and remove information from the laptop as soon as possible
- Disable the wireless connection if not currently in use
- Beware of free Internet access
  - Information can be intercepted and read unless encrypted in transit
  - Malware can be downloaded to your computer

Reviewing and Updating Security Procedures

- Many procedures have not been updated to deal with changes in technology
- Technology often not used to help implement procedures
- What procedures are ineffective?
- What procedures stand in the way of real work?
- Use an exercise to redesign a procedure that is typically either bypassed or ignored

Resources for Developing Training Materials

- Results of organizational security risk assessment
- Organizational administrative and IT security policies
- Lessons learned from security awareness training or observed employee actions
- Recent breaches experienced by other organizations
  - Identity Theft Resource Center - http://www.idtheftcenter.org/
  - Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1, Carnegie Mellon, January 2009
  - Insider Threat Study: Illicit Cyber Activity in the Government Sector, U.S. Secret Service and CERT, January, 2008
- External research on user security compliance
  - “Data Security Policies are Not Enforced – US Survey of IT Practitioners”, Ponemon Institute, December 4, 2007
  - “The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk”, RSA, 2007
  - “The 2008 Insider Threat Survey: Workers Admit to Everyday Behavior that Puts Sensitive Business Information at Risk”, RSA, 2008

Delivering the Training

A small intimate setting would be better

Training Delivery Options

- In person training
  - Formal classroom training
  - Invited speaker to staff meeting
  - Discussion of real life scenarios specific to the organization
  - Discussion of real life scenarios experienced by others
  - Use audio clips, video clips and other resources
- Annotated briefing
  - May be used by those that have missed the in person training
  - Acts as a refresher
- CBT
- Video showing acted out security breach examples
  - Check out the DISA training videos, now on DVD – “Protect Your AIS”

Follow on Training

- Maintain ongoing awareness of new threats
- Provide annotated briefing slides that contain explanation and links to other information
- Reinforce initial training by providing security reminders or in-depth information on specific topics
  - Newsletter
  - E-mail
  - Resource website
- Update training materials at least annually

Examples of Discussion Scenarios

Rogue USB Thumb Drives

“Please be advised that two USB thumb drives were discovered on the 9th Floor of the Bicentennial Building. One was discovered in the Men's restroom yesterday afternoon. Another was found this morning on a facsimile machine. The drives contain malicious code that automatically and silently executes when the drive is plugged into a system. The code captures certain system information and transmits it out of DOJ.”

(An e-mail sent out to US Department of Justice staff)

Danger of Allowing Access Following Friendly Termination

A project leader took a new position in a different department within the same organization. Because the termination was mutually agreeable, he convinced supervisors in his former department to permit him to retain an account on their system, although with lower access rights than before. That access combined with his knowledge of additional access methods on the network enabled him to repeatedly increase the access rights on his account. Using the elevated access, he logged in after hours and accessed confidential personnel and payroll files.

Reference: Insider Threat Study: Illicit Cyber Activity in the Government Sector
United States Secret Service and CERT, January, 2008

Lock Workstation When Leaving Work Area

A water meter reader for a state water department designed a scheme to lower or eliminate water bills for customers in exchange for a fee. He used his supervisor’s computer when she was in the restroom to lower bills, a function authorized only for supervisors’ accounts. Over 18 months he reduced bills by over $325,000 for 17 customers.

Reference: Insider Threat Study: Illicit Cyber Activity in the Government Sector
United States Secret Service and CERT, January, 2008

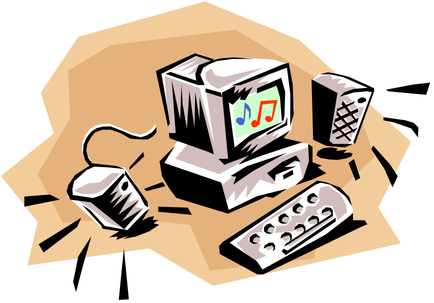
Importance of Protecting Potential Evidence

A manager suspected of fraud was placed on administrative leave. Realizing that incriminating evidence was contained on his organization’s backup tapes, he called one of his team members and told him that there was evidence on the backup tapes that would prove his innocence. The team member proceeded to obtain the tapes, took them home, and turned them over to the manager. The tapes were never recovered.

Reference: Insider Threat Study: Illicit Cyber Activity in the Government Sector United States Secret Service and CERT, January, 2008

Unattended Workstation

A short meeting was called by the Tax Department manager to inform staff of new procedures that were being implemented throughout the department. Knowing that most staff in the area would be away from their desks, a contractor that had access to the area found a workstation that was logged into the Tax system. The person then sat at the workstation and proceeded to lower the tax assessment for several persons with which he had illicit associations.



What Would YOU Do ?

A person unfamiliar to you is in the cubicle next to you taking apart your co-worker's workstation. He looks legitimate and looks like he knows what he is doing but you don't remember hearing your co-worker complain that her workstation was not working.

What Would YOU Do ?

A person filing a claim brings her child to the government office with her. The child is restless and starts to wander around the office. He sees an unattended computer in a nearby workarea, sits down at the computer and begins to surf the web.

What Would YOU Do?

A seemingly familiar person, perhaps a co-worker has got his hands full of goodies which he is trying to deliver to a restricted area such as a computer room or data preparation area. Do you use your access card to let him in?

Concluding Remarks

- Not all security breaches can be prevented by technology
- Supervisors and managers are the front line enforcers of security policy implemented via administrative procedures
- They can prevent and detect security errors before they affect the organization
- Fewer security breaches means less expenditure for cleanup

Providing Security Training for Management is a Good Investment

Contact Information

Jane Powanda
Noblis
jpowanda@noblis.org

301 513-0143

noblis™
For the best of reasons

Questions?