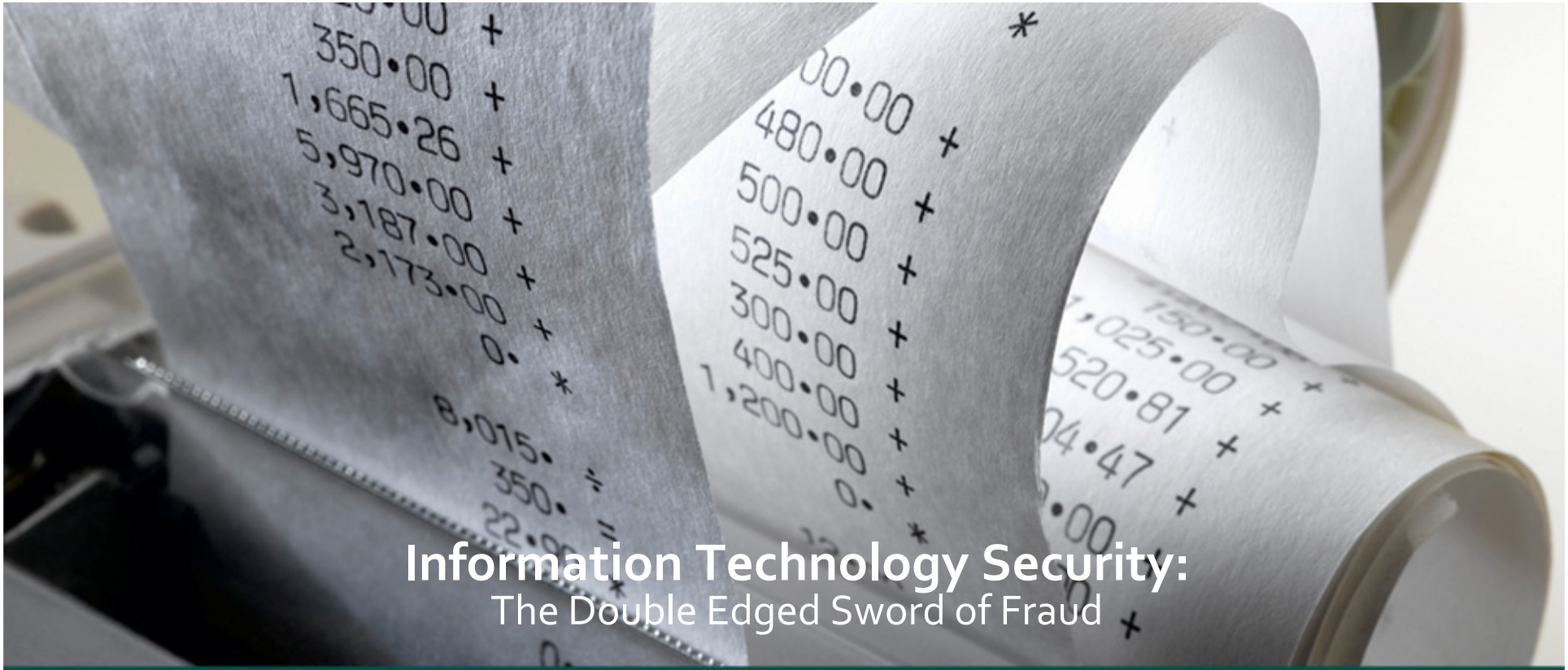


Information Technology Security:
The Double Edged Sword of Fraud

2011 WGFOA Winter Conference

December 1, 2011 – Green Bay, WI

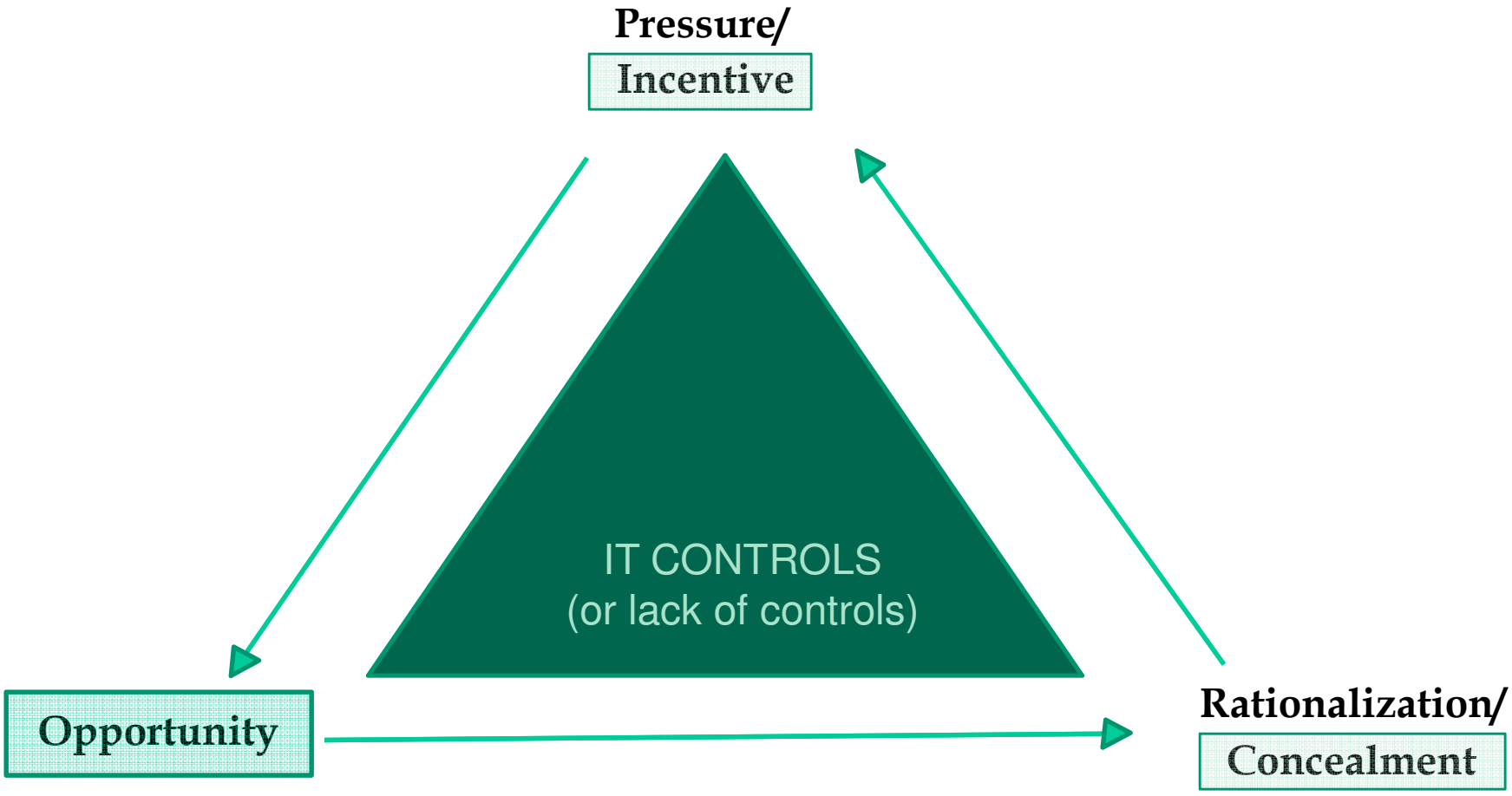
Jeffrey T. Lemmermann, CPA, CITP, CISA, CEH
Jeff.Lemmermann@cliftoncpa.com

WGFOA
WISCONSIN GOVERNMENT
FINANCE OFFICERS ASSOCIATION

Clifton Gunderson LLP
Certified Public Accountants & Consultants
COUNT ON INSIGHT®
www.cliftoncpa.com

TUNDRA LODGE
Resort & Waterpark

The Fraud Triangle



Fraud: Preemptive Tools

- Segregation of Duties
  - Rights Management – Least privilege accounts.
  - Smaller Organizations – Create oversight through reporting.
  - Account Review Procedure – Terminations / Movements
- User Awareness Training:
  - How to watch for external fraud attempts.
  - Social Engineering
  - Explain the controls that have been implemented.
  - Computer Use Policy – notification of right to trace actions.
- Ethical Considerations
  - Control access to implemented tools
  - Ensure proper and ethical use

Fraud: Detective Tools

- Computer audit logs
  - Enable auditing (default is normally not enabled)
  - Ensure size is sufficient (avoid overwriting)
  - Copied to remote storage/permanent media on regular intervals

- Utilize other logging tools:
  - Keystroke Loggers
  - Screenshot Recording
  - Shadowing Capabilities
  - E-Mail and Instant Messaging Archives

- Ethical Considerations
  - Control access to implemented tools
  - Ensure proper and ethical use

Data Security

Security Awareness Program: Tone at the top.

- Case Study: Open Records
  - How "open" do you mean?

Importance of Data Security

- Regulations
  - HIPAA
  - GLBA / SOX 404
  - FACTA
  - Red Flag Rules
  - PCI Standards

- Publicity

  "No such thing is bad publicity …except your own obituary."

  - Brendan Behan, Irish Dramatist

  - *Damage to reputation.*
  - *Loss of consumer confidence.*
  - *Redirection of resources*

City College of San Francisco

Names and S.S. #'s of 11,000 Posted on Web Site

Iowa Department of Education

160,000 personal records in file on hacked web site

Chicago Board of Elections

S.S. #'s, Birthdates, and Addresses of 1.3M voters on missing discs.

Morgan Stanley

Misplaced Data Tapes leads to courtroom loss…

Regulation Changes

Changes to the Federal Rules of Civil Procedure

Enacted December 1, 2006

1. **<u>Electronic documents are treated the same as physical documents!</u>**

2. **Requires Organizations to know what data you have and in which format it exists.**

3. Forensic Professionals on many sides of a case:
   1. Recovering lost or unintentionally deleted items
   2. Producing evidence that opponent said was not available

4. Handling of computer evidence
   1. Preserve evidence
   2. Maintain chain of custody

Computer Fraud – First Steps

1. Stop using compromised system!
   - Every action changes computer environment
   - Preservation of hard drive and memory contents

- Isolate System
  - Physically disconnect system from Internet if exposed
  - If intranet threat is possible, isolate from local network

1. Record visual information from PC
   - Running applications
   - Items in system tray

2. Utilize drive duplication tools to create copy of drive
   - Refer to item #1
   - Allows for other tests to be tried without losing original evidence

- Case Study: Preservation of Evidence

  – Understanding Your Environment

Regulation Changes

Changes to the Federal Rules of Civil Procedure

Enacted December 1, 2006

1. **Electronic documents are treated the same as physical documents!**

2. **Requires Organizations to know what data you have and in which format it exists.**

3. Forensic Professionals on many sides of a case:
   1. Recovering lost or unintentionally deleted items
   2. Producing evidence that opponent said was not available

4. Handling of computer evidence
   1. Preserve evidence
   2. Maintain chain of custody

Where Is Your Data?

You can't control what you don't know about

- The Obvious
  - Network File/Data Servers
  - Laptop Computers
  - Backup Storage Media
- The Obscure
  - Smartphones
  - Portable Storage (USB Drives)
  - E-Mail Attachments
- The Forgotten
  - Disposed Equipment – LEASED Equipment!

Proper Disposal Rules

"Disposal practices that are reasonable and appropriate to prevent unauthorized access to –or use of- information in a consumer report."

- Burn, pulverize, or shred papers so they cannot be reconstructed.
- Destroy or erase electronic files or media so information cannot be read or **reconstructed.**
- Conduct due diligence and hire a document destruction contractor.
  - Due diligence could include:
    - Reviewing contractor's independent audit
    - Obtain information from several references
    - Require certification by recognized trade association
    - Review contractor's information security policies or procedures

Hard Drive Data

- Study of 2nd Hand Drives
  - O & O Company:
    - 2004: 88% of Disks from EBay contained recoverable data.
    - 2005: 71%
  - Journal of International Commercial Law and Technology
    - 2006: 48%
    - 2007: 40%
    - 2008: 44%
- Type of recoverable data:
  - Internal company memos
  - Legal correspondence of governmental agency
  - Credit ratings (Bank owned hard drive)
- File erasing Utilities
  - Eraser (Freeware - up to 35 overwrite passes)
  - Steganos Security Suite (up to 100 passes)

- Demo: USB File Recovery

An disappearing act.

Security Points

Five Key Points of Data Security:

- Physical Security
- Network Security
- Application Security
- External Security
- Planning & Governance

Physical Security

- Access to Equipment
  - Locked server room, mobile equipment logs
- Theft Prevention Procedures
  - Cameras, user policies on mobile equipment
- Separation of Duties
  - Ordering / Inventory separate from Installers
- Hardware Inventory
  - Serial numbers, internal configurations, assignments

Network Security

- Password Policies
  - Minimum characters, forced changes, complexity
  - No sticky notes!
- Unattended Terminal Protection
  - Password protected screensavers, firm policies
- Network File Structure Security
  - User site of files, annual review process!
- Auditing Logs
  - Activate logging, review logs
- Control of Backup Tapes
  - Physical security, password protection

Final two items: preservation of evidence for tracking activities

Goals of Computer Forensics

Preservation of Evidence

Adherence to carefully developed set of procedures that address security, authenticity, and chain-of-custody.

Analysis of User Activity

Reporting of all user activity on computer and company network including, but not limited to, e-mail, Internet and Intranet files accessed, files created and deleted, and user access times.

Password Recovery

Accessing and recovering data from password protected files.

Password Recovery Demo

- Dictionary Based Attacks
  - Standard Language Dictionaries
  - Specialized: medical, movies, sports
- Brute Force Attacks
  - Importance of length & special characters
  - Reliant on computer processing power
- Rainbow Tables
  - Flaw in hashing techniques
  - Generate all password hash posibilities
- Social Engineering
  - Password guessing
  - Trick into giving password

Password Recommendations

- Secure Password Techniques:
  - Use modified pass phrases
    - 4score&7yearsago
    - Let'sg0r3d
  - Connect words with modifier in middle
    - Milwaukeejtl07Bucks
    - Aries01thejtlram
  - Stick with constant formulas
  - Use secure password database managers
    - PC / PocketPC – KeePass (http://keepass.sourceforge.net)
    - Android – KeePass, LastPass, SplashId
    - iPhone / iPad – DataVault Password Manager (iTunes store)

Application Security

- Key Application Security
  - Accounting, HR, or other sensitive data applications
  - Follow password standards of network
  - Segregation of duties / Reporting Controls
- Anti-Virus Protection (Symantec, McAfee, etc.)
  - Server based, automatic updates of workstations
  - E-mail protection
- Patch Maintenance
  - Windows Update Services
- Employee Training
  - Dangerous Files, E-Mail Concerns, Web Surfing
- Spyware Protection

Spyware – Detecting & Eliminating

- Signs you have been infected:
  - Random "Security" Pop-up windows appear when browsing.
  - Normal home page has been replaced.
  - Drop in computer performance.
  - New search bars have appeared in web browser.
- Removal help:
  - Cleaning Programs: ComboFix, SpyBot Search & Destroy
  - Monitoring & Prevention: SuperAntiSpyware, MS Defender
- Other Tools:
  - Startup Inspector
  - Pop-up Blocker - Google
  - www.processlibrary.com

External Access Security

- Cannot have without other elements!
  - Weakness in other areas can defeat the best external security.
- Access method security (vpn, citrix, etc.)
- Data Encryption
- User Education
  - Activities to avoid
  - Popular methods of capturing data:
    - Shoulder surfing
    - Key logging / capturing programs
    - Packet sniffing
    - Wireless worries

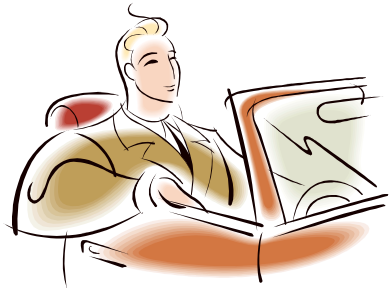
Wireless Security

- Control Access
  - Change Defaults!
    - Administrator Password
    - Network SSID
  - MAC Filtering
    - List of authorized wireless Ethernet cards
  - Minimize Access Points
    - Scan self for “rouge” access points
      - Heatmapper
      - WiFi Analyzer (Android Tool)
    - Control own equipment’s access

Wireless Security

- Control Data - Encryption
  - WEP – Wired Equivalency Protocol
    - Set to highest level supported
    - WEP has deficiencies:
      - Both 40-bit and 128-bit keys have been hacked
      - Use still will prevent or delay hack attempts
  - WPA – Wi-Fi Protected Access (WPA2)
    - Subset of developing 802.11i Standard
    - Some devices updateable to support standard

- Case Study: Wireless Risks
  - The "Cantenna" T.J. Maxx Breach



Planning & Governance

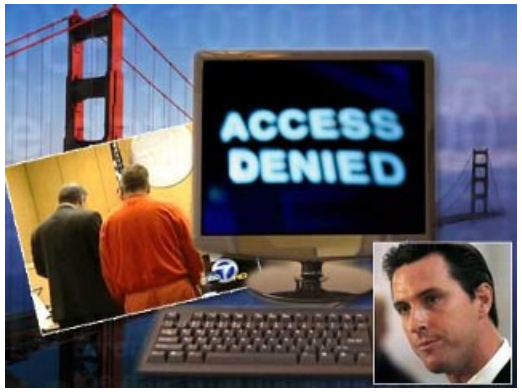
- Align IT Goals with Business Goals
  - Does the IT Department work for you or run you?
  - Is IT Planning part of the overall strategic planning process?
  - Steering committee: department head involvement!

- Must-Have Plans:
  - Disaster Recovery \ Business Continuity
    - Testing!
    - Involvement of all departments – what are their needs?
  - Incident Response Plan
    - Data disclosure events
    - Contact Requirements

Policies & Procedures

- Policies in general:
  - Signature requirements \ acknowledgement
  - Redistribution of policy \ general availability
  - Centralize & minimize total number
  - Training opportunity on changes!
- Important groupings:
  - Computer Use Policy
    - Internet / Email Use
    - Personal Devices / Social Networks
  - IT Security Policy
    - Confidentiality statements
    - Data handling and storage
    - Data retention & destruction

- Case Study: The City of San Francisco



  - Who's network is it anyway?
    - Terry Childs – Cisco Certified Internetworking Engineer
    - Built & Managed the city-wide network (core of all attached networks)
    - Elevated rights to sole administrator – <u>always</u> on call

Understand Your Enemies

- You have to understand their tactics to better stop them.
  - **Hacking for Dummies** by Kevin Beaver, Stuart McClure
  - Certified Ethical Hacking – Training & Certification
    - Vulnerability Assessments
    - Penetration Testing

Attack Origins

Points of Origins of Network Attacks

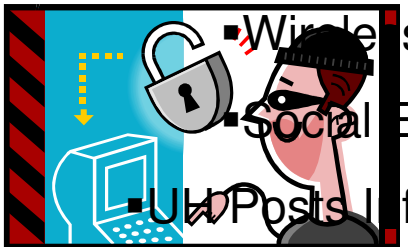
- Internal
  - Harder to protect against – productivity vs. security
  - Motivations:
    - Personal Gain
    - Revenge (Missed promotion, about to be fired)
    - Job Security
- External
  - Hard to identify source
  - Motivations:
    - Random Attack
    - Revenge (Former employee, angry client, competitor)
    - Industrial Espionage

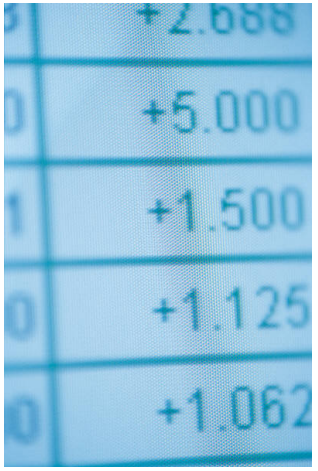
A Typical IT Hack

- SS's Information
  - Employee
  - Customer
  - Vendor

Unethical Hacker

- UH Steals Information
  - Cracks Database
  - Wireless Sniff
  - Social Engineering
  - UH Posts Information





SS's Information

Organization Data Store

- HH Buys Information
  - Transfers Money
  - Opens Charge Account

Other Threats:

- Phishing
  - Banking Spoofs
  - E-Bay Accounts
  - Other Examples
  - New Evolution: Pharming
    - "Poisoning" of DNS Record to redirect request
    - Site could be exact duplicate of intended site
- Malware
  - Key-loggers
  - Screen Capture Programs
  - Browser Hi-jacks

Scanning Yourself

- Footprinting
  - Gaining parameters of network
  - Areas of search
    - Google Searches
    - Usegroup/Newsgroup Searches
    - ARIN Records – DNS Stuff
- Vulnerability Assessments
  - Finding rabbit holes - weak points in your network
  - Online Tools
  - Nessus (www.nessus.org)
    - Registered vs. Direct Feed
    - Windows & Linux Versions
    - External Use
    - Internal Use
- Penetration Testing
  - How far down does the rabbit hole go?
  - Care in performing exploits – not for amateurs!
  - Metasploit

Questions & Answers

"There is no branch of detective science which is so important and so much neglected as the art of tracing footsteps."

- Sherlock Holmes, "A Study in Scarlett"

Jeffrey T. Lemmermann, CPA, CITP, CISA, CEH
IT Security Practice Manager
Clifton Gunderson LLP
10700 Research Dr. - Suite 200
Milwaukee, WI 53226
(414) 721-7558 Phone
Jeff.Lemmermann@cliftoncpa.com