ISACA®
Trust in, and value from, information systems
San Francisco Chapter

G32

The Changing Influences of Social Media, WikiLeaks and Whistleblowers

Future of IT Auditing: A **Definitive** Landscape

Back to Business

Agenda:

- Part One: Social Media
  - Bart (The Metaphor), WikiLeaks, OpenLeaks, LulzSec, and Anonymous et al. . .
- Part Two: Whistleblowers - A Growth Industry
- Part Three: Auditors and Their Reputation When Dealing With Fraud
- Part Four: What's Over The Horizon
- Part Five: Take Aways (aka: Tool Time)

Bart: The Metaphor

- Bart The Story
  - Who was impacted
    - Commuters, Police, Employee's of BART and Protesters
      - Friend's and Family
- Tools Used
  - Social media, Facebook, Twitter, et al. . .
    - Side Bar: Facebook handed $40,000 to hackers for finding flaws in its website as part of its Bug Bounty scheme. Facebook joins a growing list of companies, including Google, which pays **independent hackers** for this sort of information.

WikiLeaks, Its Influence. . .:

- Leaked Documents Suggest China Might Have The Upper Hand in Cyber War. . .
  - "According to US investigators, China has stolen terabytes of sensitive data, from user names and passwords from State Dept. computers to designs for multi-billion-dollar weapons systems," wrote Brian Grow & Mark Hosenball in a report for Reuters.
  - They credit **WikiLeaks** for revealing previously secret details about China's ongoing cyber assault, which the US government has code named Byzantine Hades. Specifically, they wrote, the State Dept. cables that WikiLeaks published show that the Chinese military was the source of those attacks, **not some rogue hacker group**. . .

WikiLeaks:

- A Tool For Whistleblowers
  - "A senior advisor to Gordon Brown put pressure on the commander of NATO forces in Afghanistan to play down the "**bleak and deteriorating**" situation to reduce criticism of his government, leaked documents disclose. Brown, the prime minister at the time, visited the country and met General Stanley McChrystal, the US military commander . . ."

OpenLeaks Joins The Crowd. . .:

- **26th January 2011, OpenLeaks goes public**
  - OpenLeaks considers itself a non-profit community and service provider for whistleblowers and organizations, media, and individuals who engage in **promoting transparency**. It makes leaking at a local, grassroot level possible and allows for certain scalability.
    - OpenLeaks will not accept or publish documents on its own platform, but rather create many "digital dropboxes" for its community members, each adapted to the specific needs of our members so that they can provide **a safe and trusted leaking option for whistleblowers. . . .**

OpenLeaks:

- Besides developing and building the technical platform, we want to **encourage leaking** all over the world while minimizing risks for **whistleblowers**.
  - The split between submission and publication of leaked documents makes the whole process safer for all who participate in it, and at the same time makes scaling so much easier. Watch our video, which explains this concept visually.

LulzSec: Another Member of The Social Media 'Hive'. . .

- LulzSec 'takes down' CIA website
  - The hacker group Lulz Security claims it temporarily brought down the public-facing website of the US Central Intelligence Agency.
  - Lulz Security attacks
    - » **May 10:** Fox.com user passwords,
    - » **May 15:** Database listing locations of UK cash machines,
    - » **May 23:** Sony music Japan website,
    - » **May 30:** US broadcaster PBS. Staff logon information,
    - » **June 2:** Sonypictures.com user information,
    - » **June 3:** Infragard website **(FBI affiliated organization),**
    - » **June 3:** Nintendo.com,
    - » **June 13: Senate.gov** - website of US Senate,
    - » **June 13:** Bethesda software website, user information

LulzSec:

LulzSec Opens A Hack Request Hot Line. . .

- Callers are met with a recorded message, in a heavy French accent, by an individual named Pierre Dubois. The (614) area code appears to relate to the state of Ohio. . .
  - LulzSec accesses 62,000 email addresses and passwords belonging to victims such as IBM, as well as state and federal governments. Affected agencies include but not limited to: US Army, Navy, and Air Force, FCC, US National Highway Traffic Safety Administration, Veteran's Administration and the US Coast Guard.

Anonymous: One Among Many. . .

- Sets An Example:
  - **The HBGary hack**
    - HBGary Federal position themselves as experts in computer security. . .
    - HBGary Federal **CEO Aaron Barr** thought he had unmasked the hacker hordes of Anonymous and was preparing to name and shame those responsible for co-ordinating the group's actions, including the denial-of-service attacks that hit MasterCard, Visa, and other perceived enemies of WikiLeaks late last year. . .

Anonymous. . . All Ages, All Walks of Life:

- Here's What They Can Do
  - When Barr told one of those he believed to be an Anonymous ringleader about his forthcoming exposé, **the Anonymous response was swift and humiliating**.
    - HBGary's servers were broken into,
    - its e-mails pillaged and published to the world,
    - its data destroyed,
    - its website defaced.
  - As an added bonus, a second site owned and operated by Greg Hoglund, owner of HBGary, was taken offline and **the user registration database published**.

Anonymous. . . From Europa:

- Say Brie. . .

In Conclusion, The Future of Social Media:

- Welcome To The New World of Privacy. . .

Part Two:
Whistleblowers A Growth Industry

- Enron Whistleblower. . . The Use of Dodd-Frank Whistleblower Provisions
  - Sherron Watkins, former Vice President at Enron discussing the Dodd-Frank Whistleblower Provisions at an event held by the New York State Society of Certified Public Accountants on January 28th, 2011.
    - Corporate Whistleblowers
      - Will hand over corporate fraud evidence to media such as WikiLeaks rather than the SEC thereby allowing them to continue employment in the corporate world without the stigma of being a whistleblower.

Whistleblowers & The SEC, Too:

- EFFECTIVE DATE: August 12, 2011
  - SECURITIES AND EXCHANGE COMMISSION
    - Dodd-Frank requires the Commission to pay an award, subject to certain limitations, to eligible whistleblowers who voluntarily provide the Commission with original information about a violation of the federal securities laws that leads to the successful enforcement of a **covered judicial** or **administrative action**, or a **related action. . .**
    - Dodd-Frank also prohibits retaliation by employers against individuals who provide the Commission with information about possible securities violations. . .

Whistleblowers: Cut Across All Sectors

- Swiss Bank HSBC Whistleblower. . .
  - Assets of about £13bn, could net millions in pounds in unpaid tax revenues. . .
  - A disk leaked to the French authorities, is said to contain the names of **79,000 HSBC clients in 180 countries**.
  - An employee for HSBC in Geneva, leaked the data to French officials, who passed it onto the UK. **A spokesperson for HSBC said: "HSBC in no way condones tax evasion and in no way do we assist it". . .**
- SEC
  - » A **whistleblower at the SEC** has accused the agency of destroying more than 9,000 files related to preliminary investigations into SAC Capital, Bernard Madoff, Goldman Sachs and other financial groups. . . (To Be Continued).

Part Three: Auditors, Their Reputation When Dealing With Fraud. . .

"Because the determination of abuse is subjective, auditors are not required to detect abuse in financial audits. **However**. . ."

A May 2010 COSO Study Dealing With Fraud from 1998 thru 2007 for US companies:

- The most common fraud involved improper revenue recognition, next in-line was the overstatement of existing assets or capitalization of expenses
- 89% of these incidents of fraud involved executive management at the C-Level (aka: CEO's and/or CFO's)
- 347 alleged cases dealt with financial reporting
- Dollar amount of these misstatements and/or misappropriations---nearly **$120bn** USDs

Auditors & Their Reputation When Dealing With The Global Fraud Economy. . .

Global Patterns of Fraud – 2011

- Acts of fraud are rarely one-offs, 96% of fraudsters carried out fraud on a repeated basis, up from 91% in 2007
  - Fraud at the Board level increased to 18% while fraudulent activities at the C-level increased to 26%
  - 87% were male, between the ages of 36 to 45, and committed fraud against their own employer
  - 32% work in a Finance function
  - 60% worked for the company more than 5 years, 33% 10 years and most colluded with others
- So. . .where were the auditors?

Auditors & Their Reputation When Dealing With Fraud

- Motivation for Fraud
  - Personal financial gain followed by fraudulent financial reporting. . .
  - 43% misappropriate of assets (mostly due to embezzlement and procurement fraud)
    - On avg. it took 3 years from **fraud inception to detection**
    - 50% were detected through tip-offs, both formal and informal or by **accident. . .**
    - 77% of investigations **were not reported** to the public
    - 50% of the cases revealed that a red flag had existed **but was not acted upon. . .**

Part Four: What's Over The Horizon?

- "Negligence" vs "Gross Negligence". . .
  - And Negligence wins by a nose. . .
- Clawbacks. . .
  - In the last meeting under chief Sheila Bair, The Federal Deposit Insurance Corp. (FDIC) **voted five to one in favor of a "clawback" clause in new regulations,** which will allow the government to reclaim compensation paid to executives whose banks have to be taken over and wound up by the state.

What's Over The Horizon?

- Increasing Liability Financial and Otherwise:
  - In a 2008 report issued by the GAO, between 1998 and 2008 "audit firms may have paid at least 10 settlements or awards of $100 million or more from private litigation". . .
    - In mid-2008, the six largest US auditing firms were defendants in 90 audit-related suits, each of which involved damage claims in excess of **$100 million-**--- ranging up to **$10 billion. . .**

What's Over The Horizon?

- Changing Expectations of The Auditors
  - **Internal Auditors** Rule 1210.A2
    - Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud. . .

What's Over The Horizon: Changing Expectations. . .

- **External Auditors** Rule ISA 240
  - The objectives of the external auditor; to identify and assess the risks of material misstatement of the financial statements due to a fraud:
    - **Obtain understanding of the internal controls in respect of those assertions which are subject to fraud (e.g., revenue) and ensure those controls are designed effectively. If not. . . report to the audit committee. . .**
    - **To obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatements due to a fraud, through designing and implementing appropriate responses; and such responses should at a minimum include the following:**
    - **Testing the appropriateness of journal entries, especially at the end of the reporting period. Make inquiries of individuals involved in financial reporting process. . .**
    - **Communicate fraud or suspected fraud to those charged with governance**

What's Over The Horizon?

- **In the past**, generally, the auditor did not have an obligation to disclose possible or actual fraud to third parties, unless the matter is already reflected in the audit report
- However. . .

  Not any more:

  - See the moving target referred to as Dodd-Frank. . .
    - US Regulatory Agencies Modify The Rules. . .
    - US Judiciary Modifies The Rules. . .
      - » Lets all go to court. . .

What's Over The Horizon?

- The Securities Exchange Act of 1934 **Should Be Extended to Cover Transnational Securities Fraud** [Release No. 34-631374; File No. 4-617]

Part Five:
Technical Take Aways---Benford's Law

More numbers begin with 1 than with larger numbers (2 - 9)

- Benford Analysis is likely to be useful with sets of numbers that result from mathematical combinations of numbers where the result comes from two distributions
  - » Accounts receivables (number sold x price)
  - » Accounts payable (number bought x price)
  - » Most sets of accounting numbers

Expected Frequencies Based on Benford's Law

Digit	1st place	2nd place	3rd place	4th place
0		.11968	.10178	.10018
1	.30103	.11389	.10138	.10014
2	.17609	.19882	.10097	.10010
3	.12494	.10433	.10057	.10006
4	.09691	.10031	.10018	.10002
5	.07918	.09668	.09979	.09998
6	.06695	.09337	.09940	.09994
7	.05799	.09035	.09902	.09990
8	.05115	.08757	.09864	.09986
9	.04576	.08500	.09827	.09982

Source: Nigrini, 1996.

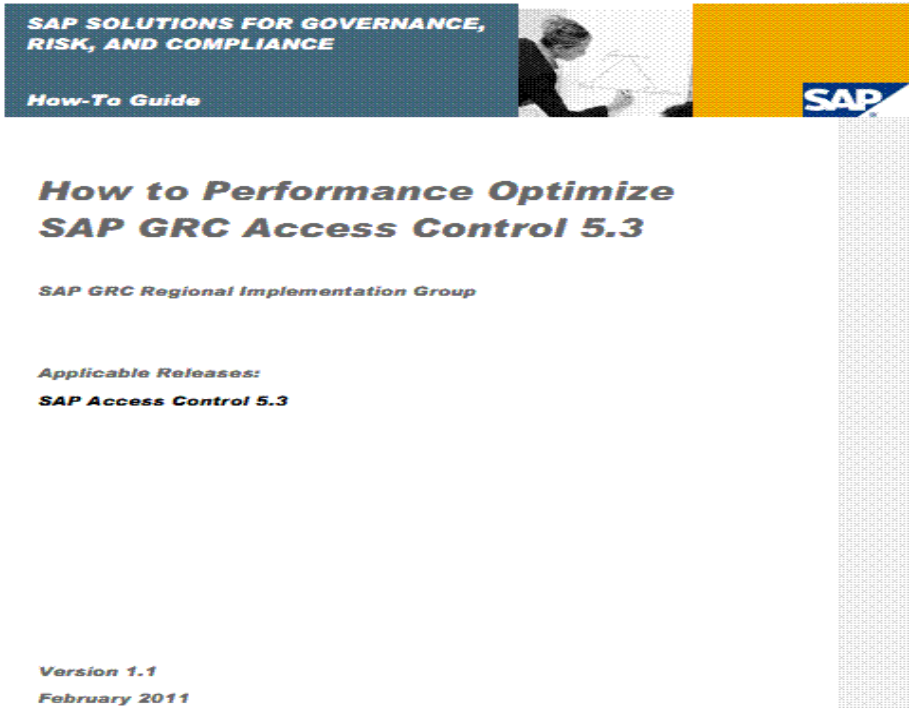
Technical Take Aways: When Not to Apply Benford's Law

- When Benford Analysis is not likely to be useful:
  - Data set is comprised of assigned numbers:
    - Check numbers, invoice numbers, Zip codes
  - Numbers that are influenced by human thought:
    - Prices set at psychological thresholds ($1.99)
    - ATM withdrawls, eg $20, $40, $60, $80, $100
  - Accounts with a large number of firm specific numbers:
    - Accounts specifically set up to record $100 refunds
  - Where no transaction is recorded:
    - Thefts, kickbacks, contract rigging, et cetera . . .

Technical Take Aways: Computer Aided Audit Techniques (CAATs)

- Benford's Law in conjunction with the following tools:
  - SAP & Oracle's EGRCM (Enterprise Governance, Risk and Compliance Manager)
    - Asking questions such as:
    - Any changes in the top 10% of transactions by value (year to year) by quarter, by month?
    - Greatest number of changes made to a customer's details file (year to year) by quarter, by month?
    - Any outliers/unusual data values?
    - Any unusual or suspicious patterns with data, dates, returns, end-of-month closeout transactions?

Technical Take Aways: SAP

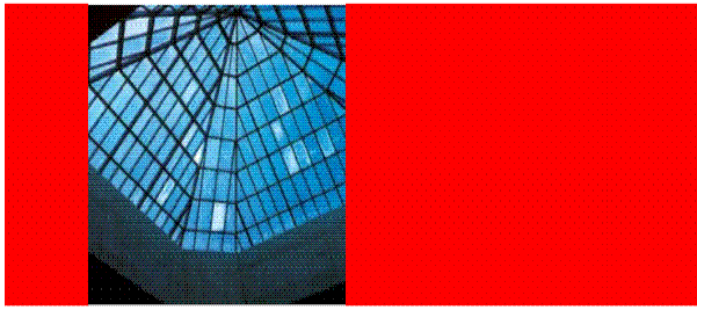


- Risk Analysis and Remediation (RAR)
- Superuser Access Management (SPM)
- Compliant User Provisioning (CUP)
- Enterprise Role Management (ERM)

Technical Take Aways: SAP's Backdoors

- Backdoors. . .
  - BACKDOORS--come about in two ways. First, they can represent access into a system that is created during the application development process and is never removed, or.
  - Secondly, after an application is put into production and sold to the customer in the field, it can represent an unauthorized and/or undetected compromise of the system for the sole purpose of securing future access to data/information for industrial or financial espionage. . .
- At a Black Hat Conference, Europa, 2010 demonstrated multiple backdoors into SAP

Technical Take Aways: Oracle



ORACLE®

Financial Audit Scoping Tool
Blueprint for Oracle GRC Applications

Implement Audit Standard 5 (AS5) scoping to streamline financial reporting compliance

- Easily set the scope of the AS5 Audit within Oracle Enterprise GRC Manager (EGRCM)
- Pre-packaged reports showing Audit coverage, status and findings

Technical Take Aways: Oracle's Backdoors

- Backdoors. . .
  - A number of modules remain un-patched and vulnerable due in part to a difficult patch & upgrade process involving complex applications in addition to an attitude that if its working, don't touch it. . .
    - » For example: National Vulnerability Database (NVD)
    - » Description: Unspecified vulnerability in the Database Control component in EM (Enterprise Manager) Console in Oracle Database Server…Oracle Fusion Middleware… allows remote attackers to affect confidentiality, integrity and availability **via unknown vectors**……(**under review**)

Technical Take Aways: In Their Defense

- Backdoors---Created and used by the vendor and created and used by individuals with criminal intent. . .can and do threaten every information system **CONNECTED TO THE INTERNET**. This is **NOT** simply a problem unique to **SAP** or **Oracle**. . .
  - Going forward are two questions you may want to ask: are there any backdoors to your system and what are they used for?
    - View a list of your vendor's backdoors. . .

Technical Take Aways: KDD, OLAP, Data Mining and Heuristic Analysis

- **KDD** (Knowledge Discovery in Databases),
- **OLAP** (On-line Analytical Processing),
- **Data Mining**
  - Multiple vendors, bumping up against a clients:
    - Lack of Confidence/Trust in the Numbers
    - Belief that data collection methodologies are flawed and that the use of the data will threaten their decision-making authority.
    - Defense against charges of negligence or gross negligence
    - Weakens the claims of plausible deniability.
    - Impacts independence and integrity of auditor's claims of non-bias, impartiality.

Technical Take Aways: Heuristic Analysis

- Heuristic Analysis is defined by the act(s) and/or processes associated with discovering the unknown thereby making it known…
- Such Tools require TESTING. . .such as EICAR:
  - EICAR is a uniquely formatted program file, is not a virus which most AV (Anti Virus) programs recognize as a test program. See also:
    - AV Comparatives
    - AV-Testing
    - ICSA Labs
    - SC Magazine/West Coast LabsVirus Bulletin?

Non-Technical: Using Your Amgydala

The Six Principles of An Auditor's Achilles Heel

- A lack of sufficient professional skepticism
- Lack of support (real or imagined) @ the C-level
- Not controlling the confirmation process especially at month end, ending quarter and year end
- Not ascertaining whether the financial statements agree with or reconcile with accounting records
- Over-relying on management (i.e., insufficient evidence to corroborate management's representations
- Not testing accuracy of computer-prepared data

Non-Technical: Using Your Amgydala & Have We Got A Tool For You. . .

- The Vulnerability Assessment and Mitigation (VAM) Methodology. . .
  - RAND Corporation developed a methodology to help analysts in:
    - » **Understanding these relationships. . .**
    - » **Facilitating the identification and/or discovery of system vulnerabilities. . .**
    - » **Suggesting relevant mitigation techniques. . .**
  - The VAM methodology takes a top-down approach uncovering vulnerabilities that are known, exploited or revealed today but also vulnerabilities that exist, yet have not been exploited or encountered to date. . .

Non-Technical: Using Your Amgydala

- Is there a Major Disconnect between the C-Level folks and their employees. . .?
  - E.g. What motivates their employees…?
    - Their answers are almost always facing 180° in the opposite direction. . .
    - See also "Kiss Up, Kick Down" corporate culture.
      - *"Social Intelligence", "Emotional Intelligence"*
      - *"Blink", "Mind Rules", and "Outliers". . .*
      - The concept of Synchronicity, (aka: your gut. . .)

In Summary: What You Have Heard Today. . .

- What steps you must take. . .to:
- Ensure your **independence**, as an Auditor. . .?
- Ensure your findings are:
  - timely, concise, clear, convincing, complete, objective, accurate and correct, with emphasis on CORRECT.
- Analyze and re-visit your First Impressions (when necessary). . .*First, Last and Always. . .*

Questions?:

- **Please Note: We'll be happy to discuss any of the issues raised this morning & best wishes the rest of the way. . .**
  - In closing, thank you for your time and attention…
  - Respectfully yours:

Pw Carey
Consultant CISA SAP GRC
Compliance Partners, LLC
Suite 200
Barrington, Illinois 60010
www.complysys.com
pwc.pwcarey@gmail.com or
pwcarey@complysys.com
1-650-267-3130 or 1-224-633-1378

Resources and References

1. *"The whistleblower's handbook: how to be an effective resister"*, by Brian Martin. Published in 1999 by Jon Carpenter in Charlbury, UK and Environbook in Sydney, Australia. This book went out of print in 2008. This is the original text, with minor changes, a different format and page numbering (89 pages instead of 167), and omission of the list of contacts (now on the web) and index.
2. *"Government Auditing Standards, August 2011, Internet Version"* (aka: The Yellow Book), GAO, United States Government Accountability Office, By the Comptroller General of the United States, Weekly Auditor Liability Bulletin 02-11-2011.
3. http://www.orrick.com/publications/item.asp?action=article&articleID=3653
4. New York State Society of Certified Public Accountants on January 28, 2011.
5. *"A Short Course on Computer Viruses"* 2nd Edition, pp 2, 49 (Dr Frederick B. Cohen): Wiley, 1994.
6. *"KPMG ANALYSIS OF GLOBAL PATTERNS OF FRAUD Who is the typical fraudster: Executive Summary"*, 2011. kpmg.com/cee
7. PwC PriceWatershouseCoopers Presentation: *"The EU Audit Directive: Auditor Liability and Auditor Independence"*, 25th May, 2011, by Gerhard Prachner, PwC.
8. PwC, UK: *Audit Today and Tomorrow*, ©2011 PwC. All rights reserved.
9. *"SAP® Backdoors: A ghost at the heart of your business"*, by Mariano Nunex DiCroce, April 14th, 2010, Black Hat Europe 2010 Briefings. © Onapsis SRL 2010 --- All rights reserved.
10. http://www.onapsis.com/research/slides/ONAPSIS-Penetration_Testing_SAP.pdf
11. *"Attacking Oracle® Web Applications with Metasploit*, by Chris Gates (carnalOwnage), RAPID7. Black Hat Washington, DC Conference, 2011. (http://www.owasp.org/index.php/Testing_for_Oracle).

Resources and References

12. *"blink: The Power of Thinking Without Thinking"* by Malcolm Gladwell, © 1997 to 2011.
13. *"Working with emotional intelligence"*, by Daniel Goleman © 1998. New York: Bantam Books.
14. *"Social Intelligence: The New Science of Human Relationships".* By Daniel Goleman, © 2006, Bantam Books. ISBN 0553803522.
15. *"Brain Rules: 12 Principles for Surviving and Thriving at Work, Home, and School"*, by John Medina, Pear Press Release Date: March 10th, 2009. ISBN13: 9780979777745.
16. *"How Does the Brain Work*?", NOVA scienceNOW,PBS Video. video.pbs.org/video/1757221034
17. *"The Criminal Mind Psychopathy as a Clinical and Empirical Construct"*, Robert D. Hare1 and Craig S. Neumann, University of British Columbia, Vancouver, British Columbia BC V6T 1Z4; University of North Texas, Denton, Texas 76203-1280
18. RAND Corp., Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology, by Philip S. Anton…[et al.]., ISBN 0-8330-3434-0
19. http://www.rand.org/content/da/rand/pubs/monograph_reports/2005/MR1601.pdf
20. David Litchfield, Oracle Forensics, The Oracle Hacker's Handbook, The Database Hacker's Handbook
21. Microsoft Excel 2000 spreadsheet: http://www.rand.org/publications/MR/MR1601