ISACA
Serving IT Governance Professionals
San Francisco Chapter

Regulation versus Reality

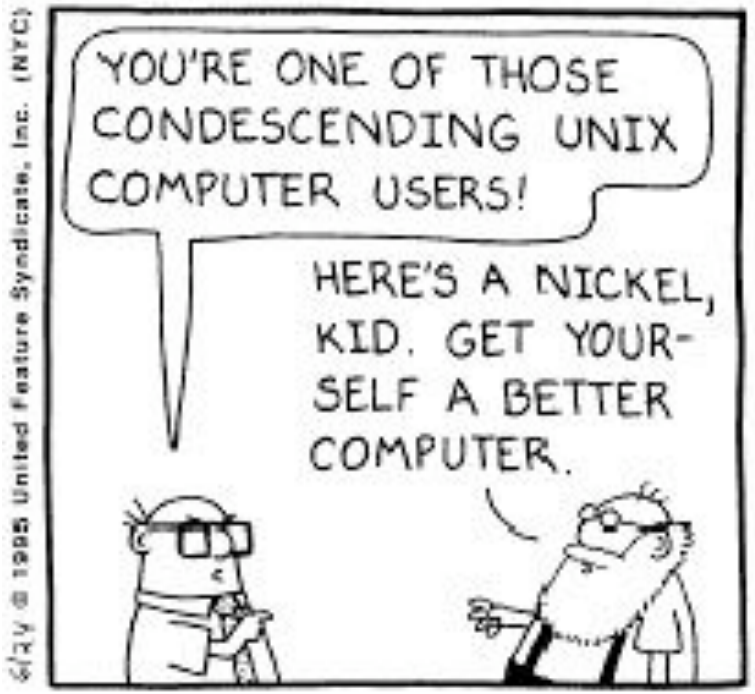
Regulatory Compliance should not be the goal of an Information Security program – it should be the result.

Introduction

(thanx Johnny for the slide)
Christian
CyberCop
CyberWarfare Researcher
CISO...

Introduction

- College Instructor – UNIX/Linux/Security



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Introduction

- and… always aspiring to be an

"International Man of Mystery!"

Introduction

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Introduction

Paul W. Poteete

CEH, CISSP, MCSE, CNE, CCA, VCP

ppoteete@gmail.com

831.333.9119

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Presentation Outline

- Introduction (complete!)
- Information Security Overview
- Regulatory Compliance
- Security Solutions
- Conclusion

Information Security

Methodologies:

Confidentiality vs. Disclosure

Integrity vs. Alteration

Availability vs. Destruction

Controlled by:

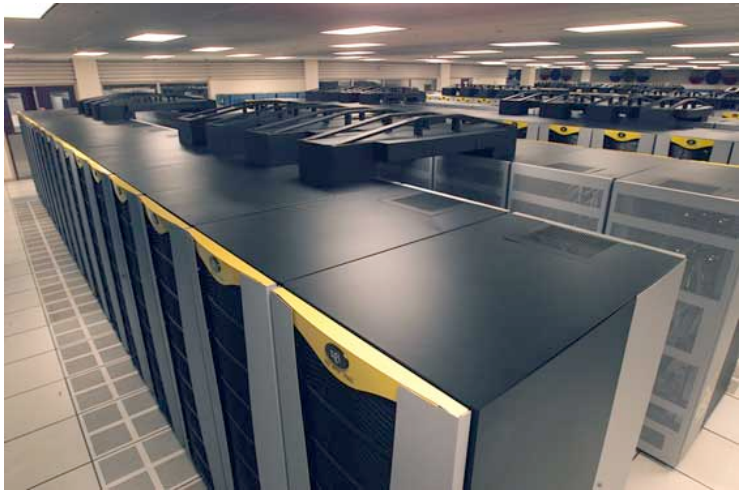
Administrative Actions

Technical Solutions

Physical Restrictions

Information Security

- Today, companies are more reliant on information technology (data) than ever before. Information Technology has become a critical component of the business architecture. Often, a firms capital budget for technology will exceed all other areas.



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Information Security

- The incredible reliance on information technology for business viability requires the implementation and systematic control of new security measures.
- Security Governance, Risk Management, and Security Program Management must be intrinsic to business process.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Information Security

Top Security Concerns (2005)

1) Insider threats
2) Spam
3) Viruses
4) Spyware
5) External Hackers
6) Theft or loss of equipment or data
7) Electronic fraud
8) Customer data breaches (Pharming, Phishing, Email, etcetera)
9) DoS attacks

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Information Security

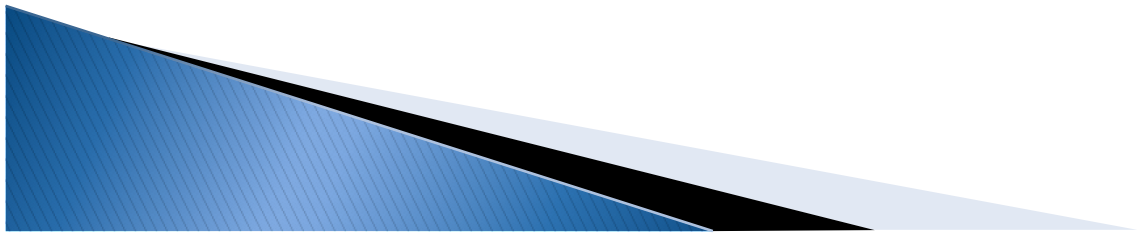
Top Security Concerns (2008)

1) Virus
2) Spyware
3) Spam
4) External Hackers
5) Insider threats
6) Auditability/compliance concerns
7) Customer data breaches
8) Theft or loss of data or equipment
9) Cost of administration

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

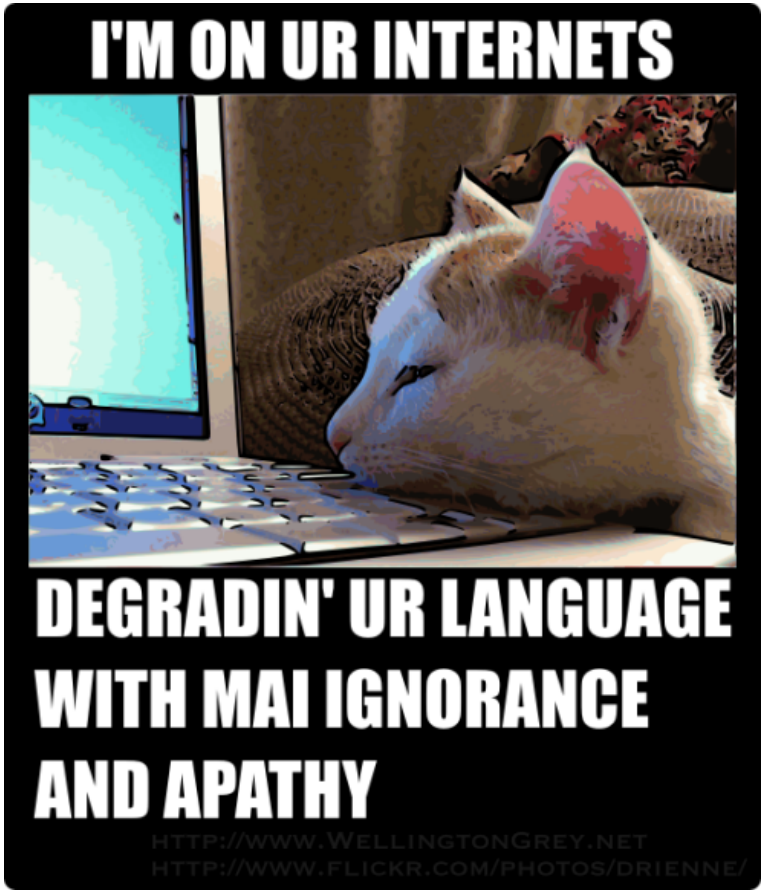
Information Security

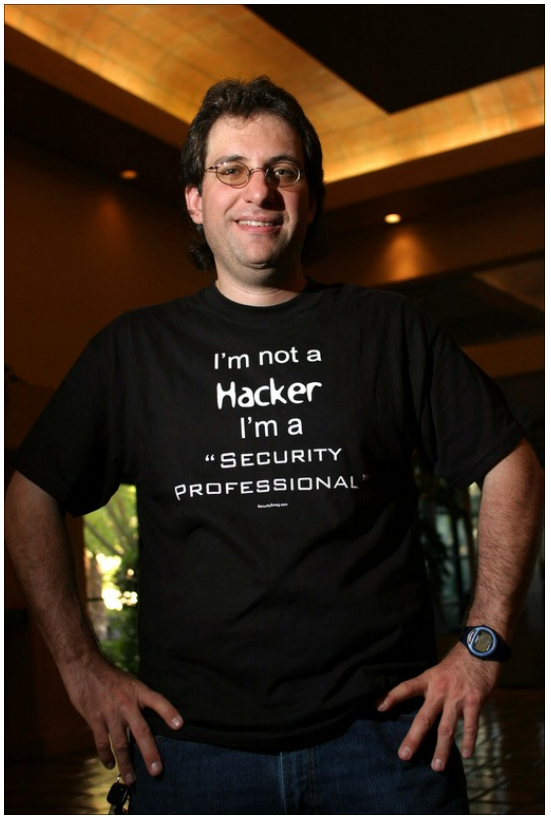
Who does this stuff?



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Information Security





ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Information Security

- Yes, the criminal hacker (or the 12 year old down the street) still makes the top 5.

- But new concerns are indicating the maturity and understanding of what security truly entails.
  - Compliance Concerns
  - Cost of Administration

Information Security

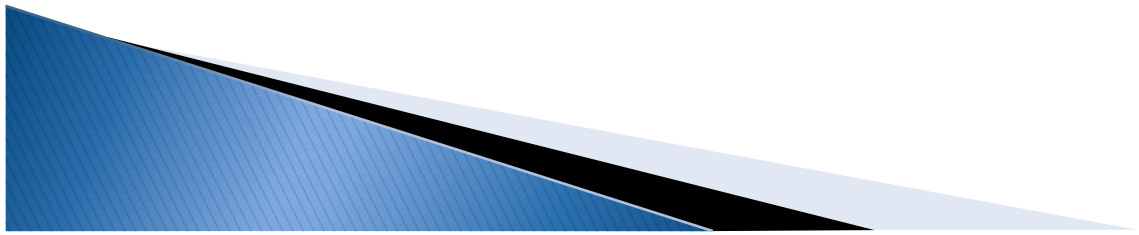
- Costs can skyrocket. The cost of IT and Security for a firm doesn't start or stop on a price tag.

- Basic Cost Functions:
  - Identify
  - Acquire
  - Implement
  - Maintain
  - Retire

Regulatory Compliance

- Enter the age of

Regulatory Compliance!



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Regulatory Compliance

- Fraud and failures to implement security controls have led to greater regulatory involvement in organizational security governance.

- We should be protecting our data from unauthorized disclosure, alteration, and destruction, not piecemeal reforms to meet basic regulatory needs.

Regulatory Compliance

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Regulatory Compliance

Oh yeah. He's also logging everything you do on WORM media at a remote location with requirements to divulge your information to third parties or law enforcement if requested.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Regulatory Compliance

- How many regulations are there?
- Thousands

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Regulatory Compliance

- **What are some of the more popular regulations?**
  - SEC 17a (3,4)
  - NASD 2210
  - NASD 2711
  - NASD 3010
  - NASD 3012
  - NASD 3013
  - NASD 3110
  - Sarbanes-Oxley
  - Investment Advisors Act
  - IDA (The Investment Dealers Association of Canada)
  - OCC Advisory: Electronic record Keeping
  - FDIC Advisory: Information Technology Risk Mgmt Program
  - Basel II
  - Gramm-Leach Bliley Act
  - California Privacy Law SB1386
  - Federal Rules of Civil Procedure

Regulatory Compliance

SEC 17a(3,4)

1) You must preserve documents and records for three to six years, the first two years of which, they must be in an accessible place.
2) All documents and records must be time-stamped, stored in a non-rewriteable/non-erasable format, organized and indexed, with a duplicate copy stored separately from the original.
3) The indexes should be also duplicated and stored separately from the original, and they should be available for examination and preserved as long as the documents and records.

Regulatory Compliance

Sarbanes-Oxley Act

1) Requires public companies save all business records, including electronic records and messages, for no less than five years.
2) All relevant audit-related documentation (including email records) must be retained for seven years.
3) Section 404 also requires companies to report on the effectiveness of internal controls over financial reporting.

Regulatory Compliance

FDIC Advisory: Information Technology Risk Mgmt Program

1) Requires encryption of electronic customer information while in transit or in storage.

Basel II

1) Banks must create internal processes to control, supervise and enforce risk management practices, including those involving internal communications.

Regulatory Compliance

Gramm-Leach Bliley Act

1) Financial institutions must ensure the security of non-public personal information; as such, they are required to maintain and store these communications in compliance with the SEC's Rule 240.17a-4 and...
2) NASD's rules 3010 and 3110 (all emails be preserved for a period of not less than six years, with the first two years in an easily accessible place.)

Regulatory Compliance

California Privacy Law SB1386

1) Businesses are required to notify California residents if personal information stored on computer systems has been breached. This regulation applies to any organization that conducts business with California residents.

- A company is exempt from the notification requirement of California SB 1386 if the personal information is stored in encrypted format.

Regulatory Compliance

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Regulatory Compliance

- PCI-DSS
  - Install and maintain a firewall to protect sensitive company data
  - Do not use vendor-supplied default passwords & security parameters
  - Protect stored sensitive company data
  - Encrypt transmission of sensitive company data on public networks
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications

Regulatory Compliance

- PCI-DSS
  - Restrict access to sensitive company data based on need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to sensitive company data
  - Track and monitor all access to network resources and sensitive company data
  - Regularly test security systems and processes
  - Maintain a policy that addresses information security

Regulatory Compliance

- In the preceding slides, do you believe that it may be possible to meet the letter of the regulation and still leave your firm vulnerable to attack and abuse?

- The PCI-DSS can point to obscure references to prove that you are out of compliance.
  - If you have a data breach; do you think that you'll pass a post-breach audit?

Regulatory Compliance

- PCI-DSS, helping the customer, or the plot of an evil genius?

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Security Solutions

Business is an art, not a science.

Be creative – not confined to a framework.

Be innovative – not critical.

Security Solutions

- Organization Security is a broad and deep topic.

- Instituting a Roadmap, a Framework (homemade is fine), and Measurement Metrics will make this navigation far less difficult and far more effective.

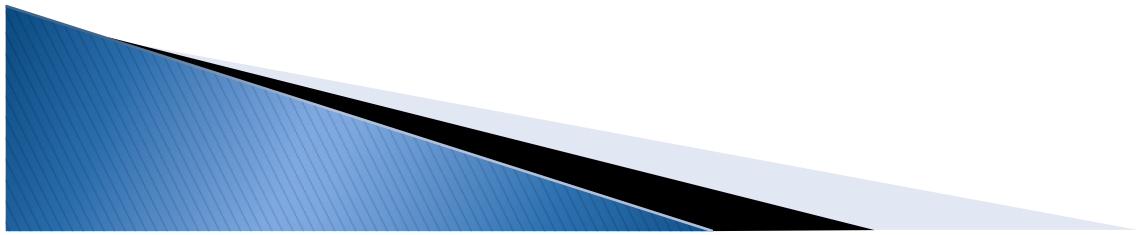
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Security Solutions

- Where are you now?
- Where do you need to be?
- How are you going to get there?

Security Solutions

Develop a Security Program



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Security Solutions

What's your Risk?

How much data do you think needs to be downloaded?
- If you database is 100GB, for 25,000 clients, a hacker doesn't need to download 100GB.

- A list of 25,000 names is only 275KBytes.

- A list of 25,000 names, addresses, account numbers, passwords, account balances, and family dog names is only about 6 Megabytes.

- - Now. How long does it take to query 6MB from a quad-core SQL server over the Internet?

Security Solutions

12 Steps to Basic Security

Action Step:

1) Security Awareness and Security Statement
(even if you don't know what you have!)

Security Solutions

Information Gathering:

2) Identify your assets and find your hidden data.
3) Determine the applicable regulations.
4) Discover network access points and try to imagine potential vulnerabilities.
5) Research the solutions for your enterprise.

Security Solutions

Communication:

6) Create a realistic plan and policy and sell it to the senior leadership.
7) Disseminate the plan.

Security Solutions

Action Step:

8) Acquire and Implement the security solutions.
9) Audit your solution. Perform "sanity checks" on your actual operations.
10) Shore-up the areas that are poorly protected or new.
11) Have third-party audits of your infrastructure.
12) Verify your compliance stance.

Security Solutions

- **Frameworks**
  - They all follow their own methodology for how security should be achieved and their own ideology for what needs to be secured.
  - Do not get caught-up in achieving compliance with the program where it doesn't make sense for your company.
  - Be innovative, don't get confined to “letter” of the framework.

Security Solutions

- **Security-Specific Management Frameworks**
  - **ISO/IEC 17799:2005**
  - **The Rainbow Books** – "Department of Defense Trusted Computer Security Evaluation Criteria" (DoD) circa 1985.
  - "**A Security Methodology for Computer Networks**" (Pierson and Witzke), (AT&T), circa 1988.
  - "**Common Criteria for Information Technology Security Evaluation**" (DoD), circa 1990
  - "**ISO15408:1999**" (DoD), circa 1999
  - RFC 2196, "**Site Security Handbook**" (Fraser), IETF circa 1997.

Security Solutions

- **Security-Specific Management Frameworks**
  - **"Open-Source Security Testing Methodology Manual"** (Pete Herzog), 2000
  - **"Octave Criteria by CERT"** (Alberts and Dorofee), 2001
  - **"Security Self-Assessment Guide for Information Technology Systems"** (NIST) 2001
  - **"Guidelines on Firewalls and Firewall Policy and Security Guide for Interconnecting Information Systems Technology"** (NIST) 2002

Security Solutions

- We have a system!

Security Solutions

- We have an accurate system!

Security Solutions

- Amazingly, criminals don't necessarily adhere to security systems protected by regulatory guidelines.

Security Solutions

"The only rules that really matter are these: "What a *man* can do," and, "What a *man* can't do."

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Conclusion – Breaches

PaineWebber

A former systems administrator for UBS PaineWebber was sentenced to over eight years in jail and fined $3.1 million last week after he was found guilty for leaving a logic bomb on UBS' systems and trading securities on the assumption that the company's stock would fall.

- He was a trusted insider who went bad
- Logic bombs are a form of malware, but like 0-Day viruses – almost impossible to prevent.
- He needed privileged access to the company's IT assets.
- Change management process controls COULD NOT prevent the bomb being installed
- There was legal and presumably corporate policy noncompliance
- The risk of recurrence presumably remains

Conclusion – Breaches

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Conclusion – Breaches

Steven E. Hutchins Associates

A Florida woman, fearing she was about to be fired from her job, was arrested this week for allegedly deleting seven year's worth of her employer's architectural data.

Marie Cooley, 41, was arrested after entering the offices of Steven E. Hutchins Associates in Jacksonville, Fla., and deleting $2.5 million in files after seeing an advertisement for a job similar to hers in classified advertisements.

Conclusion – Breaches

Medco Health Systems

A New Jersey man this week was sentenced to more than two years in prison for planting a “logic bomb” on the network of his former employer in a failed attempt to destroy sensitive health care data.

Yung-Hsun Lin, 51, of Montville, was sentenced to 30 months in federal prison by U.S. District Judge Jose Linares, who also ordered the former systems administrator to pay $81,200 in restitution to Medco Health Systems.

Conclusion

- Vulnerabilities will be present in your system.
- Exploitation of those vulnerabilities may occur.
- Proper management of identifying and correcting those issues could be the defining moment surrounding your organization's survival.

Conclusion

- Business is an art, not a science.
  - If you create security processes that confine business operations to specific scenarios, you will cause damage to the firm. Much of what is done in business is not based on strict formulas. "Cold call" lists may or may not return a result. Marketing projections might produce nothing. Advertising may return nothing but a tear in the bottom line.

Conclusion

- As we create additional requirements for our staff, we diminish our creativity and performance. If you have to jump through 6 hoops to make each "cold call" and you continuously get no results for a period of weeks or months, you'll stop making the calls – they're just too much effort. If you have too many stipulations attached to contacting prospective clients with endless documentation and process, you'll only call the prospects that you feel at the absolute most worthy of that amount of effort. If you must include endless legalese in your business communications, clients are going to prefer talking to the robot down the street rather than contacting you.

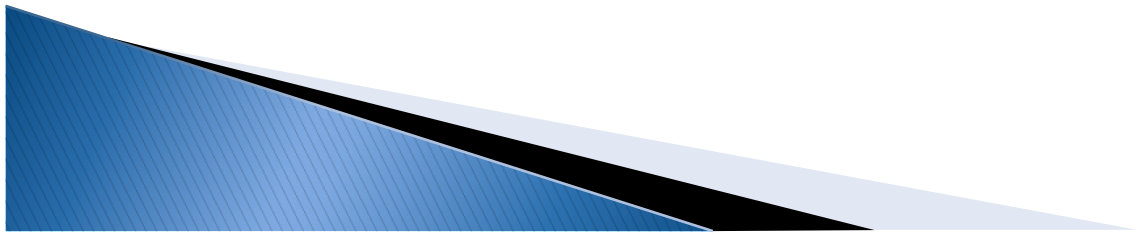
Conclusion

- If those tasks are extremely easy, you'll do them, if for nothing more than because they take no time or effort – "it won't hurt, why not." I don't know of any entrepreneurial businesses that were born from beauraucracy, but I know that businesses die from it.

Conclusion

Paul W. Poteete
CEH, CISSP, MCSE, CNE, CCA, VCP
ppoteete@gmail.com
831.333.9119

PO Box 467
Monterey, CA 93940



ISACA
Serving IT Governance Professionals
San Francisco Chapter