Interdisciplinary Studies in Information Security

Centro Stefano Franscini
Monte Verita, Switzerland

The New C-Words for InfoSec: Continuity and Compliance

Jim Herbeck
Managing Partner and Principal Consultant, Nouvel Strategies
Member of Faculty, SANS Institute

8 Jul 2008

JHerbeck@NouvelStrategies.com

Agenda

- Talking about talking about InfoSec
- The 2 C-words
- The F-word
- The R-word
- Some other words
- Miscellaneous final words

Talking about talking about InfoSec

- Confidentiality, integrity, availability, authentication, authorization, non-repudiation,

Stop using these words to talk about Information Security with management.

digital forensics, cyber-adversary characterization ...

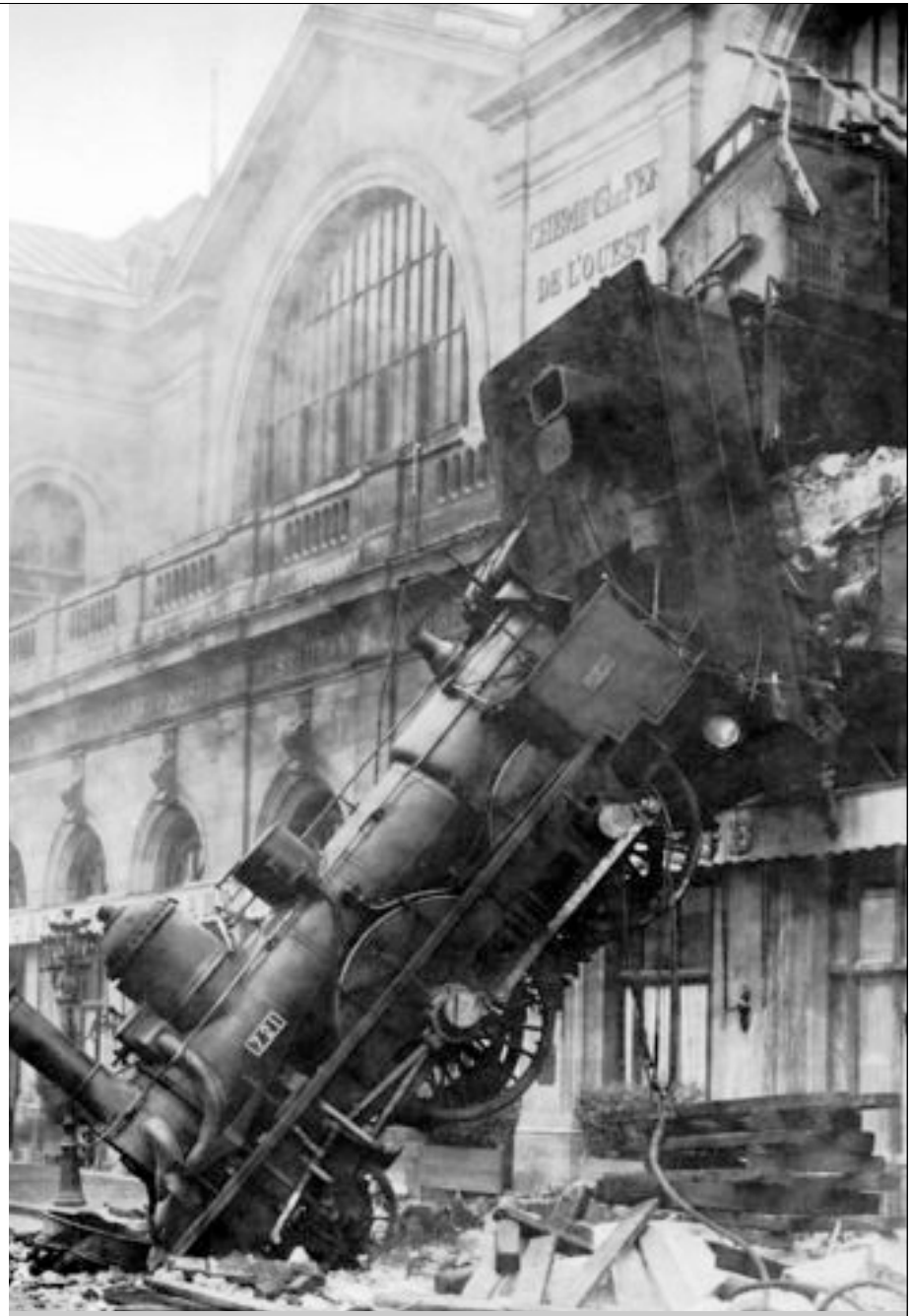
- FRR, FAR, CER, SAT, SSID, DACL, SACL, UID, GID, RSA, DES, 3DES, AES, IDEA, ECC, ECDSA, ECDH, ECMQV, MD5, SHA, RIPEMD, PGP, SSL ...

The 2 C-words

- Continuity
- Compliance

Continuity

- Is your organization prepared for an IT train wreck?
- Most organizations are very interested in this topic.



Wikimedia Commons: image is in the public domain because its copyright has expired.

Continuity factoids

- Continuity includes such diverse topics as Disaster Recovery Planning (DRP), Business Continuity Planning (BCP), data center security, network security architecture, backups, operational security, documented operating procedures.

- From 1,000 participating organizations, 48% have disaster recovery plans that have not been tested in the last year.
  UK Department for Business, Enterprise & Regulatory Reform (BERR) 2008 Information Security Breaches Survey (conducted by PriceWaterhouseCoopers)

- Of nearly 1,200 respondents, 65% have agreed to recovery timescales with the business.
  Ernst & Young 2006 9th Annual Global Information Security Survey

Compliance

- In some organizations, the compliance program has a bad name.
- Note: the guy with his head in a noose is senior management– not IT.

Legal and Regulatory Compliance

- State, national, and international law
- Regulatory agencies
- National and international standards (self-regulation)
- Intellectual Property (both consumed and produced)
- Managing the compliance burden is now an issue.
- How to create a win-win situation?

Audit and Internal Controls

- These are the organizational department(s) usually associated with compliance.
- Internal Control needs to be aligned with Information Security, but often isn't: this is a lost opportunity.
- Audit should provide feedback on the progress of Information Security, which is critical for improvement.

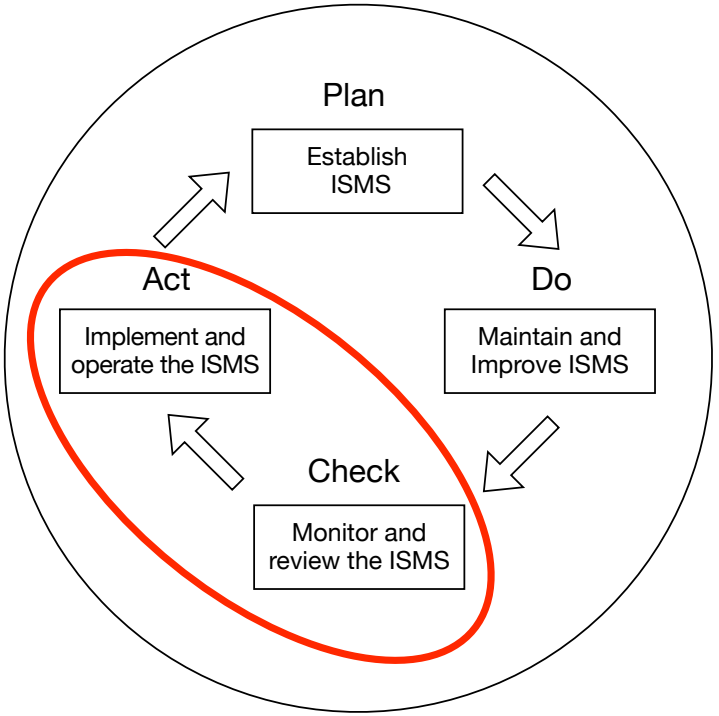
The relationship of Audit to Continuous Process Improvement (CPI)

- Most Continuous Process Improvement systems include a Plan-Do-Check-Act loop.
- The audit function provides:

  a) the “check”

  b) the mandate to “act”

- Without audit, it’s much more difficult to improve information security in organizations.



ISO 27001 Continuous Process Improvement loop

Compliance factoids

- Compared to one year earlier, from a survey of 140 “best in class” organizations: 63% reduced the number of actual security incidents, 70% reduced the average time to address incidents, 48% reduced the total cost to address incidents, and 74% reduced audit failures (instances of non-compliance).
  “Security Governance and Risk Management: The Rewards of Doing the Right Things and Doing Things Right”, The Aberdeen Group, Nov 2007

- “Security Regulatory Compliance” was listed as one of their top 5 initiatives by 49% of respondents.
  Deloitte 2007 Global Security Survey

- “Compliance with Regulations” was listed as the driver having the most significant impact on information security practices in the organization by 64% of respondents.
  Ernst & Young 2007 10th Annual Global Information Security Survey

The F-word

- Fraud

Fraud

- “Wrongful or criminal deception intended to result in financial or personal gain.”
- Organizations are interested in talking about fraud.
- Segregation of Duties is a classic control used to prevent fraud.
- Application security as it relates to business processes is complicated.

Fraud factoids

- Segregation/Separation of Duties: a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals responsibility for initiating and recording transactions and custody of assets to separate individuals.
  Information Systems Audit and Control Association (ISACA) glossary

- In Jan 2008, Société Générale, one of the largest banks in Europe, reported that a rogue employee had executed a series of “elaborate, fictitious transactions” that cost the company more than $7 billion, the biggest loss ever recorded in the financial industry by a single trader.
  “Société Générale loses $7 billion in trading fraud,” International Herald Tribune, 24 Jan 2008

- From the 40% of organizations willing to reveal monetary losses associated with computer security incidents, 31% ($21 million of $67 million) were associated with financial fraud.
  2007 Computer Security Institute 12th Annual Computer Crime and Security Survey

The R-word

- Risk

Risk

- “The possibility that something unpleasant or unwelcome will happen.”
- Organizations are interested in talking about risk.
- The ultimate purpose of information security is to mitigate IT- and information-related business risks.

Risk factoids

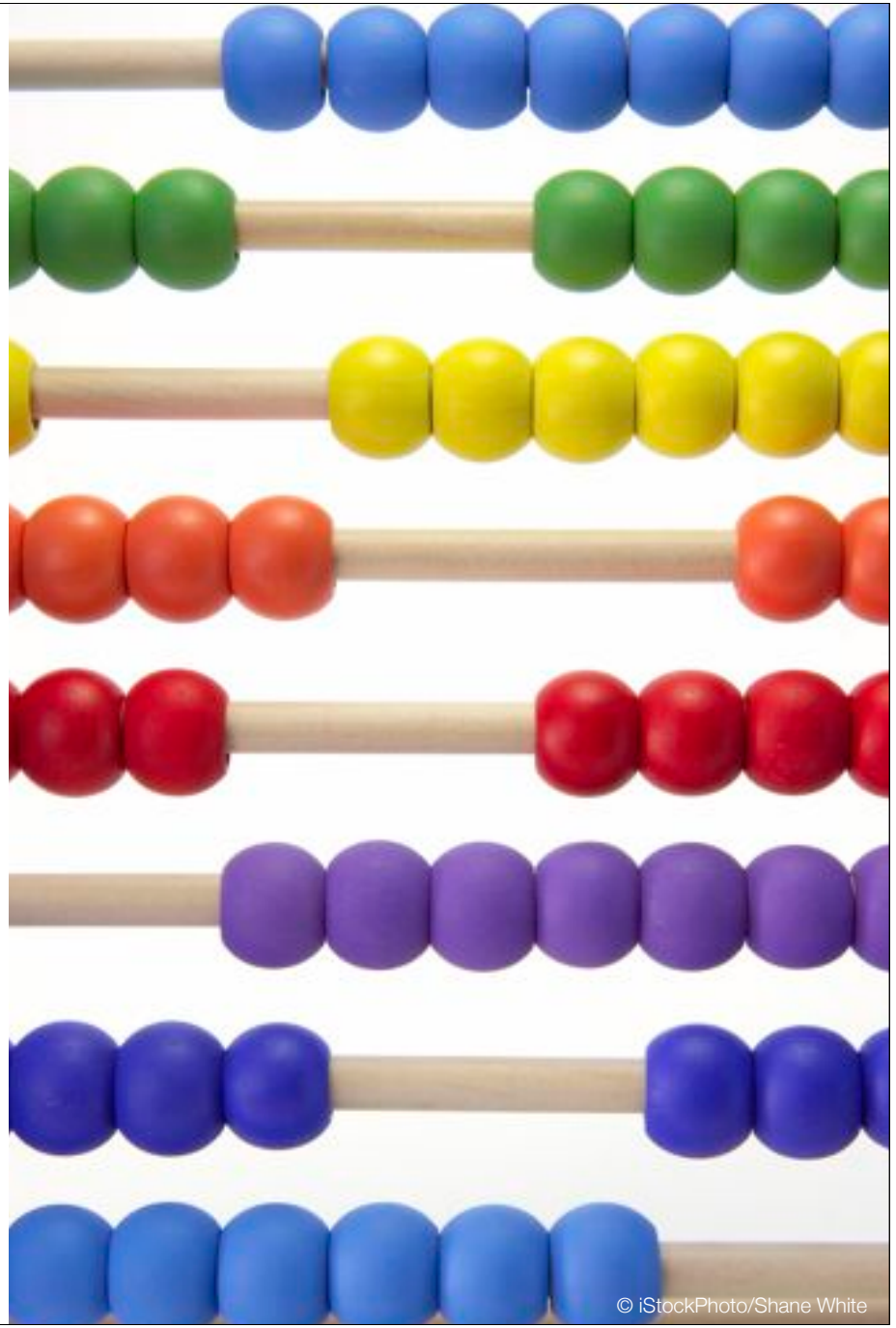
- What is at risk for organizations? Trust, reputation/brand/image, competitive advantage, market and investor confidence, relationships with business partners, customer retention and growth, business continuity and resilience.
  "The Art of Information Security Governance", Qatar Information Security Forum, Julia Allen, Feb 2008

- Information security functions are integrated with risk management operations in 82% of responding organizations.
  Ernst & Young 2007 10th Annual Global Information Security Survey

- An effective IT Risk Management program creates an IT Risk profile that supports the businesses' larger objectives, accepting more risk where business impact is low, and managing risk more closely in areas where the most is at stake.
  Symantec IT Risk Management Report Dec 2006

Other words

- Metrics
- Quality
- Governance
- Pragmatic



Other factoids

- “Information security governance means viewing adequate security as a non-negotiable requirement of being in business”.
  “Governing for Enterprise Security CMU/SEI-TN-023”, Julia Allen, Jun 2005

- From 1,000 participating organizations, 81% believe their board gives a high priority to information security.
  UK Department for Business, Enterprise & Regulatory Reform (BERR) 2008 Information Security Breaches Survey (conducted by PriceWaterhouseCoopers)

- Of 169 financial institutions responding, 81% have a defined security governance structure; 18% are in the process of establishing one.
  Deloitte 2007 Global Security Survey

Miscellaneous final words

- When you talk to organizations, use words and metaphors the organization understands.
- Appeal to the different parts of the organization to help sell information security: IT, Management, Finance, Legal, Internal Control and Audit.
- It's easier now then ever before to convince organizations to do something about information security.

The New C-Words for InfoSec: Continuity and Compliance

Jim Herbeck
Managing Partner and Principal Consultant, Nouvel Strategies
Member of Faculty, SANS Institute

8 Jul 2008

JHerbeck@NouvelStrategies.com