Security Issues in the Global Card Companies

An International Comparison

Bernardo Nicoletti
CIO
AIG GCF LatAm

Dubai
May 17th, 2009

Agenda

- The Challenges
- An Integrated Approach: Lean & Digitize
- Applications to Security Management
- Some Standards and Best Practices
- The Future

Chinese Saying ....

“May you live in

interesting times!”

"愿你生活在有趣的时代"

Changing Environment ... The 4Cs

Customers

Empowered and demanding

Complex and confused

Sometimes Malicious

Challenges

Global

Aggressive

Costs

Inflation

Complex Technology

Outsourcing

Compliance

Security Requirements

Laws and Regulations

GRC

Challenging Environment

Some Titles from the Press

Central Bank of Nigeria calls for ATM removal from public places
• 13 Apr 2009

ATM fraud more than doubles in Europe, security report says
• 13 Apr 2009

High Profile Cases in USA

	Loss
• February-05 ChoicePoint reported fraudulent access	150,000 consumer records
• March-05 - Lexis Nexis reported hacking of fraudsters	32,000 consumer records
• March-05 - Bank Of America reports it lost backup tapes	1.2M employee records
• May 2006 — CIO and CISO fired at Ohio University	137,000 account records
• May 2006 — Laptop stolen	27m VA records
• July 2006 — MySpace worm	45m account
• January 2007 – TJ Maxx discloses exposure	
• February 2007 — Wordpress backdoor	
• March 2007 — John McCain's MySpace page defaced	
• April 2007 — IRS grants extensions to TurboTax online filers	
• 2008 - The McColo takedown had the single largest impact on spam all year	

High Profile Cases in Europe

- Poland: Phishing E-mails to Citi customers; directed to pirate webpage
- Poland: Bank Millennium did not properly cleaned Hard Drive found on public trash.
- Poland: Kredyt Bank un-shredded docs found in public trash.
- UK: Mar-05 - London bank reveals key logging used in attempt to commit fraud.
- UK: £3 million Bank fraud. 9 People charged, 14 people arrested. They are suspected of being part of a group accused of opening up to 1,200 bank accounts using false documents

High Profile Cases in Asia

- S. Korea: Sep 2004 - An employee of the Korea First Bank pro the data of 400 customers to illegal bondholders, who obtain illegal loans
- S. Korea: May 2003 - An employee of LG Card sold personal data, card numbers and the passwords of 620 customers to a credit card information broker at a price of 7 million Won. The broker then sold the data of 400 customers to another broker for 10 million Won, who then sold the data of 40 customers to another broker for 20 million Won. These brokers used the information to forge credit cards and obtained 1.3 billion Won from illegal cash services.
- S. Korea: 2004 - An employee of an agent of CJ GLS obtained access to the database of CJ Homeshopping and provided the data of 2 million customers to Sion Homeshopping in return for exclusive delivery rights. Sion Homeshopping used such data to sell drinks to CJ Homeshopping customers through telemarketing

Implications for Data Loss

	Data Lost	Stock –a)	Class Action	Headlines
Lexis Nexis	**310,000**	**Flat**	Righetti • Wynne Civil Litigation Trial Attorneys	"Senators Vow Data Broker Crackdown … (Lexis) Breach May Be Worse Than Thought"
Choicepoint	**145,000**	**(9.4%)**	Lerach Coughlin Stoia Geller Rudman & Robbins LLP	"… defendants disseminated materially false and misleading statements concerning the security of the Company's systems, its results and operations … at the same time two of the Company's top officers sold $20.89 million worth of their ChoicePoint stock.."
BOA	**1.2MM**	**(6.5%)**	**?**	"Senators among up to 1.2 million federal employees affected"

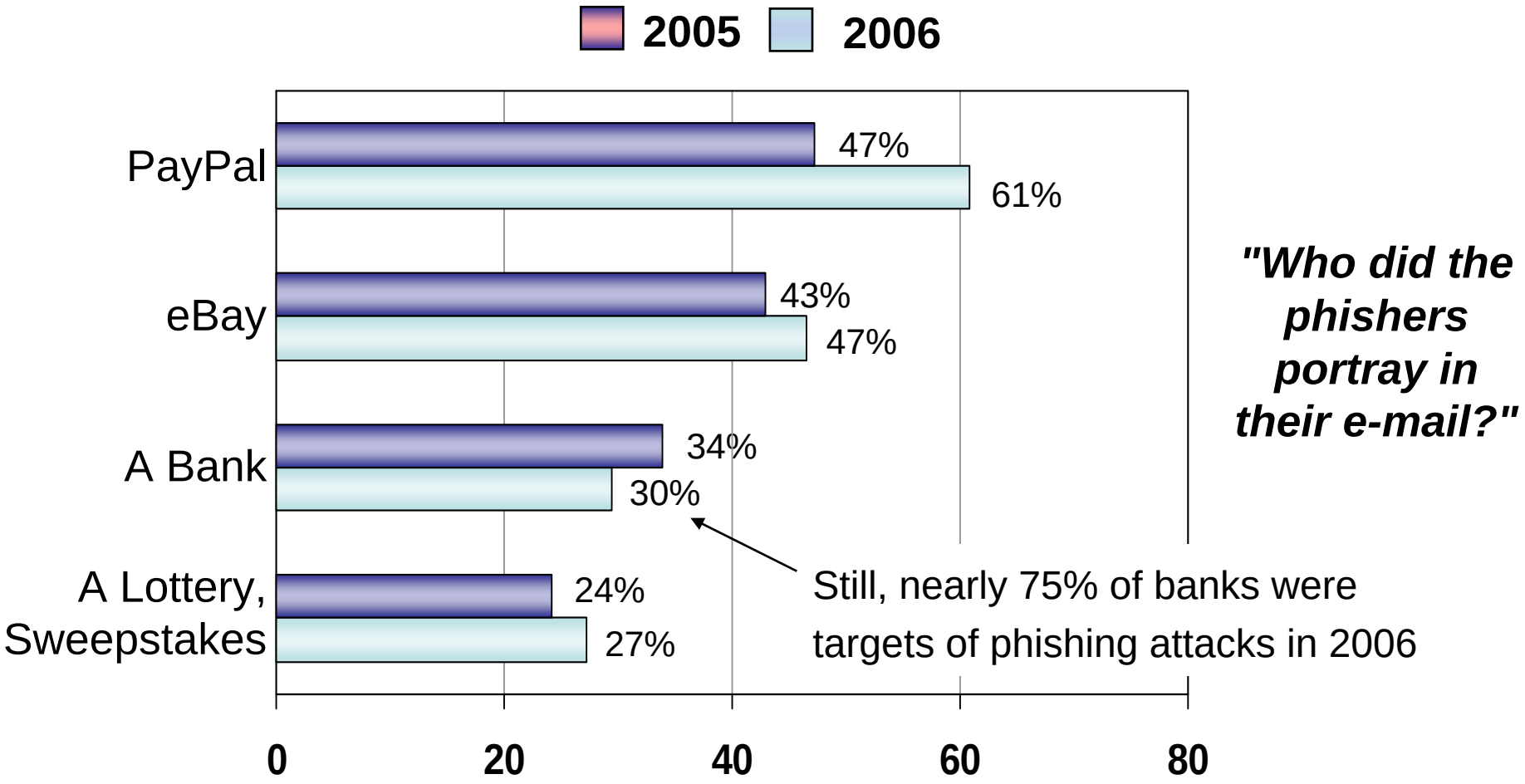
- Legislation … data security bills introduced in many states
- Regulations … introduced in many Financial Institutions

-a) Closing price +30days after incident reported

Damage is Quietly Increasing

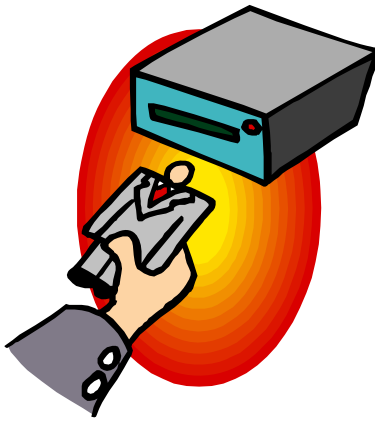
Top four targets of phishing e-mail attacks

109 million U.S. adults were "phished" in 2006; up 100% since 2005



Gartner: Through 2009, "phishing" attacks will continue to increase because it's still a lucrative business for the perpetrators (0.7 probability).

Identity Theft



- Rise in organized crime involvement in carding.
- Federal Trade Commission (FTC) claims 42% of identity theft cases involved credit card fraud from stolen credit card details
- My own credit card details are currently stored in 15 different databases around the world (.. and known in numerous restaurants)
- Hackers steal credit cards and on-sell them to carders who order products online to resell on online auction sites.
- Money is a good incentive.

Internet Black Markets for Access Codes

Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	$0.50—$5
2	Bank Accounts	21%	$30—$400
3	Email Passwords	8%	$1—$350
4	Mailers	8%	$8—$10
5	Email Addresses	6%	$2/MB—$4/MB
6	Proxies	6%	$0.50—$3
7	Fu II Identity	6%	$10—$150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5—$7
10	Compromised UNIX® SheJis	2%	$2—$10

Source: Symantec Internet, Security Threat Report, September 2007

ID Theft by Fraud Type – Total –a)

Credit Card:	32%
Phone or Utilities:	19%
Bank:	17%
Employment-related:	11%
Government Docs:	8%
Loans:	5%

Credit Card Security Violations 2006

Food	61%
Retail	12%
Higher End	7%
Other	20%

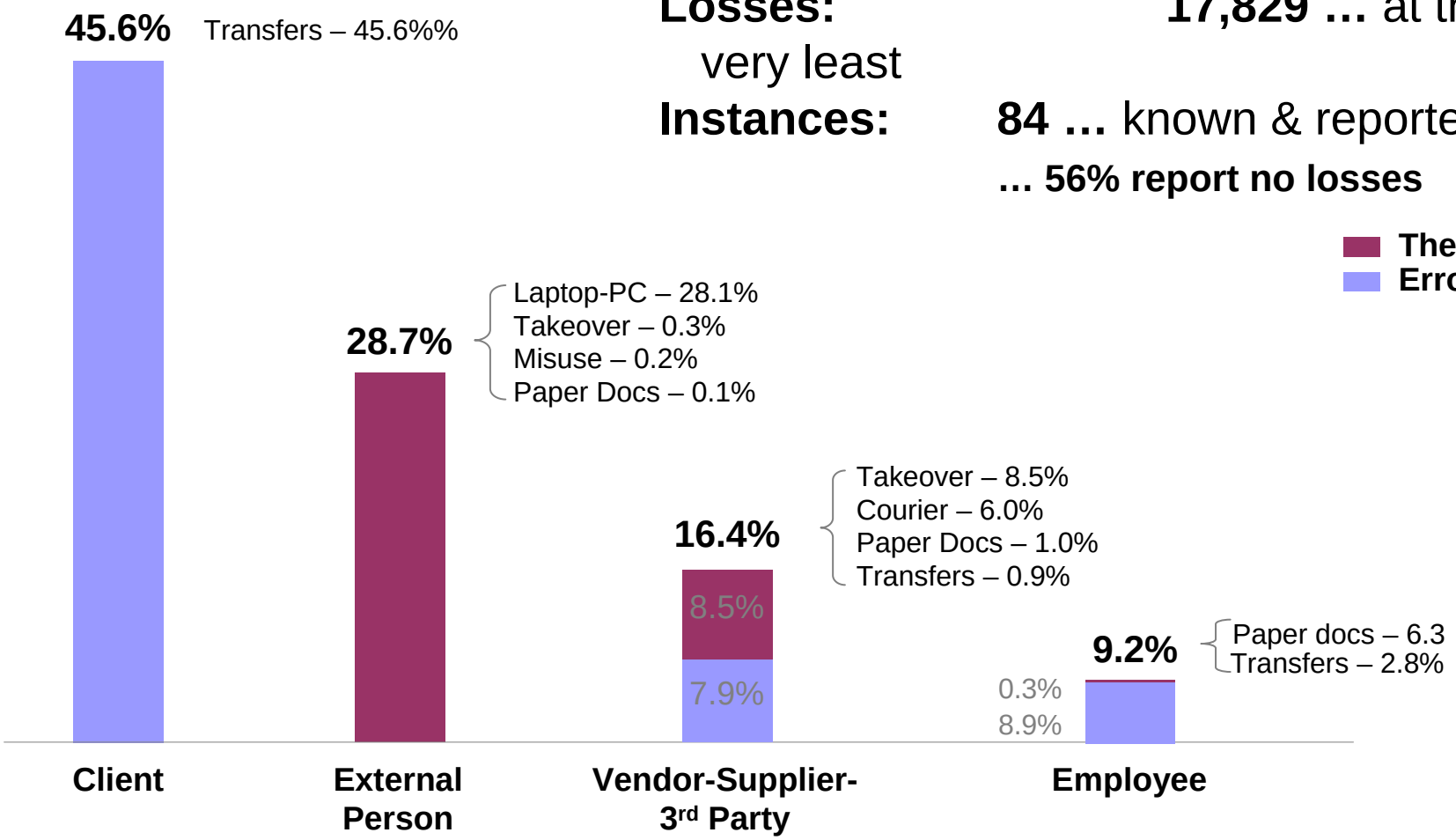
-a) Federal Trade Commission data for 2003

’05 Global Survey: Results

Losses: **17,829 …** at the very least

Instances: **84 …** known & reported

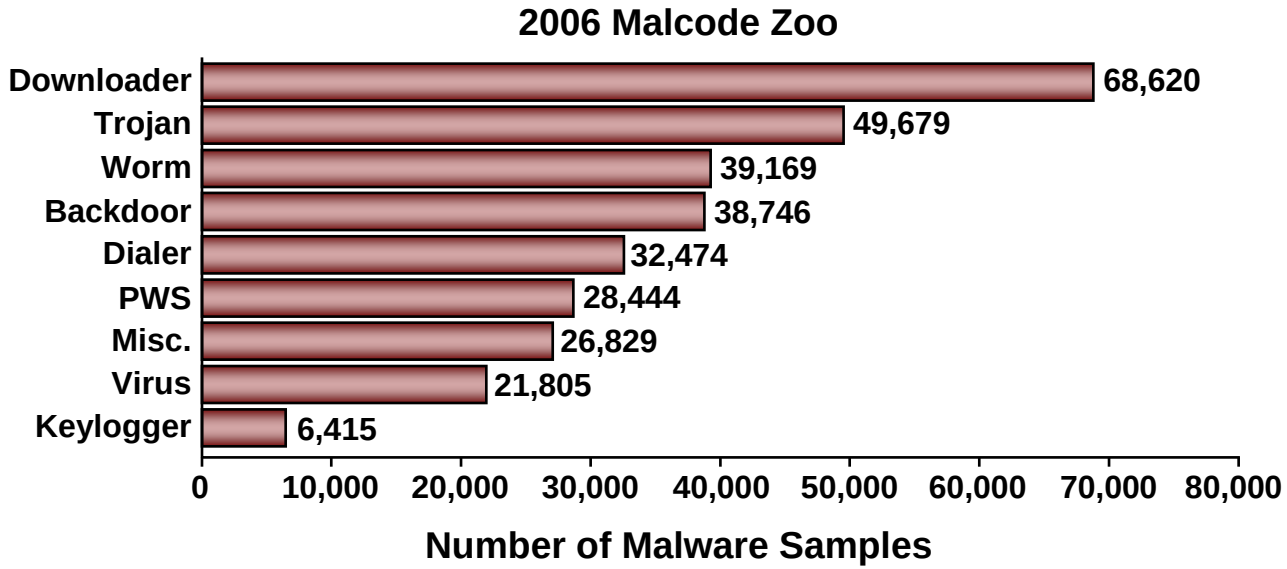
… 56% report no losses

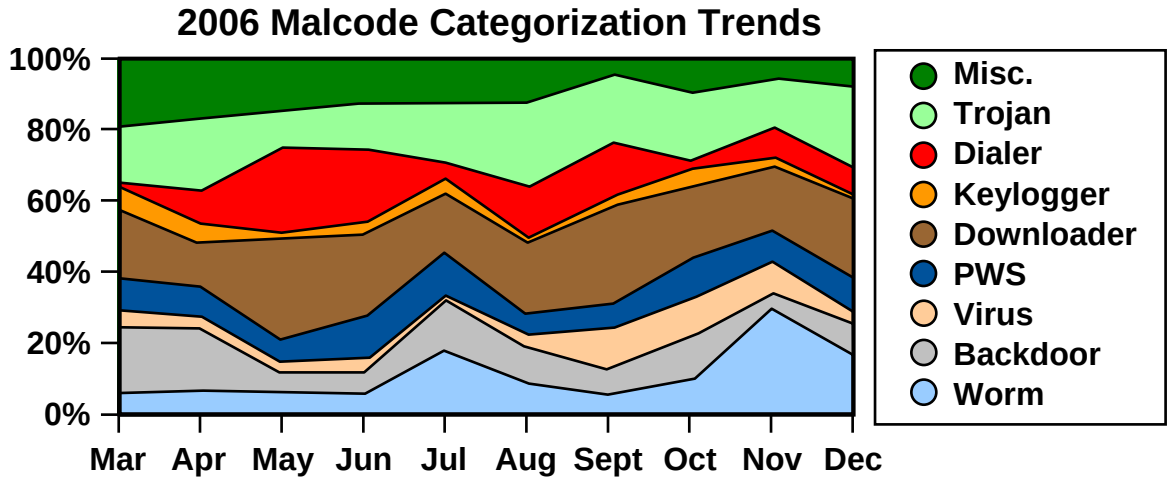


Exaggerated Chart Scale

- *Transfers: movement of data between 2 parties*
- *Paper Docs: physical paper files lost / stolen*
- *Laptop – PC: computers or other hardware*
- *Misuse: data used in a way inconsistent with policy*
- *Courier: data lost in transit with UPS / DHL etc*

Threat Types: Run Quiet, Run Deep





Source: IBM ISS 2006

More Threats on the Horizons

Business

- Globally distributed and contracted workforce: Information can be accessed in real-time
- Integrated partner networks: Reputation is shared, outside direct control
- Compliance mandates are many, increasing, complex and often conflicting
- Petabytes of information
- Managing, finding and protecting unstructured data
- Hackers and Criminal attacks (not just for the sake of it)
- Data Privacy breaches

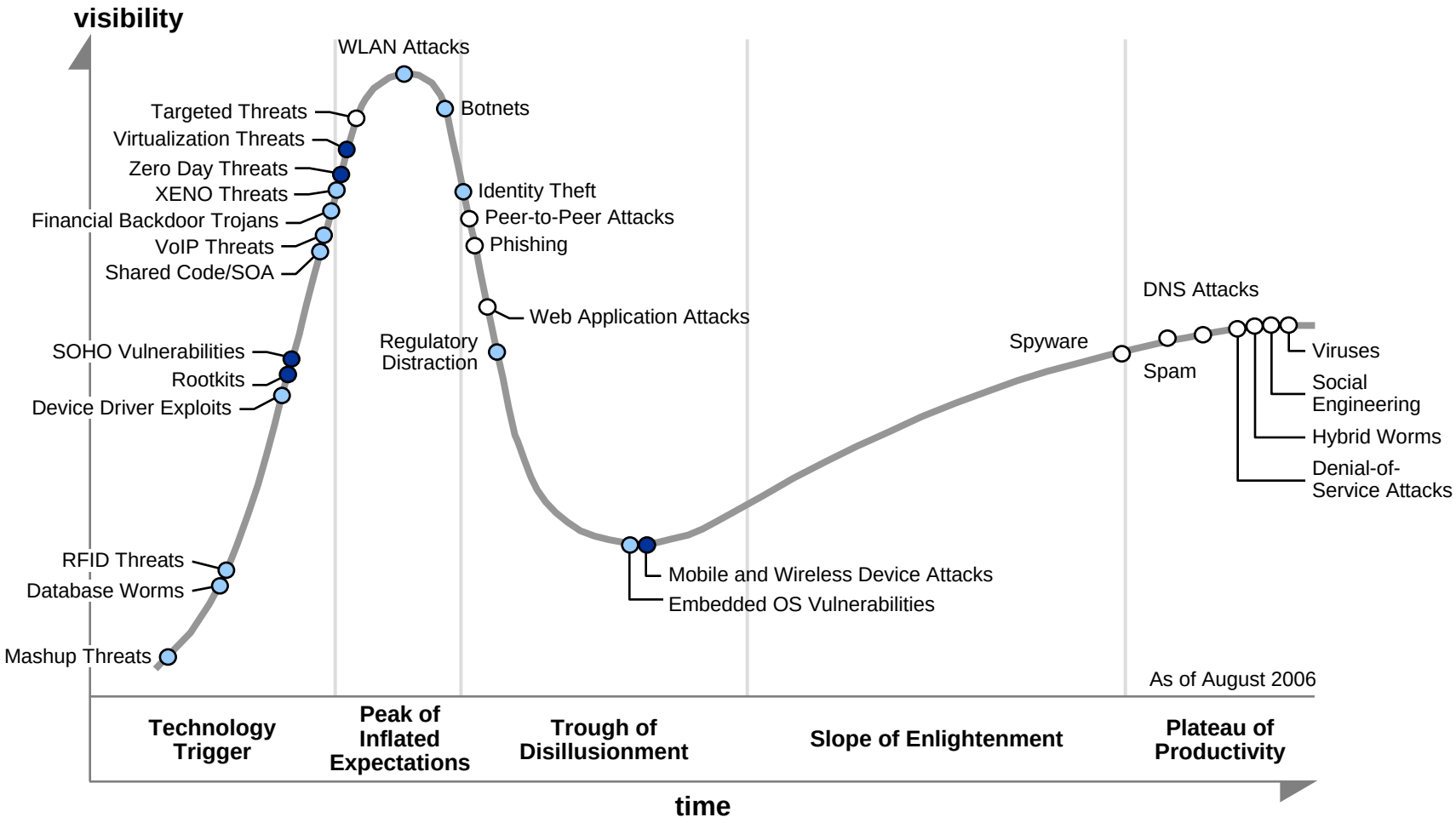
Technology

- Server/Storage virtualization
- Desktop shared directory and operations.
- Appliances that are really computers.
- Information and application sit in the Cloud computing
- New viruses: Conficker .. A, B, C, D .. ?
- Password crackers embedded in virus/worms
- New developments: SOA and Web 2.0
- Rogue Software (Pyrates, etc.)
- Faster attacks (24h after warning – getting less)

Technology Convergence Makes Risk Higher

- Technology convergence is creating new challenges
- Vulnerabilities are at a high plateau
- Secure Web presence has become the Achilles heel of corporate IT security
- Mass endpoint exploitation is happening not only through browser vulnerabilities, but also through malicious movies and documents like Adobe PDF files (possibly zipped)
- Successful exploitation typically leads to the installation of information-stealing Trojans
- China hosts the most malicious Web sites, surpassing the US for the first time in 2008
- On the Internet everyone lives next door!
- Low-cost high-speed portable data storage:4GB USB 2.0 Flash Drive at a Final Price: $9.99

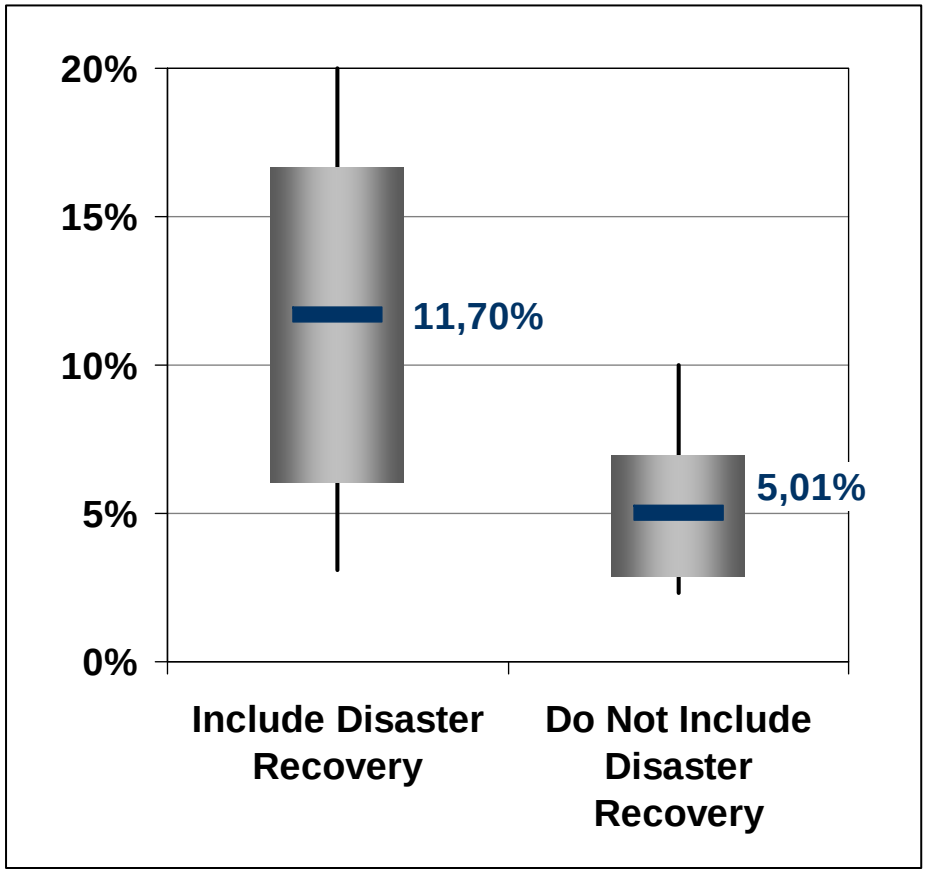
Source: IBM X-Force 2008 Trend & Risk Report



Source: Gartner

Increase the Budget is not the Solution

- Security spending has been growing twice as fast as IT spending
  - Did security get better?
  - Can you continue that growth in spending?
- There is almost no correlation between security spending and security level
- Real progress in security should reduce security spending



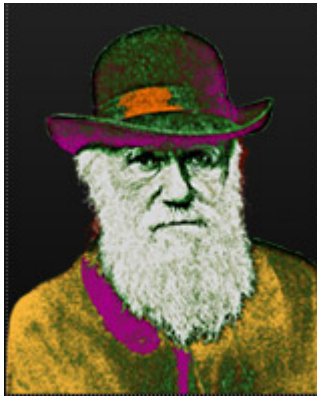
Source: Gartner Consulting Worldwide IT Benchmark Service
Gartner Information Security Research Service 2007

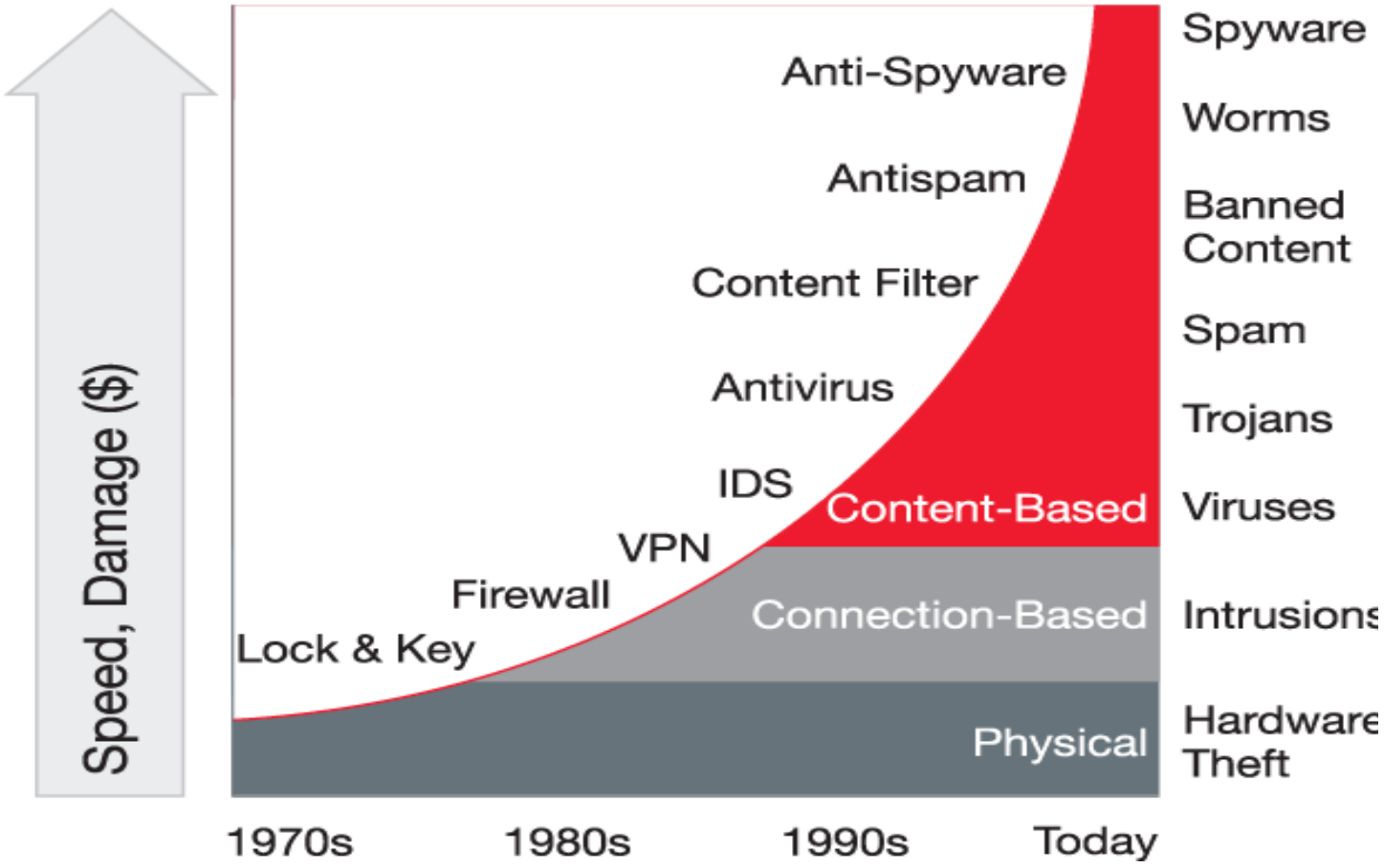
Security solutions should have a ROI of one years or less.

Call to Action

- ✓ Improving Security means change management:
  - Change how IT is bought or built
  - Change how business solutions are developed, deployed and run
  - Change who pays for what security controls
  - Change how access is managed (IDM and Segregation of Duty)
- ✓ If you can't change something right away, find the decision gate and change that
- ✓ Security might be a journey but it better have clear destinations

Information Security: A Darwinian Development





Operations Excellence

Correction

Awareness

Blissful Ignorance

What should be next? From Tools to Methodologies

Agenda

- The Challenges
- **An Integrated Approach: Lean & Digitize**
- Applications to Security Management
- Some Standards and Best Practices
- The Future

Lean Six Sigma … Faster & Better Security

Six Sigma — **works on Quality … *may* improve process speed**

+

Lean — **works on Process Speed … *may* improve quality**

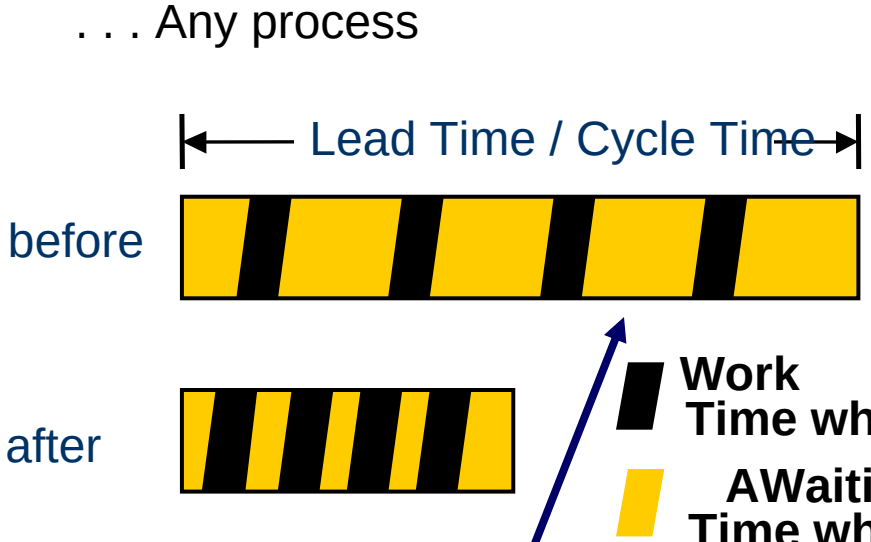
=

Lean Six Sigma — **reduces complexity and improves both Quality & Process speed**

Innovate for security effectiveness across the enterprise

Benefits of the Lean Approach

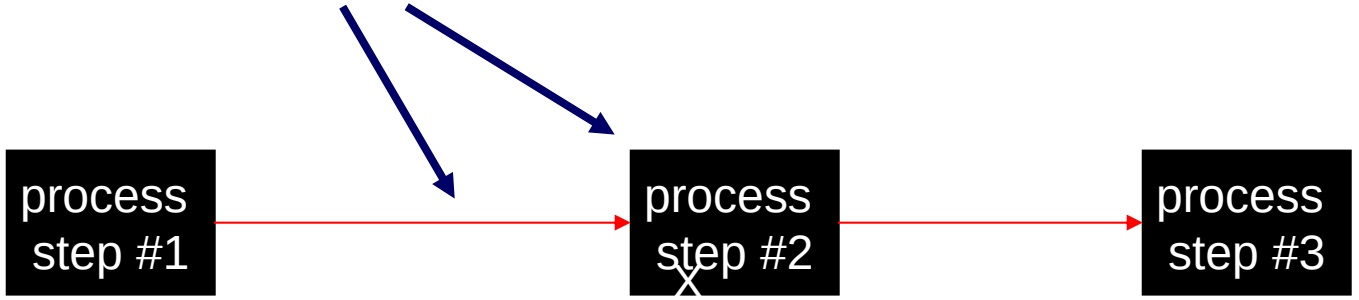
. . . Any process



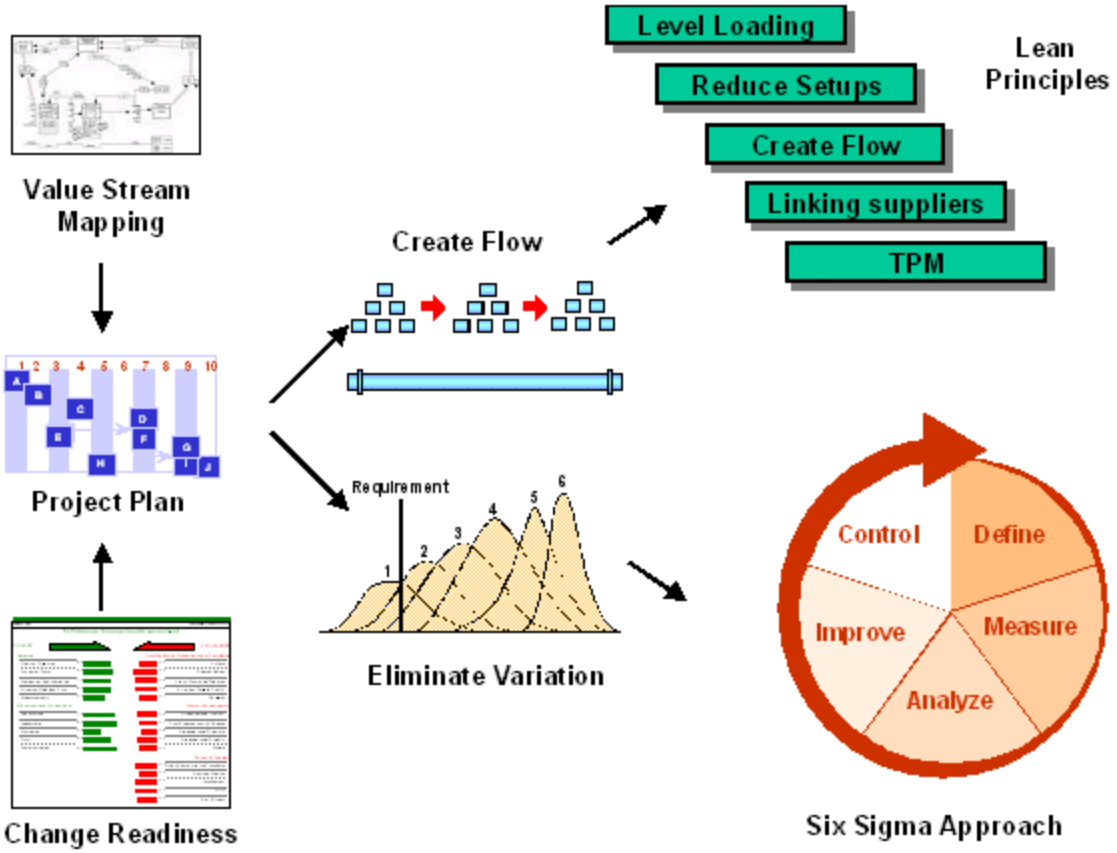
Improvements in the customer satisfaction

- Reduction in the cycle time
- Improvements in delivery
- More capacity
- Better Quality
- Efficiency

Lean attacks the Waste here

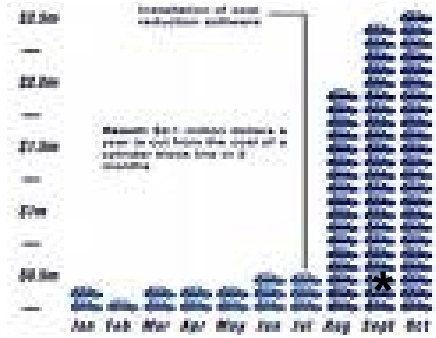


Six Sigma and Lean



Lean Six Sigma is not enough:

Lean & Digitize



Lean training

Culture

Are we really implementing changes?

Is ICT bought into Lean?

Project Management Methodology

ICT Planning

Scheduling and execution

… linked to Quality Plan

Are we profitably improving processes for the customer?

Enable process driven enterprise architecture

The Lean & Digitize Methodology*

- The Environment and the Needs
- The Vision
- The VoC and the Strategy
  - The Metrics
  - The Prioritization
- The Governance and the People in the Team
- The Components
  - Processes
  - Physical Layout
  - Digitization
- The Lean First
- The Architecture, the Build and the Deployment
- The Control and the Improvement

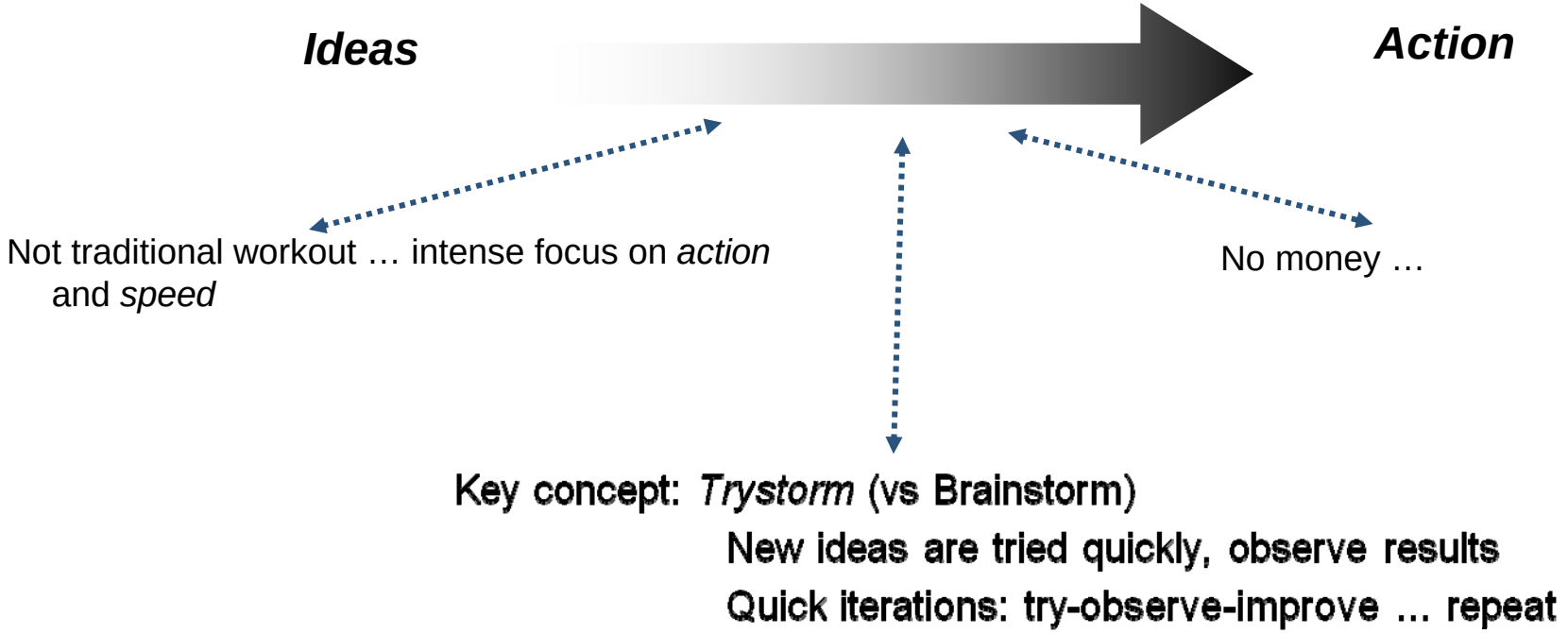
The Governance

- **Lean Leader** ... The Facilitator ... Full time job
- **The Team Coordinator** ... The Project Leader from the Department more affected for the process ... For the duration of the project (including the Digitization phase) ... In charge of the planning, monitoring and managing the team
- **The Team Members** ... From the various departments interested plus Information Technology ... Either full or part time for the entire duration of the projecty

The People ... R=Q*A

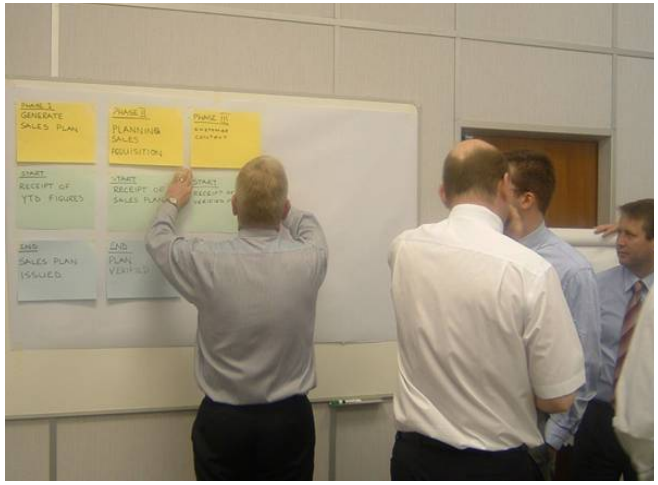
The Action Workout (AWO!

The change process to apply
the Lean and Digitize tools … target waste
with Value Creation Teams



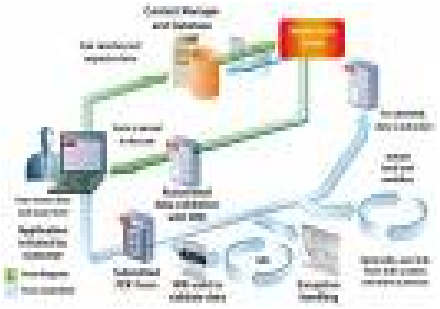
"Ask the questions that will lead to the possible insights" Jim Collins

Agenda



- The Challenges
- An Integrated Approach: Lean & Digitize
- **Applications to Security Management**
- Some Standards and Best Practices
- The Future

The Strategy



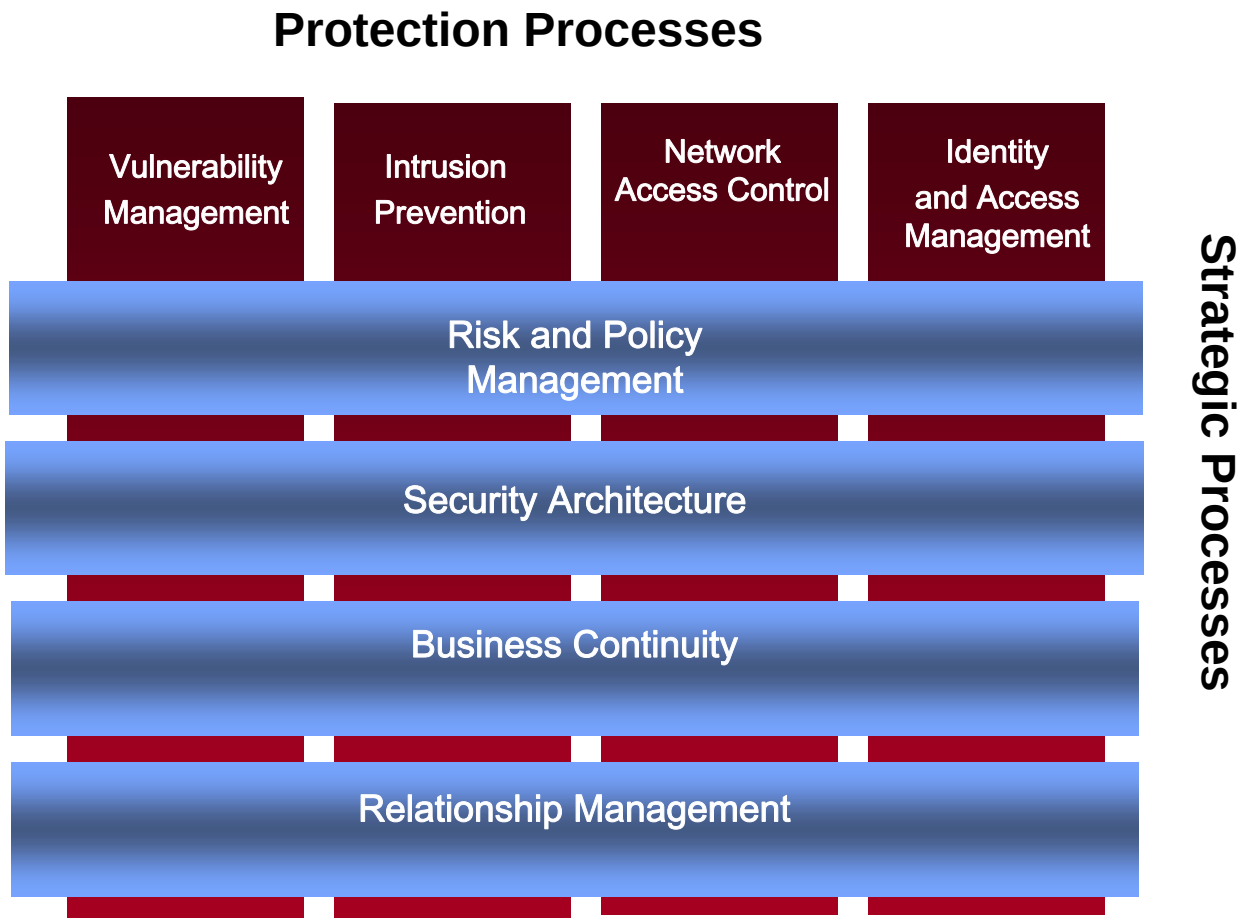
The Lean Architecture

Implement a set of improvements and best practices for the Business to gain competitive advantages through a better security management system, while removing the “waste” in:

- The process path
- The physical path
- The digitization path

“… information systems have to do more than manage huge amount of financial data...” Bill Gates

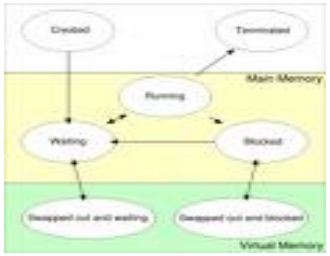
Business Viewpoint: Security Process Portfolio



The Components

Add Value

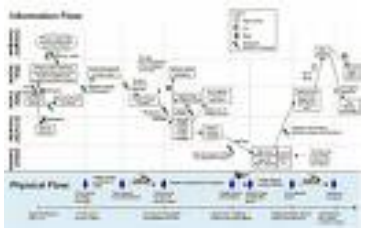
Process



Improve the SDLC
IT Governance
Security Development Lifecycle process
Engineering for security
Design threat modeling
SD3:
•Secure by Design
•Secure by Default
•Secure In Deployment

Simplify

Physical



Adaptive/integrated security architecture and controls

Risk maps

Sequencing of operations according to the improved process

One stop service

Recording video cameras

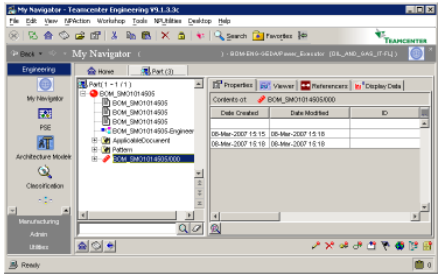
Removable media control

Encryption of Emails

Protection Against Spy-ware
More Blocking of Websites

Consolidation and Virtualization

Digitization



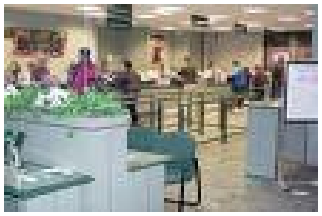
Infrastructure Protection and Management
Encryption of Off-site Back-ups
Registering of Company Equipment (PDA's)
Automated patching and update services
Protected Mode
Windows Server only installs what it needs, reduces attack surface
Non-administrator users (UAC)

"Services Organization can no longer let BPM pass..." Michael Hammer

The Architecture

User Contact Point

Access



I+4A:
Identity Claims
Authentication
Authorization
Access Control Mechanisms
Audit

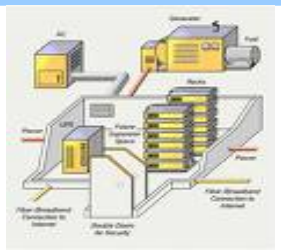
Connection

Network

NIPS
wLANs Security
Intrusion detection
Penetration testing
Appliances
Multi-purpose wireless network
Media (private and public) transfer encryption
3rd Party Network Audit
Limiting External Email Access

The Hub

Data Center

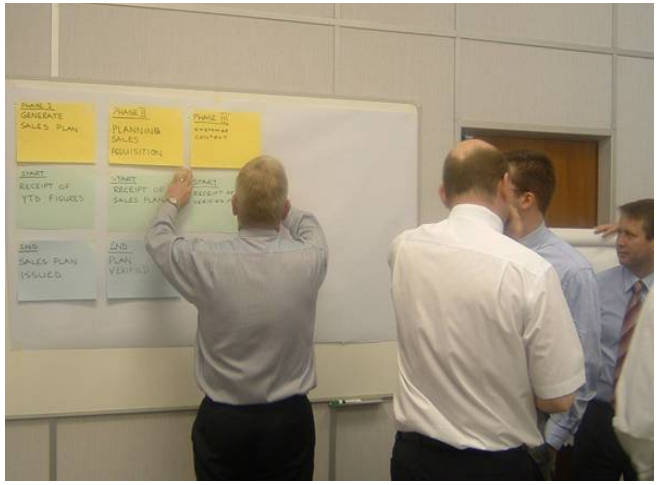


BCP/DRP Review
Hw Virtualization
IT Service Management (ITIL)
Document management
Auditing
Software asset inventory
Firewall
License management
Server & Domain Isolation (SDI)
Advanced Memory Management (ASLR)
Encrypted disk & file systems

The Metrics ... 3 E ... KSI

Development	Operations	Finance
Effectiveness	**Efficiency**	**Economics**
		
Quantity of devices patched Results of the tests MTBF and MTTR Status of the correction and preventative plans Repetition of cases	Automation of patch and configuration management Resources Used Amount of Rework Average The recovery point objective (RPO) and the recovery time objective (RTO) in the backup processes % of labeled data Quantity of data which are encrypted Quantity of media sanitized before disposition	Security budget Eliminated Waste Frontline Costs Cost of Intrusion Cost of data loss

Agenda



- The Challenges
- An Integrated Approach: Lean & Digitize
- Applications to Security Management
- **Some Standards and Best Practices**
- The Future

Standards

- Best Practice Basilea 2 (Operational Risks)
- COS Internal Controls (SEC)
- BSI

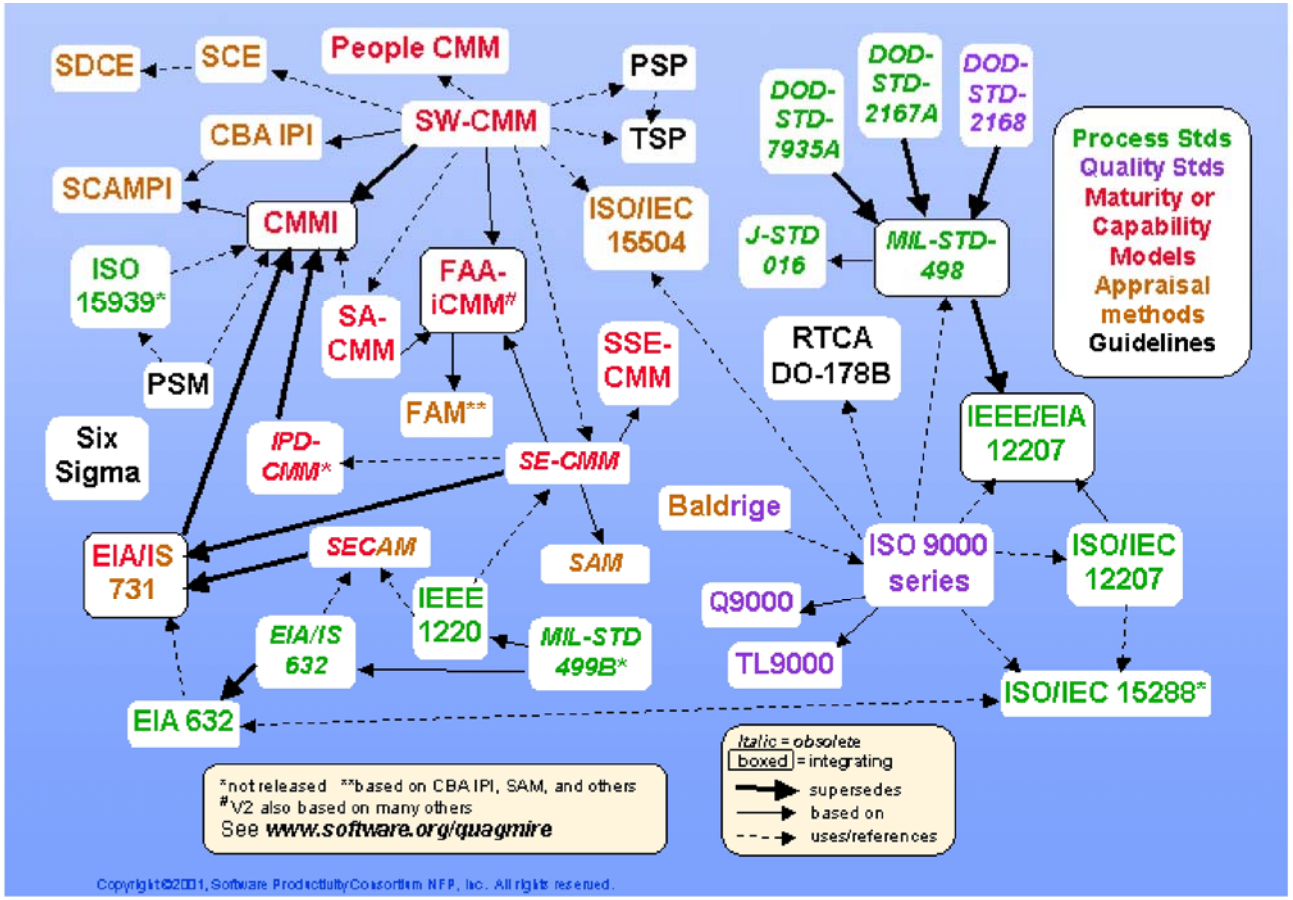
- Cob-IT
- Val-IT
- Risk-IT
- COSO 2004 Enterprise Risk Management

- ISO 15408: Criteria of evaluation of the internal controls of IT
- ISO 17799: Code of practice to administer Information Security
- ISO 2700X: Management of Information Security
- ISO 31000: Risk management

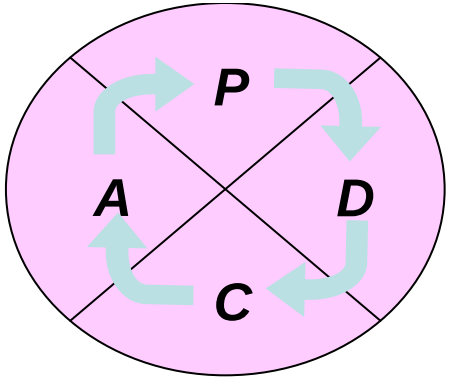
- IT Baseline Protection Manual,

- (Increasing) Regulations of the Central Banks
- Etc.

Quite a Few Standards ….



ISO 17799/27001/27002



- “A comprehensive set of controls comprising best practices in information security”
- Comprises Two parts - a code of practice and a specification for an information security management system
- “It is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce”
- Facilitation of interaction in a trusted environment

An internationally recognized information security standard

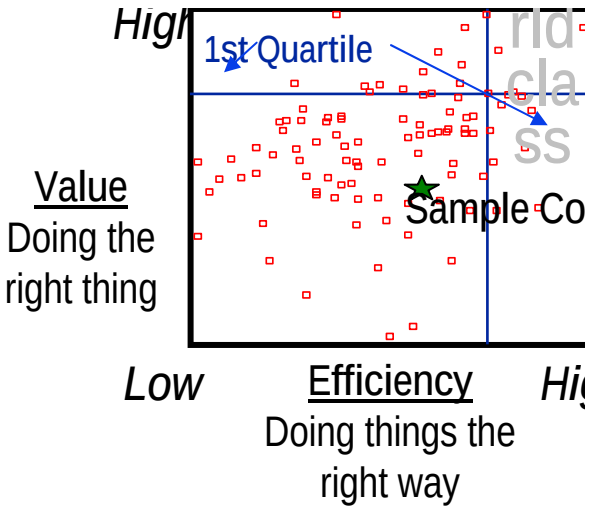
Structure of ISO 27002

- 11 Clauses
- – Main security categories
- Control objectives
  - – Regulatory controls
  - – Industry best practice

11 Clauses to Comply with ISO 27002

a) Security Policy (1);
b) Organizing Information Security (2);
c) Asset Management (2);
d) Human Resources Security (3);
e) Physical and Environmental Security (2);
f) Communications and Operations Management (10);
g) Access Control (7);
h) Information Systems Acquisition, Development and Maintenance (6);
i) Information Security Incident Management (2);
j) Business Continuity Management (1);
k) Compliance (3)
Organizational
Technical
Management

Important ISO 27002 Controls

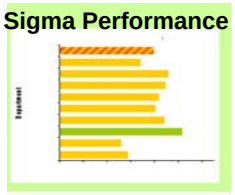


Standard includes ‘regulatory essentials' and 'common best practice” under the IS “starting point” section

These are:

- Intellectual property rights (12.1.2)
- Safeguarding of organizational records (12.1.3)
- Data protection and privacy of personal information (12.1.4)
- Information security policy document (3.1.1)
- Allocation of information security responsibilities (4.1.3)
- Information security education and training (6.2.1)
- Reporting security incidents (6.3.1)
- Business continuity management (11.1)

The Benefits



Drives down costs while improving compliance
Enables a more agile, high-performing business
Ensures information is protected and available when needed
Establishes IT as a business partner, not a cost center

CIMB GROUP

Results in improved business process

In shorter time and at lower cost

Fidelity

$2.1m savings

16% increase in satisfaction score

INTESA SANPAOLO

Reduction of 65% in the operations through Six Sigma in some processes

"There's too much waste in banking.." Carl E. Reichardt , Wells Fargo

The Challenges

Plus

Top Management Support

Organizational culture

Dedicated team

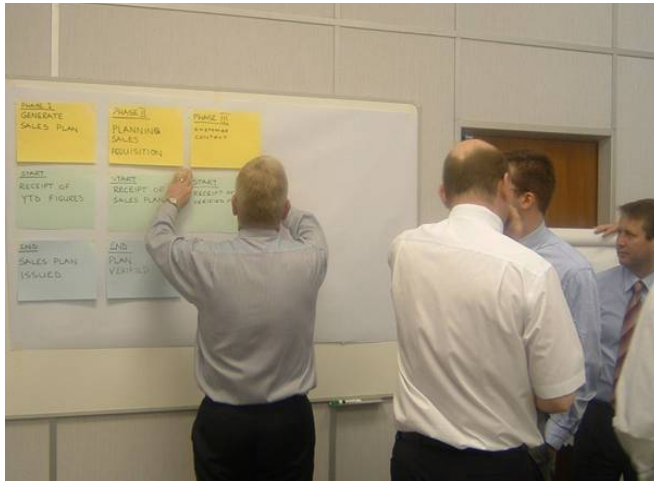
Delta

If the limit is reaction

If project focus creates local success but is not replicated

Lack of Awareness

Agenda



- The Challenges
- An Integrated Approach: Lean & Digitize
- Applications to Security Management
- Some Standards and Best Practices
- **The Future**

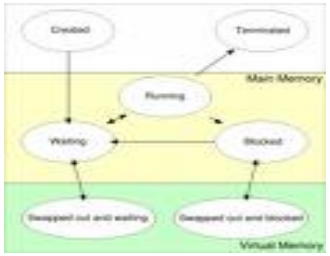
The Future of Security Management

Integration

Mobility

Collaboration

Process

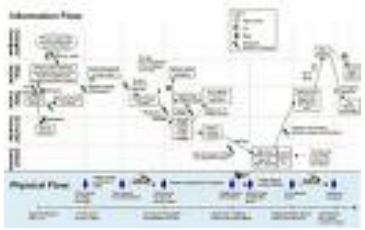


Integration of security and business process approach

Management of security in the full end-to-end processes

Go beyond the “wall” of the Businesses

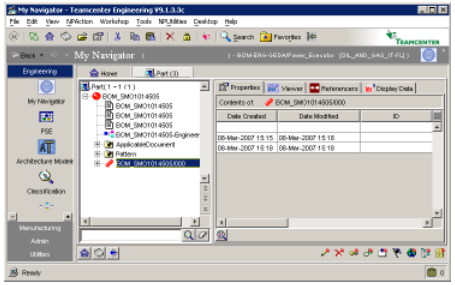
Physical



Virtualization

Green

Digitization



More and more
Web 2.0 => Security 2.0

Video: Web 3.0?

Personal devices

Infrastructure Protection and Management

EDSA – Event Driven Security Architecture

And in the Near Future ?

Gartner says that
"the continuous convergence of the technology, the models of the market and of the organizational processes offer to the businesses the opportunity of costs reduction while at the same time improving the levels of security"

Forrester Research says that
"Security will get a slightly larger percentage of IT budget dollars this year -- on average, 12.6 percent of total IT spending, compared to 11.7 percent in 2008. But because IT budgets are expected to drop 3.1 percent in 2009, that's a big jump in relative terms".

How to Cut Security Costs

- Information Security Awareness Programs
- Security intelligence from free projects.
  such as the Shadowserver project,
- Open Source
  ClamAV anti-virus software and Snort intrusion detection system are two widely used open source anti-virus products.
- Storage encryptions using free ware
  True-Crypt (but watch at Windows 7)
- Outsourcing security to the cloud.
  Forrester Research reports that 28 percent of companies that move to in-the-cloud managed security services do so to cut costs. Although e-mail and Web filtering are the most popular managed security services today, Forrester projects that more businesses will move to the cloud for vulnerability assessment and event monitoring as well.
- Cutting down on manual processes can reduce costs and refocus staff resources

An Holistic Approach is Essential

Awareness: Employee Security Policy/Risk Awareness
- Consistent messages, tools implemented across the business

Prevention: Focus on Vulnerability Management
- Network, wireless, and system vulnerability scanning and remediation incorporated into IT operations, escalation and issue resolution by Security
- Efficiencies through automation of patch and configuration management

Data Protection: Securing Access and Confidentiality
- Encryption of data based on data classification
- Access controls based on authorization

Detection: Advanced Intrusion Detection Monitoring & Response
- Ubiquitous, 24x7 monitoring of deployed HIDS and NIDS
- 24x7 business response process in place

Investigation: Core Competency in Forensics Analysis
- Standardized Forensics capabilities in all businesses for evidence preservation and analysis

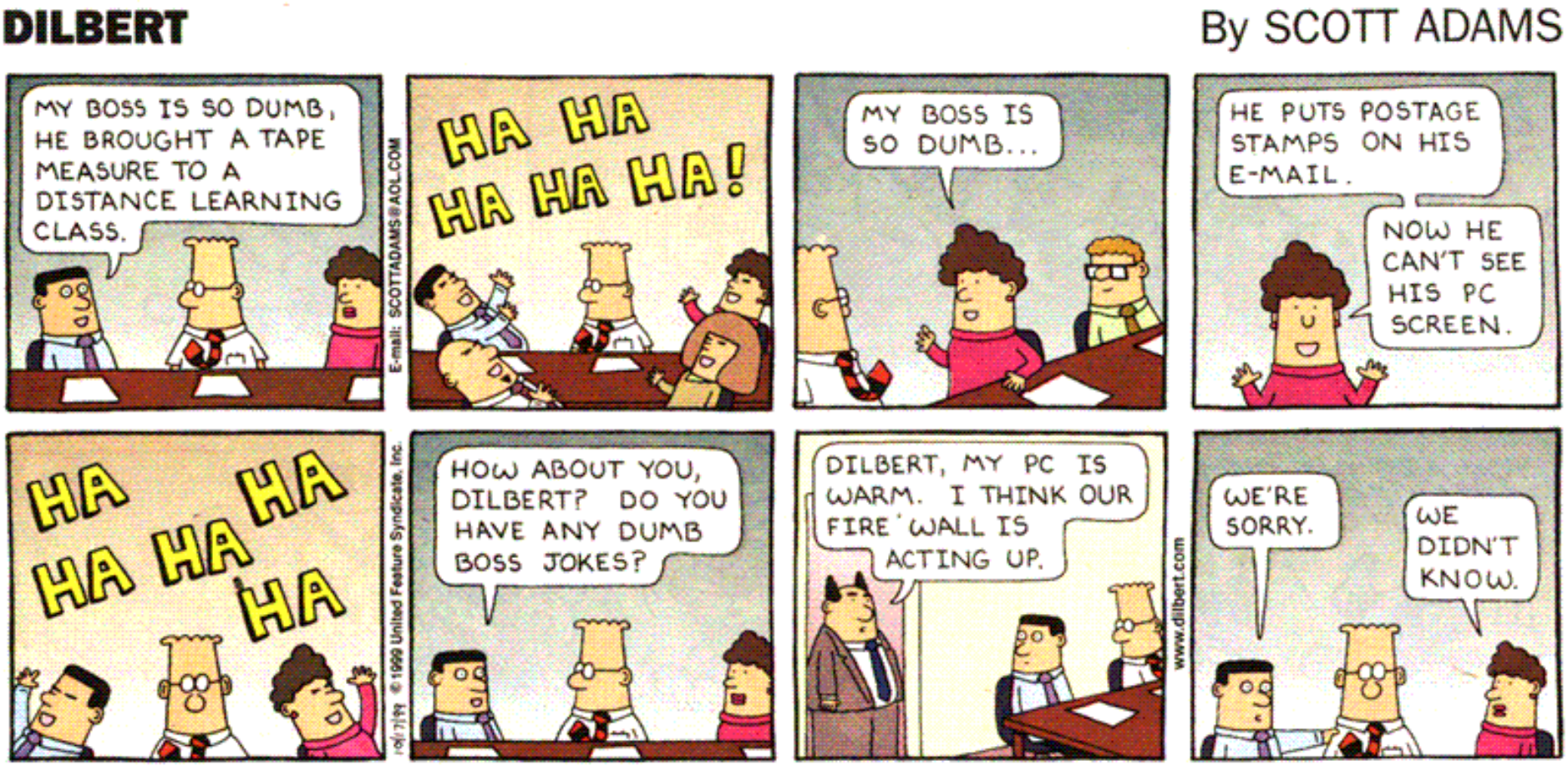
Common Baseline of a Security Awareness Program

Content

- What is Information Security?
- Why does Information Security Matter?
- How does Information Security Affect Me?
  - Entry Control
  - Clear Desk Policy
  - Secure Disposal
  - Passwords
  - Systems Integrity
  - Virus Control
  - Using E-Mail
  - Internet Security
  - Faxing Information
  - Security Out of the Office
  - Social Engineering
  - General Responsibilities
- Course Exam

Summary

- The development and convergence of technologies is creating new problems. Security has changed dramatically with the new scenarios. To prevent damage from the most damaging threats shall require cooperation between multiple security products (more and more integrated).
- It is essential a long term commitment to change and process improvements taking into account security
- It is important to define clear objectives, decide a plan and launch projects
- Integrated Governance, Risk and Compliance are essential
- The Chief Information Security Officer needs to adapt to these new situations in order to be able to provide an adequate protection to the Business
- Lean and Digitize create effective security processes, lock in them and reduces wasted time and resources



Manage Your Top Management

Thank You – Any Question ?

Bernardo Nicoletti

CIO

Bernardo.nicoletti@katamail.com

+39 348 470 7016

Appendix

Resume

- Born in Salerno, Italy
- Fulbright Scholar with a Master from Carnegie Mellon University and a Degree from the Polytechnic of Turin, Italy
- Worked in 10 Countries in several companies
    - MIS and CTO in Alitalia
    - Project Leader in Airplus
    - Program Leader in Galileo
    - CEO in Sigma Plus
    - CTO in GE Money
    - CIO in GE Oil & Gas
    - CIO in AIG CFG Latin America
    - Management Consultant
- Master Black Belt