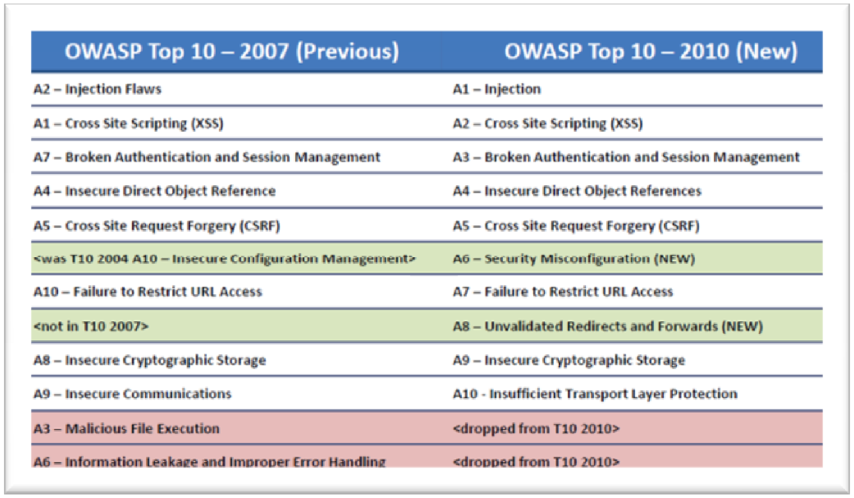
The Future of Cybersecurity

ISSA Italy Chapter Conference
Rome, Italy

28 October 2010

Things we already know…

- Our web applications are still broken…
  - with the same problems (mostly)…
- In 2009, over 143 million records were reported as inadvertently disclosed
- Several thousand active botnets (and several million systems) are being tracked, monitored, and battled within our enterprises
- Process and business unit outsourcing and offshoring are moving assets beyond our practical control
- Data is just about everywhere
- Budgets and staffing are shrinking
- We're being told…
  - Improve time to market
  - Lower costs
  - Competitive advantage



OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 - Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

The Future of Cybersecurity…

Cybersecurity Challenge #1

Challenge #1 – The Ever-Changing Landscape

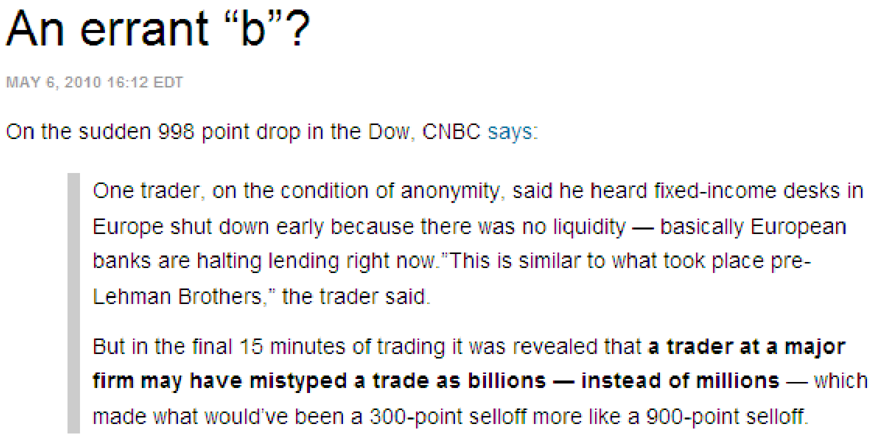
- No definable perimeter
- Data on the move
- Data and critical business processes outsourced, off-shored, or “stuffed” into the cloud
- Computing power portability is changing the way we work

Cybersecurity Challenge #2

Challenge #2 – The Attackers Are More Nimble…

- Google attack/Aurora, Zeus-delivered attacks are just examples of the next generation of cyber attackers
  - The attackers are aggressive, talented, and motivated
- Botnets and zero-day attacks are big business
  - Significant money to be had
  - Attracting world class technology talent
  - Seem to have unlimited resources
- We've increased the attack landscape to potential attacks, and are struggling to fix known problems
  - More web services
  - Mobile devices
- Achieving compliance is no longer helping security
- The technologies that are deployed are not as effective as management expects

An Errant "B"…

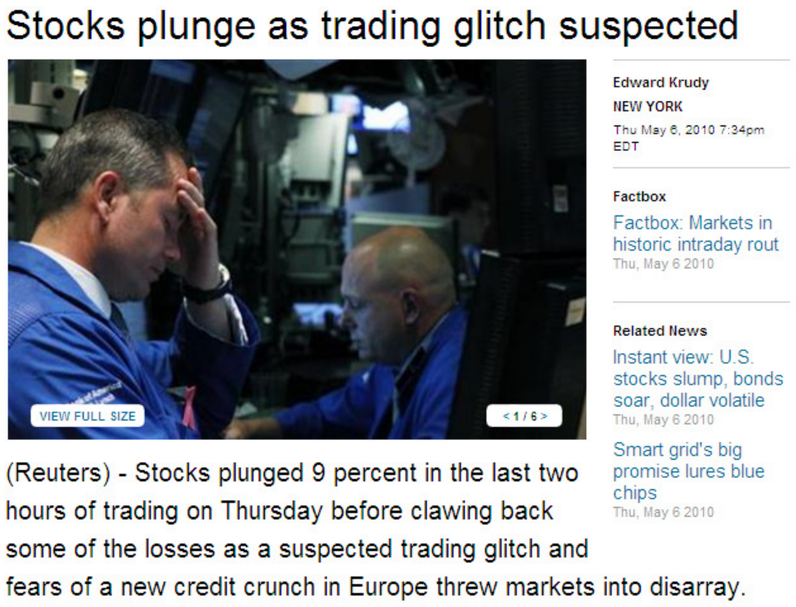


An errant "b"?

MAY 6, 2010 16:12 EDT

On the sudden 998 point drop in the Dow, CNBC says:

> One trader, on the condition of anonymity, said he heard fixed-income desks in Europe shut down early because there was no liquidity — basically European banks are halting lending right now."This is similar to what took place pre-Lehman Brothers," the trader said.
>
> But in the final 15 minutes of trading it was revealed that **a trader at a major firm may have mistyped a trade as billions — instead of millions** — which made what would've been a 300-point selloff more like a 900-point selloff.



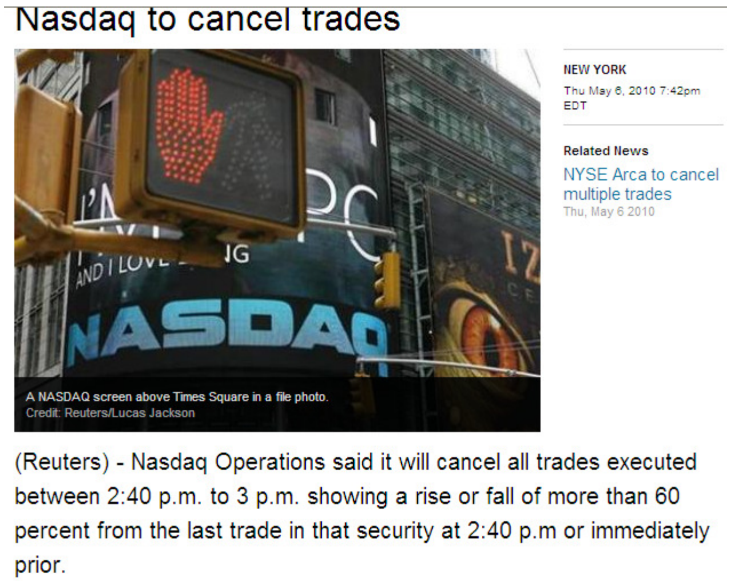
Stocks plunge as trading glitch suspected

Edward Krudy
NEW YORK
Thu May 6, 2010 7:34pm EDT

Factbox
Factbox: Markets in historic intraday rout
Thu, May 6 2010

Related News
Instant view: U.S. stocks slump, bonds soar, dollar volatile
Thu, May 6 2010
Smart grid's big promise lures blue chips
Thu, May 6 2010

(Reuters) - Stocks plunged 9 percent in the last two hours of trading on Thursday before clawing back some of the losses as a suspected trading glitch and fears of a new credit crunch in Europe threw markets into disarray.



Nasdaq to cancel trades

A NASDAQ screen above Times Square in a file photo.
Credit: Reuters/Lucas Jackson

NEW YORK
Thu May 6, 2010 7:42pm EDT

Related News
NYSE Arca to cancel multiple trades
Thu, May 6 2010

(Reuters) - Nasdaq Operations said it will cancel all trades executed between 2:40 p.m. to 3 p.m. showing a rise or fall of more than 60 percent from the last trade in that security at 2:40 p.m or immediately prior.

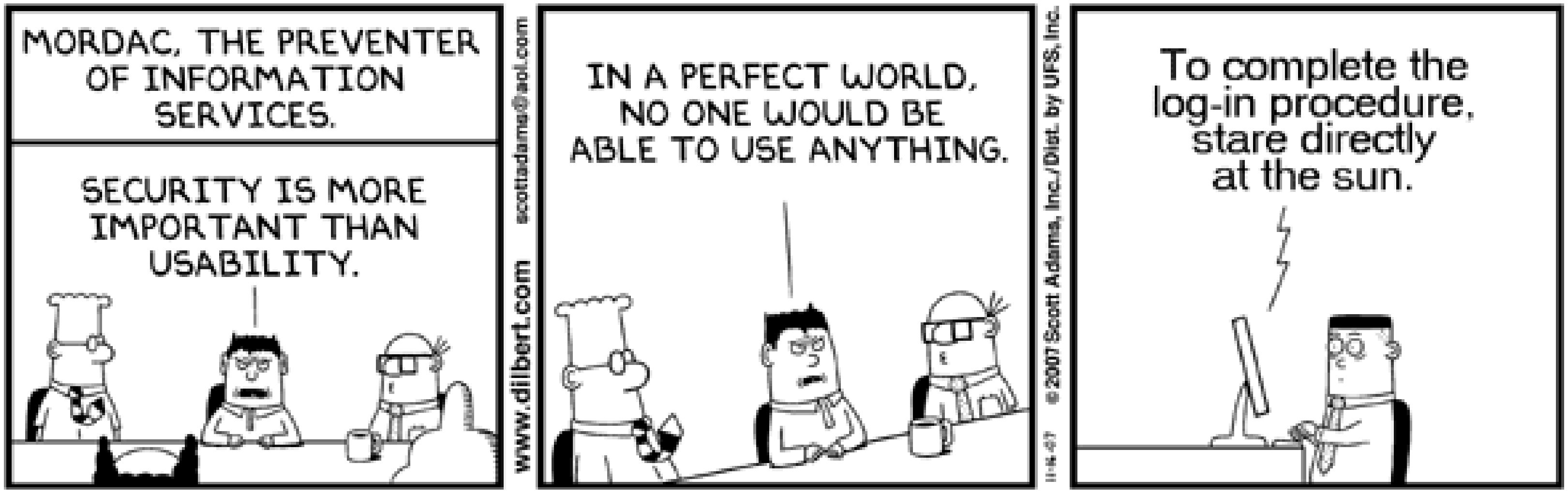
Cybersecurity Challenge #3

Challenge #3 – The Federation of Trust

- The future of cybersecurity is predicated on trust
  - Online, social networking, and e-commerce sites
  - 3rd parties and outsourcers
  - Crossing industries
    - Healthcare, Financial Services, Utilities, Transportation, Public Sector
- Competing approaches to “presenting” trust
  - ISO27001/BS7799-2, SAS70/CICA-5900, PCI, BITS, “Security Seals”, etc.
- As a profession, we have a significant challenge with trust
  - Standards and compliance can be too general
  - Professional skepticism
  - Accountability

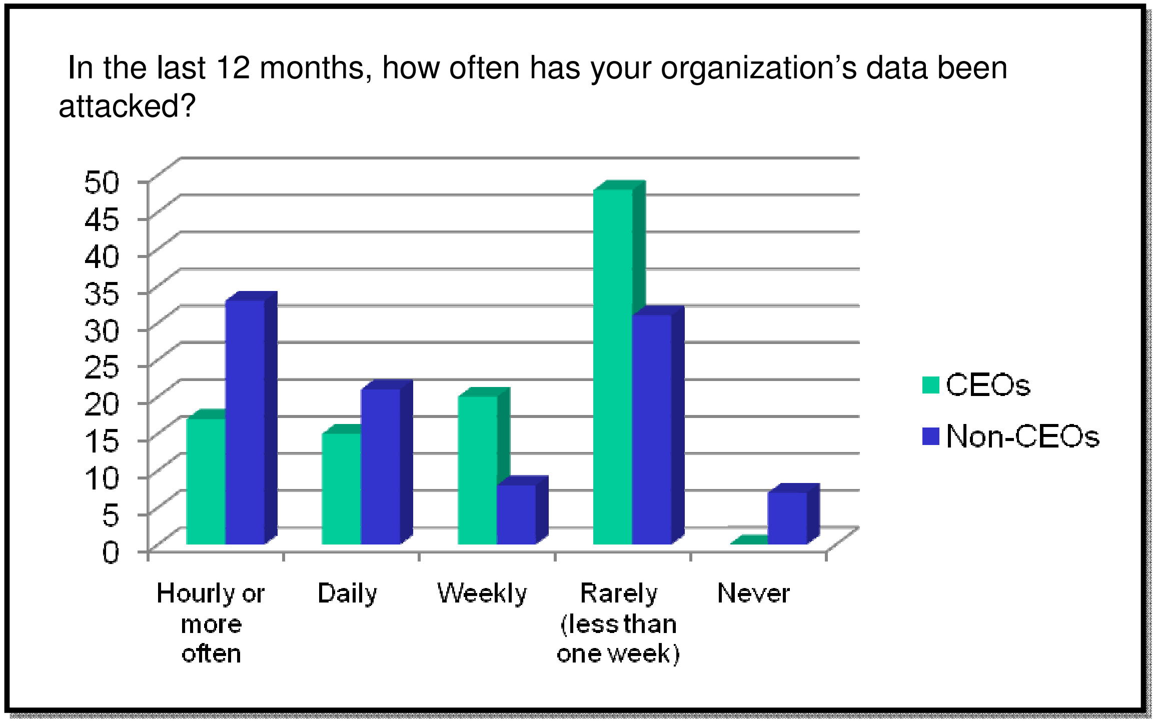
Cybersecurity Challenge #4

Challenge #4 – Growing Gap Between Infosec and ERM


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
To complete the log-in procedure, stare directly at the sun.

© Scott Adams, Inc./Dist. by UFS, Inc.

Is there a communication problem?


In the last 12 months, how often has your organization's data been attacked?

Is the budget for data protection adequate?

	CEO %	Non-CEO %
Yes	64%	55%
No	36%	45%

Source: Ponemon Institute© Research - Business Case for Data Protection

Two Worlds Separated by a Common Language

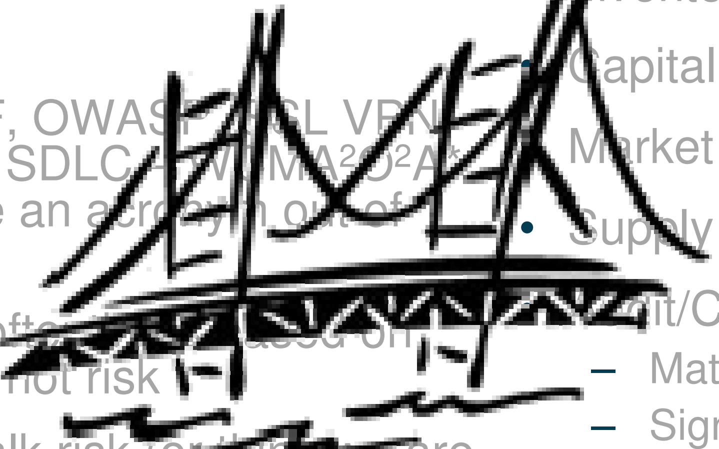
Infosec

- Buffer overflow
- XSS
- p@wn’d
- IDS, IPS, WAF, OWASP, SSL VPN, IAM, DLP, PII, SDLC – WCMA^{2}O^{2}A* (*we can make an acronym out of anything)
- Discussion is oftentimes based on vulnerabilities, not risk
- When we do talk risk (or think we are talking risk)…
  - Low, Medium/Moderate, High
  - Appeared Secure, Potentially Vulnerable, Vulnerable, Severely Vulnerable, Compromised

Business

- Liquidity
- Inventory turns
- Capital on hand
- Market risk
- Supply chain
- Audit/Compliance
  - Materiality
  - Significant deficiency
  - Material weakness

Two Worlds Separated by a Common Language



Infosec

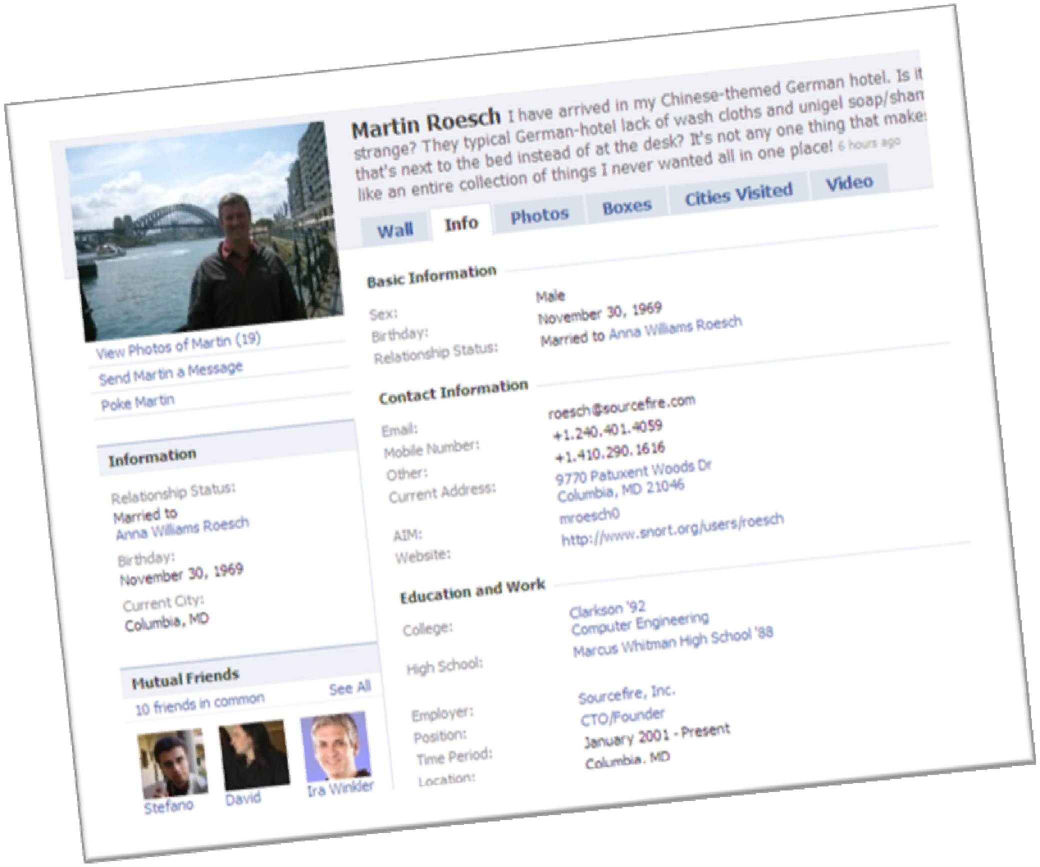
- Buffer overflow
- XSS
- p@wn’d
- IDS, IPS, WAF, OWASP, SSL VPN, IAM, DLP, PII, SDLC, HW, MA^{2}O^{2}A* (*we can make an acronym out of anything)
- Discussion is often focused on vulnerabilities, not risk
- When we do talk risk (or think we are talking risk)…
  - Low, Medium/Moderate, High
  - Appeared Secure, Potentially Vulnerable, Vulnerable, Severely Vulnerable, Compromised

Business

- Liquidity
- Inventory turns
- Capital on hand
- Market risk
- Supply chain
- Audit/Compliance
  - Materiality
  - Significant deficiency
  - Material weakness

Cybersecurity Challenge #5

Challenge #5 – The Way People Think Has Changed



Martin Roesch I have arrived in my Chinese-themed German hotel. Is it strange? They typical German-hotel lack of wash cloths and unigel soap/shan that's next to the bed instead of at the desk? It's not any one thing that make like an entire collection of things I never wanted all in one place! 6 hours ago

Information

Relationship Status:
Married to
Anna Williams Roesch

Birthday:
November 30, 1969

Current City:
Columbia, MD

Mutual Friends

10 friends in common

Stefano David Ira Winkler

Basic Information

Sex: Male
Birthday: November 30, 1969
Relationship Status: Married to Anna Williams Roesch

Contact Information

Email: roesch@sourcefire.com
Mobile Number: +1.240.401.4059
Other: +1.410.290.1616
Current Address: 9770 Patuxent Woods Dr
Columbia, MD 21046
AIM: mroesch0
Website: http://www.snort.org/users/roesch

Education and Work

College: Clarkson '92
Computer Engineering
High School: Marcus Whitman High School '88

Employer: Sourcefire, Inc.
Position: CTO/Founder
Time Period: January 2001 - Present
Location: Columbia, MD

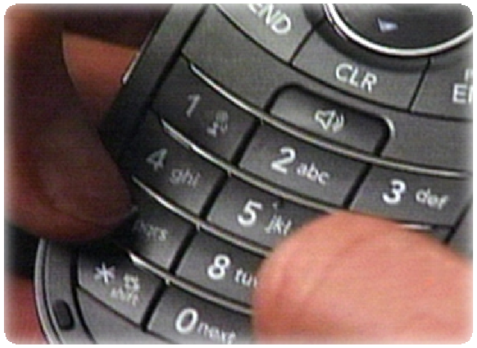
twitter facebook myspace.com a place for friends LinkedIn

ISSA

Cybersecurity Challenge #6

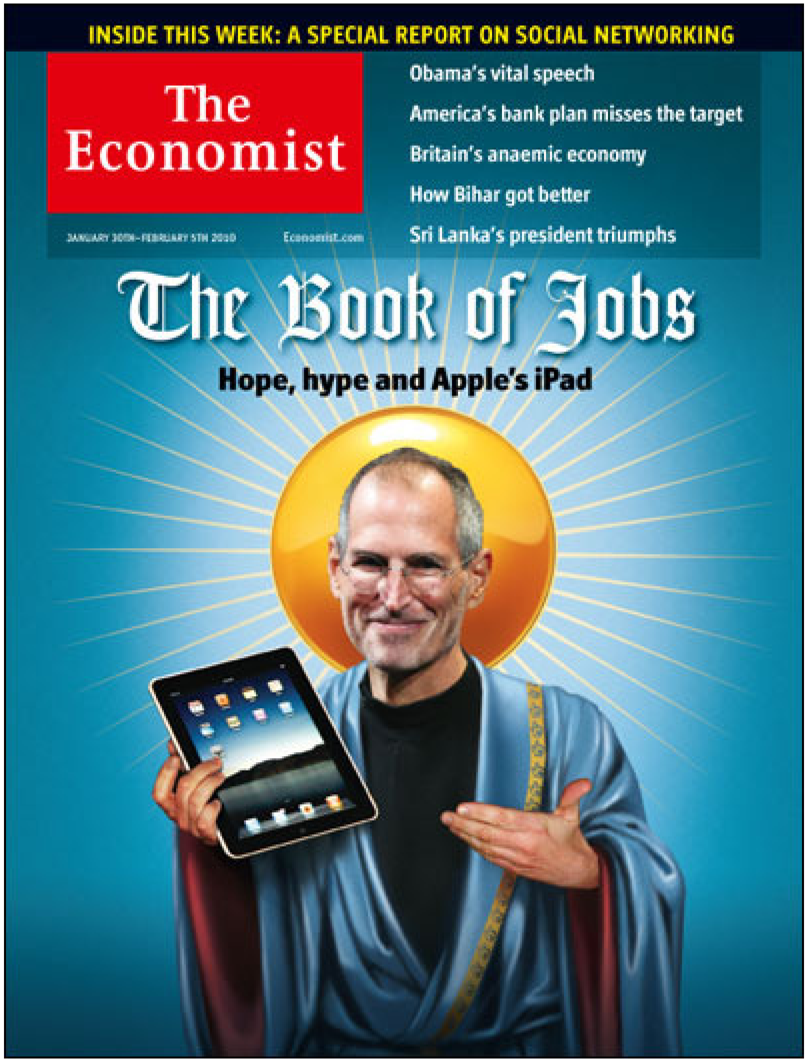
Challenge #6 – Educating the Next Generation

- Our children



- College graduates

- New hires



INSIDE THIS WEEK: A SPECIAL REPORT ON SOCIAL NETWORKING

The Economist

JANUARY 30TH–FEBRUARY 5TH 2010

Economist.com

Obama's vital speech

America's bank plan misses the target

Britain's anaemic economy

How Bihar got better

Sri Lanka's president triumphs

The Book of Jobs

Hope, hype and Apple's iPad

Thank You!

ISSA®
Information Systems Security Association
The Global Voice of Information Security

Kevin Richards, CISSP
President, ISSA International

773-269-6350

kevin.richards@issa.org