Security in tune with business

The 8 Critical Success Actions for IT security

by Alberto Partida

V OWASP Spain Chapter Meeting – Barcelona, 15 May 2009

Asociación de Técnicos de Informática

internet security auditors

ps_testWare Software Testing Services

OWASP The Open Web Application Security Project

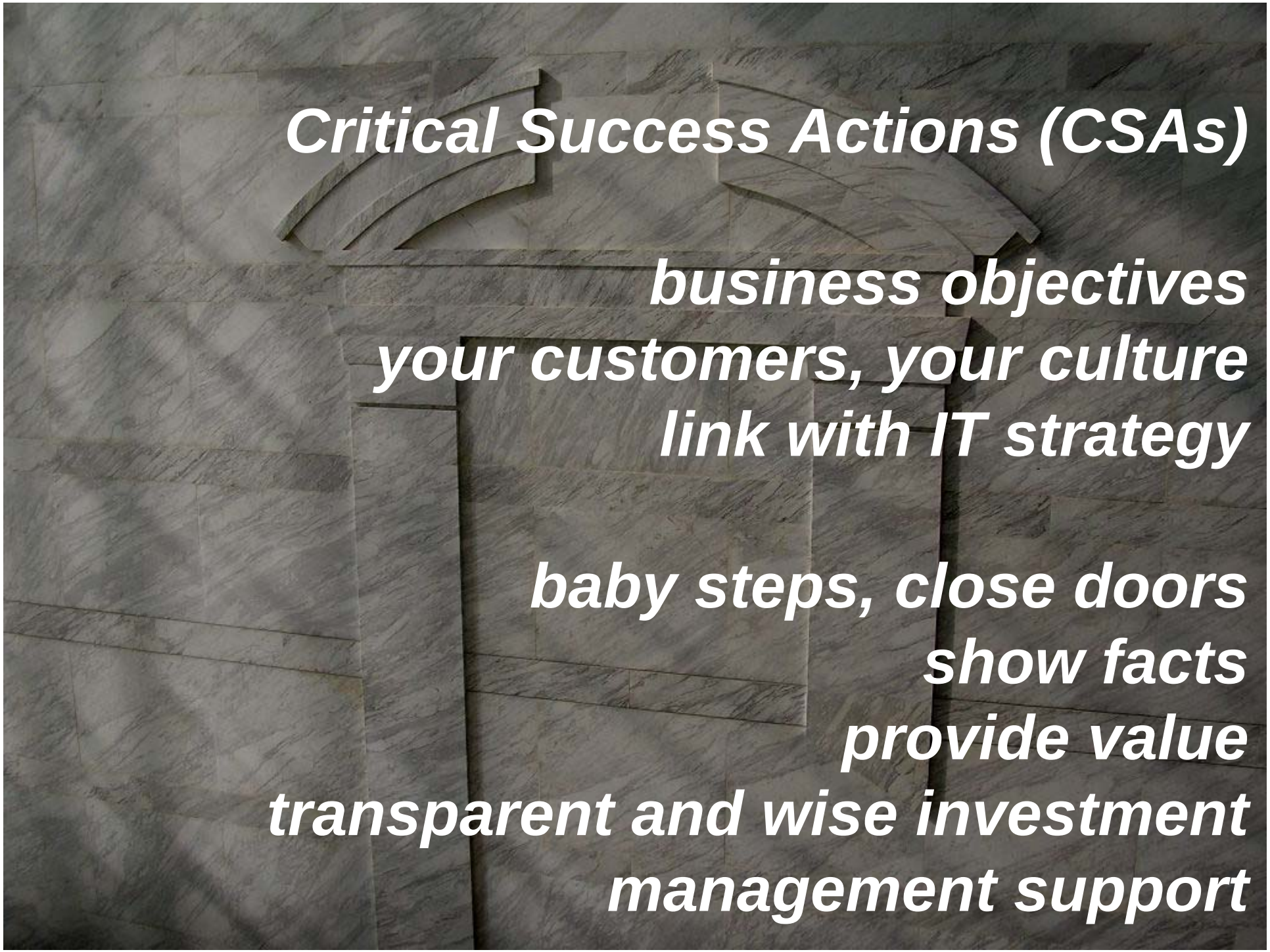
About me…

Alberto Partida

- IT security professional
- 10+ year experience
- Industry (telecom and banking) and academia

- UPM Telecommunication Engineer
- SANS GIAC Gold GSEC, Gold GCFW, Gold GCFA
- SANS GCIA & GREM
- SANS Advisory Board Member since 2003
- CISA, CISSP, Henley MBA
- Collaborator in SIC security magazine

securityandrisk.blogspot.com


Critical Success Actions (CSAs)
business objectives
your customers, your culture
link with IT strategy
baby steps, close doors
show facts
provide value
transparent and wise investment
management support

Critical Success Actions (CSAs)

From factors…

What customers want and what companies need to compete

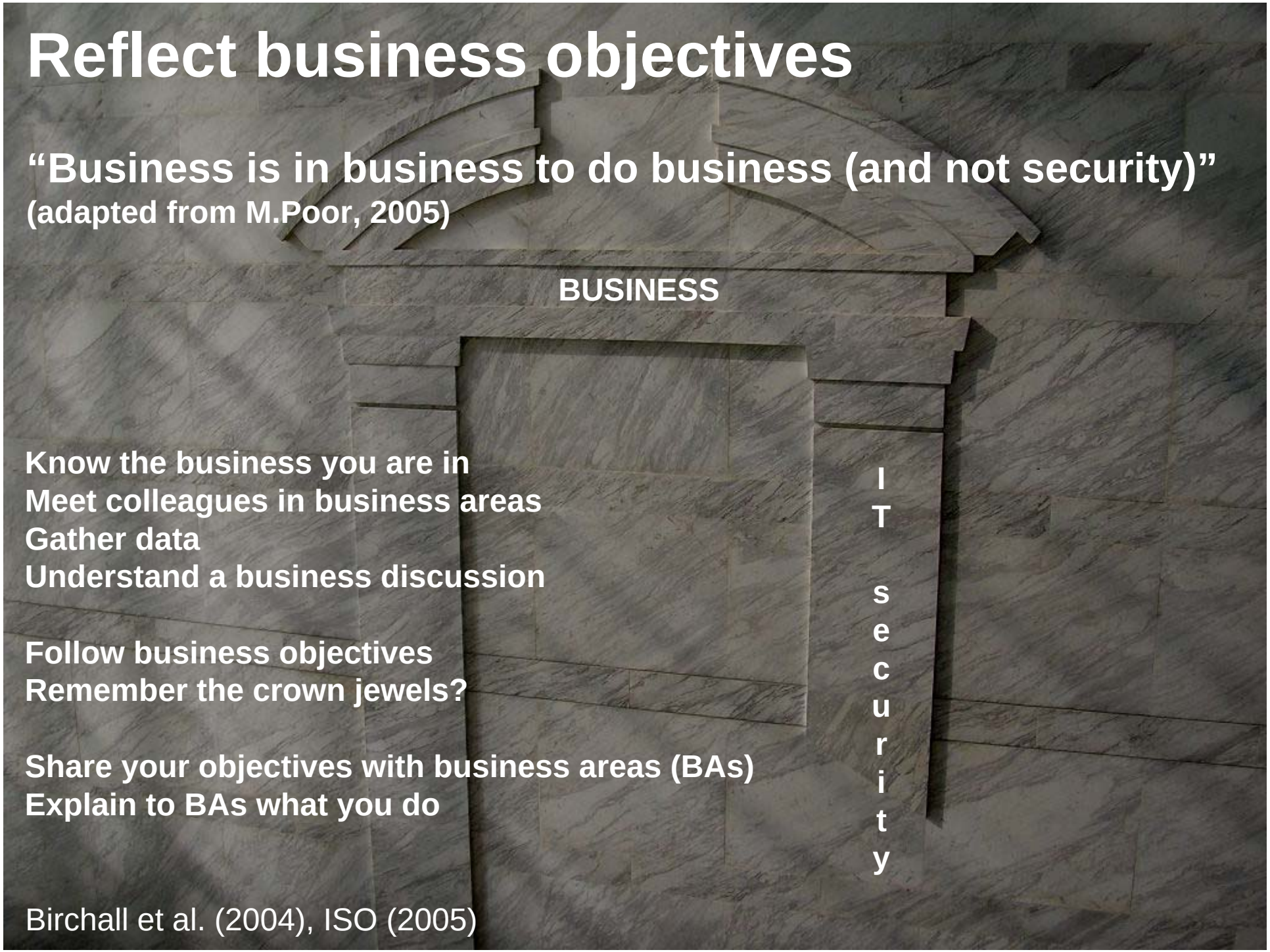
… change factors into actions …

What we need to DO in IT security to enable the business and enhance our added value (and daily experience)

Thomson (2005)

Reflect business objectives

“Business is in business to do business (and not security)”
(adapted from M.Poor, 2005)



Know the business you are in
Meet colleagues in business areas
Gather data
Understand a business discussion

Follow business objectives
Remember the crown jewels?

Share your objectives with business areas (BAs)
Explain to BAs what you do

Birchall et al. (2004), ISO (2005)

Be consistent with customers & culture

Are you trying to change the business culture?
Often not possible nor requested by the organisation

BUSINESS

Power distance
Consensus-driven?

Avoid unclear risk ownership
Stakeholder theory

Leadership
Trends and tendencies

IT security

ISO (2005)

Link IT security with IT strategy

Information resides on IT systems
IT security allocates and mitigates risk

BUSINESS

Information

Information systems

IT security

Know the strategy of your IT shop
Project-driven?
“Home-made” vs. “off the shelf”?

Managed services
Have a chair on IT management board

IT security vs. IT experts? Make swaps

Leskela et al. (2005), Booker (2006)

Follow baby steps and close doors

From a 3-year programme to a monthly schedule
Strive to finalise activities

Use a reference model, a standard
Base your work programme on it but…

Break down your plan into pieces
Start A, complete A
Then, start B

ISF (2005), Straub (1990), von Solms (2005b)

Show facts

Increase the understanding of the need for security
Follow IT security related news

Thieves take computers from 60+ businesses in one building (from www.latimes.com April 26, 2009)

Former Federal Reserve analyst charged with bank fraud and identity theft (from www.computerworld.com April 24, 2009)

Hospital data on stolen laptop were not encrypted (from www.pressandjournal.co.uk April 24, 2009)

Three years after the fact, UK's Serious Organized Crime Agency has acknowledged that a lost memory stick caused it to abandon a major drug case (from www.timesonline.co.uk April 27, 2009)

Create ubiquitous security
Raise awareness

Talk business language (no IT jargon)
Explain why you do it

Be a journalist
Get to know the risk appetite

Birchall et al. (2004), Coles and Moulton (2003),ISO (2005), OECD (2003), Scholtz (2004), extracts from SANS Newsbites

From "Britain's Antiterror Officer Resigns," New York Times, April 10, 2009, at http://www.nytimes.com/2009/04/10/world/europe/10britain.html?ref=todayspaper and "Police chief Bob Quick steps down over terror blunder," Guardian, April 9, 2009, at http://www.guardian.co.uk/uk/2009/apr/09/bob-quick-terror-raids-leak.

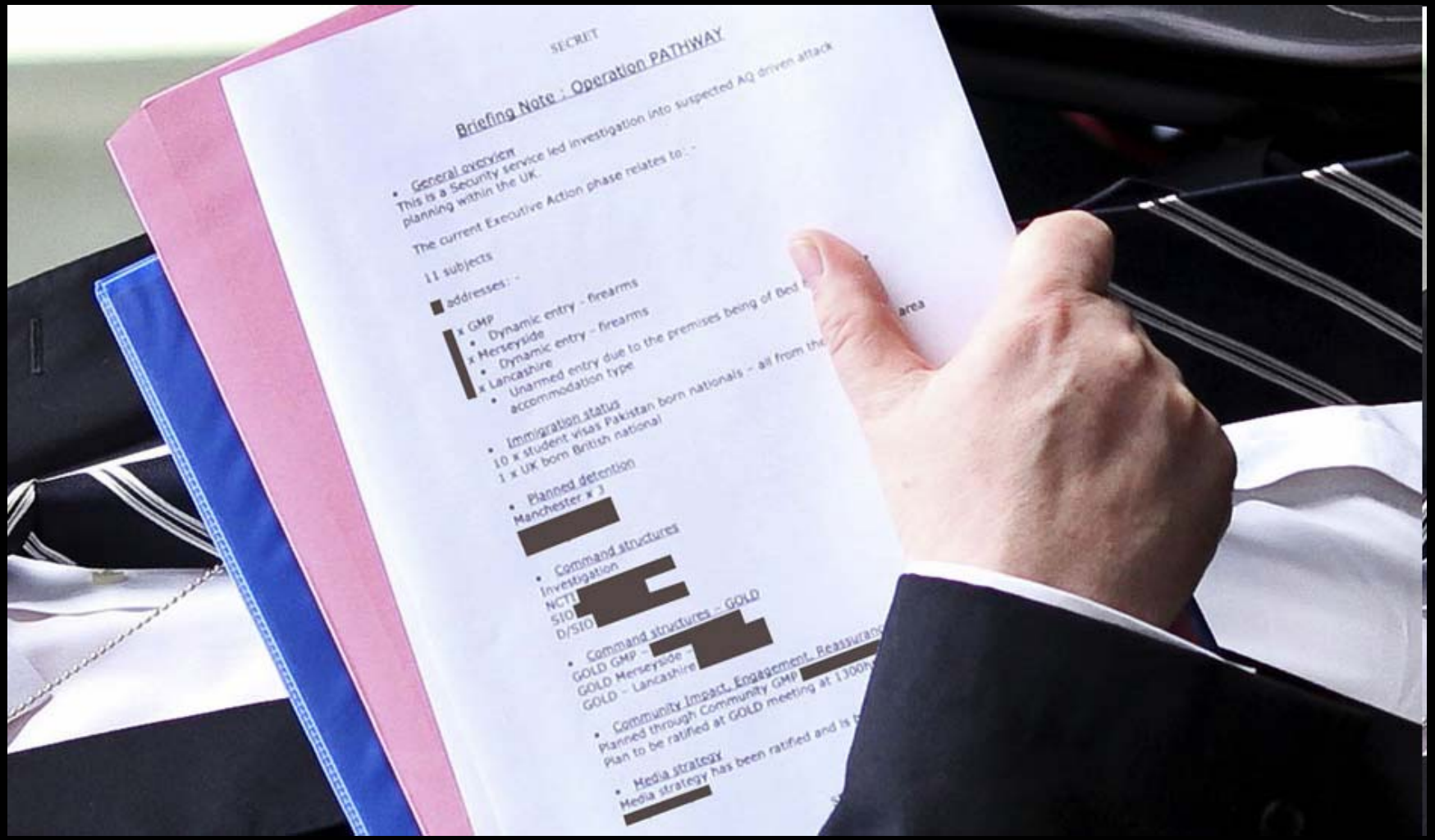
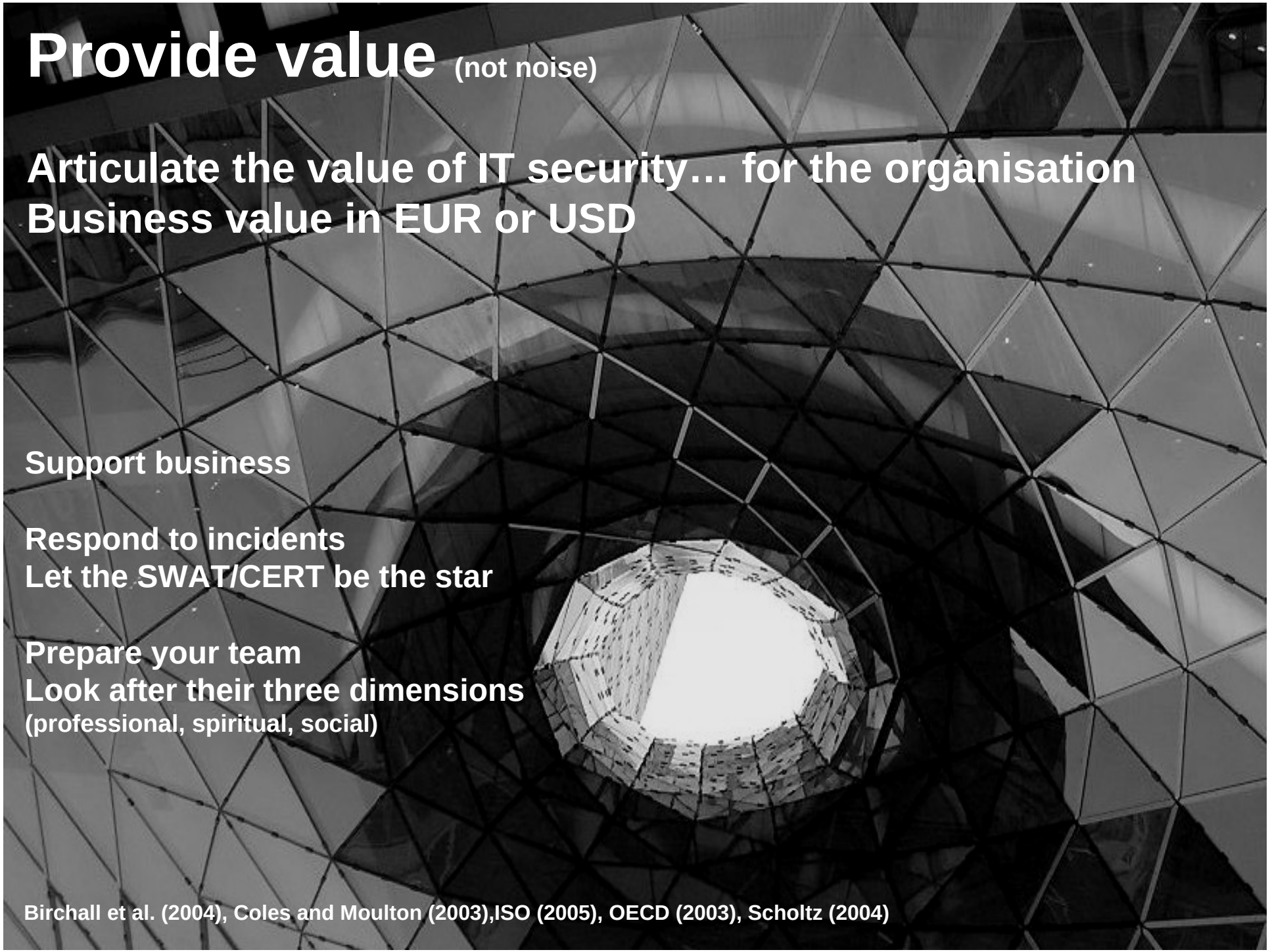


Photo from http://www.guardian.co.uk/uk/2009/apr/09/bob-quick-terror-raids-leak



Provide value (not noise)

Articulate the value of IT security… for the organisation
Business value in EUR or USD

Support business

Respond to incidents
Let the SWAT/CERT be the star

Prepare your team
Look after their three dimensions
(professional, spiritual, social)

Birchall et al. (2004), Coles and Moulton (2003),ISO (2005), OECD (2003), Scholtz (2004)

Invest transparently and wisely

Prioritise expenditures to mitigate risk
Jump on already running trains

Use the “bang for the euro” index
Provide financial transparency to risk metrics

A = Cost (mitigating measure)
B = Cost (materialised risk)
A < B but not always

Report on incidents and threats

(Aabo et al., 2004; Dillon and Paté-Cornell, 2005; Rinnooy, 2004)

Obtain management support

Support, commitment and sponsorship
Management buy-in is essential for success

BUSINESS

Business processes

Information

Information systems

Risk appetite

Risk management in job descriptions
Conscious risk awareness

Focus on people and not labels
Who communicates in the group?

But do not mix functions ;-)
Just help to close the gap

COSO (2004), ISO (2005)


If we aim for a different result…


…then we have to act differently.

References

- Aabo, Tom, Fraser, John R.S., Simkins, Betty J. (2004). *The rise and transformation of the chief risk officer: a success story on enterprise riskmanagement*. Version of December 10, 2004. Revised version available in Journal of Applied Corporate Finance, Winter 2005. Pages 1-34, Available from: http://www.gloriamundi.org/detailpopup.asp?ID=453057237 [Accessed 16 April 2006]
- Birchall, David, Ezingeard, Jean-Noël and McFadzean, Elspeth (2004). *Information assurance. Strategic alignment and competitive advantage.* Grist and Henley Management College sponsored by Qinetiq. Executive summary also referenced. Pages 1-73.
- Booker, Robert (2006). *Re-engineering enterprise security*, Computers & Security 25. 13-17.
- Coles, Robert S. and Moulton, Rolf (2003). *Operationalizing IT risk management*, Computers & Security 0167-4048/03. Pages 487-492.
- Committee of Sponsoring Organisations of the Treadway Commission COSO (2004). Enterprise Risk Management Framework - Executive summary - Exposure Draft for Public Comment (pages 1-103) downloadable from http://www.coso.org/publications.htm
- Dillon, Robin L. and Paté-Cornell, Elisabeth (2005). *Including technical and security risks in the management of information systems: a programmatic risk management model*. Systems engineering. 8. 1. Regular paper. Pages 15, 17, 18 and 24.
- Information Security Forum ISF (2005). *The Standard of Good Practice for Information Security*. Reference ISF 05-104. Pages 1-28.
- *ISO (2005) ISO/IEC 17799 Information technology - Security techniques - Code of practice for information security management*. Second edition 2005-06-15. Reference: ISO/IEC 17799-1:2005(E). Pages 1-115.
- Leskela, Lane; Knox, Mary; Schehr, David; Furlonger, David; Redshaw, Peter (2005). Client issues 2005: How to achieve regulatory compliance and ERM, Gartner, Research note. 29 March 2005. ID Number: G00126561. Pages 1-4.
- May, Cliff (2002). Risk Management - Practising what we preach, Computer Fraud & Security, 8: 10-13.
- Organisation for Economic Co-operation and Development (2003). Implementation plan for the OECD guidelines for the security of information systems and networks: towards a culture of security. Working Party on Information Security and Privacy. 2 July 2003. Pages 1-6.
- Rinnooy Kan, A.H.G. (2004). IT governance and corporate governance at ING. Information systems control journal. 2 26-31.
- Scholtz, Tom (2004). Articulating the Business Value of Information Security. Security & Risk Strategies, Security Infusion, Global Networking Strategies, Meta Group, Meta Delta 2774. Pages 1-4.
- Straub Jr, D.W. (1990). Effective IS Security: An Empirical Study, The Institute of Management Sciences, Information Systems Research 1(3):255-276.
- Thompson, John with Martin, Frank (2005). Strategic management. Thomson 5th edition. Key success factors and E-V-R congruence. Pages 114 and 125-130.
- von Solms, Basie (2005a). Information Security Governance: COBIT or ISO 17799 or both?, Computers & Security 24, 99-104.
- von Solms, Basie (2005b). Information Security Governance: Compliance management vs operational management, Computers & Security, 24, 443-447.


Thank you
Happy to go to…
Q&A
securityandrisk.blogspot.com