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
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

Power distance
Consensus-driven?
Avoid unclear risk ownership
Stakeholder theory
Leadership
Trends and tendencies

ISO (2005)
Link IT security with IT strategy

Information resides on IT systems
IT security allocates and mitigates risk

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

BUSINESS

Information
Information systems

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
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

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

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)

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

General Overview
This is a security service-led investigation into suspected Al Qaeda driven attack planning within the UK.

The current Executive Action phase relates to:

1. Subject:
   - GMP
   - Dynamic entry - firearms
   - Merseyside
   - Lancashire
   - Unknown entry due to the premises being of best accommodation type

2. Immigration Status:
   - F5 student from Pakistan born nationally - all from the same family
   - UK born British National

3. Planned detention
   - Manchester

   - Committed structures
     - Investigation
     - SW [redacted]
   - Community Impact Engagement, Reassurance and media
     - Plans to be raised at GOLD meeting at 1300

   - Media strategy
     - Media activity has been raised and is the focus

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)

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

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

If we aim for a different result...
...then we have to act differently.
References

Thank you

Happy to go to...

Q&A

securityandrisk.blogspot.com