

Risk Management in a Networked Coalition or - is security our friend?

11th ICCRTS
September 2006

Michael Stubbings, QinetiQ
Dave Biddinger, SPARTA

Objectives

- » To stimulate thought and conversation on the topics of risk in relation to command and control
- » To generate new and innovative ideas to help improve the state of risk management
- » To take forward issues raised or implied in this conference
 - Coalition policy
 - Governance, including risk accountability
 - Systems engineering – where 'system' includes people and process
 - Information management
- » To articulate a C2 community security agenda with the C2 community's priorities

- » The review of this topic is structured as a series of facilitated discussions, each topic will have some questions to stimulate the conversation. All ideas, issues and other important discussion points will be recorded for future use.

Agenda

» Kickoff and Introductions

» Topics:

- Coalition Risk Sharing
- Certification and Accreditation
- Effectiveness of current Cross-Domain solutions
- Roadmap for Success – whatever that is...

» Review and Feedback

Coalition Risk Sharing

Coalition Risk Sharing

- » Our coalition partners realize that RM methods are not adequate for today's nor tomorrow's operating environment. RM needs to be accomplished continually, in an adaptive, context-aware manner. Information needs to be delivered appropriately throughout the coalition both on-demand and as discovered.

- » Let's first explore some "starter" questions...

What is Our Experience?

- » Is there any evidence or narrative that opportunities have been lost because we observed the information security rules strictly?
- » Are there examples where flexibility in applying security rules has come at a price? – or might have done if someone had not stepped in and corrected matters?
- » What has operational military – especially Command and Control – experience got to say that information security practitioners and policy makers should heed?
- » Should we disseminate risk authority down the chain of command in an accountable and reportable manner? If so, how, and how far?

Are Information Security Risks Different from other Operational Risks?

- » Defence involves many different sorts of risk, and devolves assessment and management of these risks to field personnel. To what extent does our approach to information risk management map onto our broader military management of risk?
- » If our concepts of risk management and risk appetite are different for information security risks than for other defence risks, why is that? Is there a good reason?
- » To what extent do we want to devolve decision-making to a 'Strategic Corporal' in an accountable and reportable manner? (especially if he's someone else's Strategic Corporal)?

One Risk Posture versus Many?

- » How many risk postures do we need? Accreditation as currently practiced gives us just one.
- » If we have more than one posture – how do we manage the changes from one to another?
- » How do we recognise/manage the need for a new posture?
- » Can we manage more than one risk posture running in parallel across our networks and other assets? If the answer is 'no' do we need to change this? Does NEC imply multiple parallel risk postures?

Constraints on Risk Policy

- » National Policy – does it help or hinder us, or both? It's changed before and it can change again

- » Organisational/Departmental priorities (reputation, relationships, morale etc.)

- » Law (including passage of valid military orders)

- » Cast list – who are the players and what are their interests?
 - Coalition partners (some not known as well as we know others)
 - Civil partners (OGDs, UN)
 - Others (NGOs, press, local in-theatre authorities)

Some Policy Questions

- » Which is more important – that a risk assessment is done, or that it is done well? How good is good enough for us? How good is good enough for our partners?
- » How do we recognise a need for change in our risk posture or risk appetite?
- » Do we act on a risk assessment – at whatever level? If not, why do the assessment?
- » How do we gain assurance that we've acted appropriately?
- » How do other people (e.g. national security authorities, coalition partners) gain assurance that we continue to act appropriately?
- » How do strategic risks (e.g. reputational ones) get managed in operational risk assessments?

Common Operating Picture

- » How do we communicate risk – *and the context of risk* - to each other?
- » Does a Risk Common Operating Picture make sense?
- » Is there a smart way to overlay information?
- » How do we validate the information? Are the bogies bogus? Does risk depend on information provenance?

Risk Lexicon

» Establishing a Risk lexicon

- Is it necessary?
 - If so, why?
 - What else is out there?
 - How to move forward?
-
- Did we remember to point out our definitions of RISK and VULNERABILITY?

Certification and Accreditation

Certification and Accreditation

Our definitions (plural, since UK and US differ slightly here)

- Other definitions from the audience?

There is a generally recognized need to change the current approach to certification and accreditation. The purpose of this session is to generate ideas on how to help shape the future.

» Where are we today?

» What needs to change?

» What is happening to shape the future?

Cross Domain Solutions

- » What experience is there? What stories can be told?
- » What has worked well?
- » What has worked badly or not at all?

Roadmap

Roadmap for Success

Where to go from today?

Possibilities include:

- » Alternatives/adjuncts to the current classification schema?
 - Perishability
 - Reliability
 - Provenance
 - Do we want handrails or guidelines?
- » Strategic Corporal
- » ISO 27001 – an enabler for interoperability?
- » Lessons from other areas (e-Business)