

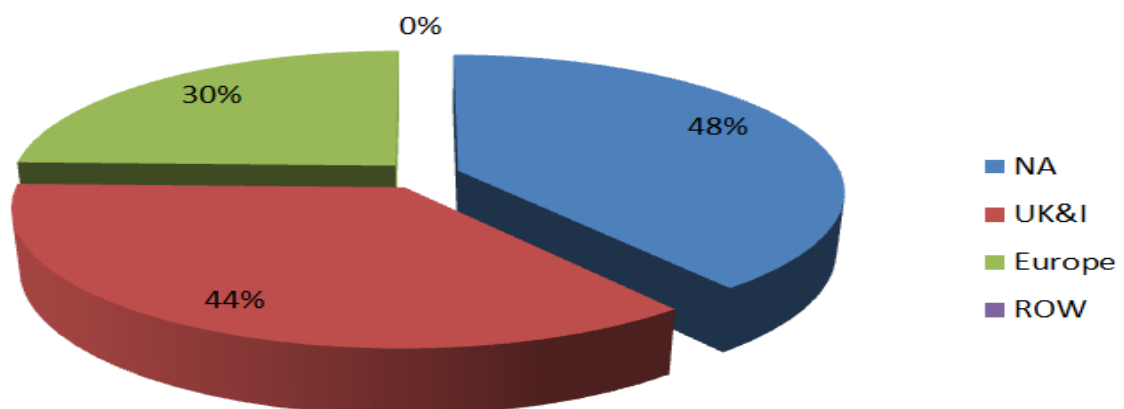
The ASIS Europe/ISAF Security Convergence Survey.

In August and September 2011 the ASIS International European Security Convergence committee and The Information Security Awareness Forum conducted a survey to determine how many medium to large enterprises are operating or working towards a converged security strategy in their organisations. 216 security professionals from across the Physical and Information Security community responded.

In about 35% of organisations polled, the Corporate and Information/IT Security functions are independent but it is also clear that around 35% work together on security risks across the business. While separate, 8% report into the same executive/director and 27% are individually responsible for their areas of security. This compares to the recent ASIS/ISC2 survey which reported that 30% share responsibility for security. In this survey 16% have combined the functions into one security organisation led by a CSO or CISO and 21% report into a common committee, risk council or steering group. This is important as risks can be identified and then discussed with an agreement for action. Admittedly this is not as effective as real-time monitoring of threats by a united team which could be achieved but it is more efficient than disconnected reporting and there should be less duplication and more cost savings as a result. The survey sought to determine how much converged activity is actually taking place and the figures show that more is going on than the organisation may realise when you look at the structures. 35% of those who responded indicated that Physical and logical access control is fully integrated, through the use of a single ID/card. A further 26% indicated that this was being developed with 38% reporting no activity. Whilst these figures reveal increasing levels of convergence the gaps could be exploited by an attacker whether they be cyber or physical. It is difficult to distinguish.

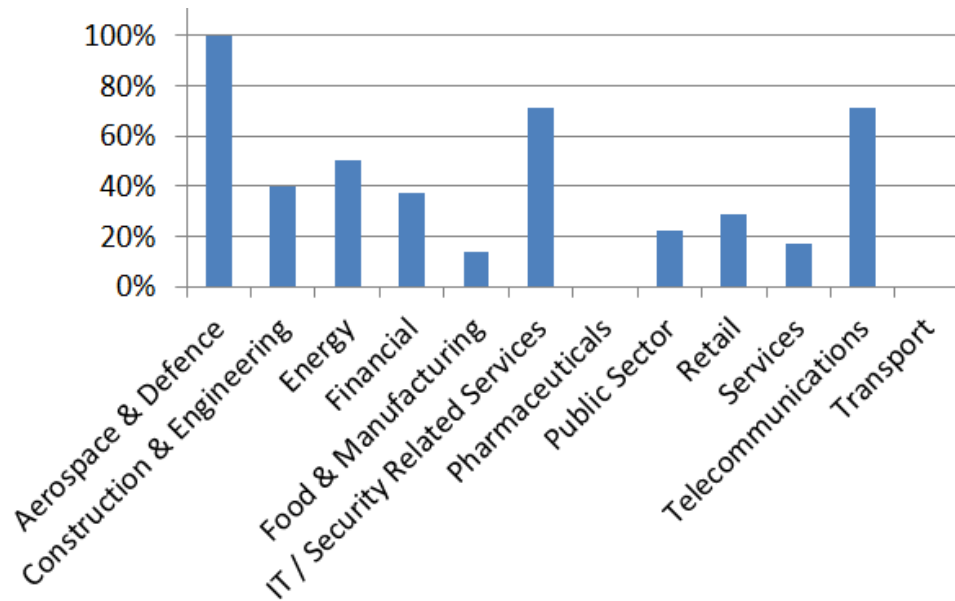
Differences in Geography or in Different Businesses?

As adoption of a converged view is still very polarised between adopters and non-adopters, we were interested to see if particular commercial business cultures were more likely to lead to a convergent security approach. In North America, for example, it is more common to have dominant central business functions and centralised services than in Europe. Companies in the UK are also often seen to be a closer follower of US management trends than other continental European companies.



The results (shown in the pie chart) certainly show that companies with a North American HQ were most likely to have converged security functions, and that the UK and Ireland were more closely aligned with that view than those in continental Europe.

We also saw differences between business sectors. As illustrated by the following bar chart:



Aerospace and Defence sectors as well as Telecommunications and IT/IT Security related companies were the most likely to have a converged corporate and IT security team. This is not surprising for telecommunications and IT/IT Security where threats to technology are fundamental to the business and arguably the focus of corporate security is on the physical protection of technology. Companies in the Aerospace and defence industrial complex see considerable threat of espionage and it may be the need for a corresponding intelligence-led threat response that is driving convergence. This could also explain the growing interest in convergence being shown by industries such as energy, which have recently seen an increase in Advanced Persistent Threat.

Do you think combing security activities is important / useful? (please select all that apply)

| | % |
|--|-------|
| a) No - we do not see combining / convergence as relevant | 10.98 |
| b) Important because of blended physical / digital threats | 71.10 |
| c) Important because of new physical security technology | 46.82 |
| d) Important because of cost saving opportunities | 45.66 |
| e) Other (please provide further details) | 10.40 |

- The above responses are very interesting in that although over 10% of respondents do not see combining / convergence as relevant, over 70% agree that it is important due to blended physical / digital threats.
- Also that both cost savings and the convergence of physical security technologies are roughly equally important for combining security activities.
- The 10% who provided further details ranged from very positive responses to explaining why the two areas could or should not be combined.

Given that the total number of people who do not see combining / convergence as relevant as being only just over 10 percent, this still leaves nearly 90 percent who do see it as relevant. This has great implications for the way that both physical and logical security people work together whether it be to deal with blended threats, changes in technology, cost savings or any other perceived benefits. The most important thing to do for all teams is to start sharing more information, or just start sharing, and teaching the most important basics as to what to look out for that would help identify potential threats.

The survey team consists of volunteers from the consultancy firms of Incoming Thought, Security Faculty and Unified Security who are researchers in the theme of convergence. We thank them for their assistance. Please contact one of the authors for a copy of the full report.

Prof Paul Dorey, Director, Security Faculty Ltd: paul.dorey@securityfaculty.com

Sarb Sembhi, Director of Consultancy Services, Incoming Thought: sarbs@incomingthought.com

James Willison, Vice chair, ASIS European Security Convergence sub committee:
jameswillison@unifiedsecurity.net