Converged Security Management Survey 2012

Supporting Organisations

ASIS INTERNATIONAL® EUROPE

CONVERGENCE

Information Security Awareness Forum

Authoring Organizations

CSO confidential

incoming thought
securing your business advantage

Unified Security

This page is intentionally blank

Table of Contents

About the authors

Professor Paul Dorey PhD. CISM, M.Inst.ISP
Director, CSO Confidential & Director, Security Faculty
Visiting Professor, Royal Holloway – University of London

Paul Dorey has over 25 years management experience in information security and established one of the first dedicated operational risk management functions in Europe. At BP he built and managed Information security, BCP, Privacy and Information Management Standards & Services globally across the corporation, including the digital security of process control systems and physical security. Prior to BP, he set up and ran global strategy, security and risk management functions at Deutsche Bank/Morgan Grenfell and Barclays Bank.
Paul has consulted to, and continues to advise, several governments and companies was a founder of the Jericho Forum, was Chairman and is now Chairman Emeritus of the Institute of Information Security Professionals (IISP) and has sat as an independent expert on the Permanent Stakeholders Group of the European Network Information Security Agency (ENISA). He was awarded Chief Security Officer of the year in 2006, IT Security Executive of the year in 2008 and entry to the Information Security Hall of Fame in 2009. In 2010 he was conferred as a Visiting Professor at Royal Holloway College, University of London.

James Willison BA, MA, MSyI

James is Vice Chair of the ASIS European Security Convergence subcommittee, a member of the ASIS International Commission on Information Security Management and Convergence project lead with the ISAF. He is founder of Unified Security Ltd and winner of the Imbert Prize 2011 for his work on Convergence with ASIS UK and the Information Security community. As vice chair of the ASIS European Security Convergence committee he is working closely with Alessandro Lega to actively promote convergence across Europe. He has seventeen years experience in the Physical Security Industry and now works in the field of security convergence including HR, FM and other business support functions. He has represented ASIS UK on the Information Security Awareness Forum since it was established in February 2008. James has spoken at several Information and Physical security conferences about Security Convergence. As Convergence project lead with the ISAF he is working with more than twenty physical and Information security organisations to raise awareness of the importance of security convergence for the C Suite. He has a Master’s degree from Loughborough University for his work on the case for the integration of Physical and IT/Information security management.

Sarb Sembhi

Sarb has a background in the public Sector as a Management Consultant, before entering the software development field as a programmer analyst and then project manager. It was as a development project manager that Sarb came into the Security field. Since his accidental entry into security Sarb has experience in all aspects of security, as practioneer, and as a contributor to the industry (through research and standards). Sarb's research includes "vulnerabilities of network CCTV systems", "data integrity attacks" and "cyber threats". Sarb is a member of: Chair of the Security Advisory Group of ISACA London Chapter; Chair of ISACA Region 3 Government and Regulatory Advisory Group Sub-Committee, and member of the ISACA International GRA Committee; member of the ISACA Cloud Computing Task Force; and was the President of ISACA (London Chapter); a member of InfoSecurity Magazine Editorial Board; a member of ISSA Advisory Board; member of the iGRC Advisory Group; Eurim; and an individual member of the Parliamentary IT Committee.

Introduction to the survey

Report on the Security Convergence survey run during the third quarter 2011 in Europe by ASIS International Europe and ISAF

By Alessandro Lega, chairman of the ASIS International European Security Convergence subcommittee.

When we planned the survey on Security Convergence in the Spring of 2011 to be administrated jointly by ASIS International Europe and the Information Security Awareness Forum we didn't expect to have the success we have achieved. We sent the survey out to our membership organisations and received a total of 216 responses, which give the survey a reliable result.

This is encouraging for two very valid considerations:

a) Being the first real survey on Security Convergence run in Europe, there was the risk of impact from a potential starvation due to the complexity of the subject.
b) It was unpredictable if corporations would have been willing to share information with us

Afterwards we can say the survey was very well received and respondents gave their valid contribution to draw a picture of where we stand right now with Security Convergence in Europe.

However, the survey would not have been so successful if the team who has worked on it had not been so dedicated and professionally excellent. I would like to officially thank the three authors: Paul Dorey (CSO Confidential), Sarb Sembhi (Incoming Thought) and James Willison (Unified Security and, also Vice-Chairman of the ASIS International European Security Convergence subcommittee). Also a thank you to Incoming Thought for hosting the survey. So, thanks to their dedication, we can have now, for the first time in Europe, a valid analysis of how the movement of Security Convergence is progressing in our Continent.

Finally I would like to thank Dr David King from ISAF. His intellectual contribution and the support from the ISAF in distributing the survey has been key for the success of our initiative.

Once again team work has paid-off! We hope the report will help all of us interested in Security Convergence and also to sceptical people not yet convinced by the validity for Converging.

I wish all a nice and interesting reading.

Alessandro Lega

From Dr David King, chair of the Information Security Awareness Forum

Convergence has been a topic of significant interest and relevance in recent years in traditional security and information security arenas alike. The prevalence of the "blended" threat and the coming together of physical and information security techniques has given some the growing sense of the need for a converged response. Indeed, organisations have been embracing convergence of their security capabilities to varying degrees. However, it has been very hard to put a figure to the extent of adoption.

This report is particularly to be welcomed as a useful addition to our understanding of convergence overall, and provides a foundation to underpin the work of those in the industry that have been pioneering convergence as a key strategic theme for their organisations. The report will hopefully provide support for directors and managers who are considering how convergence might help their organisation to defend against a present and evolving threat.

Shortly after its formation in 2008, the ISAF has been supporting work on convergence, an area that has been led by James Willison, the ASIS UK Chapter representative to ISAF. He has been instrumental in bringing the ISAF and ASIS thinking together. I would like to extend my thanks to him, the team and all those who have supported them in bringing this work to fruition

Dr David King CEng FIET M.Inst.ISP
Chair, ISAF

Introduction by the authors

Over the past decade there has been on and off interest in the subject of security convergence. Studies, articles and two key books have been written together with an alliance programme and a section in a forthcoming International security standard.

Opinions in the industry have been split with some saying that the very idea is irrelevant whilst others cite technology convergence between physical access control and IT being the main rationale driving a converged view.

The authors of this report have had a long standing interest in the effective integration and convergence of different security functions and skill sets. This comes both from actual experience of running a converged security team covering IT and physical security and working with teams in other companies who have done just that too. We have had the experiences first hand.

We were interested in getting some more recent data on what companies were really doing. We were particularly interested in testing conversations we have been having with both corporate and IT security professionals who say that they are brought to work together by the actions of our attackers. Criminals and malicious actors seem to have no barriers or boundaries on where they attack the physical or cyber world, blended threats are becoming a very real concern.

We are very grateful for the interest and support shown by both the ASIS European Chapter and the Information Security Awareness Forum. We would also like to thank the security professionals within various companies and different security functions for taking the time and interest in responding to our questions.

The findings have been so encouraging, that we feel that we should be taking this further, and to that end we are looking to perhaps hold a workshop that will enable us to follow-up on the work of this survey.

We hope you enjoy seeing the findings as much as we have.

Paul Dorey
Sarb Sembhi
James Willison

Is Convergence happening ?

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

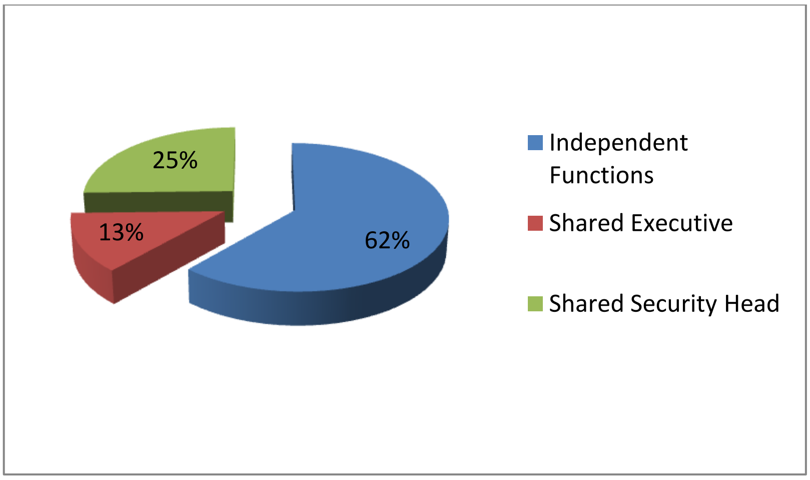
The survey considered three key issues.

- Is convergence happening?
- What is converging?
- Why is convergence important?

The following analysis looks at the responses in more detail. Hence there are insights into the importance of how security is managed at a senior level and the implications of a more aligned approach for security practises.

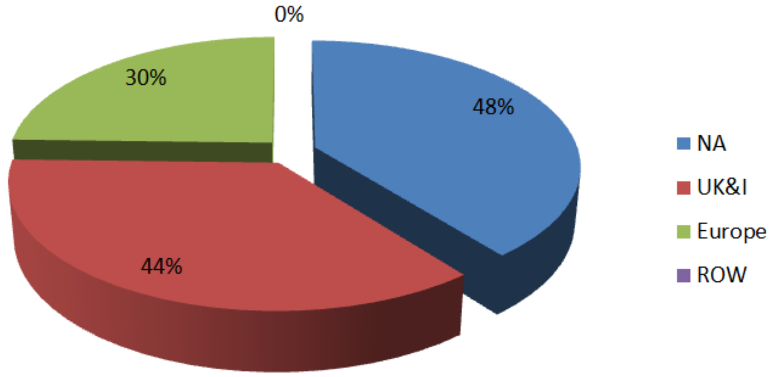
Is Convergence Happening?

The fundamental question posed by the survey was "Are security teams of different disciplines working more closely than before, and are 'converged' organisation structures emerging?" The survey showed that the majority (62%) reported that they operated as independent functions but the remaining 39% were organisationally connected either through reporting to a common Executive Director or (one quarter of respondents) by having a common security head accountable for both Physical and Information Security.



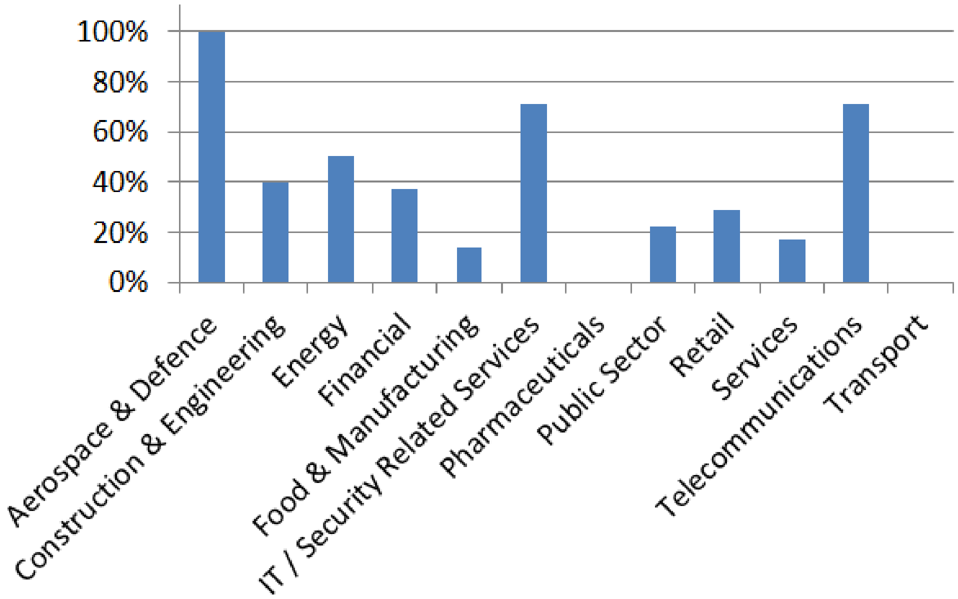
Differences in Geography or Different Businesses?

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 continental Europe.

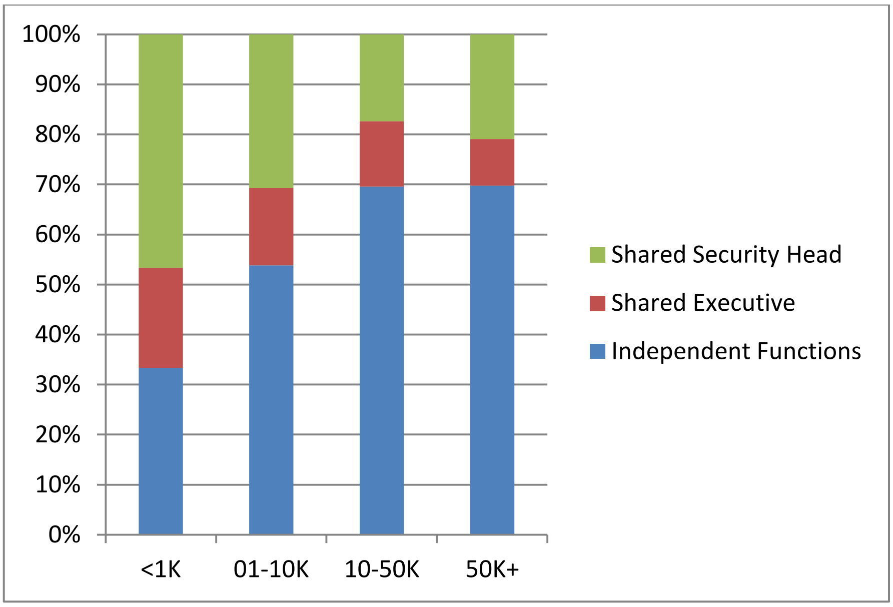
We also saw differences between business sectors. As illustrated by the following bar chart that shows what % of sector respondents had converged functions:



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, who have recently seen an increase in Advanced Persistent Threat.

Size of Company

We wondered whether smaller companies would tend to converge security functions because their lower staff levels would tend to lead to job roles being combined with individuals wearing several 'hats'. In fact the data (below) does show some size bias that leads to convergence. We didn't ask the question but we do know through experience that IT security may combine ('dual hat') with other IT roles in smaller companies and this may limit even more natural security convergence. It is important to note, however, that the majority of respondents were larger companies (only 14% were under 1K staff) and so the level of convergence reported in large organisations is very relevant.



Working Together

Even though the majority of respondents said that their organisations were separate it was clear from individual comments and responses that other approaches were used to promote closer working. 34% of those responding said that they had a formal committee where all security issues, both Information and Physical security were brought together and reported on. Of those saying they were independent organisations one third said that some form of 'dotted line' reporting did exist, if not for technical IT security but for the broader 'Information Security' subject

Many commented that relationships were very good between the security teams, and that they would collaborate on specific issues.

What is converging ?

In the survey there were a series of questions which identified different types of security activities and sought to determine which percentage of the respondents were working together in these areas. These questions ranged from whether or not the organisation had an integrated approach to fraud investigation through to an enquiry about networked based physical security systems and how much involvement physical security professionals have with their colleagues in IT in their security. It is to these questions which we now turn in our analysis as they are excellent indicators of exactly what kind of converged security practise is taking place across medium to large organisations.

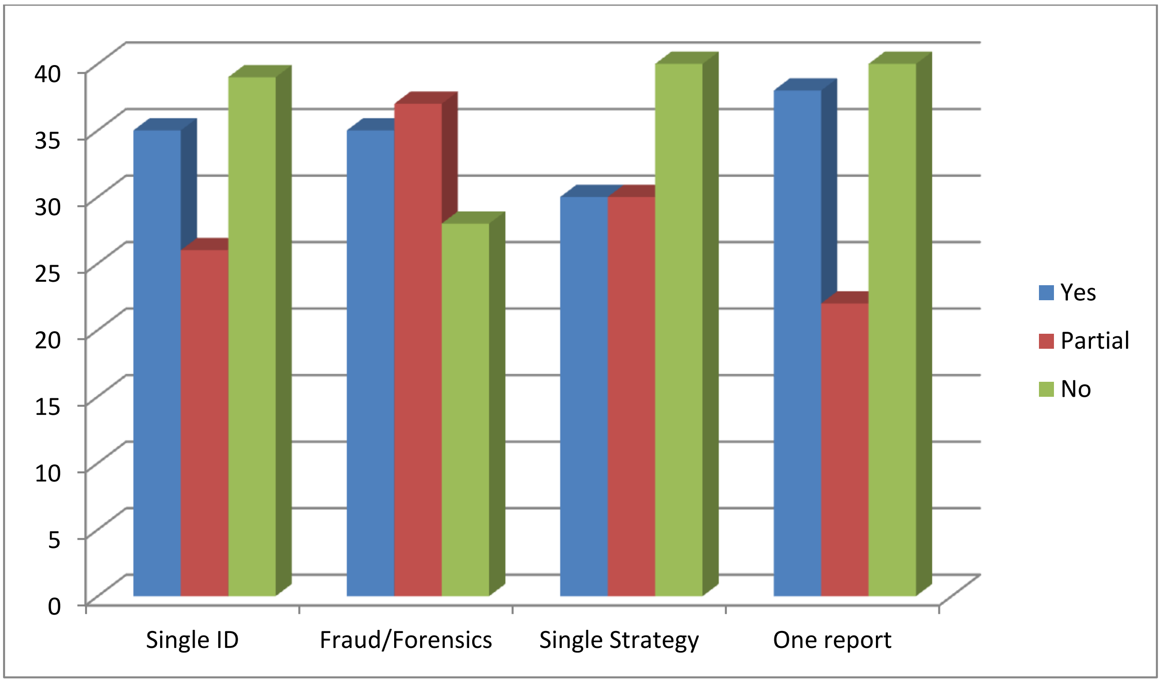
The first question asked if a single card or ID was used for both physical and logical access into the organisation. It did not go into any detail about biometric issues but clearly indicated that this is an area of growth in the industry. 35% stated that this was in place and an important 26% had partially implemented this kind of system. In fact this only left 39% who had not worked on integrated projects of any kind. As the industry continues to use more advanced technologies and internet access rapidly expands, this particular security control is likely to make even greater progress in order to help the business respond effectively to blended cyber and physical attempts to enter the organisation.

The second question examined the area of Fraud investigation. It asked if those leading the investigation worked closely with IT Forensics and shared data. The answers were particularly interesting as you might expect and hope that the majority are doing so. Actually 35% noted affirmative with 37% saying this was operational in part of the business and 28% having no involvement with IT in this regard. With ever increasing use of pcs and smart phones we think it safe to predict that these figures will swing highly in favour of more collaboration rather than less.

The next question revealed the interest at a higher level in the business as it asked if there was a single IT and Corporate security strategy. 30% stated that there was with a further 30% indicating that parts of the strategy were integrated. This however does show that companies are increasingly seeing the need to develop their thinking on security strategies and perhaps as awareness of cyber threats increases there is a correlating concern for looking at security more holistically. The rise in interest in the people factor of Information/IT security will also have an effect on this.

One of the most important indicators of how converged an organisation is and therefore how prepared it is for the blended threat is the level of common reporting that is carried out and assessed. A single report covering all areas of security risk is especially helpful to a business as they seek to determine which risks are most important and effectively prioritise these. 38% of our respondents said that a single report was produced with an additional 22% working on various areas together. The benefits of such work are not only in being able to see risks across the business but also in the saving of time for risk assessments to be carried out and in the reduction of duplication. Converged security risk assessments whilst quite new will give the business a clearer understanding of the threats they face. The risk director will have a better overview and not need to look at various reports which may be compiled at very different times and use a wide range of processes.

The table below shows the percentage of organisations which operate the described processes in a converged manner.



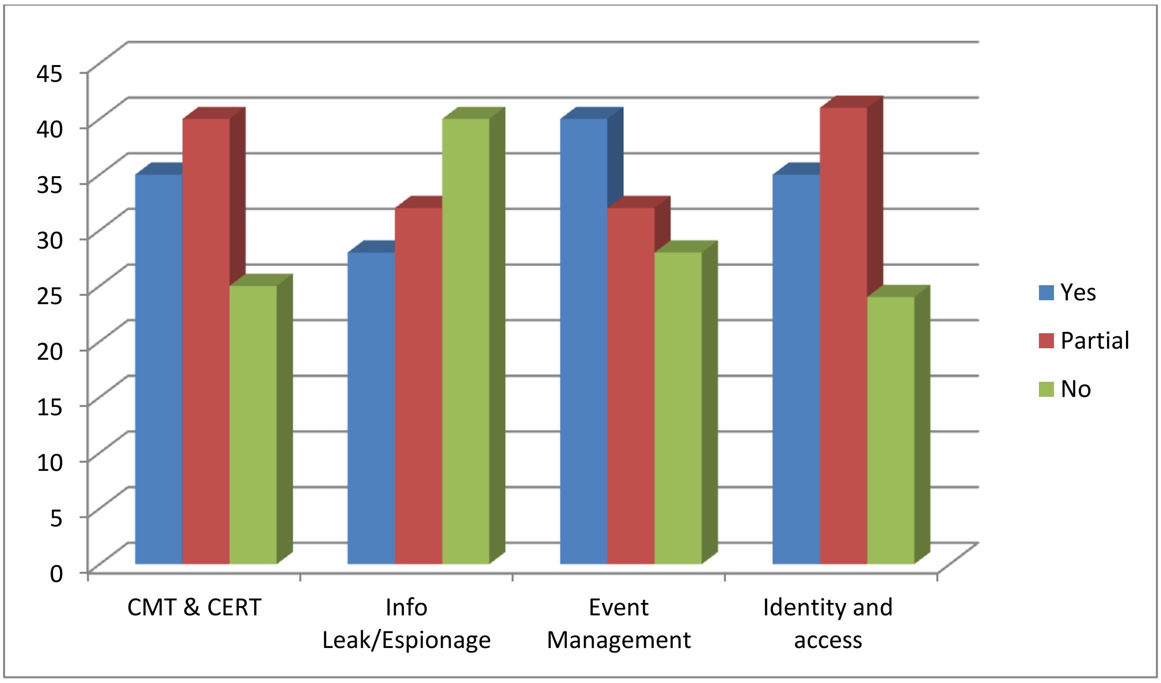
In the next question the respondents were asked whether the Crisis Management Team worked closely with the Computer Emergency Response Team. 35% said yes with another 40% indicating this was a partial process. These could be seen as disappointing figures especially when the need for IT if your systems fail is so clear. Although only 25% stated that there was no relationship. Of course not all crises involve the CERT but many serious events would. As the process of seeing security as a business support function gains momentum it would be hoped that the relationship between these two teams would only strengthen.

The next question focussed on company information and its protection. This is an area of shared concern between the security functions and of critical importance to the business. The particular aspect of the question determined whether there was a relationship between Corporate espionage and the Data leakage prevention process. It would make sense for the two to be linked although the data leakage prevention process may well be taken care of either by IT or outsourced to a third party which raises interesting issues. 28% of our respondents indicated that there were close working relations with a further 32% stating that those responsible for combating Corporate espionage had some links with the technical process. Once again it would be reasonable to expect that as technology advances this relationship will mature.

In a similar fashion the respondents were then asked about their company’s security event management processes. With the rise in blended threats the events themselves are increasingly integrated and hence an IT system which is compromised may well mean that physical access control and video surveillance is affected. Interestingly 40% report that they share an event management system with an additional 32% doing some work on this, perhaps in the areas aforementioned.

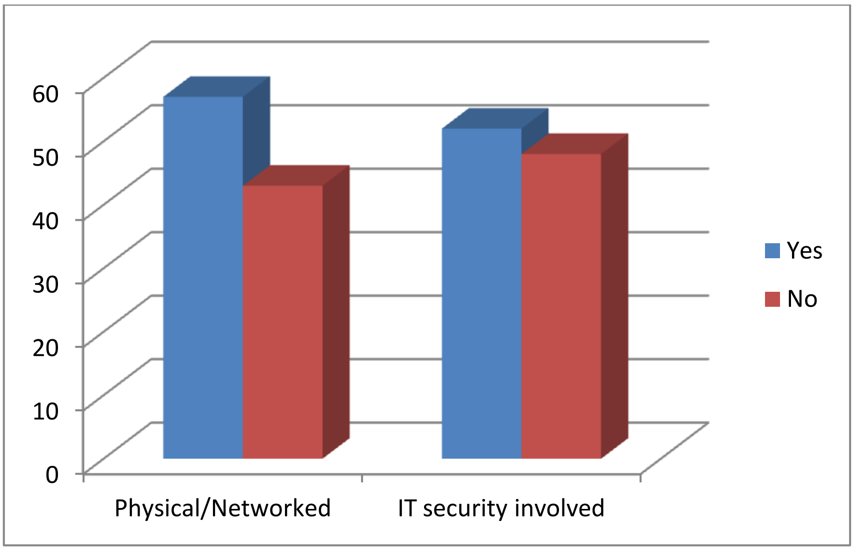
There were very similar figures for the area of Identity management but they were slightly higher with a total of almost 80% working closely or partially with each other. Again with the need to ensure that only those authorised to access company information it is crucial that both physical and logical identities are clearly linked. These encouraging figures reveal how important security convergence is. In many ways it is a name for a process which has now become inevitable for the success of any business.

The table below indicates the levels of integration between Corporate and IT security in the listed processes.



The survey also highlighted that there was a very high level of integration with Corporate, IT security and Business Continuity Management. 40% had well established processes with a further 45% developing these areas. Business Continuity Management is a key business support function and by its very nature can only be effective if there is strong collaboration between the different departments. The last question considered the issue of whether the business had adopted IP video and or network based physical security and if they had, was IT security involved in protecting these systems? The answers were very encouraging. 57% of the respondents are running networked based physical security systems with 52% ensuring IT Security is involved. These numbers show that most of those who opt for Network based physical security ensure that IT security is consulted. This is of crucial importance as these systems can be difficult to secure and can provide a criminal with access to the network which he or she might not otherwise be able to penetrate.

The chart below indicates the % of Physical Security systems which are network based and the involvement of IT security.


60
50
40
30
20
10
0
Physical/Networked
IT security involved
Yes
No

Why converge security functions when silos work?

One of the underlying objectives for this survey was to understand why any organisation today is considering a converged security response. We understood that there could be multiple drivers and that the list could be long, so we picked three keys ones and added a catch all option of others. However, we also understood that some organisations may be in situation where they are just not considering converged security now (and possibly currently conceive never considering it).

The three options we offered were those we considered to be considerably different from each other and yet the main drivers we had ourselves come across in our work on convergence. We permitted respondents to select all that applied.

These are:

Convergence is not relevant – this option captures the obvious perspective of those who do not see any relevance in the various security functions working together.

Blended Threat response – was aimed at capturing whether respondents felt that there were any efficiencies to bringing together various security functions.

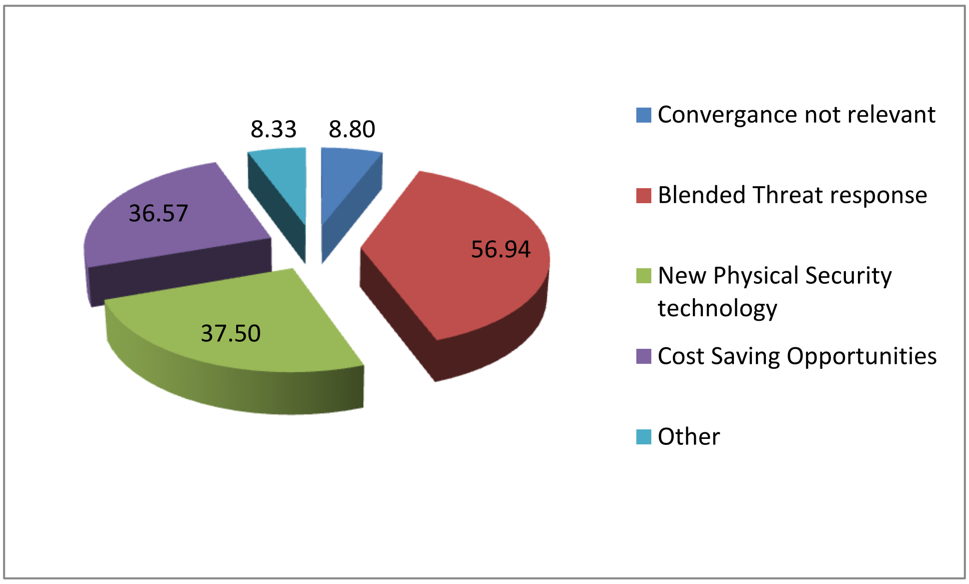
New Physical Security technology – with this response we wanted to capture from both IT and Physical Security professionals a possible driver for each to need / want to work with each other. We ourselves have seen many traditional Physical security controls now sitting on the corporate network, which has sometimes led to closer co-operation between the two functions.

Cost Saving Opportunities – we have seen this driver to converged security management as a non-brainer for an organisation to streamline functions right across the enterprise, so we wanted to understand if this was a driver for many businesses.

Other – lastly, we wanted to offer a catch all for all the many other reasons respondents may have.

The question (4) was phrased:

Do you think combining security activities is important / useful? (please select all that apply) (figures are in percentages).



It was interesting that both new technology and cost savings were considered to be equally close second to dealing with Blended Threat response as important / useful. Our understanding for why responding to blended threats had a much higher response could have been largely due to the increase in blended threats in the press and that many organisations may have personal experience of dealing with them. And further that to deal with them effectively they worked closely with their colleagues in other security functions.

Although we didn't ask any specific questions about it, we felt that personal experience of dealing with blended threats had greater resonance for respondents than experiences of benefits through new technology or cost savings. We believe that in many respondent's minds the new technology driver and cost savings were likely benefits / drivers, so were worthy of selection, but probably less likely to have been already realised.

Responses across regional areas

More than half of total respondents who indicated that convergence was not relevant were from the UK, and number is disproportionate to the breakdown of respondent's locations. Although, we separated the UK from the rest of Europe for this survey analysis, if this survey was a wider International survey and the UK were included in the European figures rather than separately, the effect would have been to bring down the figure of those European respondents who believed that convergence is not relevant. By separating the UK from Europe we see as per figures below that the Rest of Europe doesn't necessarily agree with the UK.

When looking at the breakdown by Region and then by the responses to question 4, and the option that convergence is not relevant, overall a much lower percentage of North Americans subscribed to this view. We believe that this is most likely the result of the fact that the idea of Security Convergence has been floating around North American corporations a little longer than in Europe, and that where it was working, people have shared ideas in ways that it is harder in Europe (greater cultural and language differences make it harder for sharing).

The numbers indicating the three pro convergence options were closer to each other (Blended Threats, New Physical Security and Cost Saving Opportunities) in North America than for the UK or the rest of Europe. Again this would be more expected in an environment where Convergence is being practiced and the benefits are being realised, rather than theorised.

In the UK both the New Physical Security technology and Cost saving opportunities responses showed similar figures, but the numbers indicating Blended Threats was much higher compared to other Europeans.

Responses across European sites

Within the options for question 4, around 50% (i.e. 45%-52%) of respondents, had more than ten European bases, and that there was just fewer than 18% with only one European base was for each option. This means that on average around 82% of respondents to each option for question 4 had two or more European bases. We were encouraged by the fact that such a high percentage of all respondents with European multi-site organisations done so positively.

Further, within each geographical breakdown by each (positive) option to question 4, the percentages were highest for those with 10 or more European Sites. Again, this is encouraging as it shows that interest in Convergence isn't just with small organisations, but with those working across multiple sites.

Responses across company size (employee numbers)

Of all respondents selecting options b) to d) around 38% were from companies employing 50,000+ employees.

Nearly two-thirds of respondents selecting b) to d) were companies with over 10,000 employees.

The highest response from smaller companies (between 1-10,000 employees) were for those selecting option b) (… Important because of blended physical / digital threats) compared to the other options. We believe that this could partly be that this group may have consisted of a few consultancy firms participating in the survey – who understand the benefits of convergence, and attach greater value to protection than the other options

We were aware when putting this survey together that we wanted to keep the whole survey brief so that respondents would be able to complete it in a few minutes, and as such we couldn't ask any follow-up questions. This question 4 was designed as a simple direct question about people's views on the benefits of convergence or lack of them. As mentioned above the variety of options offered could have been a much longer list and the follow on questions could also have been many.

In view of this, we were pleased with the responses we had to this question as well as what we were able to draw from the responses.

Conclusion

Even though the majority of respondents said that their organisations were separate it was clear from individual comments and responses that other approaches were used to promote closer working. The analysis of what is converging showed that 60% are working together on security projects across the enterprise. In fact 39% are working either in the same department or report to a shared executive director with a further 21% collaborating on a variety of security issues. Companies are increasingly seeing the need to develop their thinking on security strategies and perhaps as awareness of cyber threats increases there is a correlating concern for looking at security more holistically. Common reporting, advances in technology and increasing reliance on networked systems will inevitably develop converged relations.

The most striking and encouraging figures are that up to 80% work together on access and Identity management issues and this shows just how important convergence is. In our analysis of its relevance and importance our understanding for why responding to blended threats had a much higher response could have been largely due to the increase in blended threats in the press and that many organisations may have personal experience of dealing with them. We were not surprised to see the high number of responses for respondents selecting the option that Convergence is important for Blended Threat response. However, we thought it interesting that this option had been pushed into importance by responses from the UK and the rest of Europe. It was also significant that the number of large organisations (both by the number of European sites and overall large employers) was significantly high enough to provide a reasonable overview for this question. Convergence then, in many and varied ways is impacting business strategy as security professionals seek to effectively respond to the blended threat.

CSO confidential

CSO Confidential is a small boutique consultancy providing deep skills and experience in information security and business-oriented risk management. Our consultants consist of an international network of professionals who have all had top-level security and risk management roles in major blue-chip corporations or government entities. Their capability is based on proven success in these major roles. We do not employ trainee or junior consultants as we focus on strategic engagements where we can provide significant value and external context. We help governments and major companies develop their information security strategies and capabilities, including:

3-5 year security roadmaps, Board and executive security context, security capability reviews and Security Organisation Development.

incoming thought
securing your business advantage

Incoming Thought offers solutions to help secure the business advantage our clients have worked so hard to create, and in turn enable them to save money, increase profits or avoid legal and compliance issues. Typical engagements include the creation of security strategies through to practical implementations, content creation and end user training. Based on a wealth of real life experience the Incoming Thought team can build lively and engaging alternatives to the usual mundane security solution approach.In response to increased client demand we have expanded our existing services covering converged security, mobile (cell) phone risk management and investigations management.

Unified Security

Unified Security's goal is to protect people and organisations from blended attacks and enable them to operate effectively. They are committed to working with all areas of security, HR, FM and other business support functions to help the process of convergence move forward. Unified Security offer consultancy which is designed to ensure organisations align their support functions and in particular the areas of physical and information security. This includes security policy, common reporting processes, converged risk assessment and training courses. They work closely with a number of companies in the security industry including Incoming Thought and The Security Faculty. Unified Security is an implementation partner of CITICUS security risk management software.

http://www.unifiedsecurity.net