Convergence of security risks

Addressing the security dilemma in today's age of blended threats

The risks* faced by a typical organisation have never been more significant, or more complex, and as threats have proliferated, it's no surprise that many Physical and IT Security departments are struggling to keep pace. Safeguarding people, process and technology has become much more complex.

The whole concept of 'security' has expanded way beyond the traditional remit into areas like brand and IP protection, human protection, loss prevention, organised crime, parallel trading, online and traditional fraud. Many security departments are so busy fighting day-to-day crises that they're missing less obvious but equally important threats, as well as failing to address the wider issue of converged security risks. Converged security risks could seriously jeopardise the organisation's reputation and brand, long-term profitability (due to fines from regulators, loss of contracts and customer churn), or even its very existence.

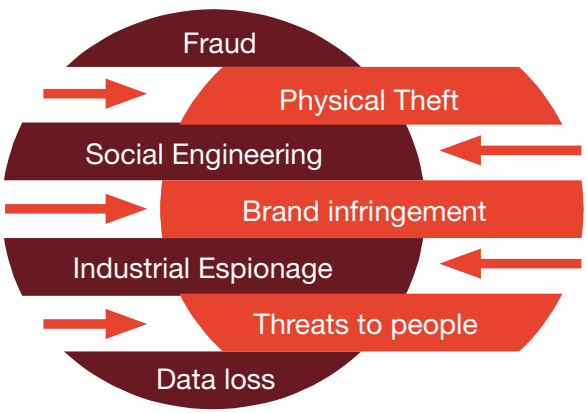
* Risks = Threat and vulnerabilities

What is convergence of security risk?

Convergence of security risks is a broad term which covers the multiplicity and interdependence of a variety of security risks which face the business. It requires a response which brings together all those dedicated to the security of the organisation to assess collective corporate risks. Risks that when looked at in isolation can increase the probability of the risk materialising. Many of the conventional physical and information security risks are viewed in isolation. These risks may converge or overlap at specific points during the risk lifecycle, and as such, could become a blind spot to the organisation or individuals responsible for risk management. Convergence of security risks is important because those blended or converged risks that pose the greatest risk to our people and organisations are often unknown. This includes converged security risks from common and complementary operating processes. To protect our people, our businesses and our assets, we need to keep ahead of those who attack us and work with business leaders to identify and understand those potential blind spots that could cause the business most damage.

This document seeks to define what is security convergence and raise the level of awareness and understanding, so that your organisation may be aware of these blended or converged security risks. Leaders from across the Security, Fraud and Business Continuity sectors have contributed and given their support to producing this first definition of the complex subject of convergence of security risks.

Figure 1. Convergence of Security Risks



This figures depicts how the multiple and complex merging of risk is causing organisations to rethink their security risk strategy.

Why should business demand more value from its security functions?

In most organisations, physical and information security are typically ensured by two separate departments, without an integrated approach to identifying converged risk. It's all too easy to focus on the wrong things and therefore overspend on their budget. Most large organisations have well-established traditional risk strategies which support clear lines of responsibility up to the board-level. This can often lull senior executives into a false sense of security. As traditional risks converge with the new risks, organisations are often exposed to security and risk gaps that are not being managed. This is principally because business functions are operating in silos and focusing on ensuring their area of responsibility is secure or protected (the 'not in my back-yard' mentality) or because they are unaware of such risks.

A recent Forrester survey* found that enterprises are overly focused on compliance and not focused enough on protecting their secrets. Other key findings included:

- Secrets comprise two-thirds of the value of the firms' information portfolios
- Compliance, not security drives budgets
- Firms focus on preventing accidents, but theft is where the money is
- CISOs do not know how effective their security controls are

Source: *The Value of Corporate Secrets, Forrester March 2010

A wider problem

Even organisations that have audited their security and risk procedures may find that they're not as resilient as they first thought. In our experience, most auditors will focus only on specific aspects of a security programme; with Internal Audit tending to concentrate on auditing existing procedural details. Yet again, we can understand that 'Potential Gaps' in the security and risk audit programme can leave an organisation vulnerable to blended or converged security risks.

"A common misconception is that different aspects of security are being reviewed by internal and external audit. Unfortunately, this can create gaps in auditing schedules and is undetected until an incident occurs"

A quote from a Head of Internal Audit

PricewaterhouseCoopers

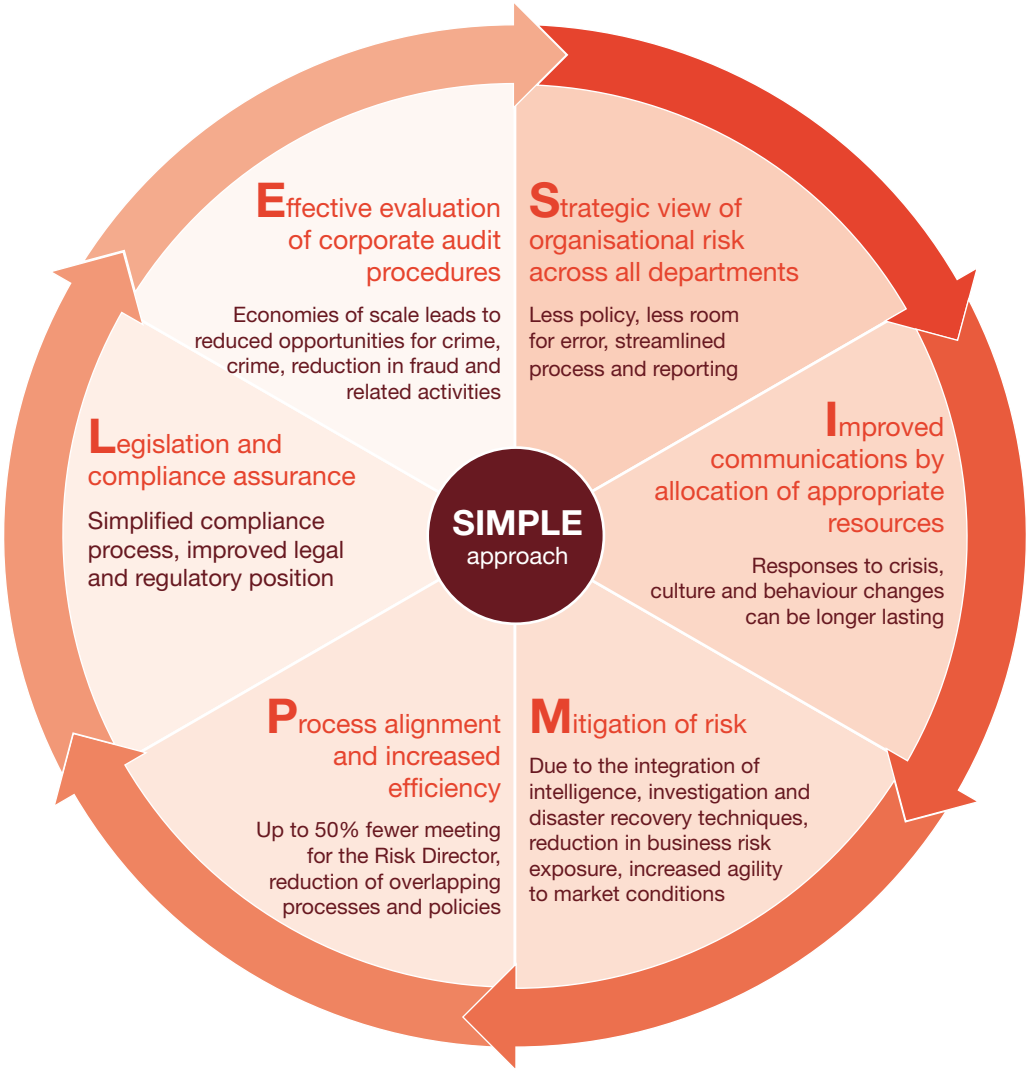
What are the business benefits of a converged approach to security risk?

There's immense value in having a single point of ownership for every aspect of your organisation's security. One option for an organisation is to appoint a Chief Security Officer (CSO) who can take responsibility for both physical and intangible assets, as well as the increasingly complex area of compliance. A dotted line to the audit and risk committees is vital, and a direct reporting line to the Chief Operating Officer (COO) can ensure that the issues raised are understood and addressed at the highest level. Many leading organisations are starting to go this way, but for those who do not it's important to ensure that the Board and the business have a complete picture of the risks the organisation really faces, and plans in place to deal with them. If you have one point of contact it could also lead to up to 50% fewer meetings for a senior director. A common line of reporting could also be established. This will enable the experts from all security areas to examine threats and vulnerabilities together and ensure all incidents receive the necessary attention they deserve. As a consequence, one report will be produced. This will help prioritise the most important risks and give a single view of the risks facing the business. Another option is for a business to form a risk council. This would meet on a regular basis to assess all risks and agree appropriate converged responses. Crucially it is those responsible for a company's overall security strategy who are best placed to determine how their organisation can respond to the challenge of blended or converged security risks.

A converged approach will recognise and address the interdependence of business functions, overlapping risks, and integrate business processes or assets i.e. people, technology and information. It will assess the security profile in terms of actual and potential blended risks, including physical, people and process risks, rather than specific risks to a single process. Therefore these risks should be identified even if they involve more than one process, person or system, or cut across existing departmental lines of responsibility.

The Acronym 'SIMPLE' provides an overview of the benefits of a converged approach to security risk management and can be used to help build a consistent approach towards security risk convergence:

Figure 2. A SIMPLE approach equates to greater benefits:



A way forward

Although security risk convergence can be achieved without merging different organisations or departments, most companies find it easier to integrate processes and views within a more integrated (physical and information security) management structure through active collaboration.

A converged approach should be driven by the board of directors, non executive directors and senior management to ensure the security risk strategy is aligned to the corporate strategy and business objectives.

However organisational change, cultural attitudes and staff behaviours can often be a barrier and can hold many back from the real goal of a cross-enterprise risk view. Hence the need for each business to determine its own security strategy, aligned to the business goals and objectives, in collaboration with the security function is imperative,. Converged security risks are then more likely to be identified and managed appropriately.

The ability to achieve meaningful convergence or a blended approach to security risk management, is the responsibility of each business functional risk leader. They need to consider the implications of what they are doing and how these actions may affect other functions, or cause other risks. They should constantly challenge their conventional way of thinking and this requires a commitment in 4 key areas:

1. Developing a deep understanding across each business and security function.
2. Building professionalism and increasing capability within each function – with clear and repeatable processes, rather than ad hoc solutions to individual challenges.
3. A willingness to share information, integrate processes and streamline reporting (including measurements).
4. A humility to accept when other risk priorities come above one's own function for funding and management attention.

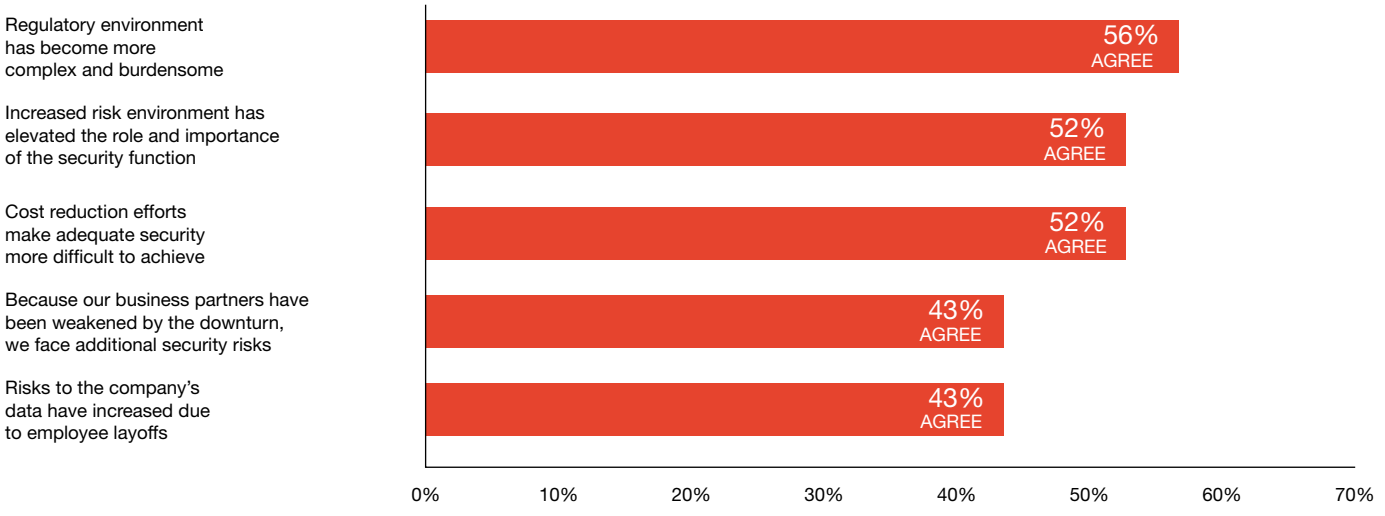
Recognising it's a journey – a case study

BP has a converged risk approach despite physical security and digital security being the responsibility of separate functions. Instead of looking at each risk in isolation, each team work closely together in parallel, ensuring harmonisation of processes, effectiveness of communication, and use both teams' collective experience to quickly identify potential overlapping risk gaps or cracks. This new converged method of working has helped ensure both physical and digital security risks are better identified, managed and monitored.

This pragmatic approach continues to help BP to identify potential pitfalls, risks and opportunities early or in advance of any pending risks materialising and therefore further safeguarding the future brand and reputation of BP.

Further evidence to support this paper can be found in the recent PwC Global State of Information Security Survey 2010. This survey revealed that Business Leaders are concerned about the more complex and burdensome regulatory environment, whilst striving for further cost reductions making adequate security more difficult to achieve. The survey also suggested that the global economic downturn has increased the role and importance of the security function.

Figure 3. Percentage of surveys 7200 respondents reporting impacts that the current economic downturn has had an impact on their company's security function



Contributors to this document

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

Our security global practice has more than 30 years experience, with over 200 information security professionals in our OneSecurity UK network, and 3,500 globally in153 countries. Our integrated approach recognises the multi-faceted nature of information security and draws on specialists in process improvement, value management, change management, human resources, forensics, risk, and our own legal firm. PwC has gained an international reputation for its technical expertise and strong security skills in strategy, design, implementation and assessment services, and as such, was recognised as a leader in the Information Security And IT Risk Consulting field by Forrester Wave in 2009.

"PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, the PricewaterhouseCoopers global network or other member firms in the network, each of which is a separate and independent legal entity.

ASIS International is the largest organisation for security professionals, with more than 35,000 members worldwide including 750 in the UK. The UK Chapter runs dynamic seminars and training days throughout the year, publishes a quarterly Newsletter containing articles from some of the country's leading security practitioners and acts as a voice for the security profession, representing members' views at the highest levels. For more information, see www.asis.org.uk.

The mission of the Institute of Information Security Professionals (IISP) is to be the authoritative body of information security professionals. We are achieving this by advancing the professionalism of information security practitioners through personal development, exchange of information, professional assessment and qualification, liaison with government, and providing other services required and driven by the industry. For more information, see www.instisp.org.

The Information Security Advisory Forum is an umbrella organisation incorporating, the BCS, the CMA, Eurim, GetSafeOnline, ISC2, The Jericho Forum, SASIG and 10 other organisations. The aim of the forum is not to create new information security awareness material, but to coordinate the efforts of its member organisations in order to reduce overlap and identify gaps for member organisations to fill. For more information, see www.theisaf.org.

With more than 86,000 constituents in more than 160 countries, ISACA® (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance of IT, and IT-related risk and compliance.

Portsmouth University – Institute of Criminal Justice Studies is one of the largest centres in research and course provision in the field of security, fraud and criminology. Its cyber security group comprises and offers a wide range of specialist educational programmes at undergraduate and postgraduate levels. For more information, see www.port.ac.uk/icjs

The Information Assurance Advisory Council is a unique partnership that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. See www.iaac.org.uk.

The Security Awareness Special Interest Group (www.thesasig.com) is a subscription free quarterly networking forum open to those who have an interest in, or a responsibility for, raising awareness about security within their organisations.

The Security Institute is one of the largest organisations for security professionals in the UK, actively involved in lobbying to raise standards in security profession. The group aim is to help minimise the gap between Information and Physical Security through a focus on the element of risk convergence thereby reducing cost efficiencies and security improvement. See http://www.security-institute.org/

The National Federation of Fraud Forums is a body that represents the 9 regional fraud forums as a single voice on national matters.

www.pwc.com/uk