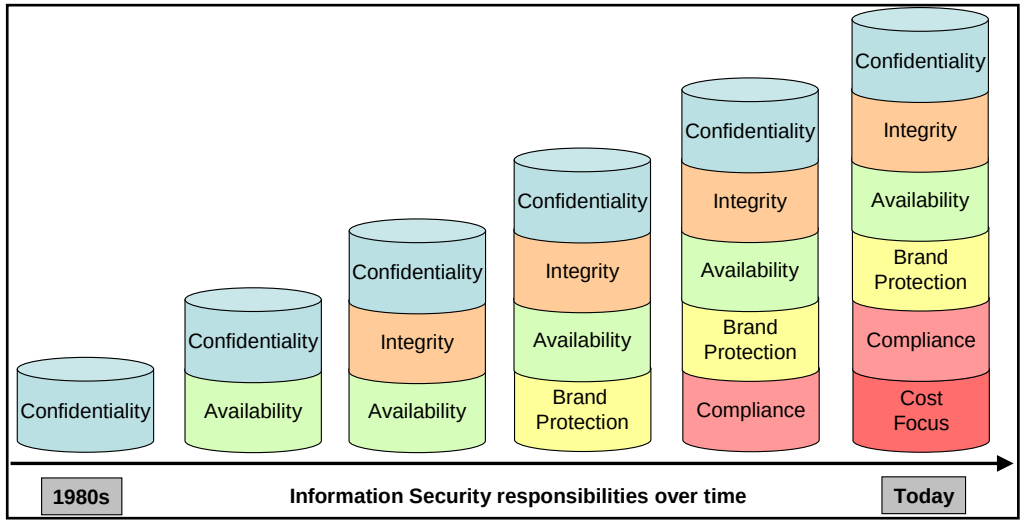
COMSEC Consulting

Managing the cost of IT Security

"The IT Security spend has continued to rise faster than any other part of the IT budget"

Working with over 600 customers in the last 20 years, Comsec has seen an increase in responsibility within the information security community.

In the past the security focus had been on the confidentiality of systems, which involved the protection of the perimeter, investigations of potential employee orientated data breaches and encrypting the channels. As the function of the responsibility changed, more budget was allocated, with the largest increase occurring at the point when protecting the brand became the most important priority to any enterprise. Interestingly, while responsibility remained within IT or Audit, the natural use of the budget was in technology which, in many cases, has increased the complexity of the security environment.



The IT security budget spend is sometimes visible to the business, as it is a centralised cost, however, more often it is hidden by being split between, audit, risk, HR, application development and infrastructure.

Security spend can be as much as 15% of IT budget

There are a number of studies which have estimated that security spend is as much as 15% of the IT budget in some industry sectors. Early in 2008, analysts were still anticipating a growth of the IT security market of 29% in the US and Europe. In addition, a recent survey of CIOs put security up as one of the highest priorities within their tactical and strategic agenda.

The risk reduction agenda, supported by a strong drive in compliance and the associated fast innovation of security products and solutions, has driven up the IT security budget line. In some cases there have been associated cost savings, especially in areas such as Identity & Access Management or Security Outsourcing, but these have been largely ignored, possibly due to the complexity/politics of the business change needed for the projects to succeed. However, up until now the return on investment case has been linked with brand protection, which in most cases can justify almost any spend. The credit crunch is already seeing a shift of focus, as cost control and reduction becomes a key driver for those responsible for IT, and this is going to impact the security budget.

"So why should IT Security focus on costs?"

IT budget holders are asked annually to reduce their operational spend, but discretionary spend has remained largely untouched, as IT has focused on CRM, ERP and Web applications to support new business channels, or improve client relationships and cross selling. However, the current market condition has shifted business priorities and many strategic programmes are on hold. Some argue that this is the right time to market and invest, but as the value of our assets and money decreases, areas such as spend on security may be seen as a "nice to have". To put it another way – there is no point in spending more on security if there is no business there to secure.

Brand protection used to be able to justify almost any IT security spend – but not any more

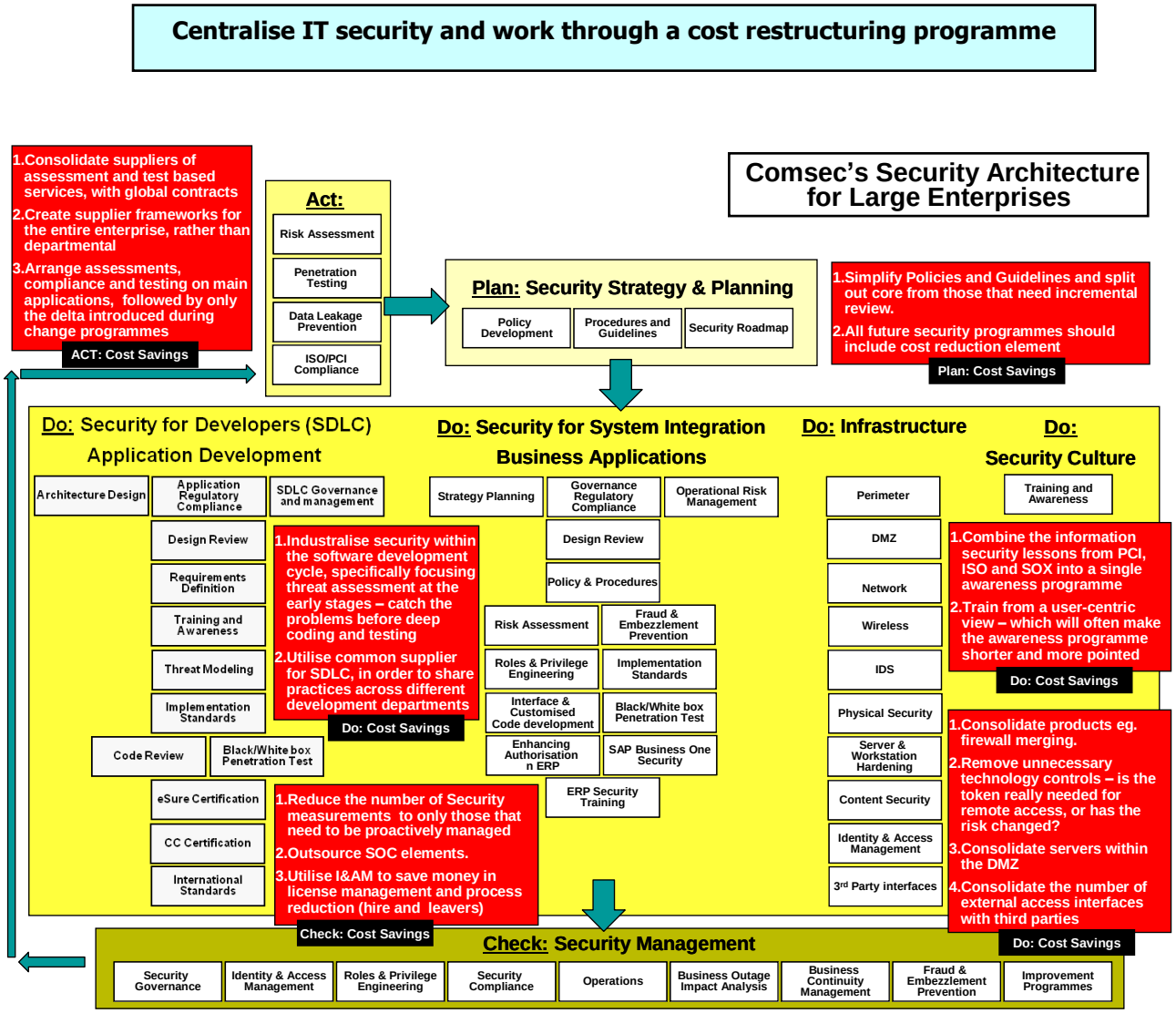
In relation to a cost focused agenda, heads of security have the following choices:

1. **Be Defensive** - Defend their budget with strong arguments around brand protection.
2. **Become Reactive** - Wait until the order comes to make wholesale cuts – which usually leads to headcount reductions, as this is often the most expensive cost within any organisation.
3. **Go Proactive** - Centralise IT security (so that the true security costs are known) and offer up a cost focused or restructuring programme.

"Approach to security cost restructuring"

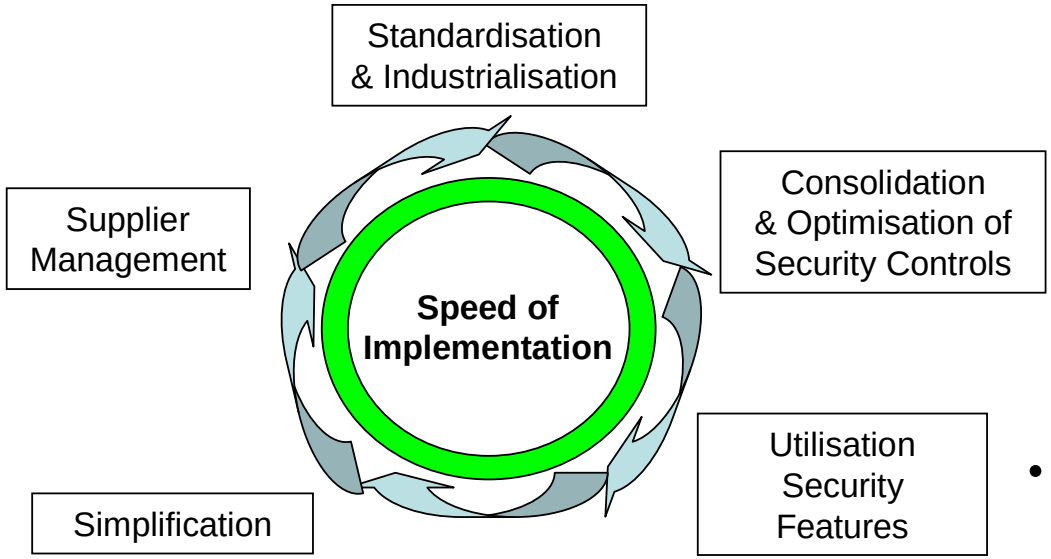
As with others parts of the business, a cost focused agenda can start in almost any area of security. By using a defined architecture the entire enterprise can be covered, with the following approaches:

- **Risk Approach** - focusing only on key asset protection controls, such as firewalls. The advantage with this approach is that high importance controls remain intact and only unnecessary or redundant controls are affected.
- **Biggest Spend** – Identifying the major costs on security and finding more cost efficient alternatives, while maintaining mitigation to the appropriate risk level.
- **Areas of responsibility** – Focus on current areas which are the key responsibility for IT security today. The advantage is that this will narrow the scope, however, it may mean that major enterprise savings are missed.



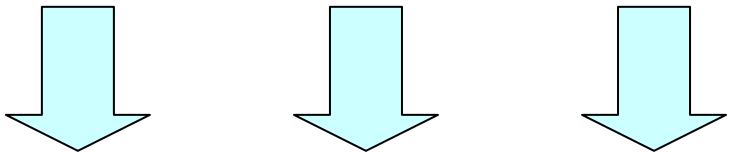
"Cost restructuring categorisation"

By using the Comsec Security Architecture it is possible to group the cost restructuring into the following categories:

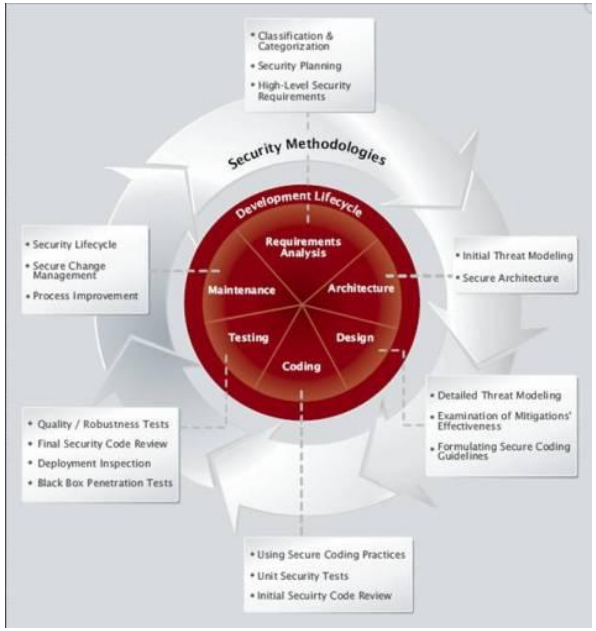


- **Standardisation & Industrialisation** – Embedding security into the enterprise, through standards, such as the Security Development Lifecycle (SDLC), will remove the threats earlier in IT projects and reduce re-coding costs. This approach has time and again proven its cost-effectiveness and has been supported by Gartner, Microsoft, NIST and many other prominent organisations. In our experience, defining security needs during the requirement stages is one hundred times more cost-efficient than in the testing phases. In addition, according to Gartner, 75% of security breaches are a result of software flaws and this is currently on the rise, therefore profound cost savings in projects can be achieved by utilising SDLC. A further benefit is that SDLC can mitigate the introduction of security flaws that delay product launches.
- **Consolidation and Optimisation of Security Controls** – In large enterprises there will be many controls that are simply no longer warranted, as the threats have changed or defence in depth strategies are no longer needed. For example, a traditional approach to security has been to isolate the network, splitting it between hostile and secure areas, usually through the use of firewalls, which present a high initial cost and ongoing maintenance charges. Today, most organisations in addition to corporate access need to support customer, partner, remote worker and consultant access to their resources. As new technologies and protocols have been introduced to support these requirements, the firewalls are being opened up to support frontend to backend communications, and in specific cases these firewalls and their associated costs may no longer be necessary. In addition, there are a number of different controls in place to deal with potentially overlapping regulatory requirements and in many cases these can be consolidated.
- **Utilising Security Features** – Many features, such as those found in Identity & Access Management can lead to cost savings in other parts of the business, for example, if there is a single view on the user-base, better software license terms can be arranged. In addition, many security features in core products, such as Windows Active Directory are not being utilised today. For example, working on the premise that the internal network is hostile, endpoint authentication solutions, using built-in host firewalls and IPsec can be considered. IPsec will allow the creation of a network, where all communication is authenticated at this level, which can include encryption. Combining this solution with network access technology and system health and validation agents, any non-compliant systems will only be able to access remediation networks. Using these inbuilt technologies adds no additional hardware costs to the budget and gives IT the ability to manage these technologies centrally, providing ongoing cost reduction, as well as increased security.

- **Simplification** – Wherever possible a simple security environment will aid in cost containment and reduction. For example simplifying training by combining SOX, ISO27001 and PCI IT security awareness will be both cost-efficient and actually more beneficial to the end users, as many of the messages in these disciplines overlap. Another example came out of a recent engagement, where Comsec analysed different authentication tokens for a financial sector client, which led to a consolidation of different solutions to a common platform, meeting the client's overall risk appetite, rather than specific departments' demands.
- **Supplier Management** – Through consolidating suppliers of security services, cost reduction can easily be achieved through economy of scale, optimising procurement costs and global pricing. However, additional improved service levels can also occur through the reduction of time to deliver or monitoring of internal information security trends. For example, a penetration testing team, conducting a white box audit, can develop an in-depth understanding of the client's environment, which would result in more agile future testing, as these would be conducted on the delta changes in an application, rather than the entire system.



Speed of Implementation – As security projects often involve several different departments and stakeholders, all with different risk appetites, they can suffer from frequent delays and scope changes. Therefore with a centralised agenda, as well as a clear cost focused business case, security programmes are going to be implemented faster.



Comsec's experience in application development is that defining security needs during the requirement stages is one hundred times more cost-efficient than in the testing phases.

"How much can an Enterprise save in security?"

Comsec recently conducted an exercise of going through our previous engagements over the last few years, pulling out any incidental cost benefits. It came as a surprise that many projects showed cost reduction benefits, even though the focus was on risk mitigation. An example was at a recent PCI engagement with a retail store that was unable to get certified, as they were running multiple payment applications on a single unit in each of the stores. The solution was to propose a hardened virtualised unit, which would both achieve PCI certification, but also allow the running of additional applications.

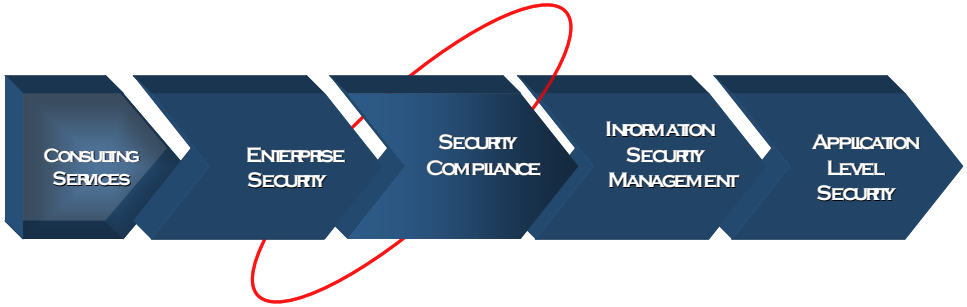
Although every enterprise will be different, the more complex the organisation the higher the cost savings will be.

Comsec is confident that every organisation, enterprise, company can significantly optimise their security costs, without increasing the risk to their business.

Company Background

Comsec Consulting (publicly listed on TASE: CMSC), is a leading provider of Information Risk Management Services to organisations worldwide. Founded in 1987, Comsec operates offices in the United Kingdom, Netherlands, Poland, Turkey, France, Israel and with affiliates in Japan, providing a wide range of security services for all market sectors.

With over 20 years of experience and more than 160 international skilled security professionals, Comsec covers all aspects of Information Security, from strategy and architecture, planning, design and advanced security solutions. Comsec's success has been achieved through developing long term client relationships, by demonstrating deep security knowledge, as well as an understanding of our clients business and risk appetite. The company is incredibly agile and fast moving, which reflects the responsiveness needed in the security arena, and this is maintained through a continuously updated knowledge base and information sharing within a controlled community.



In addition to traditional security services, Comsec operates a dedicated department for the design and implementation of advanced security technologies, adhering to the latest product releases and quality standards, hence performing as a one-stop-shop of Information Security and Operational Risk services for our clients.

Comsec's customer base consists of over 600 clients in five different continents, including banks, credit card companies, insurance and other financial institutions, as well as retailers, high-tech enterprises, telecom providers, National Government agencies and industrial corporations. Moreover, Comsec provides deep level core security services to leading software development companies across the globe.

As a leading provider of security services, Comsec participates in determining the global information security agenda, by being an active member and contributor in international security forums and standards organisations, such as ENISA, Jericho Forum, ICC, OWASP, I4, CISM, ISACA, as well as many more.

Comsec is a market leader and the largest pure Information Security consulting firm in Europe, as stated by Gartner in its international Security Summit. Comsec has been included in SC Magazine's list of the Top 30 Information Security companies worldwide.

London Workshop on 26th March 2009

Managing the cost of IT security

Deep dive into application and infrastructure security technology optimisation

Register free at www.comsecglobal.com/securitycosts

PCI: Comsec is a certified QSA & ASV

About the author

Stuart Okin is the Managing Director of Comsec UK and has over 20 years of experience in technology and architecture. Previously he was a Partner at Accenture and the Chief Security Advisor at Microsoft UK.

Stuart Okin
Managing Director, UK
stuart.okin@comsecglobal.com