Protective Security:
The Advent IM Approach to Corporate Security

Advent IM Senior Security Consultant

Introduction

The world of security is a complex one. Indeed, just trying to find a common definition of security has proved troublesome; so much so, one was not included in the Private Security Industry Act of 2001. Security, it seems means different things to different people!

In this short paper, Advent IM[1] proposes a revolution! That is, a comprehensive approach to security that many security providers understand, but never quite feel comfortable with and they therefore remain within their "stovepipe" comfort zone. This is particularly true of the Information Assurance and Physical Security disciplines.

The Government's Security Policy Framework

The Security Policy Framework (SPF)[2] has picked up this concept and developed what they describe as a new and innovative approach to protective security and risk management. Whilst SPF recognises that in general terms, the document is aimed at government Departments and Agencies, it nevertheless describes best practice and when applied appropriately, the concept will provide an effective level of security control to any organisation.

SPF recognises that security must be an enabler and actively support business goals; precisely the approach Advent IM advocates.

The Advent IM Approach to Protective Security

The Advent IM approach to security follows what it believes to be industry best practice - that is a holistic and comprehensive view. In a modern world, effective security must be driven by a risk-based approach and as described above, with the benefit of a current, but specific Threat Assessment. Advent IM believes that the

[1] Advent IM Ltd delivers Independent Protective Security Services to its clients in accordance with a variety of British/International Standards and Industry Best Practice Guidelines.
[2] The Security Policy Framework is a stand-alone, pan-government document that provides guidance on the implementation of security controls. It is aligned with the advice to commercial organisations provided by ISO/IEC 27002:2005. It includes CPNI Guidance and Mandatory Regulations

clear guidance provided by the SPF is an ideal vehicle from which a security approach should be developed and provide the foundation for effective organisational security.

When integrated, the components of Protective Security illustrated by Figure 2 provide the complete and holistic approach to corporate security.

Figure 1 - The elements of Protective Security

The Business Need

The need for security within any business will vary considerably. Nevertheless all accept that some security is required otherwise no one would lock a door! What is necessary for all businesses is an understanding of **why** security is needed, what level of protection should be applied and what security controls need to be installed. Clearly the security controls should be commensurate with the threat, the value of organisational assets and the impact that the loss or compromise of those assets would have on the business. While brand management is an impact that all organisations are conscious of, there are also financial impacts that may have significant effects on the business.

How does an organisation determine the appropriate level of security for them? First, the strategic aims or objectives of the organisation must be defined by senior management and expressed in a statement of intent by identifying their critical objectives. This will be followed by a Corporate Security Policy Statement of Security Policy and underpinned by Corporate Security Policies. Once this high-level direction has been provided, the security infrastructure may be developed. Advent IM has created its own concept for establishing this process within any business and will be described later.

The Root of Good Security Practice – A Risk Managed Approach

Advent IM believes that all aspects of security must be considered when protective security measures are being planned or reviewed. Unfortunately, information assurance has become so dominant that other aspects of security can be overlooked in favour of electronic measures, which may be seen as the panacea for solutions to security vulnerabilities. This incomplete approach is slowly being recognised or *rediscovered* within the security industry, but still remains a hurdle for many security practitioners to overcome.

The basic principles of good security practice continue unchanged despite the development of technology and the changing face of the threat. Effective risk management depends upon sound risk assessments to determine the nature and level of security controls that need to be applied.

All risk assessments should include the following elements: A detailed understanding of the Threat, the likelihood that an attack may occur, an understanding of what vulnerabilities exist within the security infrastructure, the value of organisational assets, an understanding of existing security controls and the impact, the loss or compromise of which would have on the business of the organisation. As a reminder of what is meant by Risk in the security context, and how the components are mapped, is explained in Figure 1.

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability} \times \text{Likelihood}}{\text{Business Impact}}$$

Figure 2 - Risk in a security context

The Criticality of Threat

The Advent IM view is that the first step within the Risk Assessment process is critical; the development of a detailed Threat Assessment. The importance of this element of the Risk Assessment process cannot be understated as the Threat Assessment should provide the foundation upon which all security planning should be based and be used to set the specific security controls for each organisation into context.

Unfortunately, more often than not, security measures are installed without the benefit of this essential piece of work resulting in a security system that does not provide the solution that was anticipated and more often than not, costs more than the security requirement needs.

The problem with developing a sound threat assessment is the difficulty in accurately identifying the threat sources/actors and evaluating their capability and motivation (or intent). To do this effectively needs trained analysts who can review the information available and determine an appropriate threat level based on the Threat agent *Modus Operandi (MO).*

The threat Assessment should also be a combined one which considers threats from both the technical and physical domains to ensure a full understanding of the nature of the threat and it must be both current and site-specific. Generic Threat Assessments such as that provided by HMG regarding the terrorist threat is a useful backdrop, but this must be tempered by local conditions and applicability. Advent now approaches all Threat Assessments in this manner for the benefit of its customers.

Security Direction

The application of the SPF is recognised as being aimed at the Public sector and government departments and agencies specifically. It does not stand alone however; the development of British Standards within the Private sector provides depth to the policy structure, as well as best practice for practitioners. In Advent's Pillar Policy shown at Figure 1, the two elements of Private and Public sector are drawn together to create a strong bond of security best practice across all the disciplines.

The overarching approach is "Protective Security". Across any organisation, large or small, where security is applied from the top of the organisation through a Corporate Security Policy, underwritten by the Corporate Security Policy Statement. Within this top-level policy is the organisation's mission statement which drives the supporting "pillars" of security disciplines.

Advent IM recognises that not everyone will agree that all seven of the above security policy areas are in fact security disciplines, perhaps Business Continuity being the most obvious candidate. However, we disagree and believe it essential that all aspects of security are considered together as part of any security organisation.

Clearly, by approaching security in this "holistic" manner, all aspects of the organisation will be involved and the Champions for each discipline will move across the organisation in a matrix fashion, rather than remain oblivious to other departmental and strategic needs.

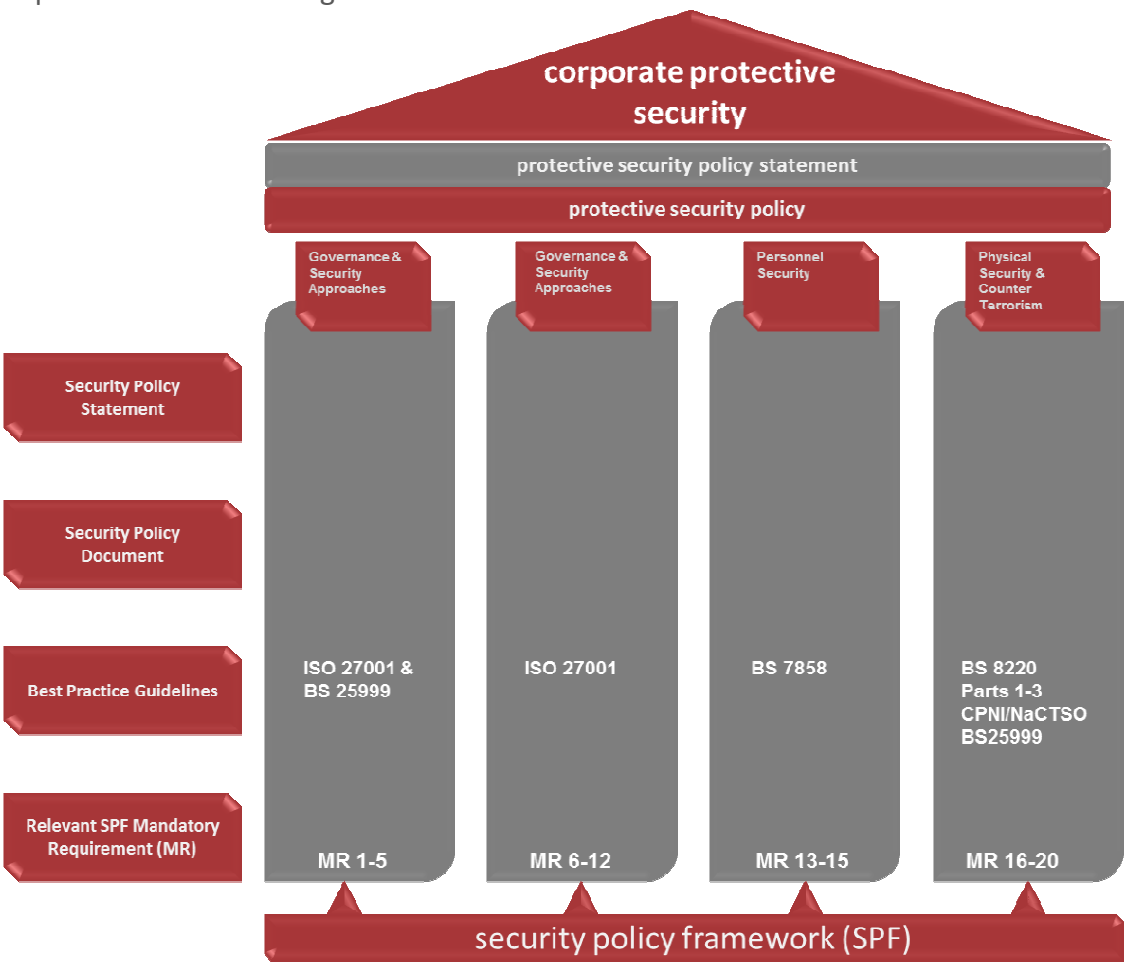

Figure 3 - Advent IM Pillar Policy

Security – An After-thought!

It seems obvious to security practitioners that security must be designed into a project from the very beginning. But how often is a security practitioner asked to apply security controls towards the end of a new project or indeed after it has been completed. Almost always, this has major cost implications and may limit the effectiveness of the security controls. By bringing security practitioners into the

planning process early will reduce the potential for unnecessary costs and maximise the effectiveness of security controls.

There are also projects that have been ill-advised in terms of their security planning and this is unfortunate. Recent experience has provided Advent IM consultants with disbelief when auditing public buildings where the security design has been "managed" internally and no advice sought from practitioners, perhaps to save money. The result in one particular case has been a costly security solution that is not fit-for-purpose and provides an inappropriate level of protection. The current economic climate may provide further examples of this practice as businesses seek to maximise their revenues by managing their security solutions internally. It may be an expensive mistake.

Conclusion

Advent IM has developed a truly holistic approach to the application of security across any organisation. This approach is underwritten by the government security policy which applies best practice within government Departments and Agencies. This is amplified by industry best practice standards to ensure that any organisation can benefit from the application of Advent's approach. However, the criticality of an effective Threat Assessment cannot be under-estimated. As we have described, the absence of an effective Threat Assessment will undermine a successful security infrastructure or at best simply waste scare resources in an age of economic uncertainty.

This approach therefore creates an alignment between the various security and business functions within the organisation which ensures that the security function becomes an enabling rather than restraining one. This may be the differentiator in competitive advantage that your company needs over your rivals.

www.advent-im.co.uk

@Advent_IM

0121 559 6699

bestpractice@advent-im.co.uk