Enterprise Security Architecture

A Business-Driven Approach

John Sherwood
Andrew Clark
David Lynas

CSI
COMPUTER SECURITY INSTITUTE
CRC Press
Taylor & Francis Group

Enterprise Security Architecture

Enterprise Security Architecture

A Business-Driven Approach

John Sherwood
Andrew Clark
David Lynas

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20141103

International Standard Book Number-13: 978-1-4822-8092-0 (eBook - PDF)

Dedications

To Amanda Jason and Mike Sherwood along with those other close and dear friends who have loved and supported me throughout the length of this project.

To Linda, Catherine and Charlie Clark for your love and encouragement.

To Marie, James, Kathryn and Stephen Lynas for your faith, support and love.

Contents

Foreword

The title of this book brings together three concepts that are overdue for synthesis. The first is the concept of enterprise, meaning the treatment of an organisation, commercial firm or public service as a single entity rather than a set of cooperating departments. It stems from the work of a number of management gurus in the late 1980s and early 1990s, amongst them Porter and Handy. They realised that improvements in competitiveness or services were only going to be achieved by optimising all parts of an organisation in a coherent way and all together, rather than locally optimising at the departmental level. The development of web-based information technologies allowed such optimisation to occur, but usually in an *ad hoc* manner, building on legacy processes and systems. It was not as coherent as it could have been.

At about this time it also was recognised that to improve the alignment of information and communication technologies (ICT) with business processes and to overcome the legacy system issue, an architectural approach to systems design was needed. This, in the hands of Zachman and others, together with a growing appreciation of the value of a systems engineering approach to large-scale ICT infrastructures, generated a structured and coherent approach to the migration of legacy environments to enterprise-wide systems. This approach has been in use for some time, and considerable progress was made at the time of the so-called Millennium Bug in replacing legacy environments with properly designed and engineered systems. However it is a process that continues today, and much improvement remains to be achieved.

The third factor, information and information systems security, has been known about for some time but was not regarded as either a business issue or as a mainstream information systems issue. Frequently, any security that was needed was added after implementation, quite often as a result of a security incident, so the information and information systems security discipline grew up in isolation from business process optimisation and from information systems engineering, except in some special cases such as defence, large-scale finance and banking, and some elements of aerospace. The advent of inter-enterprise working, the pervasiveness of the Internet as the common backbone of a global e-society and the vast increases in computing power, storage and bandwidth brought about by modern silicon and photonic technologies have dramatically exposed the weaknesses resulting from this evolutionary track. Exposure to these weaknesses has the potential to reduce confidence in e-society and e-business to such an extent as to limit the commercial and social benefits that could otherwise be obtained from well-designed, well-engineered and correctly operated secure environments and systems.

I believe society is on the cusp of making a judgement about this issue. This book, with its inbuilt optimism based on a successful set of experiences, will not only help security practitioners provide the benefits expected in their day-to-day work, but it will also help ICT professionals in general to deal with the argument of the gainsayers and doom-mongers.

Hence, the timing of this excellent book could not be better. It provides a well-argued, coherent and complete approach to the issue of how to make an enterprise safe and successful from an information and information systems point of view. The SABSA® framework, the cornerstone of the work, is derived from a mixture of experience and from the synthesis of range of well-proven methodologies and approaches. The use of a 'pervasive use case' will allow the reader to relate the theory to their real-world problems, and also provide them with the basis for the arguments needed to justify investment in their own organisations. Achieving a secure but successful enterprise is a major challenge. The description of the use of maturity models to ensure that an organisation does not undertake more than it is capable of delivering is critical to success. Successful projects, although critical to delivery of benefits, do not by themselves deliver improvements; they do however enable them. The later chapters of the book cover what is needed to run a secure enterprise and to deliver the expected benefits from the security that has been designed into the organisation and its processes. This birth-to-death treatment is unique in my view and it is why this work should be on every CIO, ICT Infrastructure and application development director's desk, as well as that of the newly appointed enterprise security architect.

The built environment which those of us who are fortunate enough to inhabit in the developed world did not happen by accident; it grew from an understanding that co-operative planning, robust, well-designed implementation and safe operation are critical to success. I believe we are approaching that threshold in our virtual environment. What this book gives us is a framework for dealing successfully with all these factors, a framework that is coherently constructed, lucidly described and grounded in real-world experience. Another small step for mankind...?

Professor Brian S Collins

Professor of Information Systems, Cranfield University and Vice President, British Computer Society

Preface

Benefits

As authors we hope that the great benefit of this book to its readers will be the insight that it gives into how to go about the process of developing enterprise-wide security architectures. To most people this is a huge, daunting task. They do not know where to begin, they do not know how to proceed, they do not know how to structure the work, and they do not know how to measure their progress. This book will show them all of these things. They will experience an enlightenment that will open the way for them to begin work on their own enterprise security architecture programme. Reading this book will be an important step on the road to success. It will change their professional lives in a significant way.

We have tried to stay at a relatively high level and have avoided descriptions of technical details that will quickly go out of date. Our intention has been to create a book that will have a long lifetime, and to do this it must be relatively independent of specific technologies and technical solutions. Thus it focuses heavily upon the conceptual and logical aspects of enterprise security architecture. The technical detail on specific solutions has been left to other authors of publications that are very different in their nature. However, we have provided as much help as possible to the reader to facilitate the search for this technical detail. References to other works, to international and Internet standards, to professional journals and to URLs where up-to-date technical detail is likely to be available have been included wherever possible.

The flow of the book follows the structured layers of the enterprise security architecture model that is introduced in the early chapters. There is strong pedagogy, with the layout structured into headings, sub-headings and bullets to make it easy for a reader to scan the pages and pick up the themes quickly. There is also strong emphasis on the use of tables, charts and diagrams wherever possible. This makes for a book that can be read sequentially from start to finish if the reader so desires but which can also be used as a book to be dipped into as a reference text.

The Evolution of Information Security

Information security and its subset, information systems security, are becoming more and more mainstream in their appeal. Information security began life in the military and government arena with very specialised applications in the field of national security. In the 1970s and 80s it became important in the banking industry as electronic banking systems were developed and deployed. During the 1990s we saw the emergence of the Internet, of e-commerce and of many other aspects of electronic business and the use of information systems to manage businesses on an enterprise-wide

basis. Thus at the beginning of the 21st century security is a topic that commands wide interest in enterprises wishing to leverage these technological innovations for business benefit.

One thing we wish to make clear at the beginning is that we take a wide view of what is relevant to information security. For those who have an existing view that it covers confidentiality, integrity and availability of information, prepare yourself to be challenged! For example, you will find discussions on topics such as customer service. What possible connection does this have with information security? Well, quite simply, information security has a great impact on the usability of information and communications technology (ICT) systems and upon the experience that users (including customers) have when interacting with these systems. Customer service is closely linked to ease of use, consistency of experience and delivery of expectations. Information security mechanisms for authentication and authorisation can damage these goals beyond repair, and so yes, customer service (and every other business issue) is highly relevant to the development of enterprise information security architecture. In this book information security is approached from a purely business perspective, and so you should expect every business issue to be viewed here as an information security issue.

Information Security Literature

The market for books has responded eagerly to the developing of interest in information security, with a wide range being published about new technologies generally and the security aspects specifically. Most of these books have a very technical focus. At the same time there is growing concern that the technology that attracts so much investment from businesses is not delivering what it promises, and it is clear that the reason is that developments are led from a technical standpoint, not a business one. There are few books that address this issue, either for ICT generally or information systems security specifically.

What is evident in this world of information security is that corporate management teams are becoming impatient with development programmes with ever-escalating budgets and time frames, and ever more disappointing results. We perceive two reasons for this: (1) that there is a lack of understanding of how to link technical development programmes to business needs; and (2) that there is a lack of strategic architectural thinking, which renders the investments in system development incapable of meeting the long-term and wider needs of the business.

There is growing interest in the concept of enterprise architecture as a means to plan, develop, implement and operate business information systems. This interest also extends to the security domain, where enterprise security architecture is becoming more and more attractive to those who are tasked with integrating adequate security into enterprise business systems. Over the next decade we expect this interest to grow substantially, especially if it is fed by the availability of suitable literature on the subject. This book is intended to contribute to that pool of literature. It is written from the perspective of the many years of practical experience that the authors have of working with large organisations in just this field of activity.

How to Use This Book

The book is intended to be the security architects' bible. It will provide a structured approach that can be followed step by step, so as to build an enterprise security architecture that meets the needs of the business. It is intensely practical but at the same time it is a complete theoretical work on how to make information security work. It is our intention that it will become the definitive work on this subject.

The book is organised into four parts:

Part 1: Introduction

Part 2: Strategy and Planning

Part 3: Design

Part 4: Operations

We recommend that the reader treat Part 1 as a text to be read from end to end. In this part of the book we expound our overall philosophy, framework and methodology, and arguably reading only this portion may satisfy a security architect who already possesses a good underlying business and technical knowledge.

In the subsequent three parts we take each layer of the framework described in Part 1 and develop it in detail. These three parts also map onto three phases of the security architecture lifecycle, also described in Part 1. These last three parts are therefore more likely to be used by the reader as reference material, rather than as something to be read from one end to the other.

Part 2 deals with business issues affecting information security and major strategic approaches to solving business problems. It is high-level and truly in the realm of architecture from the point of view of an architect, remaining at a conceptual level of thinking throughout.

Part 3 addresses the more detailed design process at the logical, physical and component architecture levels and will appeal to those readers who have an interest in the more detailed aspects of designing information security solutions.

Part 4 addresses security operations, being the day-to-day operational management of information security within the enterprise security framework. Here we focus on some specific issues but do not attempt to cover every aspect of operational security in fine detail, since after all, there are many good books that already deal with the detail of the operational and administrative aspects of information security management. However, the book would be incomplete without this part being included, since we believe that the power of the book is its unique framework approach to architectural thinking, and some flesh must be put onto the skeleton framework for operational management that was introduced in Part 1.

Since the various parts differ from one another considerably in depth and focus, it is quite likely that many readers will find that some parts of the book appeal to them more than others. This is to be expected, since few people are able to operate successfully at every level of the architectural framework we describe. What we hope is that every reader will find significant value in those parts that address their own sphere of interest, and that the book as a whole will help architecture teams to work more effectively together by understanding the relative roles that different team members play and the value of their individual contributions to the overall integrated architectural process.

It is also important that the reader should appreciate that this book is not a cookbook that provides recipes for all situations. It is much more a book on how to think in architectural terms and how some of the major issues can be approached. You may not find here the solution to your problem, but what you should find is an approach to understanding the real business problem and how that understanding should drive your technical creativity and your process design work.

About the SABSA® Model

The entire book is based upon a six-layer model of security architecture known as SABSA®, an idea first developed by John Sherwood in 1995 and published in 1996 as 'SABSA: A Method for Developing the Enterprise Security Architecture and Strategy[1]'. SABSA® is an acronym for 'Sherwood Applied Business Security Architecture' and was the basis on which the Sherwood team built their world-class consulting skills in this area of security architecture. The starting point for this work was ISO 7498-2 1989[2]: 'Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture'. This standard is relatively unsophisticated in terms of business drivers, but it sets out an important framework in terms of security services – the logical architecture, security mechanisms – the physical architecture, and security management – the operational architecture. The Sherwood team added two upper layers to provide a business-driven approach (contextual and conceptual architectures), and a lower layer to map onto real tools and products (component architecture).

Unknown to Sherwood at the time, this work was closely related to work being carried out in the USA on overall enterprise architectures, authored by John Zachman, published by the Zachman Institute for Framework Advancement and known as the Zachman Framework[3]. It is also interesting to note that in 1993 at COMPSEC 93 in London, before the Sherwood team had embarked on its journey into enterprise security architecture, Professor Brian Collins, who has kindly provided a foreword for this book, published a paper[4] with a colleague, Steve Mathews, in which they called for information security to be driven from a business perspective, and many of the factors identified in that paper are to be found in the business-focused SABSA® approach, although we did not at the time make the connection.

John Sherwood presented the SABSA® work at COMPSEC 96 in London and published the follow-up paper on it later that year. At that time he had never heard of Zachman's work. In April 1998 Sherwood was working for an international client as the security architect on a team engaged in developing entirely new global infrastructure architecture. As part of that activity he was fortunate enough to visit a conference entitled 'Enterprise Architecture' in San Francisco, and one of the keynote speakers at that conference was John Zachman. It was in many ways a great experience, because here on the platform was someone else who was doing very similar things but in a much wider context. The similarities between the SABSA® model and the Zachman Framework were amazing, and Sherwood was able to rework SABSA® to incorporate some of the language and ideas that Zachman had talked about in his presentation. However, the original concepts of SABSA® remained pretty much unchanged.

In developing the application of the methods, Sherwood was to be greatly assisted by other members of his consulting team at Sherwood Associates. Both Andy Clark and David Lynas were key players in this respect, and both managed major projects with global clients. David Lynas went on to develop a highly successful training course that is offered on a regular basis by the Computer

[1]Reference: 'SABSA: A Method of Developing the Enterprise Security Architecture and Strategy', Computers & Security, Volume 15 No. 6, 1996, Elsevier Science.

[2]Reference: http://www.iso.ch/cate/d14256.html

[3]Reference: http://www.zifa.com

[4]Reference: 'Securing your Business Process', Dr Brian Collins and Steve Mathews of PCSL Consulting, presented at Compsec 93.

Security Institute[5], entitled How to Design a Winning Security Architecture[6]. More recently David Lynas has been presenting a series of training seminars and events in Australia, New Zealand and the Asia Pacific rim under the auspices of ALC Training[7], and his work with clients in that part of the world has led to some of the more recent innovations in the methodology. There were other Sherwood team members who were also important contributors to the work, and in particular we would like to thank Anne Watt, Julie Braun, Krag Brotby and David Watson.

The SABSA® framework is described later in the book and is used as a basis to construct the entire process of security architecture development that the book describes.

Relationship to Other Methods, Models and Standards

We know that some people with a cursory knowledge of the SABSA® approach have wondered to what extent it conflicts or competes with existing methods, models and standards, and the answer to their question is that it does not conflict or compete at all. The reader will find that there are numerous references to these other methods, models and standards and that SABSA® provides an overarching framework that binds them all together into a single holistic view of how to design and manage enterprise security. Nothing in the existing canon of knowledge and wisdom is negated or challenged by the SABSA® approach. Rather, SABSA® provides that final umbrella of unification that enables the security architect to pick and mix from the plethora of available methods, models and standards so as to bring together at the enterprise level a security architecture that is based upon many years of developed ideas from many experts, whilst at the same time providing the means to structure these ideas into a single holistic view.

And Finally...

We hope that you will enjoy reading our book and that it will become one of your primary reference texts as you navigate your way through the process of developing enterprise security architectures. We wish you all success along your interesting journey.

John Sherwood, Andrew Clark and David Lynas

June 2005

[5]Reference: http://www.gocsi.com

[6]Reference: http://www.gocsi.com/winning.htm

[7]Reference: http://www.alctraining.com.au

Acknowledgements

This book would not have been possible without the support, encouragement, diligence and constructive feedback provided by many of the practitioners of SABSA® and our clients. We would particularly like to thank those who were there at the beginning when SABSA® and the ideas for this book were formed and those who helped it develop into the mature version that it is today. They include:

Chris Amery
Debi Ashenden
Michael Bacon
Alan Bernstein
Mike Bourne
Tony Bramwell
Julie Braun
Krag Brotby
Brian Collins
Mike Corby
Luc De Clercq
Paul Dorey
Stan Dormer
Marty Edelman
Tim Evans
Hans-Peter Fischer
Jon Fitzgerald
Shaun Fothergill
Ed Fulford
Eric Guldentops
Jacques Hagelstein
Mike Henson
Julien Holstein
Paul Hopkins
Andy Jones
Debbie Joy
Eva Jun
Jenny Kane
Wilhelm Koch
John McGuire
Rob Maines
John Mulholland
Richard Nealon
Dale Newnham
David Nielsen
Kosta Peric
Jane Scarratt
Martin Smith
Peter Stevenson
Paul Stubbs
Angela Taulelei
Steve Thomas
Howard Thompson
Mike Usher
Mark Waghorne
David Watson
Anne Watt
Peter Wenham
Rob Wood

In addition, we gratefully acknowledge the contribution of others who have helped improve this book by their feedback and guidance. They include:

Niels Bjergstrom	Vince Gallo	Chris Keating
Zika Milenkovic	John O'Leary	Fred Piper
David Roberts	Michael Strang	Steve Temblett
Matt Whelan		

And of course those at CMP Books; Dorothy Cox, Matt Kelsey, Gail Saari, Hastings Hart (for his superb copyediting) and the rest of the team who have done such sterling work to bring this book to publication.

We apologise to those whose names we may have forgotten to include.

We hope you enjoy reading this book on a subject about which we are all passionate. If you spot any errors or omissions we would be grateful to hear from you so that we may make corrections to future editions.

John Sherwood

Andrew Clark

David Lynas

Part 1: Introduction

This book is entitled *Enterprise Security Architecture*. Here we begin by looking at what exactly we might mean by those words. As with all of the parts of the book, we shall start with some dictionary1 definitions to help us understand the language we are using.

ar·chi+tec+ture n. 1. the art and science of designing and supervising the construction of buildings and similar structures. 2. a style of building or structure: Gothic architecture. 3. buildings or structures collectively. 4. the structure or design of anything: *the architecture of the universe*. – **ar·chi+tec+tur+al** *adj.*

– **ar·chi+tec+tur+al+ly** *adv.*

ar·chi+tect *n.* 1. a person qualified to design and supervise the construction of buildings. 2. a person similarly qualified in another form of construction: a naval architect. 3. any planner or creator: *the architect of the expedition*. [C16: from French *architecte*, from Latin *architectus*, from Greek *arkhitektōn* director of works, from ARCHI- + *tektōn* workman; related to *tekhnê* art, skill.]

se+cure *adj.* 1. free from danger, damage, etc. 2. free from fear, care, etc. 3. in safe custody. 4. not likely to fail, become loose, etc. 5. able to be relied on: certain: a secure investment. 6. *Nautical*. stowed away or made inoperative. 7. *Archaic*. careless or overconfident. ~ *vb*. 8. (*tr.*) to obtain or get possession of: *I will secure some good seats.* 9. (when *intr*., often foll. by against) to make or become free from danger, fear, etc. 10. (tr.) to make fast or firm; fasten. 11. (when *intr*., often foll. by against) to make or become certain; guarantee: this plan will secure your happiness. 12. (tr.) to assure (a creditor) of payment, as by giving security. 13. (*tr.*) to make (a military position) safe from attack. 14. *Nautical.* to make (a vessel or its contents) safe or ready by battening down hatches, stowing gear, etc. 15. (*tr.*) *Nautical.* to stow or make inoperative: to secure the radio. [C16: from Latin *securus* free from care, from *se-* without + *cura* care] – **sec+cur+a·ble** *adj.* – **sec+cure+ly** *adv.* – **sec+cure+ment** *n*. **– sec+cure+ness** *n.* – **sec+cur+er** *n.*

se+cu+ri·ty *n.* *pl.* ·ties. 1. the state of being secure. 2. assured freedom from poverty or want: *he needs the security of a permanent job.* 3. a person or thing that secures, guarantees, etc. 4. precautions taken to ensure against theft, espionage, etc: *the security in government offices was not very good.* 5. (*often pl.*) a. a certificate of creditorship or property carrying the right to receive interest or dividend, such as shares or bonds. b. the financial asset represented by such a certificate. 6. the specific asset that the creditor can claim title to in the event of default on an obligation. 7. something given or pledged to secure the fulfilment of a promise or obligation. 8. a person who undertakes to fulfil another person's obligation. 9. *Archaic.* carelessness or overconfidence.

[1]Collins English Dictionary

Security Architecture

We first look for a definition of 'security architecture' by drawing on the distilled knowledge and wisdom embodied in the dictionary definitions above.

Security architecture is the art and science of designing and supervising the construction of business[2] systems, usually business information systems, which are: free from danger, damage, etc.; free from fear, care, etc.; in safe custody; not likely to fail; able to be relied upon; safe from attack.

A security architect is a person qualified to design and supervise the construction of secure business systems, usually secure business information systems.

This book is about security architecture, in both of the above senses. It has been written for those who are, or who are striving to become, security architects. It has also been written for those who do not themselves aspire to become a security architect but who will commission and accept delivery of security architectural work. They will want to know what to request, what to expect, and how to judge the quality of the deliverables that they receive from their security architects. It is a book for anyone who has any interest at all in security architecture.

[2]The use of the term 'business' here has the broadest possible interpretation in this book. It is not confined to systems used by commercial organisations, but is meant to imply that there is some serious intent in having and running the system and that costs, benefits and risks are serious issues that need to be addressed. The word 'business' at least includes any activity of any commercial, industrial, government, educational, or charitable organisation. In some circumstances it could also include private individuals and domestic households, although we do not anticipate that this sector will be a significant consumer of this book.

Chapter 1: The Meaning of Security

If you are to understand 'security architecture' you must first be sure that you understand 'security'. It is a term that is used many times in many contexts and frequently with different meanings. Here the meaning is discussed within the context of this book – that is protection of the business.

In this chapter you will learn about:

- The misunderstanding and conflict that often exists between business users and security advisors and designers;
- The need to ensure that security is in response to perceived business risks and that any other reason for including security is almost certainly invalid;
- The benefit of seeing security not as a cost, but as a business enabler – helping to achieve business objectives.

The Cultural Legacy: Business Prevention

Security has a bad reputation for getting in the way of real business

Security, especially information security, has a bad reputation. Those of us who have worked as information system security professionals in an operational business environment know this only too well. When you walk into the room everyone groans. They say: 'Here come the security guys again! They are going to give us even more passwords to remember, more rules to enforce and they will create even more difficulties in our lives that will prevent us from getting on with real business. Why don't they just leave us alone?'

Some people even call us the 'business prevention' department!

This reputation has developed because of the way security professionals have practised

Is it an unfair reputation? Are we being misjudged and slandered by our colleagues? Well, if we are honest with ourselves, we as a profession probably deserve it all. Not you and me, of course, because we are enlightened. But the profession as a whole has certainly got that reputation because we collectively behaved like that and still behave like that. Now that I think about it, perhaps you and I were also partly responsible, before our enlightenment.

How did it happen? Why did we get this reputation? What did we do wrong?

We need an accurate definition of what we mean by 'security'

Well, in our view, it is because we have not been using a very good definition of the terms 'security' and 'secure'. What do they mean to you? Have you ever had the experience of being asked (as consultants are often asked) by a client or user: 'Have a look at this system; do you consider it to be secure?'

A technical definition of security may not be helpful

Some people, in order to prepare an answer, will start to look at the technical nuts and bolts of the system. They will give opinions on how this and that widget is weak, and how someone could get access to these and those files, and so on and so on. It's a technical analysis of the system, which may or may not be useful. Whether or not it is useful will depend on the answer to an important question. The prudent and experienced security professional will already have asked this question before answering the enquirer. The critical question is: 'What do you mean by "secure"?'

Security can be defined only relative to the value and risk propositions of the business

'Security' is a relative term. There is no absolute scale of security or insecurity. Both terms, 'secure' and 'security', have a meaning only when interpreted as attributes of something that you consider valuable. Something valuable that is in some way at risk needs to be secured. How much security does it need? Well that depends upon the value and upon the operational risk. How do you measure the operational risk? Now you are getting to the real questions that will lead you to an understanding of what you really mean by the term 'secure'.

Measuring and Prioritising Business Risk

Risk is a combination of asset value, business impact, threat and vulnerability

Security is used to protect things of value. In a business environment things that have value are often called assets. If assets are in some way damaged or destroyed, then you will suffer a business impact. The potential event by which you can suffer the damage or destruction is a threat. To prevent threats from crystallising into loss events that have a business impact, you use a layer of protection to keep the threats away from your assets. If the assets are poorly protected (i.e. your security is poor) then you have a vulnerability to the threat. To improve the protection and reduce the vulnerability you introduce security controls, which can be either technical or procedural.

Risk management is a combination of risk assessment and 'risk mitigation'

The process of identifying business assets, recognising the threats, assessing the level of business impact that would be suffered if the threats were to crystallise, and analysing the vulnerabilities, is known as operational risk assessment. Applying suitable controls to gain a balance between security, usability, cost and other business requirements is called operational risk mitigation. Operational risk assessment and operational risk mitigation jointly comprise what is often called operational risk management.

The main objective is to prioritise risks so as to make wise control decisions

Later chapters in this book examine operational risk management in much greater detail (see Chapter 15). The main thing that you need to understand at this stage is that risk management is all about identifying and prioritising the risks through the risk assessment1 process and applying levels of control in line with those priorities.

Control objectives are the abstract statement of business needs

Not all risks are worthy of implementing additional security and control, either because the potential losses are not significant enough or because the costs of implementing the controls are high compared to the potential losses. What you get from the risk assessment is a set of business requirements for security and control, ranked in some kind of order of priority. These are often expressed as a series of control objectives – abstract descriptions of a business requirement for control. These in turn are used to drive the selection of risk mitigation approaches: broad security and control strategies, logical security services, physical security mechanisms, and eventually the security products, tools and technology components with which you construct your security architecture.

---

[1]Some people make a distinction between 'risk assessment' – by which they mean taking a qualitative view of the risks, and 'risk analysis' – which they mean taking a quantitative view. In this book we shall advocate only qualitative risk assessment. However, we are equally comfortable with the use of 'risk analysis' to describe this qualitative approach, and we do not make a distinction in the definitions of these two terms.

Enablement objectives are another type of abstract statement of business need

Although the term 'control objectives' is well known and widely used, especially within the auditing community, we like to think of a complementary term: 'enablement objectives'. This is to emphasise one of the key messages of the early chapters of this book – that security is primarily all about business enablement and not at all about business prevention. Although 'control' is a valid term, it does lack the imaginative flair that we hope to inspire in those who read this book, and so these phrases are complementary so as to give a more balanced view of what the business objectives really are.

Enablement is often the flip side of control

For example, consider the brakes on a car. The brakes have a clear control function – they are used to prevent the car from going too fast and to reduce the speed if the driver judges that it is too high. However, another way of looking at this function is that having better brakes enables the car to be driven at much higher speeds, because the driver now has the confidence that if the need arises, braking will be fast and efficient. It is a completely different way of viewing the same function – one way is about reducing overall speed, the other about increasing it.

Security should be business risk-driven

By adopting this risk-based approach (in terms of both control objectives and enablement objectives) to developing your security strategy you can more closely align your information systems security with the needs of the business. However, there is much, much more you can do to get value from your efforts. This is only the beginning, and in the following sections we shall look at other ways to build up the business case.

Information Security as the Enabler of Business

Security professionals would like to have a positive reputation with their business colleagues

The reputation that we (information security professionals) would really like to have is very different from the one that we actually have. When we walk into the room we would like to hear: 'Hoorah! Here come the security guys. They're going to help us to meet our business objectives. They're going to help us to realise our wildest dreams by using information and communications technology in new and exciting ways to facilitate business growth, without us losing sleep because of all the risks we would have to take. Our investments in information security are a key success factor for this business. Our information security strategy is critical to the current and future business growth. Invite the guys in, sit them down, give them a drink, and a salary increase.'

We wish!

Not the 'business prevention' department, but the 'business enabling' department.

Your good reputation will depend upon your abilities to serve the business well

But if you do your job properly it could happen. That's what your goal should be. Information security is the enabling technology of electronic business. You have to sell these ideas to your business colleagues and then make them come true. If you don't offer this sort of value to the business then why are you there? What possible benefits does information security have if not these?

New technologies are impacting the way that business is being done

There are several key technologies that are changing the way that business will be done in the future. These include:

- The Internet and the World Wide Web with all its services and protocols, especially the emerging 'web services' protocols;
- Mobile handsets with sophisticated communications and processing capabilities;
- Web-enabled digital television and the prospect of other web-enabled domestic appliances, especially for delivering entertainment and information services;

- Client-server distributed architectures and advanced middleware products;
- High-bandwidth digital communications, including broadband, cable, cellular telephony, satellite and terrestrial broadcast;
- Advanced data networking protocols;
- Wireless communications;
- Public key infrastructure;
- Network computing, thin clients, and mobile code.

The effect is to migrate the point of sale and the point of delivery right into the customer's premises

The major change that we shall see as a result of the deployment of these technologies is the continued migration of both the point of sale and the point of delivery right into the premises of the customer in what is called the B2C (business-to-consumer) model. That is what 'electronic business' or 'digital business' really means. People who want to buy something or transact some business no longer need to make a physical visit to the supplier. They can use some type of information and communications technology system to make contact from their home base. They can browse through virtual shops, looking at virtual products on the virtual shelves. They can click the mouse to examine the product more carefully and click again to select their purchase. The products themselves may be picked automatically in the electronic warehouse and dispatched to the customer with minimal human intervention.

Business-to-business is where most of the initial growth is seen in digital business

More often than not both the supplier and the customer in digital business transactions are business organisations. This is known as the B2B (business-to-business) model. 'Supply chain management' and 'eProcurement' are amongst the most popular phrases used to describe the goals of business organisations in applying this model.

Lack of customer confidence is an obstacle to digital business and eBusiness development

However, the number of possible threats, impacts and vulnerabilities that arise in all of these complex systems is enormous. The major obstacle to the development of electronic business (or digital business) on a huge scale is the low level of confidence that is inspired in the customer community as more and more news items give the grisly details of security breaches.

Think of the major business risks:

- Disclosure of private, personal information, such as details of bank accounts, medical history, personal business interests, etc;
- Fraudulent buyers;
- Fraudulent sellers;
- Theft of payment authorisation details (such as credit card data);
- Errors and mistakes on a large scale (you ordered how many?);
- Disputes that are difficult to resolve because everyone refuses to take responsibility;
- Frustration and loss of confidence in systems that do not work properly.

On-line banking security breaches are very damaging to reputations

Here are a few examples of firms that have experienced some of these risks firsthand. The first one concerns retail on-line banking.

Case Study: The Wrong Accounts

A major retail bank with a global brand name had established an on-line banking service that boasted 1.2 million customers. It had decided to undertake a major overhaul and re-launch of the web site, and as part of this re-launch one of the much-vaunted features was to be improved security. This was at a time when the lack of public confidence in Internet security was suffering heavy battering in the popular press, and the bank had decided to take a pro-active stand on this issue.

The upgrade was implemented over a weekend. On Monday morning customers began to log on to the new service. Several of them (not the majority, just a very few, but plenty to be newsworthy) were presented with the account details of another customer in place of their own!

The technical explanation seems to have been that when two customers logged on at virtually the same time, the second customer was shown the same details as the first. Oh dear!

As soon as the bank became aware of the problem and had verified its existence they shut down the site (at 15:30 on Monday afternoon). The service was closed for several hours and the old version of the system was restored later that evening.

The bank tried to stress that only a very few customers (around 10 in fact) had experienced the problem, but that did not prevent the Tuesday newspapers from carrying the story on the front page with headlines such as 'Security fear shuts on-line bank'.

The embarrassment and the damage to the reputation of the bank were substantial. Perhaps even worse, coming as it did in the midst of a stream of similar incidents and adverse newspaper headlines, the damage to the online banking industry as a whole, and to the growth of eBusiness in general, was also significant.

The second case study relates to a major public utilities company. The story appeared on the front pages of the newspapers in the same month in which the on-line banking incident above was reported.

Public relations management is just as important as technical expertise in the protection of reputation

Case Study: In Denial

A public utilities company selling both gas and electricity had developed a web-based interface for its customers to manage their accounts on-line.

One customer discovered quite by accident that by removing part of the URL on his browser command line, he could display a file that contained the bank account details and credit card details of all of the customers who used this service – approximately 2,500 customers. He had stumbled on this fact by pure chance as he mistyped the URL command.

He immediately telephoned the company, through their customer help line, and informed them of the problem. They did nothing. He telephoned again to find out what was being done, and was informed that 'it could not happen' and that there was no problem. He offered to show them the evidence but they told him to stop annoying them.

In frustration he then copied the file onto his own PC and contacted another web site that specialises in publishing juicy details such as these. They were delighted to help and published the entire file. He then contacted the company again and told them where they could look at their file.

Their first response was to report this gentleman to the police and have him arrested on suspicion of hacking into their system. The newspapers loved this! Eventually they came to their senses, dropped the charges, offered a statement of public thanks to the man for his assistance, and invited him to advise them on security matters in future. (We are not sure that this last point was entirely wise, but then we are seeing here a company that has little idea how to handle Internet security issues. We would hazard a guess that this whole incident was managed from a very technical perspective, with little or no input from people with any real business acumen.)

This incident tells you a lot about business risk and Internet services. It is not just the fact that when these problems occur and they get into the newspapers then the organisation suffers reputation damage. This incident was handled with such crass lack of public relations finesse that you can see immediately that there is more to business risk than technical failure. When the technology fails (as indeed it will from time to time) then there must be an adequate crisis management response that includes the very critical issue of public relations management.

The bank in the earlier case study had some major problems, but at least it knew how to handle them when they occurred.

Here is another banking tale now. This one is of a different nature to the first, and emphasising the broader nature of security as we define it. It actually combines two cases, both very similar in nature.

Scaling and capacity planning are critical issues with respect to service availability

Case Study: Failure to Deliver

(a) A major retail bank had planned and developed a new Internet banking service for its retail customers. The web site was launched amid the usual marketing hype, and people started to use it.

During its first week of operation it was crippled by the surge in demand, and had to be taken out of service several times for several hours at a time to fix the problems. It was hopelessly under-scaled for the level of business that it attracted.

(b) Another retail bank with a very similar market profile to the first one in this example had also planned and developed a similar on-line banking service, but this one was a combination of Internet banking and telephone banking.

Perhaps in response to an analysis of what had happened to the first bank, it delayed the launch of the new service just one day before it was due to go live. Of course by that time it was too late to avoid the humiliation of the newspapers trumpeting this news and the reasons for it.

Both of these incidents underline an important point – that availability of a business service is one of the key goals to be protected and enabled by good security practices, and that security includes anything that has a bearing upon the operational stability and continuity of the business service. Capacity planning and scalability are amongst the issues that must be addressed within the security architecture.

Another case study concerns the movement towards electronic government. In this case the provision of an electronic interface for handling personal tax returns.

Electronic government will only succeed if the citizens can have confidence in the correct operation of the systems

Case Study: A Taxing Problem

A national government personal taxation department launched a new web-based service so that its tax-paying citizens could log on via the Internet and file their personal tax returns on-line.

The service received very large amounts of advance publicity and even more publicity once it was launched. A key goal was to save government money on administration of paper systems, and so financial incentives were offered to users to tempt them to use the service. A modest reduction in the tax bill was to be the reward for filing and paying on-line.

The service was aimed to attract around 300,000 users within its first year of operation. It was therefore very embarrassing for the department concerned to have to admit publicly that the software on the site contained serious bugs that introduced errors into the tax calculations for those using this method.

It seems that errors of several thousands of pounds (in favour of the tax authority, not in favour of the taxpayer) were a regular feature of the calculations, resulting in taxpayers receiving tax demands for far greater amounts of money than they actually owed. If you knew that the service behaved like this, would you use it?

At the same time as this was going on, it was revealed that another computer system that identifies people who may be under-paying their tax and should be investigated, was also malfunctioning. This meant that some people who were quite innocent of any wrongdoing were being identified by the system and subjected to interrogations by investigative tax officers.

If the introduction of electronic government requires the confidence of the citizens in its correct operation, incidents like these are not helping. Electronic government will only succeed if the citizens can see concrete evidence that these issues have been addressed.

Finally, from the same page of the same newspaper where we found the account of the tax problems, here is an insurance group suffering major problems in launching its new service.

Systems integration is a major challenge in the delivery of legacy back-end services through new front-end portals

Case Study: Disintegration

An insurance portal was launched on the web promising consolidated on-line access to a range of household insurance services from several major insurance companies. The marketing budget for this new service has been reported as being 5 million pounds sterling per year.

The launch and the weeks and months following it were dogged by a series of serious technical problems and failures. The site was only partially operational, and the faults and excuses seemed to vary from day to day. An example message was reported as 'Although we can offer a full service for travel insurance, we are currently resolving technical difficulties on home and motor insurance'.

One part of the web site promises: 'Our mission is to make buying insurance quicker and simpler'. So, if that's the key business goal, why isn't the technical department aware of that and performing to a level that supports it?

The public relations speak is well honed: 'It is not that the site isn't working, it's just that some of the insurers have had a problem integrating their systems.'

So here is lesson to be learned – security is not just about confidentiality, integrity and availability. It requires a much wider view to be taken. In this case the overall service was unavailable because of systems integration problems. In our view, control over systems integration is all part of 'security management' and 'security architecture'.

The current environment is a huge opportunity for security professionals to excel

So here is your opportunity to show how good you are. You have the whole world pleading for security of information systems to enable them to do business. You have the technology to provide the solutions. What you must also demonstrate is that you have the associated skills to apply that technology to solving the problems of electronic business.

Technology alone is not enough to produce effective security

You need much more than pure technology. You also need:

- Good understanding of the business needs and risks;
- Strategic architectures;
- Project management;
- Systems integration;
- Security management policies and practices;
- Enterprise-wide security culture and infrastructure.

Adding Value to the Core Product

There are different issues for retail business and corporate business

In the section above we have focused on 'electronic commerce' in a very retail sense of the phrase. Let us now move on to a more corporate view of the electronic business world.

ICT is impacting on traditional bricks-and-mortar companies in several ways

Many companies have been supplying traditional products in traditional ways for many decades. To move very far indeed from the retail end, consider for a moment the civil aerospace industry. The products here are aeroplanes – not something you or I would normally buy for ourselves.

Information and communications technology (ICT) is impacting this industry in two very different ways:

- The products themselves are incorporating more and more embedded ICT systems;
- The support of these products is very information-intensive, and the supply of this support information is becoming more and more automated.

Most traditional industries have similar experiences

We choose civil aerospace as an example because it is easy to see how information and communications technology is critical to this industry. However, almost every industry has a similar story to tell. Electronics are becoming an integral part of many products, and on-line information available to customers is a key aspect of product support.

Customer confidence in safety-critical systems is created and maintained through a comprehensive assurance programme

Case Study: Safety Assurance

First consider the embedded systems in civil aircraft. Not only are aeroplanes very expensive items, but they also carry passengers whose safety is of the utmost importance both to the customers themselves and to those who build and operate the aircraft. The correct functioning of these embedded systems is critical to the success of the business mission.

Assurance of design and implementation, elimination of operational errors and failures and prevention of malicious interference are all absolutely at the heart of providing confidence that the product (and the service that is delivered through it) will function as intended.

The manufacturers and the operators need this confidence – but most of all it is the end-customers (passengers) who need to be confident that they are travelling in a safe aircraft. The way to provide this confidence is through the provision of appropriate quality management and information security practices.

This is a clear example where the key goal is assurance. We shall return to this goal later in our discussions.

The second example looks at the issue of product support during and after delivery.

New ways of working enabled by new technology have a significant impact on customer expectations

Case Study: Raising Expectations

It is said that when you buy an aeroplane you also get a pile of documentation equivalent to the weight of the aircraft. The supply of this information is not only to tell you how to fly and maintain the aircraft. It is to meet the requirements of the industry regulators who enforce strict traceability of all aspects of the design, construction and operation of the plane. The certification of the aircraft as being airworthy depends to a large extent upon this documentation.

The pile of paper equal in size to the plane itself (or however large the pile really is) is very difficult to manage, and so electronic information is replacing it. Electronic solutions require less storage space, are easier to keep up to date, are easier to search for specific items, and are much easier, quicker and less expensive to deliver to the customer (that is, the airline that operates the aircraft).

Not surprisingly the civil aircraft manufacturers are moving as quickly as they can to deliver support documentation to their customers through on-line information systems. When the major manufacturers compete for business, the support of the aircraft during its lifetime is one of the most critical factors to be considered by the airline (customer), since the operational lifetime of good civil aircraft can be anything up to about 30 years. The use of on-line information systems to improve this support is therefore a competitive advantage.

This raises several important information security issues:

- Authenticity of design documents, drawings, service bulletins, etc. Are the electronic documents that were received through the on-line delivery system really from the manufacturer? Customer confidence (and safety) is at stake.
- Information service availability. Once a major airline gets used to a 365 day x 24 hour service[2] and plans its flight operations around a dependence on such a service level, then any failure to meet this service level will result in very unhappy airlines and many potential risks to their own businesses.

Any service that is to be completely successful in this environment in the long term must address these issues. The really challenging aspect is that the potential problems may not emerge at all during the early days of operation. It is downstream, when total dependence has set in, that these problems will become business-critical, and by then it will be too late if the design has not mitigated these risks.

Customer decisions are affected by perceptions of service

These information services that are used to support the core product add real value and become competitive factors for customers making buying decisions. However, customer confidence will be maintained only if these services are secured to an appropriate level, taking into account the business risks.

Empowering the Customers

Customer empowerment means giving the customer choices

We have looked at examples from both the retail world of electronic commerce and the corporate world of electronic business. In all cases we see that electronic information systems are the means to empower the customer to gain greater benefits. These information systems therefore become important competitive factors for the suppliers, because the customers will use their power to select those suppliers who can meet the challenge of providing these benefits.

Understanding the concept ofcustomer service is critical to business success in the new economy

Case Study: Supplying Power to the Customer

The utilities industries have become an interesting example of this phenomenon of empowering the customer through the web.

The product that arrives at your house or your office is essentially a commodity of unvarying quality (provided that service outages have been all but eliminated,

[2]In this industry 365 by 24 really does mean every day of the year in a global, multicultural world where religious diversity means that major festivals vary greatly in their timing.

which is the case in most economically developed countries). Electricity sold by one company is indistinguishable from electricity sold by another. The same is true for gas and for water.

Once the industry has been deregulated (as for example in the United Kingdom), there is one company that is responsible for distribution infrastructure and other companies who have relationships with customers and who sell the commodities.

In this environment one of the key things that distinguishes one supplier from another is customer service. The core product remains unaltered. The customer is only ever a couple of mouse clicks away from changing supplier within the comfort of his or her own home, and the only thing that will keep the customer on board (or conversely, that will drive the customer away) is customer service.

At this point you need to look at customer service in its widest possible context. Some points to consider are:

- What do customers see as the intangible aspects of customer service? In other words, how does it feel to do business here? Is it a good or a bad experience?
- How do you manage customer expectations and how high should you build them? (Because if you build them high, you had better be able to deliver to that level of expectation).
- How do you manage customer relationships so as to avoid a confrontational style of relationship (in which customers have complaints) and maintain a long-term service relationship (in which customers remain happy with the service and are content to let it continue indefinitely)?
- What contributes to the 'psychological contract' (as opposed to the legal contract) in a customer service relationship? This is important, because no matter what the strictly legal contractual terms are, there are always customer expectations of service that can never be articulated in a legal document, and meeting these expectations is a matter of trust. The legal document is just a safety net and a definition of the minimum acceptable level of service. In reality people expect much more than this.
- How do you develop consistency in customer service communications across all the people and departments who interact with customers and who therefore have an impact on the customer's perception of service?
- What are the current and projected patterns of communication with the customers and what are the service offers that will be made?
- What are the critical moments of truth in your customer relationships at which the customer relationship is at highest risk because the customer's service expectations are being tested to their limit, and how should you deal with these moments of truth?

So, is the design of a utilities business web site a technical issue? We do not think so. Refer back to the case study in an earlier section that discussed the

security breach in a public utilities web site. Had that company understood these concepts of customer service? What do you think?

Once you empower the customers in this way, you have empowered them to leave you on a whim. So the business relationship that you value so much must be protected. Security procedures such as user authentication and login potentially have a major impact on whether or not the user has a good experience using a web site. How personal, private information is protected and safeguarded also affects the customer's perception of the service level being provided, as does the availability of the site and services delivered through it. For these and many other reasons, customer service considerations are a major driver of security strategy and security architecture.

Information security practices can deeply affect perceptions of customer service

Information security is a critical component, without which it will be difficult for suppliers to meet this customer service challenge. Customers will evaluate suppliers not only on the products themselves but also on the means by which those products are marketed, sold and supported. Where on-line information systems are involved, that means that the quality, reliability, integrity and availability of those information services will be key factors in determining which suppliers succeed and which do not.

Service quality and information security are closely linked

To maintain that quality of service, one of the major tools you will need is an effective, risk-based information security programme and a structured information systems security architecture.

Protecting Relationships and Leveraging Trust

Business relationships are based upon trust

There is another security-related dimension to business relationships that we have not yet explored here: the concept of trust. We shall return to this in great detail later on in the book, but for the present time let us take a first glance at the subject.

Trust is a business relationship attribute, not a technical attribute

When you do business with someone, at whatever level (personal or corporate), you establish some level of trust in the other party. You usually evaluate a number of signals that you receive, perhaps over some time, to determine how much you trust this person. How do they present themselves (standard of dress, location and type of premises, eye contact, handshake, etc.)? Have you done business before? How did it go? How long has the firm been established? Can you get a reference from someone else you know and trust (a trusted third party) – someone that already knows this person and can vouch for him or her? And so on.

Technical systems need to protect the trust that exists in a relationship

Trust is an essential pre-requisite to doing business, and trust is entirely a relationship thing. Trust is not created through technical systems but through some mutual knowledge between the parties. However, technical systems are used to protect the trust in the relationship that already exists.

If you trust the source of an information service, you must also be sure that you are talking to the authentic trusted party and not to an impostor

Case Study: Trusted Sources

We return here to our civil aerospace example.

If an airline buying an aeroplane from a major aircraft manufacturer has built up a high level of trust in the product and its supplier, then a drawing or a technical specification supplied by that manufacturer will be trusted to be

> correct. This trust comes from a relationship that has been built up between the supplier and the customer.
>
> The protection of that trust is through a technical service that verifies the authenticity of such a document when it is delivered electronically through an on-line information system. Thus a digital signature on the received electronic document, supported by a certified public key to verify that signature, is a mechanism that supports an authenticity service, which in turn supports and protects the trust that exists between the parties.
>
> To build an information distribution service for the purpose of distributing aircraft design documents would require this sort of technical approach in order to protect the level of trust that exists at the business level.

Trusted third parties act as intermediaries to introduce business partners to one another

These technical services are no substitute for trust. They do not create trust. They merely protect trust that already exists. However, indirect trust, through a third party (sometimes called transitive trust), is an important part of setting up digital business networks. It is obviously an advantage for both customers and suppliers to be empowered to do business with one another even though they each have no previous direct knowledge of one another. This is where the third-party referee comes into the picture. The third party needs to be trusted by both of the other parties. This trusted third party is then able to play the role of 'introducer' by vouching for each of the two business parties to the other. This is usually achieved by the trusted third party issuing each entity with some certified credentials. This is called a digital certificate and is certified by a digital signature of the trusted third party.

Business relationships are formed in similar ways to social relationships

It's a bit like the situation where you go to a cocktail party at someone's house – someone who is an old friend of yours and with whom you have a long-standing trust relationship, built up through experience and mutual interaction. At the party another guest, someone who you have not met before, nor heard of them, approaches you. It's quite different from meeting this person in a downtown bar or on the street, where you might be very cautious and even suspicious of being approached by a stranger. The first thing you each ask one another is your name and how you know the host of the party. This establishes the credentials – 'Oh, I'm an old friend from college days' or 'I'm his sister-in-law'. It gives the new friendship a kick-start, because you have established that you are both trusted by the host, who in this case acts as a trusted introducer for you both, giving both of you some confidence that it is alright to proceed with a friendship. You can begin to interact with a level of trust that would not be possible in the downtown bar. That's why house parties are such a success!

Business relationships are driven by human factors, not by technology

This trusted third-party mechanism is an important part of human life, both in social interactions and in business relationships. In many cases the two are heavily intertwined. The cynical observer might point out how much business is done on the golf course, but business is primarily about relationships between business people, and it so happens that many relationships are built whilst playing golf.

Mutual trust is essential, and must be protected by technical systems

Many business deals are founded upon a personal introduction by a mutually trusted third party, or upon belonging to some business community that is in some way regulated by a trusted overseer. Thus, when you build information systems, these technical systems can leverage trust that already exists, whether directly or indirectly, and they can protect those trusted business relationships in the course of doing business through this new information system-based medium.

To Summarise: What Does 'Security' Mean?

Security is all about protecting business goals and assets. It means providing a set of business controls that are matched to business needs, which in turn are derived from an assessment and analysis of business risks. The objective in risk assessment is to prioritise risks so as to focus on those that most require mitigation.

Risk is a complex concept, and for any given course of action there is a risk associated doing that thing and a risk associated with not doing it. Thus one must take care not to mitigate a specific risk whilst unintentionally increasing the overall risk to the wider range of business goals and objectives.

In its best possible light, security should be seen as enabling business by reducing risks to acceptable levels and thus allowing business to make use of new technologies for greater commercial advantage.

Security can also be a means to add value to the core product by enabling information services that are essential to the enhancement of the product itself or to the operational support of the product in the field.

Secure information services can empower the customers, enabling them to do business more easily, and providing them with enhanced services that will have competitive value.

Security in business information systems also protects and leverages the trust that exists between business partners, allowing them to establish relationships and to do business in new ways using new technologies.

Chapter 2: The Meaning of Architecture

This chapter explores what 'architecture' might really mean. In particular it examines the essential differences between 'architecture' and 'plumbing'. Both of these disciplines are of great value, but they are the not the same thing. In the world of ICT people sometimes get confused about which is which.

In this chapter you will learn about:

- The concept of architecture as a means to integrate solutions to a diverse range of complex needs, and as a means to manage that complexity;
- Conceptual layered approaches to architecture and the use of architectural reference models;
- The benefits of taking a holistic, strategic architectural approach as opposed to applying point solutions with tactical goals.

The Origins of Architecture

Architecture is best understood in the context of buildings

Architecture has its origins in the building of towns and cities, and everyone understands this sense of the word, so it makes sense to begin by examining the meaning of 'architecture' in this traditional context.

Architecture fulfils the needs of those who experience it

Architecture is a set of rules and conventions by which we create buildings that serve the purposes for which we intend them, both functionally and aesthetically. Our concept of architecture is one that supports our needs to live, to work, to do business, to travel, to socialise and to pursue our leisure. The multiplicity and complex interaction of these various activities must be supported, and this includes the relationship between the activities themselves and their integration into a whole lifestyle. Architecture is founded upon an understanding of the needs that it must fulfil.

The needs that architecture must fulfil are very diverse

These needs are expressed in terms of function, aesthetics, culture, government policies and civil priorities. They take into account how we feel about ourselves and about our neighbours and how they feel about us. In these various ways, architecture must serve all those who will experience it in any way.

Goals, environment, materials and skill are key drivers of architecture

Architecture is also both driven and constrained by a number of specific factors. These include the materials available within the locale that can be used for construction, the terrain, the prevailing climate, the technology and the engineering skills of the people.

This all boils down to three major factors that determine what architecture we will create. These factors are:

- Our goals;
- The environment;
- Our technical capabilities.

The Sydney Opera House could not have been built in piecemeal fashion

Case Study: An Icon of Australian Culture

The Sydney Opera House is perhaps one of the most famous buildings in the world. More than that, it is probably the most well-known example of modern architecture.

How does a building such as this come into existence? Could many small project teams build it, each with its own ideas about how things should be done, each designing its own piece of the building from scratch, and each having a narrow view of the overall business goal as its motivator?

Clearly this would not work. A building of this calibre (whether you are an enthusiast for the design or not) could never be designed and built in piecemeal fashion. The only way that something truly architectural can be created is from a single central vision of its design – an overall concept. Later sections of the book, especially Chapter 10, discuss conceptual architecture at some length.

It is the job of the architect to create the vision and the direction, taking into account the very widest view of all the possible requirements from all possible interested parties. This vision then becomes the road map that guides all others who will work on the project. The architect remains in control throughout, supervising the work and ensuring that the integrity of the architectural design is not compromised at later stages.

Managing Complexity

A major function of architecture as a tool is to manage complexity in large projects

One of the key functions of architecture as a product of the architect is to provide a framework within which complexity can be managed successfully. Small, isolated, individual projects do not need architecture, because their level of complexity is limited and the chief designer can manage the overall design single-handedly. However, as the size and complexity of a project grows, then it is clear that many designers are needed, all working as a team to create something that has the appearance of being designed by a single design authority.

Architecture also acts as a road map for a collection of smaller projects that must be integrated into a single homogenous whole

Also, if an individual project is not isolated, but rather is intended to fit harmoniously within a much wider, highly complex set of other projects, then an architecture is needed to act as a road map within which all of these projects can be brought together into a seamless whole. The result must be as though they were all indeed part of a single, large, complex project. This applies whether the individual projects are designed and implemented simultaneously, or whether they are designed and implemented independently over an extended period of time.

Architecture provides a framework within which many members of a large design team can work harmoniously

As complexity increases, then a framework is needed within which each designer can work, contributing to the overall design. Each design team member must also be confident that his or

her work will be in harmony with that of colleagues and that the overall integrity of the design will not be threatened by the work being split across a large design team.

This is achieved through layering techniques and through modularization

The role of architecture is to provide the framework that breaks down complexity into apparent simplicity. This is achieved by layering techniques – focusing attention on specific conceptual levels of thinking, and by modularization – breaking the overall design into manageable pieces that have defined functionality and defined interfaces. This process is also known as systems engineering and is discussed in greater detail in Chapter 5.

Information Systems Architecture

Architecture has been adapted to other spheres of creativity

The concept of architecture in buildings has been adapted to areas of life other than the building of towns and cities. For example one talks about a naval architect being someone that designs and supervises the construction of ships. In more recent times the term has been adopted in the context of designing and building business computer systems, and so the concept of information systems architecture has been born.

Information systems architecture addresses the creation of business computing systems

In the same way that conventional architecture defines the rules and standards for the design and construction of buildings, information systems architecture addresses these same issues for the design and construction of computers, communications networks and the distributed business systems that are implemented using these technologies.

Information systems architecture has influences similar to buildings architecture

As with the conventional architecture of buildings, towns and cities, information systems architecture must therefore take account of:

- The goals that are to be achieved through the systems;
- The environment in which the systems will be built and used;
- The technical capabilities of the people to construct and operate the systems and their component sub-systems.

Architecture addresses a wide range of issues beyond the technical domain

If one accepts this analysis then one is already well on the way to recognising that information systems architecture is concerned with much more than mere technical factors. It is concerned with what the enterprise wants to achieve and with the environmental factors that will influence those achievements.

An inadequate understanding of architecture can lead to failure to deliver business value

In some organisations this broad view of information systems architecture is not well understood. Technical factors are often the main ones that influence the architecture, and under these conditions the architecture can fail to deliver what the business expects and needs.

This book addresses the wider issues, not just the technical dimension

This book is mainly concerned with only one aspect of information systems architecture: that is the security of business information systems. However, in addressing this specialist area the authors have tried to provide as much advice as possible on how to take the broader view. Thus the focus is on an enterprise security architecture, to emphasise that it is the enterprise and its activities that are to be secured and that the security of computers and networks is only a means to this end.

Business systems architecture is the highest-level framework

First, however, here are some general ideas of modern information systems architecture, since a security architecture must fit within this overall framework. Figure 2-1 shows a reference model for the overall business systems architecture[1]. For most people this has several major component sub-architectures, as described in the sections below and as represented in the diagram.

[1]This reference model is a creation of the authors of this book. It does not appear in any international standard.

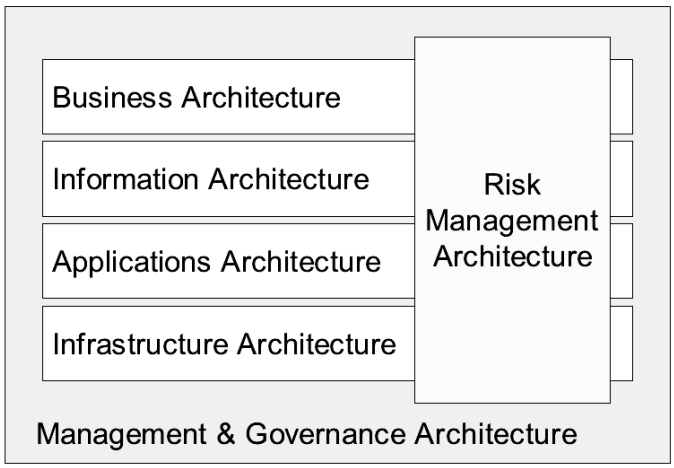

Figure 2-1: A High-Level Reference Model for Business Systems Architecture

Business Architecture

Business architecture is the primary component

The business architecture describes from an enterprise-wide perspective how the business itself is structured into an organisational model, a set of processes, functions and so on. This is the primary architecture of all. The other sub-architectures are all created in support of this single overriding framework of how the business actually works. In other contexts this is often called the 'business model'.

Information Architecture

Information architecture is an abstract representation of the business

The business is represented by information. Every business relationship, every business process, every business transaction, indeed everything about the business, its planning, its control, its management and its success or failure, is represented by information. Information is an abstract representation of something that is real and tangible. This is why information is so important to business, because information is the business, represented in a particular form.

Information architecture is the framework for business information management

The information architecture describes the framework within which business information is created, organised, processed, stored, retrieved and communicated, and in the reference model (see Figure 2-1) it has been represented as the next level of abstraction down from the business itself.

It describes information types and their behaviour

Information architecture describes information types and their overall structured relationships and organisation, information behaviour, information management processes, and physical locations and repositories for information. In particular it identifies and describes the major categories of information that are needed to support the business strategy and goals.

Applications Architecture

The applications architecture supports the information architecture

The applications are the suites of computer programs that carry out actions on business information on behalf of real business users. In the reference model (see Figure 2-1) the applications architecture is shown as the third level, supporting the information architecture, which in turn supports the business architecture.

Applications represent and support real business processes

The applications mirror critical automated parts of the business processes. The applications architecture describes how applications are to be designed, how they inter-operate with one

another, and how they are supported within the infrastructure (hardware, software and communications networks). The applications must of course relate to the business processes that they support and the information resources that they create, maintain and process.

Modern applications architectures are likely to exhibit certain common properties

Characteristics of modern applications architecture are likely to be:

- Component based – re-usable, generic modules, and hence quickly adaptable to new business needs;
- Service oriented – components offering services to one another;
- Built on a strategic middleware layer – for services integration;
- Offering distributed processing.

Applications architecture enables business flexibility

The main objective of applications architecture is to enable business processes. It accomplishes that by creating applications that are flexible, economic and responsive to changes in the business.

Infrastructure Architecture

Infrastructure is the logical and physical medium for supporting applications

The applications need to be supported on logical and physical infrastructure. The term 'infrastructure' will be discussed in detail later on, but for now it is defined as being inclusive of:

The computer platforms (hardware and operating systems);

The computer networks (cables, lines, switches, routers, etc.);

The layer of software that bridges between infrastructures that have different physical characteristics and presents a consistent virtual interface to the applications. This is commonly known as 'middleware'.

Infrastructure architecture is highly technical

Infrastructure architecture is at the heart of what most people would recognise as 'technical architecture'.

Risk Management Architecture

Risk management architecture cuts across all others

In the reference model (see Figure 2-1) the four layers already described are represented as lying one on top of another. Cutting right across this layered structure is another front-plane box labelled 'Risk Management Architecture'.

Risk management architecture is pervasive

The reference model represented here is more of a business model and not quite a systems model (although it exhibits some signs of being a framework for information systems design). It is essential to see risk management as a pervasive activity that happens within all of the other four layers. This risk management architecture is close to the notion of security architecture, but it is not quite the same. A more detailed discussion of risk management is provided in Chapter 9 and Chapter 15.

Management and Governance Architecture

Management and governance architecture is all-pervasive

Finally, surrounding all other components in the reference model (see Figure 2-1) is the all-pervasive piece labelled 'Management and Governance Architecture' and shown in the diagram as a backplane, wrapping around everything else.

It describes how the management team controls the business

The representation of this as an all-encompassing component is critical. It is through this architectural framework that the senior management team controls the business, manages risk, and governs the business use of information, applications, and infrastructure.

Management and governance architecture describes levels of authority and decision making

The management and governance architecture describes the decision-making processes and levels of authority that are assigned to decision-making entities (individuals or committees). It is essentially a model of how power is wielded within the organisation and what span of control is associated with each entity.

Information Systems Architecture Reference Model

Definition of information systems architecture

This reference model for business systems architecture (see Figure 2-1) is a useful conceptual model of the various major components and how they relate to one another. An overarching definition of 'information systems architecture' might be:

> 'A consistent set of principles, policies and standards that sets the direction and vision for the development and operation of the organisation's business information systems so as to ensure alignment with and support for the business needs'

Infrastructure Architecture Reference Model

Infrastructure is a multi-layered technical architecture

However, a more detailed reference model is needed for the infrastructure component, since it is this part in which most of the technology of business systems is focused. Figure 2-2 shows a reference model for this technical infrastructure architecture.

Service integration is middleware plus data management plus common services

The applications sit on top of a layer shown here as 'Services Integration'. This is really traditional middleware plus data management services and a wide range of common services that are made available to applications transparently through the middleware layer. In the detailed discussions about conceptual security architecture later in the book the common services needed within the security architecture are examined more closely.

Data processing means 'platforms'; Information transfer means 'network'

Beneath the services integration layer are two other layers. The 'information transfer' layer is the communications network, and the data-processing layer comprises the platforms, including both

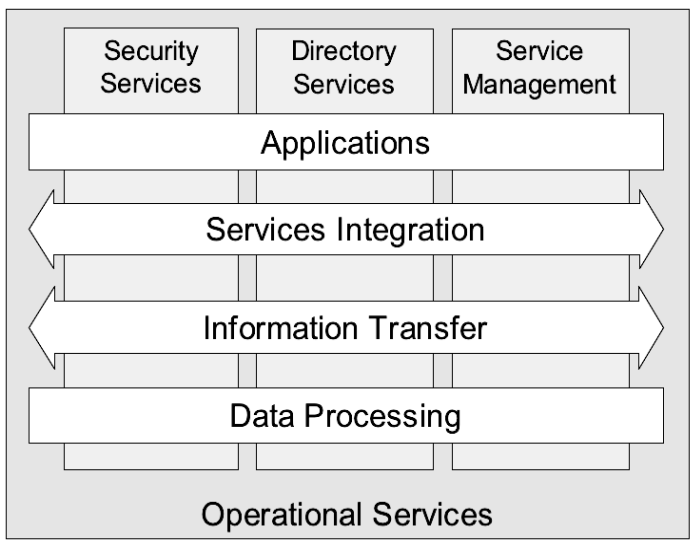

Figure 2-2: Infrastructure Architecture Reference Model

hardware and operating systems, in which the raw manipulation of physical bits and bytes takes place.

There are three pervasive service types

Behind these components the reference model shows three backplanes that cut across all of the other layered components. These service types are pervasive throughout the entire infrastructure:

- Security services (including all services used to control the infrastructure, such as time service);
- Directory services;
- Service management.

'Operational services' means people and the tasks that they perform

Finally, the entire infrastructure model is overlaid on another backplane labelled 'operational services'. The operational services represent the people and the operating processes and procedures that they carry out. Operational services are concerned with people, not technology, but nevertheless are an integral part of the systems infrastructure.

Enterprise Security Architecture

Many organisations have a long history of piecemeal implementations of security

It is the common experience of many corporate organisations that information security solutions are often designed, acquired and installed on a tactical basis. A requirement is identified, a specification is developed and a solution is sought to meet that situation. In this process there is no opportunity to consider the strategic dimension, and the result is that the organisation builds up a mixture of technical solutions on an ad hoc basis, each independently designed and specified and with no guarantee that they will be compatible and inter-operable. There is often no analysis of the long-term costs, especially the operational costs which make up a large proportion of the total cost of ownership, and there is no strategy that can be identifiably said to support the goals of the business.

Case Study: User Authentication

The total cost of ownership of multiple systems is often driven by the complexity of the diverse user authentication methods in use

One of the most commonly occurring examples of how a piecemeal design approach causes business problems is that of authenticating business users to multiple business applications.

Often each application requires a separate user ID, and often enforces different syntax rules so that a user cannot simply replicate an ID across several systems. For each user ID there is a password, again often requiring heterogeneous syntax rules, different change regimes and so on, such that each user ends up with a different user ID and different password for each system.

Setting aside the security implications of this approach (which is a contentious issue often debated by security professionals) the cost of ownership of these applications is adversely affected by the level of user support that needs to be provided simply to ensure that users can login to their authorised systems. The complexity of multiple user IDs and passwords leads to great confusion and many operational problems. The costs include:

- Administering the creation, maintenance and deletion of multiple user IDs and passwords;

- Providing help desk support for a flood of user login problems;
- Lost productivity of the users whilst they are trying to solve their authentication problems.

It is precisely this type of common problem that has led to the adoption of strategic approaches to providing user authentication services across multiple business applications (single sign-on).

True architecture never happens by accident

Those enterprises that suffer these problems are often well aware of the issues, but struggle to find an approach that will make things better. However, the Sydney Opera House could never have been built with this approach. True architecture never happens by accident, and so the enterprise must find skills, methods and tools that help it to succeed with a more strategic architectural approach.

Enterprise security architecture is the solution to the business problems of piecemeal development

An approach that avoids these piecemeal problems is the development of an enterprise security architecture which is business-driven and which describes a structured inter-relationship between the technical and procedural solutions to support the long-term needs of the business. If the architecture is to be successful, then it must provide a rational framework within which decisions can be made upon the selection of security solutions. The decision criteria should be derived from a thorough understanding of the business requirements, including the need for cost reduction, modularity, scalability, ease of component re-use, operability, usability, inter-operability both internally and externally, and integration with the enterprise ICT architecture and its legacy systems.

Business strategy for security is closely linked to operational risk management goals

Furthermore, information system security is only a small part of information security, which in turn is but one part of a wider topic: business assurance. Business assurance embraces three major areas: information security; business continuity; physical and environmental security. Broader still is the view that business assurance is concerned with all aspects of operational risk management. Only through an integrated approach to these broad aspects of business assurance will it be possible for the enterprise to make the most cost-effective and beneficial decisions with regard to the management of operational risk. The enterprise security architecture and the security management process should therefore embrace all of these areas.

The SABSA® model is used in this book as the framework for developing an enterprise security architecture

The authors of this book have been working for some years (since 1995) with a model for enterprise security architecture. This model, known as SABSA®[2] is the basis they have used for major consulting assignments with many clients, and over the years the methodology has been reviewed and refined in the light of experience and in response to new inputs of ideas from various sources. This book is essentially a description of the SABSA® model and its application. The model itself and its derivation are described in greater detail in Chapter 3.

Everything in a security architecture must be a reflection of business requirements

The primary characteristic of this model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. The model is layered, with the top layer being the business requirements definition stage. At each lower layer a new level of abstraction is developed, going through the definition of the conceptual architecture, logical architecture, physical architecture and finally at the lowest layer, the selection of technologies and products (component architecture) – in other words, the shopping list. In addition the whole area of security management, administration and operations is addressed through the operational architecture.

[2] SABSA® is a registered trademark of SABSA Limited. It stands for: Sherwood Applied Business Security Architecture.

The model is generic and defines a process for architecture development – each solution will be unique to the individual business

The model itself is generic and can be the starting point for any organisation, but by going through the process of analysis and decision-making implied by its structure, the output becomes specific to the enterprise and is finally highly customised to a unique business model. The output from applying the model becomes in reality the enterprise security architecture and is central to the success of a strategic programme of information security management within the organisation.

Why Architectures Sometimes Fail to Deliver Benefit – and How to Avoid that Fate

Historical Background

> "Those who cannot remember the past are condemned to repeat it".
>
> –*George Santayana*

The piecemeal approach to security is commonly found

Many corporate organisations implement technical solutions to business security requirements on a tactical basis. Usually a requirement is identified and a product is sought and acquired to meet that requirement without regard to the broader implications. A point solution is implemented which is often effective in providing some security, but frequently no one is really sure that the security is appropriate to the risk, or that the cost is commensurate with the benefit, or that it meets a wide variety of other business requirements which are not specifically risk-related. Security is often the last thing to be considered in business information system design, and often gets relegated to the status of a few add-on fixes when all other design decisions have been frozen.

Far from rendering business benefits, this leads to business problems

This can lead to many problems. The security solutions are often isolated and incapable of being integrated together or of inter-operating with one another. The variety of security solutions leads to increased complexity and cost of support, and in particular can lead to an exploding workload with regard to administration and management. Worst of all, because there has been inadequate attention paid to the business requirements, the 'solution' can sometimes hinder the business process rather than helping it, and the reputation of security among the business community gets worse and worse.

Good security is business-led and business-serving

Appropriate business security is that which protects the business from undue operational risks in a cost-effective way. If business security is to be effective in enhancing the business process and achieving business goals (and what other possible use could it have?) then the approach described above must be avoided. A much more strategic view should be developed, in which the business requirements are the primary driver for developing effective information security solutions.

The Wider Business Requirements

Information security is only one part of the business assurance picture

For the moment let us return to the issue of information security, using it as an example, whilst remembering that our requirements for business assurance and operational risk management also span the areas of business continuity and physical and environmental security. The same principles developed below can be applied across the entire area of business assurance.

Availability, integrity, authenticity, confidentiality, accountability, auditability

The primary business requirements for information security are business-specific. They will usually be expressed in terms of protecting the availability, integrity, authenticity and confidentiality of business information, and providing accountability and auditability in information systems. To understand these requirements, a detailed analysis of the business processes is required, using as source data information gathered by direct interviews with operational business managers.

Security has to be balanced against other requirements

However, there is much more to the business requirements than pure security and control. Information security provides for the confident use of information for business purposes across the entire organisation. The generic business requirements for an information security solution often include the following:

Usability
The solution must be appropriate to the technical competence of the intended users and ergonomically acceptable to those users.

Inter-Operability
The solution must provide for the long-term requirements for inter-operability between communicating information systems and applications.

Integration
The solution must integrate with the wide range of computer applications and platforms for which it might be required in the long term.

Supportability
The solution must be capable of being supported in the environment[3] within which it has been designed to be used.

Low Cost Development
The solution should be of modular design and hence capable of being integrated into a development programme at minimal cost.

Fast Time to Market
The solution should be capable of being integrated into a development programme with minimal delay.

Scalability of Platforms
The solution should fit with the range of computing platforms[4] with which it might be required to integrate.

Scalability of Cost
The entry-level cost should be appropriate to the range of business applications for which the solution is intended.

Scalability of Security Level
The solution should support the range of cryptographic and other techniques that will be needed to implement the required range of security strengths.

Re-Usability
The solution should be re-usable in a wide variety of similar situations to get the best return on the investment in its acquisition and development.

Operations Costs
The cost impact on systems operations should be minimised.

---

[3]Including number of end users and service delivery points, geographical location and distribution.

[4]Potential platforms range from high-end mainframes, through mid-range servers, down to PCs, workstations, laptops and palmtops. Increasingly, platforms may also include digital TVs, mobile telephones and indeed any consumer electronics goods that provide processing and communications capability.

Administration Costs

The solution should provide an efficient means for security administration to optimise the costs of this activity.

Risk-Based Cost/Benefit Effectiveness

The reduction of risk (the benefit) should be appropriate to the costs of acquisition, development, installation, administration and operation.

Dealing with Conflicting Objectives

Requirements often pull in conflicting directions

One of the most difficult challenges is that these various business requirements are often in conflict with one another. By simplifying the set of wider requirements to a basic set of three – cost control, security and usability – it becomes clear that these three pull against one another in conflicting directions. To obtain higher security or usability will cost more. To increase security often impacts upon usability, and vice versa. Figure 2-3 illustrates this conflict as an eternal triangle in which the three requirements are in constant tension, pulling in opposite directions.

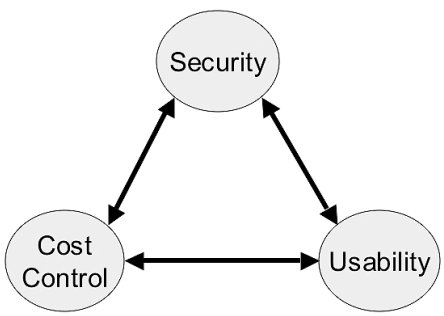

Figure 2-3: The Eternal Triangle of Conflicting Objectives

Enabling Business

Some requirements are specific to the business of the enterprise

Finally there are usually a number of business-specific requirements that influence the security strategy. These include requirements where security has an important role in generating the appropriate level of confidence so as to enable new ways of doing business using the latest advances in information and communications technology, such as:

- Exploiting the global reach of the Internet;
- Using global e-mail and e-messaging;
- Outsourcing the operation of networks and computer systems;
- Providing remote access to third parties;
- Developing on-line business services;
- Delivering digital entertainment products (video, music, etc);
- Improving customer service through integration of information and consistent presentation of a user interface;

- Obtaining software upgrades and system support through remote access by vendors;
- Tele-working, mobile computing, road warriors and the virtual office.

Being a Successful Security Architect

Security architecture must address the wider range of requirements

Unless the security architecture can address this wide range of operational requirements and provide real business support and business enablement, rather than just focusing upon security, then it is likely that it will fail to deliver what the business expects and needs.

Failure to address the wider range of issues is common

This type of failure is a common phenomenon throughout the information systems industry, not just in the realm of information systems security. In this book the whole emphasis is on the need to avoid this mistake by keeping in mind at all times the real needs of the business. It is not sufficient to compile a set of business requirements, document them and put them on the shelf, and then proceed to design a security architecture driven by technical thinking alone.

Successful architecture is business-focused

Being a successful security architect means thinking in business terms at all times, even when you get down to the real detail and the nuts and bolts of the construction. You always need to have in mind the questions: Why are we doing this? What are we trying to achieve in business terms here?

Success as an architect requires strength of character and good communications skills

It will also be difficult to battle against the numerous other people around you who do not understand strategic architecture and who think that it is all to do with technology. These people will constantly challenge you, attack you and ridicule you. You have to be ready to deal with this. You have to realise that being a successful architect is also about being a successful communicator who can sell the ideas and the benefits to others in the enterprise who need to be educated about these issues.

Senior management buy-in and support is a critical success factor

One of the most important factors for success is to have buy-in and sponsorship from senior management levels within the enterprise. Enterprise architecture cannot be achieved unless the most senior decision-makers are on your side. The fruits of the architectural work will be enjoyed throughout the enterprise, but only if the enterprise as a whole can begin to think and act in a strategic way. Creating this environment of acceptance and support is probably one of the most difficult tasks that you will face in the early stages of your work.

Geoff Rob's Ten Rules for the Solution Architect

Finally on the subject of being a successful security architect, here are Ten Rules for the Solutions Architect[5].

Ten Rules for the Solution Architect

Listen and Learn: Clients will appreciate much more your understanding their environment and business requirements fully before you try to sell them your solution. This builds the customer's trust in you.

Lead Diplomatically: In most cases the client is paying not only for a service but also a motivated person to take charge of the situation and provide a clear direction. Always be prepared to give other people time and space to express themselves.

Your Area of Expertise: Understand in depth a specific area of technology and take leadership in it. Collaborate with other leaders who can supplement your knowledge in other areas.

[5] Courtesy of its author, Geoff Rob.

Repeatability: Capitalise on work already done for other clients. By using experiences from similar client situations and adapting them to your client's situation, you can deliver a solution faster with a higher success rate.

Market Awareness: Have a global view of alternative solutions available on the market and be able to discuss and compare them with your solution.

Business Sense: Understand the costs and business impacts of the technology and the solutions you are proposing. Keep business benefits and the client's priorities paramount.

Design Acceptance: During the initial part of the design phase, be open and frank with the client and look for acceptance of a solution. This is far better than spending weeks developing something in isolation and then fighting for acceptance later. Discuss design principles and constraining factors and be prepared to defend the design rationale behind your solution.

Don't Go to Extremes: Adopt a common-sense approach to planning and design of a solution and match it to the client's situation. What the marketing hype promotes, or what you think might be interesting to experiment with, may not always be suitable. What is good for one client may not be suitable for others. Keep an open mind.

Best Fit: If a solution is too complex or costly for a client to implement, look at the part that could solve a majority of problems. Suggest an optimal solution that stays within the client's budget and yet brings a maximum of benefits.

Leverage Client's Investment: Wherever possible use the infrastructure already in place to effect transitions. Question the sense of putting in technology for short-term use with doubtful benefits. An example of this is a transitional infrastructure put in place at heavy cost and that becomes obsolete when the project is finished.

Security Architecture Needs a Holistic Approach

Security can be analogous with a chain – one link breaks, the chain is broken

Many people make the mistake of believing that building security into information systems is simply a matter of referring to a checklist of technical and procedural controls and applying the appropriate security measures on the list. However, security has an important property that most people know about but few pay any real heed to: it is like a chain, made up of many links, and the strength and suitability of the chain is only as good as that of its weakest link. At worst, if one link is missing altogether, the rest of chain is valueless.

Complex systems have a holistic design quality and are not described by checklists alone

The checklist approach also fails because many people focus on checking that the links in the chain exist but do not test that the links actually fit together to form a secure chain. The chain is a reasonably good analogy, but the problem is actually much worse than this. Imagine a checklist that has the following items: engine block, pistons, piston rings, piston rods, bearings, valves, cam shaft, wheels, chassis, body, seats, steering wheel, gearbox, etc. Suppose that this list comprehensively itemises every single component that would be needed to build a car. If you go through the checklist and make sure that you have all of these components, does it mean that you have a car? Not exactly!

Complex system example

A car is a good example of a complex system. It has many sub-systems, which in turn have sub-systems, and eventually a very large number of components. Designing and building a car needs a systems engineering approach. (Refer to Chapter 5 for a detailed discussion of systems engineering as a discipline).

Checklists often miss out key questions

Some of the key questions not addressed by the checklist approach to car construction are:

- Can you be sure that all the parts have been designed to work together as one smoothly running system?
- Do you have any assurance that the car has been properly assembled?
- Has the engine been tuned?
- Is the system actually running smoothly at this moment?
- Is there someone at the controls governing the speed, lubricating the moving parts, maintaining its fuel supply and monitoring its performance?

You need a holistic approach

Checklists are not the entire answer. Security architecture, as with all other forms of architecture, needs a holistic approach:

- Do you understand the requirements?
- Do you have a design philosophy?
- Do you have all of the components?
- Do these components work together?
- Do they form an integrated system?
- Are you assured that it is properly assembled?
- Does the system run smoothly?
- Is the system properly tuned?
- Do you operate the system correctly?
- Do you maintain the system?

The analogy of the car as a complex machine that needs a holistic architectural design is much more powerful than the idea of a chain. Security architecture is more like the car, not the chain.

To Summarise: What Does Architecture Mean?

Architecture means taking a holistic, enterprise-wide view, and creating principles, policies and standards by which the system (building, car, ship, business information system) will be designed and built.

The purpose of architecture is to ensure consistency of the design approach across a large complex system or across a complex array of smaller systems. Architectural approaches break up the complexity so as to present greater simplicity and thus make the design activity easier to manage.

One of the ways to simplify complexity is to create architectural reference models that use layering of functionality to break down the complex whole into a series of less-complex conceptual layers.

Enterprise security architecture must be driven from a business perspective and must take account of a wide range of requirements that may often be in conflict with one another. The successful architecture balances the tensions between these conflicting objectives.

Piecemeal approaches used instead of strategic architectural approaches usually fail to satisfy the business needs and to provide true business benefits. Enterprise security architecture needs a holistic systems engineering approach that implies much more than simply satisfying all the points on a checklist.

The successful security architect is an experienced and intelligent person who is a good communicator and can bring together many skills and wide-ranging knowledge from many parts of the team – someone who can grapple with the business requirements and use architectural skill to transform complexity into simplicity.

Chapter 3: Security Architecture Model

The approach to developing an enterprise security architecture that is proposed in this book is based upon a six-layer model. This model is used as the basis of an architecture development process – a methodology. By following the development of the enterprise architecture in line with the layers of the model, the methodology becomes somewhat self-evident. Later chapters provide guidance as to the steps in these various methods.

In this chapter you will learn about:

- The six-layered SABSA® Model of and its relationship to the Zachman Framework;
- The detailed interpretation of each of the six horizontal layers of the SABSA® Model;
- The SABSA® Matrix showing the vertical analysis of each horizontal layer by applying the six critical questions: What? Why? How? Who? Where? When?

The SABSA® Model

Continuing with the analogy of building architecture

To establish a layered model of how a security architecture is created, it is useful to return for a moment to the use of the word in its conventional sense: the construction of buildings.

The architecture model used in this book has six layers

The SABSA® Model comprises six layers, the summary of which is in Table 3-1. It follows closely the work done by John A. Zachman[1] in developing a model for enterprise architecture, although it has been adapted somewhat to a security view of the world. Each layer represents the view of a different player in the process of specifying, designing, constructing and using the building.

Table 3-1: The SABSA® Model Layered Architecture Views

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Facilities Manager's View	Operational Security Architecture

[1]Published through the Zachman Institute for Framework Advancement. Reference: http://www.zifa.com

The layers can also be arranged so that Operational Security Architecture is a vertical bar

There is another configuration of these six layers which is perhaps more helpful, shown in Figure 3-1. In this diagram Operational Security Architecture has been placed vertically across the other five layers. This is because operational security issues arise at each and every one of the other five layers. Operational security has a meaning in the context of each of these other layers.

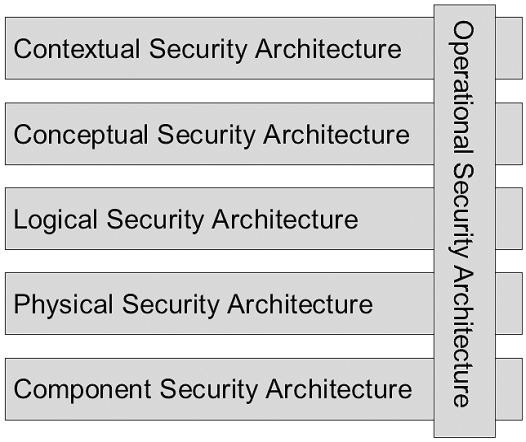

Figure 3-1: The SABSA® Model for Security Architecture Development

Kipling's poem provides six key questions

For detailed analysis of each of the six layers, the SABSA® Model also uses the same six questions that are used in the Zachman Framework and which were so eloquently articulated by Rudyard Kipling in his poem 'I Keep Six Honest Serving-Men'.

I Keep Six Honest Serving-Men

I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest.

I let them rest from nine till five,
For I am busy then,
As well as breakfast, lunch, and tea,
For they are hungry men.
But different folk have different views;
I know a person small-
She keeps ten million serving-men,
Who get no rest at all!

She sends them abroad on her own affairs,
From the second she opens her eyes-
One million Hows, two million Wheres,
And seven million Whys!

The Business View

Before an architect can begin work the business owner has to specify what sort of building is needed

When a new building is commissioned, the owner has a set of business requirements that must be met by the architecture. At the highest level this is expressed by the descriptive name of the building: it is a domestic house, a factory, an office block, a sports centre, a school, a hospital, a warehouse, a theatre, a shopping centre, an airport terminal, a railway station, or whatever. Each one of these business uses immediately implies an architecture that will be different from all the others, an architecture that will fulfil expectations for the function of the building in business terms.

Five more key questions

Having stated *what* sort of building is needed the owner must then decide some more detail about its use:

- *Why* do you want this building? The goals that you want to achieve.
- *How* will it be used? The detailed functional description.
- *Who* will use the building, including the types of people, their physical mobility, the numbers of them expected, and so on?
- *Where* should it be located, and what is its geographical relationship to other buildings and to the infrastructure (such as roads, railways etc)?
- *When* will it be used? The times of day, week, year, and the pattern of usage over time.

Understanding requirements is a prerequisite to effective design

This type of analysis is essential before any type of design work is done. It is through this process that the requirements of the building are established, and understanding the requirements is a prerequisite to designing a building that will meet those requirements.

We take a similar approach in developing an architecture for a secure information system

When designing a secure business information system, the same applies. There are many possible architectural approaches that one could take, but the one that will be the most suitable will be driven from a clear understanding of the business requirements for the system.

- *What* type of information system is it and for *what* will it be used?
- *Why* will it be used?
- *How* will it be used?
- *Who* will use it?
- *Where* will it be used?
- *When* will it be used?

By asking these questions you establish the business requirements

These are the characteristic questions that you must ask. From the analysis of the replies you receive, you should be able to gain an understanding of the business requirements for the secure system. From those you should be able to synthesise a systems architecture and a security architecture that meets those requirements.

The result is the contextual security architecture

In the SABSA® Model this business view is called the *contextual security architecture*. It is a description of the business context in which your secure systems must be designed, built and operated.

Shortcuts that omit this step are likely to result in failure to meet business needs

Any attempt to define an architecture that takes a shortcut and avoids this essential step is unlikely to be successful. Even so, simple observation reveals that many enterprises undertaking architectural work do not take this stage seriously. It is very common for systems architecture work to begin from a technical perspective, looking at technologies and solutions whilst ignoring the requirements.