Managing Security in Outsourced and Offshored Environments
Managing Security in Outsourced and Offshored Environments

How to safeguard intellectual assets in a virtual business world

David Lacey
## Contents

**Acknowledgements** x  
**Foreword** xi

### 1 Introduction 1
1.1 Purpose 1  
1.2 Audience 1  
1.3 Scope 1  
1.4 Limitations 2  
1.5 Provenance 2  
1.6 Content and structure 3

### 2 Fundamentals of outsourcing 5
2.1 The case for and against outsourcing 5  
2.2 What's special about outsourcing? 8  
2.3 What changes when we outsource? 10  
2.4 The implications for information and security governance 13  
2.5 Key requirements for success 16  
2.6 Learning points from this chapter 19

### 3 Forms of outsourcing and offshoring 20
3.1 What we mean by outsourcing and offshoring 20  
3.2 A global industry 20  
3.3 Wide variation in scope 21  
3.4 Outsourcing options 22  
3.5 Subcontracted services 22  
3.6 Outsourced services 27  
3.7 Offshored services 29  
3.8 Cloud computing services 31  
3.9 Learning points from this chapter 32

Managing Security in Outsourced and Offshored Environments v
4 Business drivers for outsourcing 34
  4.1 How business motives shape security expectations 34
  4.2 Common business motives for outsourcing 35
  4.3 Cost savings 35
  4.4 Headcount reduction 37
  4.5 Moving to a variable cost basis 39
  4.6 Access to a broader skills base 40
  4.7 Managing legacy systems and infrastructure 42
  4.8 Moving data or processes to a new platform 43
  4.9 Building a global support capability 43
  4.10 Achieving global network leadership 44
  4.11 Gaining a quality improvement 45
  4.12 Learning points from this chapter 46

5 Planning and preparation 49
  5.1 Security throughout the outsourcing lifecycle 49
  5.2 Strategic considerations 50
  5.3 Reviewing the scope of the outsourcing 53
  5.4 Classifying information assets 55
  5.5 Conducting a risk assessment 62
  5.6 Reviewing policies and standards 71
  5.7 Learning points from this chapter 86

6 Selecting a supplier 89
  6.1 Key questions to consider 89
  6.2 The selection process 89
  6.3 The importance of due diligence 91
  6.4 Conducting security checks on suppliers 92
  6.5 Independent audits and certificates 94
  6.6 Questions to ask a supplier 95
  6.7 Security selection criteria 97
  6.8 Learning points from this chapter 99
<table>
<thead>
<tr>
<th>7</th>
<th>Developing and negotiating the contract</th>
<th>101</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>The importance of a good contract</td>
<td>101</td>
</tr>
<tr>
<td>7.2</td>
<td>Steps in negotiating the contract</td>
<td>103</td>
</tr>
<tr>
<td>7.3</td>
<td>Negotiating strategy and tactics</td>
<td>105</td>
</tr>
<tr>
<td>7.4</td>
<td>Ensuring confidentiality and privacy of data</td>
<td>108</td>
</tr>
<tr>
<td>7.5</td>
<td>Building flexibility for future change</td>
<td>109</td>
</tr>
<tr>
<td>7.6</td>
<td>Developing the security schedule</td>
<td>111</td>
</tr>
<tr>
<td>7.7</td>
<td>Customer responsibilities</td>
<td>120</td>
</tr>
<tr>
<td>7.8</td>
<td>Avoiding common legal pitfalls</td>
<td>121</td>
</tr>
<tr>
<td>7.9</td>
<td>Learning points from this chapter</td>
<td>124</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8</th>
<th>Implementing the new arrangement</th>
<th>127</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Planning considerations</td>
<td>127</td>
</tr>
<tr>
<td>8.2</td>
<td>Critical success factors for security governance</td>
<td>130</td>
</tr>
<tr>
<td>8.3</td>
<td>The Deming Cycle</td>
<td>131</td>
</tr>
<tr>
<td>8.4</td>
<td>Risk management</td>
<td>133</td>
</tr>
<tr>
<td>8.5</td>
<td>Business continuity</td>
<td>135</td>
</tr>
<tr>
<td>8.6</td>
<td>Audit rights</td>
<td>136</td>
</tr>
<tr>
<td>8.7</td>
<td>Security investigations</td>
<td>138</td>
</tr>
<tr>
<td>8.8</td>
<td>Learning points from this chapter</td>
<td>139</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9</th>
<th>Managing the relationship</th>
<th>142</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Building a successful relationship</td>
<td>142</td>
</tr>
<tr>
<td>9.2</td>
<td>Relationship management</td>
<td>144</td>
</tr>
<tr>
<td>9.3</td>
<td>Managing diversity and different cultures</td>
<td>145</td>
</tr>
<tr>
<td>9.4</td>
<td>Resolving disputes</td>
<td>148</td>
</tr>
<tr>
<td>9.5</td>
<td>Managing incidents across organizational boundaries</td>
<td>152</td>
</tr>
<tr>
<td>9.6</td>
<td>Security improvements</td>
<td>154</td>
</tr>
<tr>
<td>9.7</td>
<td>Learning points from this chapter</td>
<td>155</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10</th>
<th>Review, termination and exit</th>
<th>157</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Planning for a major change</td>
<td>157</td>
</tr>
<tr>
<td>10.2</td>
<td>Exit and termination strategies</td>
<td>159</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>Information security considerations</td>
<td>161</td>
</tr>
<tr>
<td>10.4</td>
<td>Learning points from this chapter</td>
<td>165</td>
</tr>
<tr>
<td>11</td>
<td>Security and risk in cloud computing</td>
<td>167</td>
</tr>
<tr>
<td>11.1</td>
<td>Cloud computing services</td>
<td>167</td>
</tr>
<tr>
<td>11.2</td>
<td>Forms of cloud computing services</td>
<td>168</td>
</tr>
<tr>
<td>11.3</td>
<td>A hierarchy of services</td>
<td>169</td>
</tr>
<tr>
<td>11.4</td>
<td>The importance of architecture</td>
<td>171</td>
</tr>
<tr>
<td>11.5</td>
<td>Benefits and risks</td>
<td>171</td>
</tr>
<tr>
<td>11.6</td>
<td>Security services in the cloud</td>
<td>172</td>
</tr>
<tr>
<td>11.7</td>
<td>Security opportunities presented by cloud technologies</td>
<td>172</td>
</tr>
<tr>
<td>11.8</td>
<td>Models for cloud computing usage</td>
<td>173</td>
</tr>
<tr>
<td>11.9</td>
<td>Risks associated with cloud computing</td>
<td>176</td>
</tr>
<tr>
<td>11.10</td>
<td>Learning points from this chapter</td>
<td>178</td>
</tr>
</tbody>
</table>

### Bibliography

181

### Index

184
David is one of the rare breed of security professionals, possessing an encyclopaedic breadth of knowledge about security while, at the same time, having a depth of understanding that you know has been won from long and hard experience. What really makes David stand out is that he always has an interesting point of view, often with a fresh perspective on the challenges of security, and is clear about what needs to be done. He is also well respected for expressing his views, and can do so in a clear and concise way as a blogger, an author, a presenter, or even as a consultant.

Dr Alastair MacWillson
Global Managing Director, Accenture Technology Consulting

Outsourcing key business services or moving to cloud computing is not without risk but can be managed. David Lacey has drawn upon 20 years’ experience and a significant industry study to write the handbook every manager should read before they sign the contract.

Professor Paul Dorey
Visiting Professor, Royal Holloway, University of London
Acknowledgements

This book could not have been written without the advice and insights of experts and colleagues from many different fields: outsourcing consultants, lawyers, procurement managers, programme directors and information security specialists. I am especially grateful for the advice and contributions of my professional security colleagues, including Jericho Forum luminaries Paul Dorey, Nick Bleech and Andrew Yeomans, who contributed valuable perspectives on outsourcing and cloud computing from a large customer perspective.

I’d also like to thank my expert legal friends Clare Wardle and Dai Davies, who have unparalleled experience in translating business security aspirations into commercial agreements. Further thanks go to Jim Reed and David Craig, my former colleagues at the Royal Mail Group, for teaching me many of the ‘tricks of the trade’ for achieving successful large-scale procurement and outsourcing.

I am grateful also to the UK Government’s Cyber Security Knowledge Transfer Network for allowing me to draw on previous research on this subject, as well as the Jericho Forum for allowing me to include their ideas on the different models of ‘cloud computing’ service delivery and use.

Special mentions also go to Philip Virgo, Secretary General of the Information Society Alliance EURIM, for contributing some gems of wisdom on outsourcing and offshoring, Nick Bleech (again) and Dick Price for reviewing the manuscript, and to Dr Alastair MacWillson of Accenture for contributing an enthusiastic, insightful forward.

Finally, special thanks go to Julia Helmsley of BSI, without whose constant enthusiasm, encouragement and support I could not have completed this book.

David Lacey
Foreword

I have known David for over 15 years now and bump into him from time to time, mostly at security conferences, where he is to be seen absorbing key messages and casting an analytical and sometimes critical eye over the issues of the day, the opinions, and the proffered ‘solutions’ that are often promoted. David is one of the rare breed of security professionals, possessing an encyclopaedic breadth of knowledge about security while, at the same time, having a depth of understanding that you know has been won from long and hard experience. What really makes David stand out is that he always has an interesting point of view, often with a fresh perspective on the challenges of security, and is clear about what needs to be done. He is also well respected for expressing his views, and can do so in a clear and concise way as a blogger, an author, a presenter, or even as a consultant.

It was in that context, at a conference in London, that I met with David last. As we do when we meet, we shared experiences of things we’d seen or done in the security space, hitting on aspects of security that were topical, hot, or even controversial. At that meeting we talked about the security challenges presented by the move to ‘cloud’-based services, and how they differed to those challenges that organizations already have to deal with when they outsource or offshore aspects of their business IT systems and processes. David mentioned to me that he was finishing a book on managing security in outsourced and offshored environments, and asked me if I would be willing to write a foreword for the book. This is my attempt to do the subject, and David, justice.

If you are an IT or security professional, you would have to have been hiding for the past five years not to notice the inexorable move towards outsourcing and offshoring initiatives by most major organizations. While these ideas are certainly not new, until now the alternative sourcing of IT has generally been the preserve of the big corporations and organizations, where the maturity and benefits of such services, in terms of costs, performance and flexibility, are assumed to be understood and proven in practice. They are considered a common rather than an extraordinary feature of IT procurement across the Global 5000.

However, over the past couple of years there has been a noticeable growth of interest in third-party services from a wider variety of business and
organizations, in more and more geographies, and at all scales on the size spectrum. Why is this? There is no doubt that the economic recession has heaped further pressure on most organizations to do more at much lower cost, which is what the third-party IT sourcing model promises to deliver. In many cases, the business models for the use of such services have been proven, and the returns and benefits of cost reduction, flexibility, performance and usability demonstrated. But I think the real fuel powering this change, and the reason some think we have reached a tipping point on third-party services, is technology innovation in areas that enable new business models around the provision of infrastructure, platforms and applications. Innovations such as virtualization, improving open standards, the development of identity management and better cryptography, to name a few, have all come together to make outsourcing, offshoring and, ‘as-a-service’ multi-tenancy models more accessible, more acceptable and more desirable for many.

This brings me to the main theme of the book: ‘how to safeguard intellectual assets in a virtual business world’. While I have described the growing rush towards alternative sourcing of IT services, I haven’t mentioned the risks (old and some new) posed by these new IT models, and the security measures needed to combat them. I’m going to do the sensible thing and leave most of that to David. I would say, however, that the risks and security requirements for such services have usually been thought through, and that there are tried and tested solutions available. But, just looking at press reports of breaches in recent months, I should add that this is not always the case!

What increases the security challenge for many organizations is that they are operating within an increasingly complex and fast-moving business landscape, with growing security threats to worry about, while wrestling with an ever-expanding flood of regulatory compliance demands. New business models and increasingly sophisticated and globally interconnected business processes have outpaced not only regulations designed to ensure security and data protection, but also many organizations’ own ability to effectively secure sensitive data. All this requires management to give much closer attention to managing the risks to sensitive data and protecting key information services than they have in the past. Who said the CISO’s job is easy …

On a closing note to this introduction, I should declare that I am a great advocate of outsourcing, offshoring and the new ‘cloud’-based, ‘as-a-service’ models of service provision, when it makes business sense, where the risks are fully understood or dealt with and when it is done well! However, organizations
considering this direction should collaborate only with business partners that take equal or greater care with data, and rigorously assess partners’ knowledge, practices and experience in managing sensitive data across organizational and national boundaries, and in accordance with local privacy laws and industry regulations. Organizations must be vigilant when it comes to confirming the security posture of the companies with which they do business, especially as business takes them to countries with differing standards for data protection and privacy. Always remember the maxim: choose your business partners with care!

Dr Alastair MacWillson
Global Managing Director Security Practice, Accenture
1 Introduction

1.1 Purpose

Outsourcing and offshoring of IT services and business processes are powerful business improvement practices, which are capable of delivering impressive cost savings and operational benefits. At the same time, they introduce many significant changes to the supply chain. In particular, they bring about a major transformation of business, technology and security risk profiles. With growing concerns about fraud and espionage set against a background of increasing regulatory compliance demands to safeguard personal data, the implications for security and privacy have become one of the most significant issues for any organization planning a major outsourcing or offshoring initiative. There is surprisingly little published guidance, however, on how to go about specifying and managing the security issues associated with outsourcing and offshoring. This book aims to fill that gap by setting out practical advice, methods and best practices for identifying and managing the security risks associated with the outsourcing and offshoring of IT or business services.

1.2 Audience

The contents of this book will naturally be of interest to information security managers involved in outsourcing or offshoring initiatives. But the book is also aimed at a wider audience of general business managers, CIOs, risk managers, auditors, legal advisers, procurement managers, management consultants, as well as university students studying IT, information security or business studies. Even small-to-medium enterprises will find this book of use when considering the benefits of outsourcing or offshoring services. No prior knowledge or qualifications are required to understand the general points and principles of the book, though many of the checklists include some specialist terminology.

1.3 Scope

Safeguarding intellectual assets in a virtual business world is the major theme of the book, but this book is much broader than security. It also contains many lessons for successful IT governance, procurement and operational excellence, as well as for general business risk mitigation. The book is also much more than...
Introduction

just a useful set of security checklists and references, as might be found in a security standard, guideline or code of practice on the subject. In particular, it aims to address not only the numerous security risks and requirements associated with outsourcing, but also the crucial ‘softer’ management issues, such as how to go about managing the inevitable politics, negotiations and relationship issues associated with virtual partnerships. These softer issues are generally the key factors that will ultimately determine the success or failure of an outsourcing programme.

1.4 Limitations

A word of warning: this book is neither a complete security manual, nor a comprehensive commercial guide to outsourcing. There is much more to these extensive subject areas than can be accommodated in a single book of this size. The scope of this book is strictly confined to the security management issues associated with outsourcing and offshoring. As such, it covers a broad range of topics, including relevant security, commercial and human resources issues.

This book aims to provide many useful insights, tips and warnings about legal and procurement considerations and problems. It is anticipated, however, that any organization setting out to outsource business services would be well supported by professional legal and commercial advisers. In practice, most of the routine, detailed contractual aspects of the contract will be comfortably dealt with by the organization’s legal and commercial functions.

The book therefore focuses primarily on the practical and specialist security management issues associated with outsourcing and offshoring. It is not intended to be a detailed, prescriptive handbook on how to go about outsourcing a set of services or processes.

1.5 Provenance

You might be wondering about the reliability and provenance of the advice contained in this book, especially as this is a subject area demanding both security and outsourcing experience, a combination of knowledge that is rare to encounter in practice. In fact, it is based largely on my own experiences as a senior security and technology director, including two decades of practical experience in specifying and managing the security, governance and risk
management requirements for large commercial contracts, including a few in excess of a billion pounds in value.

I have aimed to augment my own personal perspective with advice gathered through interviews and workshops with other experienced practitioners from a variety of fields including IT management, security, risk management, human resources, internal audit, procurement and legal services. The book also builds on an earlier research project carried out on this subject, sponsored by the UK Government Cyber Security Knowledge Transfer Network, to whom I am grateful for their kind permission to include some of the findings of that study.

1.6 Content and structure

The material in this book is designed to be accessible to business, IT and security managers with no specialist technical or security knowledge. The contents are structured in a logical sequence, reflecting the lifecycle of outsourcing: from conception through definition, selection, negotiation, implementation and management until the eventual termination of the outsourced services.

Chapter 2 explains some of the fundamental principles and concepts behind outsourcing.

Chapter 3 explores various types of outsourcing arrangement and the risks they introduce.

Chapter 4 examines the business drivers for outsourcing and their impact on security.

Chapter 5 considers the key areas of planning and preparation required prior to outsourcing.

Chapter 6 examines the security considerations associated with selecting an outsourcing supplier.

Chapter 7 looks at the security issues and requirements for developing and negotiating the outsourcing contract and supporting schedules.

Chapter 8 discusses the considerations and activities involved in implementing a new outsourcing arrangement.
Chapter 9 covers the issues and considerations involved in successfully managing the outsourcing relationship.

Chapter 10 examines the planning considerations and issues concerned with the eventual termination of the contract.

Chapter 11 explores the security issues associated with the adoption of Internet-based ‘cloud computing’ services.

Each chapter also contains a useful summary of key learning points. For the impatient among you, this might be a useful starting point to grasp the salient issues.
2 Fundamentals of outsourcing

2.1 The case for and against outsourcing

2.1.1 The hazards of change

‘Better the devil you know than the devil you don’t’ is an old proverb which means that it’s generally better to deal with someone or something you are familiar with, even if you don’t like them, rather than take a risk with an unknown person or thing which could turn out to be worse. Regardless of the fact that IT managers are not the most popular company staff, it’s clear that contemporary business has consciously decided to ignore this 16th-Century pearl of wisdom.

Outsourcing and offshoring of IT services and business processes are expanding management practices, attracting impressive, double-digit annual growth. Today’s outsourcing industry is mature and competitive. It is an established practice, not just a management fad. Organizations across all sectors are embracing outsourcing and offshoring, despite the fact that many enterprises have found that, in practice, the cost and complexity associated of outsourcing services is not quite as simple as they might have originally anticipated.

Why should outsourcing and offshoring be so popular? Any major change in the sourcing of IT services is bound to be disruptive, involve unpopular decisions and demand a good deal of advance planning, significant up-front expense, and substantial procurement effort, often for little or no visible improvement in the services that are to be delivered. Executive boards often complain of service quality and organizational culture, but achieving a major change is always difficult and often hazardous.

As the Italian philosopher, Machiavelli famously put it:

*It must be considered that there is nothing more difficult to carry out, nor more doubtful of success, nor more dangerous to handle, than to initiate a new order of things. For the reformer has enemies in all those who profit by the old order, and only lukewarm defenders in all those who would profit by the new order, this reticence arising partly from fear of their adversaries, who have the laws in their favour; and partly from the incredulity of mankind, who do not truly believe in anything new until they have had actual*
Fundamentals of outsourcing

experience of it. Thus it arises that on every opportunity for attacking the reformer, his opponents do so with the zeal of partisans, the others only defend him half-heartedly, so that between them he runs great danger.\(^1\)

In the case of outsourcing, the change agent is rarely intimidated by such threats, as this agent is often – though not always – the management team, supported by the executive board and an outside team of advisers. But the hazards remain. Outsourcing is a high-risk initiative, with a mixed track record that includes many examples of expensive failures. Looked at from that perspective, it raises the obvious question of why outsourcing should be such an attractive management practice. In fact, the answer is quite simple. The benefits are simply irresistible.

2.1.2 Irresistible benefits

There are three highly persuasive factors that are guaranteed to compel most managing directors to seek to externalize the source of their supplies and services.

The first persuasive factor is that externalizing any internal service opens up an opportunity for short-term savings and a potential injection of cash through the sale of the associated assets. Such returns are always welcome to hard-pressed business directors. Guaranteed cash today is always more attractive than projected savings tomorrow.

The second factor is that outsourcing transforms a fixed set of costs into a variable on-demand payment. And that is essential for any organization that’s planning to slim down, freeze investment, cut operating costs or reduce headcount, especially when facing a recession. Many directors will commit to a higher rental rate in future years, if it enables immediate cost reductions to meet business targets this financial year.

The third factor is that the outcome of outsourcing is an apparent increase in the revenue generated per individual employee, which is an attractive target for many senior executives. Shareholders and investors pay close attention to such ratios. It’s the type of outcome that chief executive officers like to achieve in order to bolster their personal reputation and market value.

\(^1\) Niccolo Machiavelli, *The Prince* (1532)
Fundamentals of outsourcing

There are, of course, other important business factors that make outsourcing attractive, but they are generally the arguments that are used to justify the action of outsourcing, rather than to compel directors to take it. Typical examples might be the possibility of achieving an injection of new skills, or perhaps establishing a new global support capability. But these goals are the icing on the cake rather than the primary drivers.

2.1.3 The downside of outsourcing

There are also many risks associated with outsourcing, both commercial and security risks, and these are progressively increasing with the growing ambition, complexity and size of modern outsourcing contracts, coupled with the increasing loss of visibility and direct control over day-to-day operations as sources of supply become more remote and anonymous.

A further negative factor is the inevitable commercial reality that a significant profit margin will need to be extracted by the outsourcer in order to justify taking on the task. This is a guaranteed overhead that must be taken into account in any business case for outsourcing, unless the customer believes that they are smart enough to haggle a cost-price deal with an outsourcer, which can be a dangerous tactic from a quality of service perspective.

The simple fact, however, is that despite all the risks, the overheads, the extra effort and the potential longer-term penalties, outsourcing continues to be an attractive option to executive boards. And that is because the benefits mentioned above are more compelling than the risks.

Outsourcing and offshoring are double-edged swords. Managed well, they represent a smart business strategy that delivers major benefits, such as reduced costs, easier scalability of services or access to a broader pool of specialist skills and resources. Managed badly, they become an inflexible, expensive millstone that restricts future innovation and growth. Without adequate planning and prudent management controls, outsourcing and offshoring can introduce unacceptable levels of new risks, such as the possibility of a breach of confidential data or a sustained outage of essential services.

These risks will need to be contained through proactive governance and controls. In fact, the critical success factors for both effective service delivery and prudent security management are the same. Success in both areas requires careful planning and preparation; good understanding and management of risks;
Fundamentals of outsourcing

professional specification of services; prudent negotiation of the contract; close alignment of objectives with the supplier; and continuous, proactive relationship management.

2.2 What’s special about outsourcing?

2.2.1 More than just a division of labour

Outsourcing and offshoring of business services might be contemporary and relatively modern management trends, but there is nothing new about the concept of externalizing the source of supplies and services. The process of contracting out work is a longstanding one. In fact, it’s a natural form of the long-established principle of ‘division of labour’. For centuries, enterprises have elected to farm out selected activities to specialist outside companies or individuals who are able to deliver a better product or service at a lower cost.

What’s different about outsourcing and offshoring programmes, compared to traditional contracting out, is that these initiatives represent a step change in the approach to the transfer of in-house work to an outside agency, generally on a much larger scale and for a much longer period of time. In terms of management complexity and organizational disruption, there is simply no comparison between the employment of an external supplier of raw materials to the outsourcing of a critical business process or a portfolio of computer applications. The procurement process is longer and more complex, the returns and risks are substantially higher, and the consequences are likely to have a significant impact at a higher level in the business value chain.

Outsourcing of IT services is also very different from the externalization of well-understood, ‘commodity’ business services such as accounting or legal services. Each situation is different of course, but a typical portfolio of information systems within a medium or large organization is likely to contain many bespoke elements that will require careful consideration, meticulous specification and supervised migration. In many cases this will demand a substantial in-house planning effort, lasting perhaps one or even two years. Such a programme should not be undertaken lightly, nor without due consideration of the full, longer-term implications and the eventual longer-term exit strategy.

Offshoring introduces the additional risk of a transfer of work to a different country, enabling a potentially greater cost saving, but also presenting a new set of management challenges. In fact, the limited experience of many
organizations in managing such arrangements suggests there is still a good deal of uncertainty about what constitutes best practice in mitigating these risks. A further factor is that what looks like a good deal today might not appear so in future years. Changes in labour costs, exchange rates and regulatory compliance requirements, for example, are continuing to transform the cost–benefit equation as well as the risk profile associated with such initiatives.

2.2.2 A growing management challenge

The size of the challenge is also steadily increasing. For the past two decades, the scope of outsourcing and offshoring programmes has become progressively deeper and more radical, as both service providers and customer organizations are tempted to stretch the boundaries of outsourcing arrangements: from selected individual services to entire business processes; and from local delivery of dedicated services to the global provision of virtual services, shared with many other clients.

Emerging technology is also accelerating the move of business applications from secure servers sited within private data centres, towards Internet-based services operating across a virtual ‘cloud’ of shared, networked infrastructure. These trends are changing the nature of the financial benefits and the operational risks, as well as introducing challenging new security, compliance and business exposures.

The world of outsourcing and offshoring is characterized by a constantly changing landscape. We continue to encounter new terms describing emerging variants or fashions in outsourcing and offshoring: ‘multi-sourcing’ to describe the provision of outside services from a range of different suppliers, or ‘near-shoring’ to suggest the delivery of services from a country nearer to home, or at least nearer in culture. The decision, for example, by German car manufacturer BMW in 2008 to extend its manufacturing operations in North America made many observers think again about the validity of traditional assumptions about the economics of offshoring.

The major implication for security practitioners, either in-house or external, is that they must all raise their game. Senior decision makers need incisive input on the risks and consequences of outsourcing decisions. Outsourcing demands the resolution of complex interrelated problems across multidisciplinary virtual teams. It requires considerable, detailed work to understand the many security issues and to overcome them.
The skills involved in conducting due diligence and management of external relationships demand a broader perspective than that required to perform traditional security reviews and compliance audits, especially when dealing with unfamiliar social or political cultures.

2.3 What changes when we outsource?

2.3.1 Unavoidable changes

Outsourcing and offshoring offer substantial business benefits, but they also introduce a number of new security risks. These risks cannot be avoided and must therefore be accepted or mitigated in some way. The most significant of these risks arise from the following fundamental changes to the services that are outsourced:

- a major loss in visibility of operating practices, risks and events and incidents associated with the delivery of the outsourced services;
- the removal of direct control over the development, operation and maintenance of outsourced services and products;
- a substantial reduction in communication with and access to the staff delivering the services;
- changes in security responsibilities, affecting both customer and outsourcer;
- changes in IT and business governance processes, including compliance, risk management, business continuity and internal and external audit, on both sides of the partnership;
- a shift in loyalties, from the customer to the service provider, for the staff tasked to deliver the services;
- a potential change in the location of services and data, which might have an impact on the legal environment;
- strictly limited access to facilities and staff to perform audits, reviews or security investigations.

Later paragraphs in this chapter examine some of these changes in more detail.

2.3.2 Responsibilities that do not change

Despite the transfer of control of day-to-day service delivery, ultimate responsibility for security, privacy, compliance, and the consequences of risks relating to the outsourced services and information will remain firmly with the
Fundamentals of outsourcing

customer. It is simply not acceptable to leave all decisions on security to the outsourcer. The customer has an obligation to ensure that legal and regulatory compliance requirements will continue to be met from the outset, and that the interests of shareholders, business partners, customers and staff are adequately safeguarded under the new arrangements.

The customer must anticipate and plan for the changes in security responsibilities that will occur when a service is outsourced. Although many responsibilities remain the same, the way they are executed will change considerably. In particular, the customer must identify, specify and oversee many security requirements. In practice, this will require the development and maintenance of a new layer of formal documentation, as well as the design and operation of a new set of management processes.

2.3.3 New loyalties

Responsiveness and eagerness by a contractor to meet short-term commercial requirements should not be confused with a commitment to serve the longer-term interests of the organization. Contractors are servants of business, and might appear keen to go the extra mile, but they will never match the motivation of in-house employees.

It might sound cynical, but it’s worth taking note of Machiavelli’s shrewd observations on outside agencies:

Mercenary and auxiliary forces are useless and dangerous; and if one holds his state based on these arms, he will stand neither firm nor safe; for they are disunited, ambitious, and without discipline, unfaithful, valiant before friends, cowardly before enemies; they have neither the fear of God nor fidelity to men, and destruction is deferred only so long as the attack is; for in peace one is robbed by them, and in war by the enemy. The fact is, they have no other attraction or reason for keeping the field than a trifle of stipend, which is not sufficient to make them willing to die for you. They are ready enough to be your soldiers whilst you do not make war, but if war comes they take themselves off or run from the foe.²

² Mercenary forces are troops hired to fight for a wage. Auxiliary forces are troops borrowed from an ally. Machiavelli believed that auxiliary forces are more dangerous because they are united under their own interests and controlled by capable leaders who may turn against their employers.
Fundamentals of outsourcing

Such a perspective might seem unduly pessimistic perhaps, but it underlines the importance of recognising the fact that loyalties will be markedly different following an outsourcing initiative.

2.3.4 Loss of visibility and communications

Managing security is always more difficult across an external partnership. Visibility and control of threats, vulnerabilities and events lie at the heart of effective security and risk management. If you can’t see what’s happening on the ground, then you can’t really determine what to do, or when and how to intervene. At the same time, the service provider lacks visibility of business developments at the customer end that might shape the nature or significance of a security risk or its impact.

Organizations considering how best to manage business processes that extend across a virtual supply chain should heed the advice of the late W. Edwards Deming, the renowned author and management consultant, who included in his seven deadly sins of management (that plague Western business) the sin of: ‘running a company on visible figures alone’. Customers should never be content to rely solely on the information that is routinely provided by the outsourcer. Prudent managers need to identify the information they will need to manage the partnership, and make appropriate arrangements to obtain it.

Any externalization of services inevitably places greater distance of user management from the staff taking day-to-day operational decisions, and the circumstances surrounding their analysis. Understanding the context of a decision or event is important to fully appreciate its significance. A little knowledge can be a catalyst to jump to a misleading conclusion.

Statistics can easily be misinterpreted when taken out of context. ‘Chinese whispers’ and hearsay are also rife across business partnerships, especially those where there is tension arising from differences in interpretation of requirements or unresolved disputes. Assumptions based on incomplete information should be avoided. Facts need to be gathered and assessed in an objective way, within a defined, well-understood context. New systems will be necessary to enable this.
2.4 The implications for information and security governance

2.4.1 The need for new structures

Given sufficient resources and budget, most risks associated with outsourcing and offshoring can either be prevented or contained at an acceptable level. One overriding risk must, however, be accepted with open eyes: there will be an inevitable, immediate loss of visibility and direct control of activities and events, yet accountability for the impact of security breaches will remain firmly with the customer organization.

Risk profiles are also likely to change considerably over time, with changes in the business, legal and security landscapes. New governance structures must therefore be developed to extend management oversight across the new supply chain. Suppliers must be willing and able to support these new arrangements.

The major challenge is to establish an effective means to ensure that the day-to-day management of security remains in step with the evolving requirements of the business. This requires, among other things, a number of key conditions to be met:

- appropriate confirmation that the service provider remains willing and capable of meeting the customer’s level of security;
- a contract specifying a minimum level of controls that meets the customer’s security requirements;
- a formal process for specifying and agreeing changes in customer security requirements;
- a process for reporting changes in services that might impact the customer;
- a governance process that can operate effectively across the partnership;
- an assurance process to confirm that the service provider is continuing to manage security, as specified and required.

Achieving these goals is not trivial. It demands careful planning and attention to detail in specifying requirements, as well as sound governance of the services actually delivered. If this sounds more like advice on management rather than security, it’s because good security and risk management are primarily achieved through sound management. They are, in fact, two sides of the same coin.
2.4.2 The impact on risk management and business continuity

New processes will need to be established to ensure security and business continuity, to manage security and business risks, and to demonstrate continuing regulatory compliance and data protection requirements. It should never be assumed that the supplier will automatically establish and address the risk profile and compliance requirements of the business customers without the input, demands and agreement of the user organization.

Existing risk management, business continuity and crisis management processes will need to be significantly revised to operate across the supply chain. This will mean, among other things, harmonising standards, structures and procedures for assessing and addressing risks, as well as for identifying, investigating and responding to security incidents.

The overall risk profile, post-outsourcing, might in fact be very different. In particular, there might well be greater scope for data security breaches. But there will certainly be new, longer-term business and security risks, including the impact of becoming locked into a particular supplier or product, which could result in significantly higher charges, new security exposures, reduced options for business continuity plans and a potential loss of business agility.

No organization should proceed with a major outsourcing or offshoring commitment without careful consideration of the full range of associated security risks. The budget for developing and implementing new processes and new business and security controls should be factored into the projected costs of the proposed outsourcing arrangement.

Small companies, in particular, should consider how much they can actually afford to lose from a failed arrangement. In serious cases, such failures might lead to a major loss in cash flow, which could result in bankruptcy. Larger companies might be better equipped to ride out short-term losses, reflecting the fact that what might constitute an acceptable risk for a large organization could well prove to be fatal for a smaller one.

Small and medium-sized enterprises are also less likely to have the experience and skills on hand to identify and assess the wide range of security risks associated with a major change in service provision. Where possible, therefore, smaller companies should seek specialist external information security advice. For a small company, a small up-front cost for consultants or lawyers might be highly unattractive. But it will prove to be an acceptable charge if it helps avoid...
Fundamentals of outsourcing

substantially larger, longer-term penalties or, in the worst case, a damaging incident or situation that results in bankruptcy.

2.4.3 The changing compliance landscape

Outsourcing is generally a long-term arrangement, though there is a current trend towards shorter contracts. Organizations must think beyond today’s security threats and compliance requirements and anticipate what new risks or regulatory requirements might emerge during the lifetime of the arrangement.

We cannot predict the future precisely, but one trend is very clear at present, and that is that security and compliance demands are steadily growing, and the impact of data breaches is becoming increasingly serious. It is sensible, therefore, to anticipate a tighter future security and regulatory regime, and ensure that policies and standards can be extended or raised when required.

One of the major shifts in the business landscape has been the slow but seemingly inevitable rise in the power, scope and demands of regulators and, in particular, the global growth in legal and regulatory requirements to safeguard personal data and notify regulators and customers of data breaches. This trend seems set to continue.

Stewart Room,3 a partner in the law firm Field Fisher Waterhouse, describes this trend of growing compliance expectations as a ‘bear market’, fuelled by a tendency for politicians and regulators to respond to reported data breaches with ever tougher demands.

The characteristics of a bear market are a loss in confidence, a negative sentiment and a growing pessimism about the likelihood of organizations delivering on their commitments. This certainly applies to data security and privacy. It’s no exaggeration to suggest that even regulators have lost confidence in their own ability to prevent major data breaches. When such a situation is reached, there is likely to be a trend towards more disputes and litigation, and a progression from data protection being an implied legal requirement to that of an express requirement.

3 Stewart Room is the author of Butterworth’s Data Security Law & Practice.
Fundamentals of outsourcing

Political interests shape emerging laws and politicians understand that consumer-friendly initiatives are potential vote winners. Strong security governance creates a better impression with citizens and tough legislation is easy to implement at little cost to the government purse. Such considerations might help explain why Governor of California Arnold Schwarzenegger was minded to introduce a data breach notification law in 2003, an idea which has subsequently been adopted and extended, with enthusiasm, by other politicians and regulators across the world.

This trend suggests that user organizations should make tougher security demands over the services delivered by outsourcers than might have previously been accepted in earlier contracts. In the past, many smaller organizations were happy to adopt the terms, conditions and security posture of an outsourcer with few questions asked and little direct consequence. That will not do for the future. Regulators and customers will expect a higher degree of due diligence, strict contractual demands, and a capability to monitor day-to-day operations and events. Otherwise, directors might eventually find themselves vulnerable to steep fines, jail sentences and the prospect of class actions by customers.

2.5 Key requirements for success

2.5.1 The ‘Golden Triangle’

Regardless of the specific security and regulatory requirements, successful management of any outsourcing arrangement will always demand close attention by all parties, both customer and supplier, to three fundamental, underpinning requirements:

1) a good contract that is comprehensive and unambiguous, yet sufficiently flexible to accommodate future change;
2) a healthy relationship that is built on shared incentives, good diplomacy and efficient communications;
3) a sound set of management processes that are fully understood, accepted and adhered to by both parties.

These three key requirements can be thought of as the interconnected points of a ‘Golden Triangle’: a management model that represents both the problem space associated with outsourcing and offshoring, as well as the potential solution space for addressing these risks and issues. Figure 1 illustrates the interaction and relationships between these factors.
2.5.2 Vehicles for achieving success

Figure 1 highlights three important vehicles for the successful security management of any outsourcing or offshoring programme:

1) attention to governance and compliance, especially the alignment and visibility of management processes;
2) good management of change, including the agreed approach to manage legacy gaps between current requirements and the actual delivery of services, as well as a capability to address future changes;
3) extended-enterprise teamwork, including the establishment of governance processes to manage activities and relationships that span organizational boundaries.

In practice, the majority of organizations focus most effort on the challenging task of getting the paperwork right to support the outsourcing arrangement, especially the contract schedules and the specification of the services to be delivered. This is an understandable tendency, sometimes reinforced by the fact that the project team responsible for planning and managing the outsourcing programme might not be tasked with the longer-term implementation and management of the arrangement.
Fundamentals of outsourcing

There are countless cases of organizations that have spent dozens of man-years of effort in defining the requirements for outsourcing, confidently anticipating that these will be translated into action with minimal oversight. But the reality is that few operational staff actually read the fine detail of the contract. The delivery of customer services will be primarily based on the outsourcer’s existing capabilities, shaped by the contract and also by the demands of the client’s governance processes and day-to-day management of relationships.

2.5.3 Getting the balance right

Experience indicates that the real keys to successful service delivery are a good working relationship and a set of well-aligned management processes. But all of the factors mentioned are interdependent. A bad contract, for example, will encourage a bad relationship. And that in turn will reduce the quality of services delivered.

Remedying such a difficult situation requires close attention to the needs and behaviour of the people on both sides of the partnership. It’s easier to mend a broken relationship or design a better governance structure than it is to change a bad contract. And, given time, a good working relationship supported by a good set of management processes can help to overcome the constraints of a bad contract.

Successful service delivery and security both depend ultimately on a sound contract, good cross-organizational teamwork, and a set of interfaces and processes that are practical and acceptable to all players. Clearly, it’s better to get all of these things right from the outset. But it should also be remembered that when things have gone wrong it’s never too late to introduce good working practices into an established partnership.

Every outsourcing or offshoring programme is different. Each situation presents a unique blend of management challenges, regulatory demands and security risks. It’s also a fast-changing and evolving field where traditional assumptions might not always apply to emerging issues. Past experience is not necessarily a reliable basis for smart decision-making. What has been known to work in previous contracts is a good starting point, but no organization should proceed without first establishing the associated risks, the current compliance requirements and the longer-term business implications.
2.6 Learning points from this chapter

This chapter has explored the fundamental principles of outsourcing and offshoring. Key learning points to note can be summarized as follows.

- Outsourcing and offshoring are growing management practices. There are many associated costs and risks, but the benefits to senior management are irresistible. Key benefits include short-term savings, a variable cost basis and a perceived increase in revenue per employee.

- Outsourcing is different from traditional contracting out of business services, because of the greater scale, complexity and organizational disruption. Offshoring introduces additional risks through the change in environment, culture and communications. The economics and risks associated with outsourcing and offshoring are constantly changing, and the level of ambition for organizations to go broader and deeper is progressively growing.

- Security risks result from complexity of management, loss of visibility and control, and an inevitable change in loyalty. They need to be contained through proactive governance and controls. Security needs to be addressed at all stages of the outsourcing lifecycle, but early identification of risks is crucial to the business case and the design of the outsourcing programme. New governance systems will also be required to maintain regulatory compliance and stakeholder assurance.

- Key requirements for success are: a good contract that is comprehensive, unambiguous, but flexible; a healthy relationship built on shared incentives; good relationship management; and sound management processes that are understood and followed by all parties. Important vehicles for success are: attention to the alignment and visibility of management processes; good management of change; and effective virtual team working across the partnership.

- Every outsourcing or offshoring programme is different, presenting a unique set of management challenges, regulatory considerations and security risks. Outsourcing is also a fast-changing field where existing assumptions might not apply to emerging issues. No organization should proceed without first establishing the risks and the longer-term business and compliance implications.