# The Business Case for Information Security

# White Paper

**Version 1.0**

Blueprint™ | tailor-made information security strategies

**Security Classification: Public**

## Background

Creating a compelling business case for information security can be a challenge. It's sometimes difficult to identify or articulate tangible benefits that justify the security expenditure. We all know that security is important, but it's often hard to clearly define the return on investment (ROI). How do you sell 'insurance' to your business when they have happily done without it for the last 10 years?

This paper provides advice about how to develop a robust business case for information security based on defined business benefits. It highlights and clearly explains some of the common benefits of information security.

## What is it and why is it needed?

Many people don't have a clear understanding of information security. On the rare occasions it is mentioned, images of viruses and hackers often spring to mind. Although protecting your brand and valuable customer data against viruses and hackers is important, this is only a small part of what information security is about. It's a good idea to set the scene early in the business case by explaining the broad scope of information security and why it's important to your organisation. This will help overcome the common belief that "information security isn't important for our organisation because we're not a bank and don't have anything a hacker would want".

In general terms, the objective of information security is to protect the confidentiality, integrity and availability of information. But how does this translate into business benefit?

Most business processes are heavily dependent on information. This information is generally stored and processed on complex and sensitive IT systems. Some of these systems may exist within your office or a dedicated server room, while others may be hosted externally. It is vital to protect the accuracy (integrity) and availability of such information so that critical business processes can continue to function effectively and efficiently.

It's also essential to protect the confidentiality of any sensitive information in the organisation. This may include corporate intellectual property, personal information and client data. The old adage of "you are only as strong as your weakest link" holds especially true for confidentiality of data. Consider the amount of confidential information flowing through your business every day - what would the impact be if this were compromised, lost, or sent to a competitor? A data breach can have a dramatic impact on an organisation's reputation, leading to a sharp reduction in sales and directly impacting on the bottom line.

## Compliance and Risk

The initial driver for information security is often related to compliance. Depending on your area of business, compliance with regulations (e.g. PCI DSS), legislation (e.g. the Australian Privacy Act) or client requirements may be a key driver. If your business provides services internationally then you may be subject to many more regional compliance obligations (UK, EU and US requirements can be particularly stringent). Compliance requirements differ between businesses. It's important to identify what's relevant to your business and whether you meet the requirements. The risks of non-compliance (or the risk of not knowing what your compliance requirements are) can then be added to the business case.

Another major driver for information security is reducing the probability and impact of security incidents. Clearly outlining the specific risks to your business is critical to the success of the business case. This requires an understanding of your critical business processes, how sensitive information is stored and processed, and what threats there are to the information. The likelihood of the threats occurring and the possible impacts to your business should then be considered.

It's important that the risks included in the business case are plausible. Avoid using exaggerated risks to obtain buy-in for information security initiatives. People will generally see through the hyperbole (the fear angle has already been over-exploited by the media and product vendors) and the integrity of the business case will be damaged. Instead, focus discussions on rational threats and vulnerabilities that present a real risk to the organisation.

## Positive Business Benefits

Information security is often viewed as just an overhead – a necessary expense that is required to do business in today's environment. It is usually considered a cost centre rather than a business enabler.

Maintaining compliance and reducing risk are certainly important drivers to include in a business case, but they tend to focus attention on costs rather than benefits. They should be tempered with the inclusion of more positive business benefits. "This will help you make money" generally produces a better response than "you need to have it, or else".

So, what are the other benefits of information security? How does it facilitate and support the business?

## Increased sales

Information security is becoming an increasingly important market differentiator and can add value to an organisation's existing services. Many companies are finding that their customers are increasingly asking difficult questions about risk, compliance and information security. Demonstrating effective management of information security can provide a real competitive advantage when responding to tenders and pitching for business, especially if your competitors are still not taking security seriously. It can also help retain existing customers who might otherwise look elsewhere for reassurance that their information will be secure.

In many sectors having a robust information security management system in place is becoming a requirement for doing business. Clients expect it and demand it, and these expectations are only set to increase year on year. What is the opportunity cost of losing client business because of a lack of proven information security practices and controls?

## Quicker response

Many organisations sink a considerable amount of time and resources into responding to client questions, concerns and pro-forma templates about information security. The amount of questions related to information security in RFIs and RFTs has increased dramatically over the last few years and this trend will only continue. A comprehensive information security programme within your business will give you a full suite of policies and procedures which can be leveraged on an ongoing basis to dramatically reduce the time it takes to respond to client requests. Clear and succinct answers can be provided, with reference to documented security policies, instead of spending time crafting lengthy, non-committal responses to hide inadequacies.

## Transparency

Many organisations are unclear about where to focus their security resources. Information security covers a whole spectrum of business areas from IT to operations, and from HR to building security. Ultimately, it impacts on senior management, the Board, and the ongoing success of any company, large or small. There's a tendency to jump in too quickly and get lost in the detail, implementing point source solutions to combat threats as they spring to mind. Unfortunately, it's all too easy to be influenced by hype and the latest buzz words from product vendors and the media.

This lack of clarity has given information security a bad reputation in some organisations. It can appear that there's an endless stream of money being spent on 'essential' technical security products with little tangible return.

There is an opportunity to improve this situation by developing a clear picture of information risk across the organisation. Stepping back, looking at the big picture and assessing where the biggest risks are allows resources to be allocated much more efficiently. Getting more bang for your buck is a powerful business case. Efficient management of security, based on a clear understanding of an organisation's risks and requirements, can also help to reduce existing overheads.

Implementing a simple risk management system can help demystify the confusing world of information security and introduce transparency and accountability. Increased visibility can also help to justify future security budgets. A risk assessment is a good place to start to gain a full understanding of exactly where the information security gaps in your business are and what is required to close those gaps. Increased transparency – and the action plan which is developed after understanding the risks – will help demonstrate to your internal and external stakeholders, as well as your customers, how strong your commitment to information security really is.

## Efficiency

Greater visibility of information security requirements and the controls currently in place can uncover opportunities to streamline business processes. For example, implementing the appropriate level of security early in the procurement and development cycle of a new business information system can reduce overall costs considerably. Likewise, keeping an inventory of assets and software licensing can both increase your understanding of the total cost of ownership (TCO) of your assets, and ensure you're getting the best value for money. Greater visibility may also allow an organisation to reduce the overheads of duplicated and other unnecessary processes or security controls.

Furthermore, through a centralised information security management system and accompanying documented policies, finding the most appropriate and secure method of performing a task becomes a repeatable, sustainable activity, rather than a case of guesswork or searching the internet.

## Resilience

Can you answer the question, "how long can I live without my website for?" or "what would we do if all our emails went down", or "if there was an outbreak of flu, how many staff can I afford to be without before the business loses money"? Availability is a core objective of information security. During the implementation of an information security management system, the availability requirements of critical information and business processes are assessed and controls are implemented to ensure that those requirements are met. This may involve changing backup regimes, improving disaster recovery capabilities and developing a business continuity plan. Comprehensive business continuity and disaster recovery plans provide the business with confidence that critical business activities can continue operating, or can be recovered quickly with minimum impact if disaster strikes.

## Assurance

A well-managed information security function provides your organisation with the confidence to move into markets that previously may have been considered too risky. For example, an organisation that understands the resilience of its existing business processes, and can effectively assess the risks of new ventures, will be better placed to develop online services that process sensitive information. This assurance can allow an organisation to be the first to market with a service that its competitors simply cannot provide because of a lack of confidence in their systems and processes.

## Conclusion

The business benefits of information security are broad and varied. They can be summarised as:

- compliance - addressing legal and regulatory requirements
- decreased costs over time – reducing the probability and impact of incidents which may have a detrimental impact on your business and its bottom line
- increased client sales - meeting and exceeding client requirements and using security as a market differentiator
- time savings - reducing time spent responding to client questions and tenders
- transparency - knowing what to protect and why
- efficiency - streamlining business processes and security controls
- resilience - ensuring continuity of critical business processes
- assurance - ability to scale into new ventures and grow your business with confidence

We can help you to develop a solid business case by providing expert advice on compliance requirements, risk management, information security management systems, and business continuity. Call us to find out more on 1300 977 774 or email info@blueprintis.com.au.

Share this whitepaper:

facebook LinkedIn Twitter