Security Strategy Toolkit

Perpetuity Research Team

June 2009

CONFIDENTIAL

Perpetuity Research & Consultancy International (PRCI) Ltd
148 Upper New Walk · Leicester · LE1 7QA · United Kingdom
www.perpetuityresearch.com
prci@perpetuitygroup.com
Tel: +44 (0)116 222 5555
Fax: +44 (0)116 222 5557

Copyright

This toolkit is the result of the Security Research Initiative (see http://www.perpetuityresearch.com/sri.html), supported by the British Security Industry Association, The Security Institute and ASIS International

Index

The index below provides a summary of all pages within the toolkit. You can skip to the sections of interest by clicking on the links below. You can also return to this page at any time by clicking the 'index' link at the top of each page.

Section 1. Toolkit Introduction

Research has found that very few companies have a full security strategy in place and where they do, it is rarely seen as 'fit for purpose'.

Recent work by Perpetuity found that only one-third of organisations had a security strategy that had been approved by the Board. Many did not have specific objectives to guide the work of the security function within the organisation and less than a third had a security strategy with measurable deliverables linked directly to organisational objectives. Furthermore according to security providers, nearly two-thirds estimated that fewer than 15 per cent of their clients had a security strategy in place. In addition where security strategies did exist most were not deemed to be fit for purpose.

It seems clear that there are many organisations without a security strategy to guide their development. Whilst the majority of organisations seemingly do not have a security strategy, many directors recognise that they should.

Why is a security strategy so important?

Without a security strategy it will often not be clear how the security function contributes to the overall aims of the organisation. Unsurprisingly then security can be marginalised, or at least it does not fulfil its potential to generate competitive advantage. A good security strategy helps an organisation to have good security management and indeed good corporate governance of the organisation. A security strategy linked directly to the wider strategy for the host organisation provides direction, and also a reference point to establish priorities and guide action. This is as important for security personnel as it is for others in the organisation who are provided, via the strategy, with insights into why security is important and how it adds value. So developing a good strategy and learning how best to implement it is crucial to successful security and good business.

> *"If you don't have a strategy you end up being highly responsive to events."*
>
> *"If you want to make sense of the world, set a direction, manage your resources effectively and understand and evaluate your work better, you need to have a strategy in the first place."*

Security leaders need to have at least a basic understanding of strategic planning, including its development and implementation. Strategic planning is a fundamental element of successful companies and is a crucial part of managing delivery.

The benefits of having a security strategy

Having a good security strategy in place can provide you, your security department and the organisation with a range of (overlapping) benefits. A security strategy can:

- Provide stakeholders, including the board, shareholders, staff and partners with a clear understanding of what your security function is trying to achieve and how.
- Facilitate contact with the board and encourage board support for security programmes.
- Help in aligning the security function with the business priorities to achieve competitive advantage.
- Improve the corporate resilience and sustainability.
- Enable all staff, and not least managers of other functions to better understand why security is important and how it can add value.
- Provide a means of engaging with staff and managers in the aims and purpose of the security function.
- Offer a framework to guide the direction and focus of your security function, and help you to allocate resources to priorities and targets more effectively.
- Help you to be proactive in your response to security anticipating security issues from emerging external threats or changes in the corporate strategy.
- Help to embed security within systems, procedures and processes.
- Inform budget development.
- Provide you with measures from which to review the performance of your security function. (See Performance monitoring.)

> *"A security strategy gives a greater awareness of the challenges you are facing, a shared platform that colleagues and other departments or divisions can discuss relevant topics. A base from which you can develop resource allocation processes, a method of evaluating your successes and failures."*
>
> *"A security strategy is a useful communication tool between the security department and the rest of the organisation. It allows them to see what it is your doing, when and it's easier to get other organisations involved in what you are doing."*
>
> *"It helps me when I'm trying to put forward a case to line management. It helps to inform them about what I am thinking, and justify the reasons why."*
>
> *"A security strategy can act as a guide to action, to show the company you are adding value, to bring people on board to the security message."*
>
> *"A sound security strategy impacts positively and directly upon the standing of the security function and its leadership. It embeds security within the core heartbeats of the company and dispels once and for all that the function is merely a cost centre and drain on profits."*

- Enable you to gain a detailed understanding of the environment in which your organisation operates and greater awareness of the challenges and risks you face.
- Demonstrate to staff that the organisation takes security seriously. It can be a useful tool for communicating to employees to make them aware of potential security threats and associated business risks and obtain buy in for the security function. (See Communicating strategy.)
- Help to reduce ambiguity, provide clear management direction and commitment, and to establish agreed roles and responsibilities with regards to security.
- Document the value security adds to an organisation.
- Aid the development of a well-designed security management approach and thereby help to mitigate your organisation's legal and actual level of exposure to a range of security threats. In turn this can help to protect your organisation's profit, reputation, brand, assets, customers, suppliers and employees.

1.1 Introduction to security strategy

This toolkit will walk you through developing your own security strategy by providing case study examples, tools and templates. It will provide good practice advice based on interviews with security directors, other managers with experience of implementing strategy, and academic strategy experts. These have been supplemented with a review of a range of books, articles and documents that offer guides to good practice.

What has become apparent, and this needs emphasising up front, is that there are many different ways of devising and presenting strategy. What we have not tried to do is decide for you ‘what is best’, that would be difficult anyway because organisations have different needs. Instead we have tried to distil the important features that can help to provide a guide to determine what is appropriate for you. We have, where possible directed you to sources of further information.

It is important to remember why the security strategy is essential; it ties the function more tightly into the overall objectives of organisations as well as contributing profits and/or cost savings. For this reason we have provided a toolkit that is applicable to different aspects of security, including:

- The security of people
- Physical security
- Information security
- Intellectual property
- Fraud protection
- Brand protection
- Business continuity
- Crisis Management
- Corporate Governance

At some point during the development of your strategy you will need to decide which areas will be covered, the deciding factor is likely to be who owns the strategy and what their areas of responsibility are. Whilst it may be beneficial to discuss all of the different security strands in one security strategy - in order to ensure consistency and coherence - in some organisations this may not be possible due to structure, budgets and/or culture. It is important to document within the strategy which areas it covers in order to ensure that its scope is clear to all readers.

The strategy typically assumes a basic level of knowledge of security and as such would rarely discuss how to carry out a risk audit for example. This is

In this section:	Toolkit Introduction	1.1 Introduction to Security Strategy
		1.2 Preparedness
		1.3 How long will it take?
		1.4 An Introduction to Strategy
		1.5 The Key Strategic Steps

widely documented elsewhere and the toolkit directs readers to sources of guidance and advice.

1.2 Preparedness

Are you ready for a security strategy?

Before you start to develop a security strategy it is worth assessing how prepared the organisation is to receive it. One way to think about this is in terms of 'security preparedness', put simply, organisations can fall on a continuum from being unprepared to accept a security strategy to very prepared. It may be helpful to characterise these extremes.

Unprepared: Those organisations that are unprepared might not understand the potential impact of security threats, or they may view them as something that happen to the organisation, not something that can or need to be managed. In these organisations it is likely to be a challenge to drive through a security strategy, more groundwork may be needed in order to make the organisation more aware of how security issues impact upon the organisation and how they can be prevented or managed. Where this is the case you will need to draw together information to demonstrate the value that good security will bring to the organisation (see Demonstrating value).

Very prepared: Organisations that are very prepared to accept a security strategy are likely to recognise that security impacts upon the success of the organisation and therefore recognise the need to manage its impact. They are likely to have a security management system in place including security policies and procedures. In these organisations it may be easier to introduce a security strategy.

There are likely to be a number of factors which will positively influence how prepared an organisation is to accept a security strategy and these will include:

- a recent security crisis, for example a terrorist attack;
- a concern about reputational damage;
- a compliance/regulatory requirement;
- or a dedicated individual keen to raise the status/perception of security within an organisation.

1.3 How long will it take?

> *"Developing a strategy and implementing it is at the very least a 12 month initiative. Although it depends on the organisation, some might move faster."*
>
> *"It would take about a year to get a strategy developed and implemented, it depends on the size of the organisation, it could take three months."*
>
> *"It has taken two years to get it right from the development plan to the finalisation of the strategy in a local government. The culture of the organisation plays a major role and the energy of the executive management team and the managing director or chief executive officer. That's one of the major elements that should be taken into consideration. Without that energy nothing will really happen. They need to drive it and ask the right questions and put the energy into it."*

It is important to be realistic about the time it will take to develop and implement strategy, if done properly it will not happen overnight. This section will give you some indication of how long you can expect it to take so that you can plan accordingly. It is useful to think of the process in separate chunks, the development of the strategy is the first stage and is followed by its implementation.

Strategy development is a lengthy process and drafting your strategy will take time. (See Key issues in strategy development) For some it may take as little as three months, for others it may take up to a year or longer; the length of time it takes will depend on a range of different factors. Much depends on where you are in the process; if, for example, you already have some of the data required for the strategic analysis easily available, it may be a much quicker process. On a similar note, those organisations with meaningful corporate objectives are likely to find it easier to develop the security strategy.

Furthermore, the time it takes to develop a strategy will vary according to the organisation's size and culture. (See Understanding organisational culture) For example, some organisations may be slow moving and bureaucratic, in which case developing strategy and achieving sign-off from the board might take longer, in other fast moving cultures it may take just a few months. Moreover the level of buy-in from the top is also likely to make a difference.

1.4 An introduction to strategy

What is strategy?

The word strategy is used in a range of different ways and as a result, for many, its meaning has become confused. Some use the word ‘strategy’ interchangeably with ‘policy’, while others see these as completely different. A good way to define strategy is ‘the long term direction’.

Some argue that strategic decisions are those that are fundamental to the future of the organisation, for example they are decisions about:

- how the organisation can achieve competitive advantage;
- the organisation’s scope, for example its products;
- matching activities to the environment, for example to take advantage of new opportunities.

Strategy can develop in a number of ways; this toolkit will walk readers through the formal planning process of strategic development and implementation. This is a commonly recognised way of developing strategy and the way that all of the interviewees and experts that we spoke to advocated; however it might not suit all organisations. If you are interested in developing a strategy but do not think that the formal planning process is the right way for your organisation you can find out more about the other ways in ‘Exploring Corporate Strategy’, (2008) 8th edition, Johnson, G., Scholes, K. and Whittington, R. Prentice Hall: London. ISBN 978-0-273-71192-6

The different levels of strategy

Within text books, strategy is generally recognised to exist at a number of levels:

- Corporate strategy is the overall purpose of the whole organisation.
- Business strategy relates to an individual business unit strategy, for example a subsidiary company.
- Operational strategy, or sometimes known as a functional strategy, is how parts of the organisation, such as specific departments, will deliver the corporate strategy.
- A security strategy is the latter, an operational or functional strategy.

Strategy versus policy and plans

The terms strategy, policy and plan are often used interchangeably and therefore it is important to clarify their meaning up front. Most text books agree that:

- A strategy documents the long-term direction.

- A policy is an organisation's standpoint on a subject documenting how it will operate and respond.
- A plan documents the actions required to meet a desired outcome or end point.

Why is strategy important?

Strategy enables an organisation to ensure that it is aligned with environmental influences and changes. It also has a key role in motivating, communicating and coordinating staff towards future success:

- Strategy can be used to communicate aims and objectives throughout the organisation creating consensus and understanding;
- Strategy can be used to motivate staff towards meeting key aims and ambitious goals;
- Strategy has a co-ordinating role ensuring that all staff understand their roles and responsibilities.

1.5 The key strategic steps

The process of developing and implementing strategy is generally agreed as consisting of four main steps. The steps that we suggest here are based on a review of the literature and interviews with experts in the field. This toolkit walks you through each step.

Step 1: Strategic Analysis (Click here to go straight to Step 1: Strategic Analysis)

The first step in developing strategy is analysis. You need to carry out an analysis of the organisation and the environment that it is operating in to be able to make informed decisions. There are 5 main areas that you need to analyse before starting to write your security strategy. You need a good understanding of:

1. The organisation; its values, vision, mission and objectives (see Understanding the organisation)
2. The organisation's strengths and weaknesses (see SWOT)
3. The opportunities and threats (see SWOT)
4. The resources (including the assets, systems and facilities) and competencies of the organisation (see Risk Assessments and Security audit)
5. The security risk/threats (see Risk Assessments, Security audit and PESTEL)

Some of the information will need to be gathered through consultation with stakeholders (see Understanding the organisation); such as the board, the senior executives, partners and staff. Good consultation at this stage can help to encourage buy-in once the strategy is drafted (see Obtaining board approval). This toolkit provides guidance on each stage and also suggests a range of tools that can help you to do this.

Step 2: Developing your strategy (Click here to go straight to Step 2: Strategy Development)

Once you have a good understanding of the organisation and the environment that it is operating in the next step is to decide how to respond. The analysis will provide you with an understanding of what is important to the organisation and where it wants to be in the future. This can help you to decide how the security function can best align itself to the organisation, and what actions need to be taken, to help the organisation meet its objectives. This should be documented in your vision and strategic mission (see Mission & Vision). You may need to generate and consider a number of options for the future before deciding on which is the most appropriate.

Once you have decided where you are heading you can devise your strategic objectives (see Objectives) which will take you there. Ideally, your objectives should include performance targets (see Performance monitoring) (ideally financial, percentage improvement or milestones) and state how they will be measured. You will then need to decide the steps required to meet your objectives and those responsible.

Throughout the whole process you will ideally need to continue to engage with the board or the senior management of your organisation (see Obtaining board approval), in order to ensure its support. Once the strategy is complete it should be endorsed at board level.

To summarise the key stages in this part are:

1. Defining the vision and strategic mission (see Mission & Vision)
2. Setting strategic objectives and performance targets (see Objectives and Performance monitoring)
3. Formulating a strategy to achieve the objectives
4. Obtaining board approval (see Obtaining board approval)

The VMOST tool (see VMOST tool) provides a useful framework to follow. Indeed there are a range of tools (see list of Tools) that can support strategic development which have been included in the toolkit.

Step 3: Implementing your strategy (Click here to go straight to Step 3: Strategy Implementation)

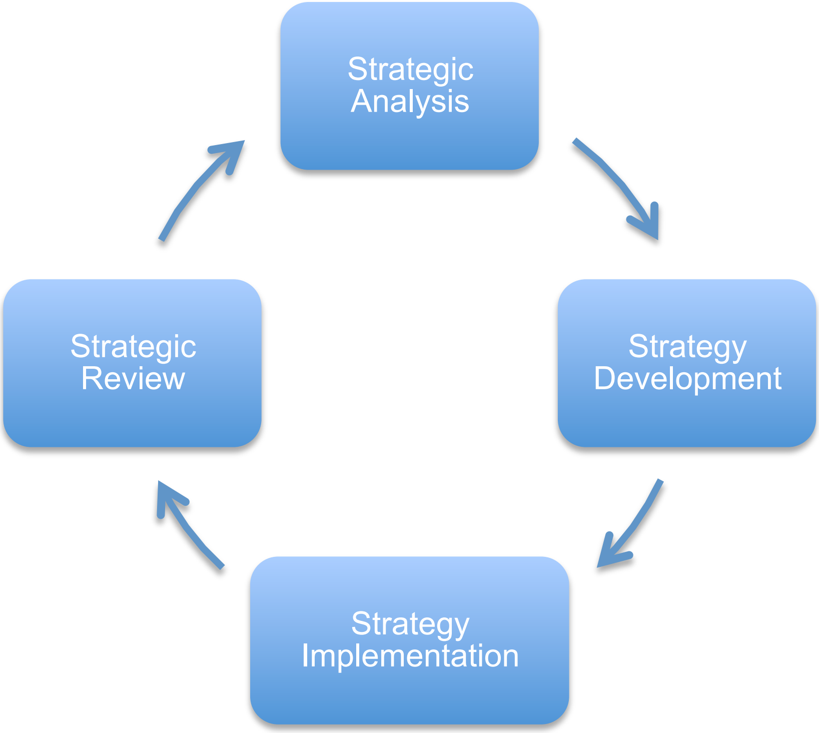
The next step is to implement your strategy. You will need to devise an implementation plan (sometimes known as a business or project plan) (see Implementation plan) which will document the various actions required to meet the objectives. This will also record the owners of objectives/actions and timescales for implementation. There may need to be a reallocation of resources in order to implement the strategy.

Implementing strategy is equally dependent on good communication (see Communicating strategy). For a strategy to be effective it needs to be well-communicated to staff and stakeholders.

Step 4: Reviewing your strategy (Click here to go straight to Step 4: Strategic Review)

To ensure that the strategy is working it is important to carry out regular performance monitoring (see Performance monitoring). This will determine whether progress is being made against the action plan and whether objectives are being met.

As well as regular performance monitoring it is important to review the strategy document regularly (see Strategic review), at least annually to ensure that the assumptions on which it is based, and the objectives and mission, are still relevant and appropriate. This review will determine when the strategy needs updating or re-writing. In some cases it may be necessary to re-write the strategy before its end date, due to changes in the economic environment for example.



Section 2. Step 1: Strategic Analysis

The first step in developing strategy is analysis. You need to carry out an analysis of the organisation and the environment that it is operating in to be able to make informed decisions. There are 5 main areas that you need to analyse before starting to write your security strategy. You need a good understanding of:

1. The organisation; its values, vision, mission and objectives (see Understanding the organisation)
2. The organisation's strengths and weaknesses (see SWOT)
3. The opportunities and threats (see SWOT)
4. The resources (including the assets, systems and facilities) and competencies of the organisation (see Risk Assessments and Security audit)
5. The security risk/threats (see Risk Assessments, Security audit and PESTEL)

Some of the information will need to be gathered through consultation with stakeholders (see Understanding the organisation); such as the board, the senior executives, partners and staff. Good consultation at this stage can help to encourage buy-in once the strategy is drafted (see Obtaining board approval). This toolkit provides guidance on each stage and also suggests a range of tools that can help you to do this.

2.1 Security Policy Statement

The terms strategy, policy statement and plan are often used interchangeably and therefore before we start to think about policies, it is useful to separate them from strategy and plans. These are the generally accepted meanings:

- A strategy documents the long term direction.
- A policy statement is an organisation's standpoint on a subject documenting how they will operate and respond.
- A plan documents the actions required to meet a desired outcome or end point.

Many companies underpin their security strategy with a security policy statement. Indeed it is a good idea to have a security policy statement in place before writing your security strategy. A security policy statement can be a useful step towards encouraging high level support to developing a security strategy. Indeed some of the strategies that we reviewed included their policy statement as the opening section to their security strategy, this helps to indicate commitment to the strategy from the organisation. This section will explain what a security policy statement is and why it is important.

What is a security policy statement?

Often the terms “policy” and “strategy” are used interchangeably, however they are very different. A strategy is typically referred to as the long term direction of an organisation and how it will get there. It generally involves some kind of change within the organisation in order to get to a desired end point.

A security policy statement is the basis for building and maintaining security. The security policy statement is the first step in the process by which management’s expectations for security are translated into specific, measurable, and verifiable goals. In the absence of a security policy statement specifying and communicating these expectations, staff will make their own policy statement.

Policies are static; they guide and regulate business as usual stating the desired conduct of people and activities of the organisation. A policy statement states the organisation’s stand on a subject and how it will operate and respond. Unlike a strategy, the policy statement should not change greatly as long as the core business remains consistent, but it can evolve. Assuming legislation does not change, a policy statement might stay the same for five or ten years.

A security policy statement will detail how the organisation views security and the roles and responsibilities of different groups. For example it might state that the board of directors hold responsibility for ensuring that the workplace is secure, however there may be a section stating employees’ responsibilities such as carrying personal identification cards at all times in the building and reporting incidents.

Some organisations may have more than one security policy, for example they may have an overriding security policy statement supported by an incident report policy. An example of this can be seen in the Cabinet Office which has an Overarching Security Policy Statement and 5 core security principles supported by seven security policies http://www.cabinetoffice.gov.uk/spf.aspx

More examples of security policies can be seen here:

- http://www.cabinetoffice.gov.uk/spf/sp5_ps.aspx
- http://www.wlv.ac.uk/PDF/its_info_security_policy.pdf
- http://www.brookes.ac.uk/infosec/isp.html

- http://www.ccrg.ox.ac.uk/datasets/policystatement.htm

The security policy statement should be communicated to all staff in writing and referred to in staff induction and security manuals.

A security policy statement provides the following benefits, it:

- Reduces ambiguity;
- Provides clear management direction and commitment; and
- Establishes agreed roles and responsibilities.

2.2 What information should a security policy statement include?

A security policy statement should include:

- The scope of the policy statement for example, information security, asset protection, etc.
- A statement of management intent regarding security within the organisation
- The organisation's legal and regulatory obligations
- The roles and responsibilities of staff relating to security
- An explanation of any related documents, such as related policies like IT security or workplace violence policies, or principles, standards and compliance requirements
- What action will be taken in the event of a breach of the policy statement

The policy statement should be endorsed at the highest level, for example, by the Managing Director, Chief Executive or board level. For examples of security policies go to:

- http://www.cabinetoffice.gov.uk/spf/sp5_ps.aspx
- http://www.wlv.ac.uk/PDF/its_info_security_policy.pdf
- http://www.brookes.ac.uk/infosec/isp.html
- http://www.ccrg.ox.ac.uk/datasets/policystatement.htm

There is a lot of guidance available on the internet on what to include in IT security policies, for example http://www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1075423299

In this section:	Step 1: Strategic Analysis	2.1 Security Policy Statement
		2.2 What Information Should a Security Policy Statement Include?
		2.3 Understanding the Organisation
		2.4 Risk Assessments
		2.5 Security Audit
		2.6 Legal and Regulatory Issues

2.3 Understanding the organisation

In order to understand the organisation the first step is to fully familiarise yourself with its corporate or business strategy, this should state its values, vision, mission and objectives. This will inform you where the organisation is headed and therefore will help you to decide what the security function will need to look like to help the organisation to reach that destination. This information will also inform your security audit (see Security audit) and risk assessment (see Risk assessments).

If your organisation does not have a corporate or business strategy then you may be able to obtain the mission statement and values from other documents, such as a constitution, an annual report or other publicity material. Your Human Resources department may be able to help you. If your organisation does not have any of these you will need to rely on a stakeholder analysis.

It is also a good idea to review the departmental strategies or plans that may exist within the organisation such as the marketing or finance strategies as these may well inform your strategy development. It is important to remember that different parts of the organisation may relate to it in different ways and these may create security issues that you need to consider.

Stakeholder Analysis

In addition to reviewing the organisations' strategy it is important to consult with key staff to understand how the security function fits in with the business objectives and their own functions in the organisation. Indeed in order to ensure that the security strategy truly meets the organisation's requirements you will also need to have an awareness of the organisation's strengths, weaknesses, opportunities and threats (see SWOT). These can be identified through consultation with staff.

Clearly who you should consult will depend on the organisation; you will need to consider who your strategy is likely to impact. However it is important to recognise that security touches upon all aspects of an organisation; therefore it is usually a good idea to meet with:

- The Chief Executive Officer
- The Finance Director
- Heads of business units
- Heads of departments
- Security managers
- The members of the board with responsibility for security, compliance and related portfolios

In this section:	Step 1: Strategic Analysis	2.1 Security Policy Statement
		2.2 What Information Should a Security Policy Statement Include?
		2.3 Understanding the Organisation
		2.4 Risk Assessments
		2.5 Security Audit
		2.6 Legal and Regulatory Issues

One security director said, *"I start with the senior level, and then work down from there"*.

The list above merely provides examples, you will need to determine who has a good understanding of the organisation's strengths, weaknesses, opportunities and threats, as well as where the organisation is going. Depending on who you are consulting with and the ways in which your organisation typically does business you may prefer to carry out one to one interviews, and/or run workshops to discuss the issues. Workshops can facilitate the exchange of ideas and promote productive working relationships between people. You could start with a SWOT analysis or a PESTEL to help to guide the discussion and gather the information (see SWOT and PESTEL).

The review of documentation and stakeholder analysis will need to identify the following information for both the organisation as a whole and for individual departments or business units:

> *"I think a key part is stakeholders understanding of what they need. This is crucial, do not assume anything. Security needs to happen in the business so stakeholders are crucial but you really need to tease out what their security needs are."*
>
> *"It's essential to include others."*
>
> *"Get their understanding of how they see security; they see things the security department don't see. Each department has a role to play."*
>
> *"It is very important to know other business functions; security touches every work function every day."*

- Mission(s) and Vision(s)
- Values
- Objectives
- Plans for the future
- Strengths
- Weaknesses
- Opportunities
- Threats
- Views of the security function
- The effectiveness of security measures in place
- Compliance

Examples of the kinds of questions you might want to ask are listed below, remember to select your questions carefully according to the information you collected in the review of key documents and who you are speaking to. You will need to think about phrasing the questions in a way that is appropriate for the person you are addressing, in some cases it may be a clarification or verification exercise.

Understanding the Organisation

- Where do you see the organisation or department in five years time?
- What is critical for the organisation to deliver its key objectives?
- What are the organisation's/department's key objectives?
- Do you intend to enter into new markets in the next five years? If so where, what, when and how?
- What are the organisation's/department's strengths and weaknesses?
- What are the organisation's/department's opportunities and threats?

Security Specific

- What is your perception of the current internal and external security threats?
- What are your current key security risks?
- Does the security function address them?
- Do the current security measures address the risks that you perceive?
- How confident are you that you can comply with the measures in place?
- How well do you think the risks we articulate meet the risks you perceive?
- What's your perception of the future internal and external security threats?
- Does the existing security function address them?
- How could they be addressed?

Some stakeholders will need guiding through what their security risks are. One security director noted that rather than ask about security, he would enquire about their priorities and what would stop them from achieving them. He found that it was easier to engage them and would help them to come up with security-related threats that they might not have thought about if asked directly. It can also help to be away from the work environment as some of the Security Directors we spoke to found that this helped people to open up. Carrying out the consultation over lunch or on an awayday can be effective.

The point of this is to encourage stakeholders to think and communicate what they like or don't like about security and what they need. You might also want to consider consulting with staff, for example through a staff survey, to explore opinions of the security service.

External Stakeholders

Your stakeholder analysis should also explore the requirements of external stakeholders such as:

- Partner agencies
- Key clients
- Key contractors

Again the first place to begin is to understand their strategy, if available. This can be supplemented or replaced by consultation with stakeholders to explore their future intentions and requirements.

Environmental Scanning

This process involves identifying changes in the environment which may impact upon your strategy. It will identify changes in the business and externally, for example new legislation or the release of a new product by your organisation. A PESTEL is a good tool and structure which can help you to identify aspects in the environment that might affect your strategy (see PESTEL).

Continuous Process

The process of drafting your strategy may take some time and things may change that will impact upon your strategy. Therefore it is important to remember to continue to scan the environment and the organisation throughout the process of its development, and thereafter. The last thing you want is to draft a strategy based on one corporate strategy and then find out that it has been replaced. Indeed in the ideal world and with the right resources this process should be continuous, some security functions employ a member of staff to scan the environment for any changes which may impact the security strategy.

2.4 Risk assessments

Before drafting a security strategy it is vital to know what the security risks facing the organisation are. As such the strategic analysis will need to include a security risk assessment. The techniques for conducting a security risk assessment have been described in a range of different texts, and therefore will not be covered in detail here. If you need more information on how to carry out a security risk assessment the following may be helpful:

- Broder J.F. (1999) Risk Analysis and the Security Survey, New York, Butterworth-Heinemann
- Roper C.A. (1999) Risk Management for Security Professionals, New York Butterworth-Heinemann
- Burns-Howell, T. Cordier, P. and Eriksson, T. (2003) Security Risk Assessment and Control, Leicester: Perpetuity Press
- http://www.airmic.com

Perpetuity Training run courses on how to carry out security risk assessments for more information go to:

http://www.perpetuitytraining.com/securitysurveys.html

Optimal Risk can also provide support to carry out a security risk assessment, for more information go to:

http://www.optimalrisk.com/Home/Risk-and-Security-Consultancy/Threat-and-Risk-Assessments.aspx

The security risk assessment will identify the risks to the organisation that need to be addressed; this must consider the opportunities and threats to:

- The department
- The organisation
- The environment

The next step is to decide how to respond to the risks. Responses to security risks may be considered in one of five ways. Firstly, the risk may be accepted and insured where possible. To view and treat a security risk in this way, the organisation must be able to legitimately bear these losses. Examples could include accepting a level of cash or stock losses as a consequence of doing business such is sometimes the case in retailing. This will not be appropriate where an organisation has a zero tolerance stance.

Most organisations would probably seek to manage their security risks. Usually this would be undertaken within certain risk tolerances by establishing control procedures to reduce these risks to acceptable levels and monitoring them. A further way an organisation may respond to risk is to modify the risk. This would normally involve changing the way in which an organisation carries out its business with a view to reducing the risk. This may include for example, contracting out security services to professional security companies.

Sometimes an organisation may find that certain risks are so unacceptable that the organisation does not want to, or believes it cannot manage them. In these instances, they may choose to eliminate the risk or manage it down to an acceptable level, such as withdrawing from certain services so that the risk is removed.

Finally, in some instances it may not be possible to adequately reduce or avoid the risk, for example in emergency and catastrophic situations. Therefore, where such events are recognised as a risk, such as a terrorist attack, business continuity (see Business continuity) and disaster recovery plans need to be drawn up to address the situation and ensure that business disruption is minimal and the recovery situation is resumed as soon as possible. The National Risk Register sets out an assessment of the likelihood and potential impact of a range of different risks that may affect the UK which will help to assess the likelihood of a disaster or other serious incident and its impact on your organisation. For more information follow the link to: http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx.

The risk assessment also needs to consider the security implications of the corporate, business or operational strategies, new environments (for example new geographical markets), technologies, social trends, economic changes and political and legislative changes. A PESTEL is a useful tool to carry out this review (see PESTEL).

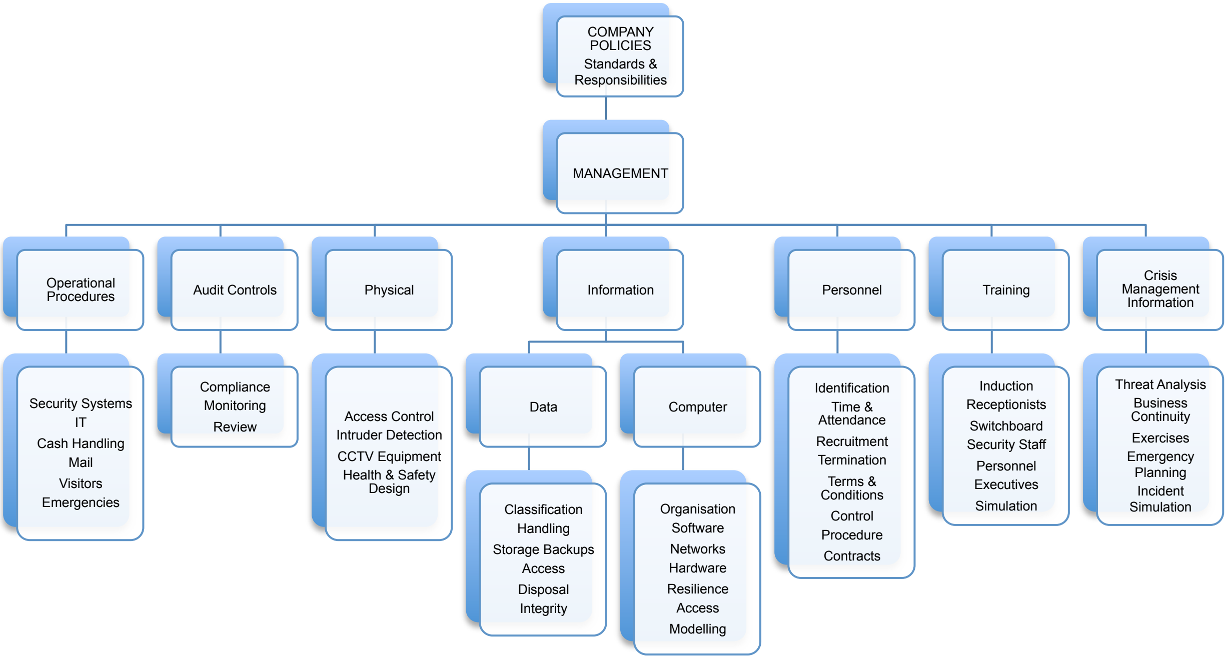
2.5 Security audit

Your strategy will also need to be informed by a security audit. This takes account of the security measures you currently have in place and will consider the capabilities of measures and the extent to which they meet any compliance requirements. An audit will typically cover the following areas:

- Managers
- Staff
- Technology
- Equipment
- Financial resources
- Methods of working
- Reporting systems
- Procedures, etc.

As part of this process you will need to assemble all of the security related documentation, such as policies, processes and procedures together in order to inform your strategy. It is helpful to also review documentation from areas outside your sphere of control which will also relate to the security strategy such as IT security or business continuity (see Business Continuity). There may well be procedures and processes in different parts of the organisation – not within the remit of the security function – that directly or indirectly impact on security and these should be considered too.

The diagram below is an example; it provides an overview of the different aspects of one security management system and the areas that you should be reviewing as part of the security audit. It is important to note that this is not exhaustive.



Advice on how to carry out a security audit is documented in a range of different texts including:

- Fay, J. (2002) Contemporary Security Management, Woburn: Butterworth-Heinemann
- http://www.securityfocus.com/infocus/1697

Perpetuity Training run courses on how to carry out security audits - for more information go to http://www.perpetuitytraining.com/securitysurveys.html

Optimal Risk can also provide support to carry out a security audit, for more information go to: http://www.optimalrisk.com/Home/Risk-and-Security-Consultancy/Security-Surveys-and-Audits.aspx

The information from the stakeholder analysis will help to inform your audit (see Understanding the organisation). When considering the security opportunities and threats it is important to remember the threats to intangibles such as the organisation's brand or reputation. A SWOT analysis can help to carry out the security audit (see SWOT).

The audit will enable you to identify your 'security gap'. That is the difference between the capability of the security function and what it needs to be to allow the organisation to meet its long term objectives. Your security strategy will document what is required in order to address the security gap.

Benchmarking

You may also find it helpful to explore the security practices and perceptions within your sector, through networking or benchmarking for example. This will help to

- identify any areas that the organisation needs to bring itself in line with standard sector security practices
- offer insights to developing competitive advantage through security

One way to determine the effectiveness of your security is to complete the Security Health Check and will provide you with feedback on over 130 features of security.

2.6 Legal and regulatory issues

Some sectors will have specific legislation which they are required to meet, for example Sarbanes Oxley, health and safety requirements, or security vetting of staff. These also need to be considered in the strategic analysis. The impact of changing legislation can be explored in the PESTEL analysis (see PESTEL). Legal and regulatory issues can also act as helpful levers to encourage buy in or support from the board or senior management, one way to do this might be by providing an example of the financial and reputational costs of a breach.

In this section:	Step 1: Strategic Analysis	2.1 Security Policy Statement
		2.2 What Information Should a Security Policy Statement Include?
		2.3 Understanding the Organisation
		2.4 Risk Assessments
		2.5 Security Audit
		2.6 Legal and Regulatory Issues

Section 3. Step 2: Strategy Development

Once you have a good understanding of the organisation and the environment that it is operating in the next step is to decide how to respond. The analysis will provide you with an understanding of what is important to the organisation and where it wants to be in the future. This can help you to decide how the security function can best align itself to the organisation, and what actions need to be taken, to help the organisation meet its objectives. This should be documented in your vision and strategic mission (see Mission & Vision). You may need to generate and consider a number of options for the future before deciding on which is the most appropriate.

Once you have decided where you are heading you can devise your strategic objectives (see Objectives) that will take you there. Ideally, your objectives should include performance targets (see Performance monitoring) (ideally financial, percentage improvement or milestones) and state how they will be measured. You will then need to decide the steps required to meet your objectives and those responsible.

Throughout the whole process you will ideally need to continue to engage with the board or the senior management of your organisation (see Obtaining board approval), in order to ensure its support. Once the strategy is complete it should be endorsed at board level.

To summarise the key stages in this part are:

1. Defining the vision and strategic mission (see Mission & Vision)
2. Setting strategic objectives and performance targets (see Objectives and Performance monitoring)
3. Formulating a strategy to achieve the objectives
4. Obtaining board approval (see Obtaining board approval)

The VMOST tool (see VMOST tool) provides a useful framework to follow. Indeed there are a range of tools (see list of Tools) that can support strategic development which have been included in the toolkit.

3.1 Alignment

This section will explain why it is so important to link your security strategy with the organisational strategy and priorities.

Linking the security strategy to the organisational strategy

There are at least four guiding principles here:

1. It is essential that security functions are driven by the organisation’s priorities.
2. Security measures need to be aligned with the organisation’s appetite for risks.
3. The security function must protect the organisation without significant interference with its essential activities.
4. Internalisation of good security practices within the dominant operating culture of the organisation requires relevant, simple and practical steps

For example within a retail business it would be ludicrous to develop a security strategy that makes it too difficult to sell goods the company would lose business and could potentially even go bankrupt. In any event the security function would soon lack credibility among senior managers. Security must allow the organisation to function, and support as far as possible not impair, its purpose in achieving its strategic objectives.

An example of a security vision which demonstrates alignment to the organisation’s objectives might be:

The selection and distribution of security measures that contribute to the success of the organisation.

It is clear from this that the security departments’ guiding principle is to ensure that security supports the organisation to be successful. Two of the strategies we reviewed had a specific section on aligning the security function with the business needs.

> *"You’re ultimately securing the business, if you become too overbearing or the security strategy impacts in a negative way on business development or the business there’s something wrong with your strategy. It should be a form of competitive advantage for your business."*
>
> *"You have a security department to help you do business securely but you want to do business."*
>
> *"If we had a standalone security strategy we’d become a security company instead of a healthcare company."*
>
> *"If you don’t continuously focus security strategy with business strategy its useless, its just a cost."*
>
> *"It is very important, we have to make sure that the security strategy is not going to impinge on the profitability and well being of the company.”*

3.2 Mission and vision

Writing a Mission and Vision statement

This section provides information to assist you when writing a Vision and Mission statement for your strategy. It defines what is meant by a Vision and Mission statement and how the two differ. It also highlights the significance of these statements and discusses why they can help to provide strategic direction. It demonstrates some of the problems you may encounter if you don't have a Mission or Vision for your strategy.

What is a Mission statement?

Put simply, a mission statement documents the overall purpose and primary objectives of your security function. Some examples of Mission statements are:

- To work together to provide a safe and secure working environment for all of our staff and customers.
- A collaborative approach to protect company profits, assets, people and stock.
- Safeguarding people, information and facilities.
- To provide the best possible security, car parking and risk management service.

What is a Vision statement?

A Vision statement documents security aspirations for the future; what do you want to, and need to, look like in the future to meet the organisation's requirements? By way of example, a Vision statement may read as follows:

- To provide an enjoyable and safe environment for all visitors and employees.
- All security measures to contribute to the success of the organisation
- To be seen as the most secure transport network in the United Kingdom.

Why would I want a Mission and Vision statement?

The Mission and/or Vision statements can be the starting point of your strategy. You may not feel that it is necessary to have both a Vision and a Mission and may prefer one or the other; however they are useful because they provide clarity about the overall purpose and aspirations of your organisation. Whether you decide to include a Mission and or a Vision, and we found that Visions were more common in security strategies, it is important to spend time agreeing them before developing your strategy. There are a number of benefits to having a Mission and Vision statement including:

- It ensures that all stakeholders are clear of the aims
- It ensures that the strategy is focused on the desired outcomes
- It provides clarity of purpose to staff

Without a Mission or Vision statement you run the risk of your organisation or stakeholders disagreeing about the overall strategic direction. This could result in individuals working in silo or towards different aims.

How to write a Mission and Vision statement

Your Mission and Vision will be informed by your strategic analysis (see Step 1: Strategic Analysis). In particular:

- The organisation's corporate objectives, Mission and Vision statements
- Your security threats
- Stakeholders perceptions of risks
- Your existing objectives and priorities
- The environment in which you work
- Internal and external resources
- The organisation's values
- The risks and rewards of alternative Mission statements
- Involving stakeholders

A common way of deciding what a Mission or Vision will be is as a group where the key priorities of the security function are discussed and agreed. It is important that your Mission is not too wide that it becomes meaningless, yet not too narrow or vague that it results in a lack of focus.

Although the Vision and Mission should be fairly stable due to their long-term nature, they should be reviewed annually as part of the strategic review to ensure they are still fit for purpose (see Step 4: Strategic Review).

3.3 Objectives

Writing Goals and Objectives

This section will provide an overview of goals and objectives explaining what they are, why they are important, how to decide what they should be and how many you should have. It also provides some examples of good and bad objectives.

What are goals?

Goals tend to be general statements of aim or purpose, ideally meeting your goals should help you to meet you vision. For example a goal might be:

- To improve the measurement of security
- To provide protection of people, property, assets and processes against risk of injury, loss or damage from criminal, hostile or malicious acts
- To integrate security into the business processes
- To have secure products, systems and services
- To protect our customer data
- To have efficient processes

What are objectives?

Objectives tend to be a more precise statement of the goal and, where possible, they are measurable so that you know when they are met. An objective relating to the goal of improving security measures might be:

- To implement incident management systems by year X
- To reduce staff assaults by 5% year on year

Why do you need goals and objectives?

When we reviewed security strategies we found that goals and objectives were common. Some organisations had goals while others had strategic objectives, in both cases these tended to be overarching aims of what the security department wanted to achieve. For example

- To ensure that existing security, safety provisions and systems are effective, fit for purpose and fully compliant with all relevant legislation.
- Improve the profile of security in the organisation, raise awareness and broadcast success.

These were usually supported by more specific, and sometimes measurable, objectives or actions. The terminology used needs to be consistent with that of your organisation. Whichever term you choose to use goals (or strategic objectives) and supporting objectives are essential in order to have a recognised and agreed output to work towards. If you chose to include objectives which can be measured they can also help you to know whether the strategy has been achieved or not. For more information on goals and objectives and the differences between the two go to http://edweb.sdsu.edu/Courses/EDTEC540/objectives/ObjectivesHome.html.

3.4 Measuring your objectives

In order to know whether you strategy is successful you will need to identify and agree a way of measuring the impact of your objectives. Although your strategic objectives or goals will not be measurable you will have either measurable objectives or measures to support them. If you are using measurable objectives remember to ensure that they are SMART (specific, measurable, attainable, result-orientated and time-specific). For example:

- To provide a security service that achieves over 90% customer satisfaction each year

This is specific, measurable (using customer satisfaction surveys), attainable, (100 percent might not be), results oriented and time-specific. Or:

- To reduce stock loss from 2 percent of the turnover to 1 percent in the next three years

These might not be documented in the strategy itself, as one Security Director argued:

> *"I think a strategy should have very high level objectives, to reduce the impact of crime on staff, reduce our impact on the crime environment. I think you should say that, but not the measurables, that's not strategic, that's a tactical plan. It might be embedded in the document you can draw a schematic of how tactical plans fall out."*

In this case you would record the measurables in a separate document, for example in a scorecard (see The Balanced Scorecard). There is more information on performance monitoring and possible measures in the Performance Monitoring section (see Performance monitoring).

3.5 How do you decide what your objectives should be?

The objectives will be informed by the strategic analysis (see Step 1: Strategic Analysis); they are likely to fall out of the security audit (see Security audit) and risk assessment (see Risk assessments) and will be the overarching actions required to fill your security gap. They should be challenging but attainable. The key thing to remember is that they should improve your existing services and add value. When setting objectives for a security strategy it is vital to align these with the available resources, that is human, financial, technical and other to ensure that they are achievable.

Your objectives are likely to relate to different parts of the security management system (see diagram). Of the strategies that we reviewed some had objectives to tackle their threats, for example:

- To reduce staff assaults

Some were related to the security services they provided or intended to provide, for example:

- To provide the best service possible, always putting the customer first

Others had a mix of the two. As a guide the security strategies we reviewed tended to include objectives taken from the areas in the table below; this is not exhaustive.

Theme	Area	Example objectives
Threats	Threats, can occur from a number of sources for example criminality, including terrorism, and may be classified as internal or external to the organisation	• To reduce staff assaults by 5% as against 2007/8 • To create a full understanding of any risk and possible known terrorist threat • Prevent hostile reconnaissance • Reduce staff theft
Security services	Such as technology, the security department, physical/ environmental security e.g. access control, emergency planning/business continuity, business continuity and crisis	• To provide the best possible security in the form of protection of assets and a sustainable reduction in crime • To ensure that the organisation takes a pragmatic view of risk and is well prepared in the event

	management or investigations	of a major incident • To establish a Security Guarding Contract that meets operational requirements, is flexible and cost effective and conforms to agreed procurement procedures • To provide a Central Monitoring Station (CMS) with improved functionality for the integration and operation of security systems and security management throughout Southbank Centre and its remote sites
Service delivery	Such as cost effectiveness and value for money, customer satisfaction, efficiency or staff professionalism through training and staff development	• Add value to our core services by ensuring security staff are happy to help whatever the situation • Provide the best possible equipment to ensure staff are able to effectively carry out their work as visibly as possible • To provide comprehensive and relevant training to all staff on a regular basis to maintain high standards, widen understanding of security and risk management, provide excellent customer service and to ensure we are compliant with all regulations and UK law • To reduce the fear of crime amongst staff, students and visitors
Security policies, standards and procedures	Such as audits or risk assessments, data collection, monitoring and analysis, compliance, procurement processes, legislation, governance, measurement	• To develop a CCTV Code of Practice • To establish an effective and transparent Procurement Policy for Security Services and equipment • To ensure regular audits of physical security are carried out • To establish Crisis and Contingency Planning

		procedures
Security culture	Such as security awareness, education and training	• Improve the profile of security, raise awareness and broadcast success • To raise security awareness by means of security and crime prevention education and awareness campaigns

The objectives will also need to link into the organisation's overall strategy and vision (see Alignment and Mission & Vision). Without this the security department is working in isolation and is not supporting the organisation. It is important to use the information collected through the analysis process of understanding the organisation to inform the objectives. So for example, if the organisation intends to enter into new markets in the middle-east the security department would need to have an objective which will support this, for example the overarching objective might be:

- To ensure that the organisation and its staff are safe and secure in new markets

There might be a range of measures supporting this such as the number of incidents or the target frequency of risk assessments. The specific actions to meet the objective, for example assessing the risks of new markets, sourcing technologies or staff etc., would typically be detailed in the tactics and implementation plans.

Depending on the size of the organisation and the other security objectives it might not be possible to have such specific objectives; instead it might be covered by an overarching objective, for example:

- To provide safe working environments for all staff
- To ensure that the organisation is secure in all the areas it does business

These are wide enough to capture the organisation's growth whilst still covering other functions performed by the security team. Other examples of security strategy objectives are:

- Providing and maintaining a working environment that is safe, secure and free from the dangers of crime for all people who may be effected by the organisation's activities
- Preventing loss of, or damage to, the organisation's assets and property as a result of crime, malicious acts, damage and trespass
- Support our security providers to understand our business and enable them to improve their service to us (see Managing contractors)
- To make security a source of competitive advantage
- To improve the use of security technologies
- To reduce the number of staff assaults by 20 percent over the next 12 months
- To minimise the risk of terrorist attacks

How many objectives?

Ideally you should only have around five strategic objectives, if you have many more than this they become difficult to manage and implement. A small number will help ensure focus and clarity.

3.6 Guidance on writing objectives

When writing your objectives avoid being too vague:

- Issues relating to the organisation’s zero tolerance policy

What issues? What is the role of the security function? This might be better:

- Implement the zero tolerance policy

Another example of where an objective lacks clarity:

- Personal safety at all times of its staff and visitors

Again what exactly is the objective? To achieve the personal safety of staff? Instead this might be better:

- Ensure that all staff and visitors are safe and secure in our buildings

Bad objectives

Some examples of bad strategic objectives are:

- Formulation of a long-term strategy to move to an integrated system serving the whole organisation
- The use of risk assessments by departmental managers
- Providing support for any staff involved in a security incident and supply up to date information for all parties especially after any incident

These are specific actions that might support the strategic objectives, they are not strategic objectives; instead the following would be better:

- To implement an integrated security system for the whole organisation
- Provide full staff protection including after the event

Other examples of poor strategic objectives are:

- Revision of all security policies, procedures and guidelines
- Risk assessments, incident investigations, incident analysis, surveillance and feedback from staff
- Submission of the annual work plan to the board with an annual report on security issues
- Liaising with police and other agencies

Many would argue that the security function should be doing these on a regular basis as part of everyday running of the security function; they should not need to be included in a strategy.

Example: Linking the Mission, objectives and actions

(See Mission & Vision and Objectives). This provides an example of how one organisation used objectives within their strategy. The strategy covers a five year period and documents the Mission (see Mission & Vision), strategic goals and strategic objectives to meet the objectives.

- Our mission is to provide the best possible security, car parking and risk management service.

This is supported by five goals, for example:

- To provide the best service possible, always putting the customer first

Supporting the goals a further eight objectives are listed which will ensure that the goals are met, for example:

- Identify short, medium and long term crime trends by using the best possible crime management tools in order to target our patrols and security advice most effectively
- Providing a flexible, modern uniformed security presence to ensure staff are on duty when and where needed to reduce and deter crime and maximise reassurance

3.7 Performance monitoring

This section explores whether your strategy should include performance indicators and how you can monitor the performance of your strategy.

There is contention over whether or not a strategy should have measurable objectives, what is clear, however, is that you will need to know whether the strategy has been successful and whether its objectives have been achieved. Measuring the success of the strategy can also help to demonstrate the value of the strategy (see Demonstrating value) and the security function to others, for example demonstrating the reduction in incidents and the costs saved.

To monitor the performance of the strategy you might use performance indicators that are quantitative, such as the number of incidents reported or the number of complaints, or qualitative outcomes, such as feedback from staff or directors. Whichever type of indicator you use it is important to recognise that performance monitoring is a continual process and you will need to collect information on and review the performance of the strategy on a regular basis.

How can the performance of the strategy be monitored?

There are a number of ways that you can monitor the performance of your strategy. Some examples might include:

- All incidents reported and recorded on the incident reporting system.
- A demonstrable reduction, over time, in the number of security incidents.
- Security costs
- Percentage of staff receiving training on security in their induction.
- A positive evaluation of the effectiveness of training programmes.
- Staff satisfaction surveys
- Complaints
- Percentage of business continuity tests successful

There are more examples at the bottom of this section that came out of the review of security strategies. It is worth noting that introducing new recording processes and practices can increase recording making a problem appear worse before it reduces.

It is, however, important to remember that what you choose to measure will influence behaviour and in some cases this can be counter productive. For example measuring the number of security site visits will simply increase the number of site visits, it will not improve their quality or effectiveness. Another example would be if a call centre has a target to end all calls in 3 minutes. If the call actually takes 6 minutes to resolve and the staff end the call in 3 minutes to meet the targets the customer will not be happy which may result in an increase in customer complaints and the associated costs. As one Security Director stated:

> *"Metrics will drive behaviour; think about the metrics you put in place. If the metrics drive people to default behaviour that's counter productive that's what they will do."*

Furthermore it is also important to remember that as one Security Director explained 'what gets measured gets done'.

There needs to be open dialogue between you and your stakeholders to ensure the strategy is working. It is important therefore to build in time to routinely consult your stakeholders (see Consultation and Communicating strategy) to gather feedback on what is working and more importantly what is not working and why. Some interviewees found that useful information could be collected using a staff satisfaction survey with appropriate questions on security.

You can use a scorecard to monitor the performance of your strategy, for example using Kaplan and Norton's Balanced Scorecard (see The Balanced Scorecard).

3.8 How to choose performance indicators

The Royal Statistical Society suggests that when designing performance monitoring the following questions should be considered:

- What is the purpose of performance monitoring?
- What is the unit of study?
- What should be measured?
- For reasons of cost, convenience or burden, have proxy indicators been substituted?
- How should the data be collected?
- How will the data be checked and audited?
- How should the data be analysed, including how frequently and adjustment for context?
- How should the results be presented, including the dissemination rules according to which institutions or individuals may be named publicly?
- and how will uncertainty be conveyed to safeguard against over-interpretation and misinterpretation?

When deciding on what the indicators should be they state:

- Indicators should be directly relevant to the performance monitoring primary objective, or be an obviously adequate alternative measure.
- Definitions need to be precise but workable.
- Survey-based indicators, such as of customer satisfaction, should use a standardised methodology.
- Indicators and definitions should be consistent over time.
- Indicators and definitions should prevent, rather than create, perverse behaviours.
- Indicators should be straightforward to interpret, avoiding ambiguity about whether the performance being monitored has improved or deteriorated.
- Measurement costs should be commensurate with the performance management's likely information gain.

Further advice on performance monitoring, developing indicators and targets can be found here http://www.rss.org.uk/pdf/PerformanceMonitoringReport.pdf.

Examples of performance indicators

These are some of the measures that were used in the security strategies that we reviewed and is not exhaustive.

Incidents	• Number of incidents reported • Number of incidents identified by the Security Team • The number of security incident hot spots • Incident handling errors
Offender management	• Percentage of incidents resulting in prosecution • Percentage of offenders interviewed under caution • Percentage of prosecutions concluded • Percentage of successful prosecutions
Risk assessments	• Number of risk reviews • Number of security survey reports • Number of inspections • Improvement trends in inspections • Outcomes of security assessments/reviews
Staff and customer satisfaction	• Security service coverage officers to staff • Fear of crime surveys • Number of system faults reported • Customer satisfaction
Financial	• Direct financial ➢ Recovery of losses ➢ Reduction in compensation paid • Indirect financial ➢ Improvement in profit and loss forecasts ➢ Contribution to value of contracts won or retained

Staff	• Sick absence • Number of staff in post

3.9 Time period

What timescale should your strategy cover?

The period of time that your security strategy covers will depend on the organisation and its environment. However for most organisations they tend to cover three to five years. Factors which are likely to influence the period of time your strategy covers are the organisational culture (see Understanding organisational culture), the sector, the time period covered by the corporate strategy and the nature of risks and threats and how they are likely to change. So for example if you work within a fast moving sector with changing demands and threats, such as the telecommunications or technology industries, a three year strategy may be more appropriate than a longer strategy.

"The time period for a strategy depends on the business and the industry."

3.10 Costs

Costs and Resources

The resources available are likely to be a key factor in deciding what your strategy will look like. It is important to be clear about the costs that will be involved in implementing the actions and objectives included in the strategy, including financial, human resources and others. You will need to calculate each of these in order to state the required budget. Within this it is important to remember:

> *"You have to be budget feasible, costs and risk ratio is high on the list. You need to be aware of your budget restraints and what they might be before you develop a strategy."*

- Staff costs
- Consultancy costs
- Outsourcing costs
- Technology or equipment
- Training costs

It is important to link the strategy to a budget to ensure that the necessary funds to deliver the actions identified in the strategy are available. It might be a good idea to state the resources that the success of the strategy is dependent on, for example additional security staff.

3.11 Demonstrating value

This section considers why strategies should demonstrate value, and if so how. It also looks at the different kinds of value.

Why should you demonstrate value?

Demonstrating the added value that a strategy can bring to an organisation can help to encourage board support and buy in. Indeed to achieve support for the strategy the board must believe that the value added by the strategy at least justify, if not exceed, the resources required to execute it. The value added by the strategy is also an important factor in decision making, determining which response will be the most cost effective. This is also known as a value proposition, and should document what the security strategy will do to create tangible results for the organisation. This is when every part of the strategy can be shown to add a value to the overall aims and objectives of an organisation.

> *"You need to demonstrate where you can add value to the business."*
>
> *"…if it cannot be defined or shown to be adding value it's not done."*
>
> *"I would say nobody considers the value in having security. It is a loss leader."*

However, with security it can often be difficult to quantify what exactly that added value is. This is intensified by the tendency for people to view security as a cost to the organisation.

Demonstrating the added value generated by security is a relatively new concept for many organisations: indeed during consultation we found that few security strategies explicitly identified how added value would be measured. In terms of security in general, it was stressed that the added value is often only apparent when an incident occurs that highlights how well, or not, the security function works when it is required.

How do you demonstrate value?

Although it is hard to quantify the value added by security there is no doubt that it does add value to an organisation, both 'hard' and 'soft'. Hard benefits can usually be described in financial terms, whilst soft benefits tend to be more qualitative such as increased staff morale (which can be measured, by for example, a survey of staff). Indeed a security strategy may add value in one or more of the following ways:

- Cost savings through efficiencies
- Reduced insurance premiums
- Minimising loss, for example through employee or customer theft or fraud
- Reclaiming loss through, for example, civil recovery, or compensation orders from convicted thieves
- Ensuring staff are safe resulting in increased morale, recruitment, retainment and productivity
- Improved perceptions of security and the security function and thereby of the organisation
- Tighter controls and governance of the organisation resulting in better risk management
- More freedom to use capital in financial institutions
- Compliance with regulatory requirements avoiding fines and reputational damage
- Minimising business interruption in the case of a crisis or disaster
- Protecting brand or reputation
- Protecting information

Specific methods which can be used to demonstrate value include:

- Cost benefit analysis
- Cost effectiveness
- Activity based costing

The Demonstrating the Value of Security report provides more detail on how to use these methodologies to calculate added value http://www.perpetuityresearch.com/publications.html. You may also find the following books interesting:

- Security Metrics Management: How to Manage the Costs of an Assets Protection Program, Dr G. Kovacich and E. Halibozek
- The Value Imperative: Managing for Superior Shareholder Returns, J. McTaggart, P. Kontes, and M. Mankins

3.12 Obtaining board approval

This section looks at how you can get board approval for your security strategy. It explains why it is so important to acquire board buy-in and how this can be achieved. Throughout this section we refer to the board, however within your own organisation you may have a senior management team or another group that have ultimate responsibility in this area.

Why it is important to get board buy-in

Without senior level support a security strategy is unlikely to be effective. Indeed it can even act as a barrier to the development and implementation of a security strategy. One security director noted that if the Board does not take the strategy seriously, by approving it and then supporting it, and acting consistently with it, then how can staff be expected to do so? You might also need board buy-in to agree the resources required to execute the strategy.

One of the main difficulties you are likely to face – highlighted by a number of interviewees - is that directors do not always recognise the importance of security and therefore the need for a strategy.

> *"When you develop a strategy you need support from the top otherwise it will not happen."*
>
> *"Unless you've got buy in from the organisation it's impossible to implement. You get lots of nods but it never really happens."*
>
> *"Sometimes the high level bosses see security as something they have to have instead of something that contributes to the bottom line."*

To get board buy-in you need to be able to explain why the organisation should have a security strategy. You need to point out the benefits (see Security Strategy Toolkit) and the added value (see Demonstrating value) of having a security strategy as well as the risks of not having one in place. You will need to demonstrate that your security strategy is cost effective and appropriate to the size of your organisation.

Although board approval is fundamental it is important to recognise the role of all staff (and probably contractors too as well as visitors) to implementing the strategy. As security threats can occur in every business activity and against all people, all staff are likely to be needed to be engaged at least to some extent. Board approval is one step in facilitating that.

How to get board buy-in

This section provides some suggestions on how you can get the board to recognise the importance of a security strategy and therefore buy-in to it.

Your relationship with the board

It is a good idea to keep the board as informed as possible during the development stage of the strategy and to build a good relationship with the board (see Consultation).

In reality you need to have a good relationship with the board in order to be able to influence it. The ACT acronym (see ACT) can be useful to think about your relationship with the senior level of the organisation and may help to identify what actions you need to take to improve the relationship.

> *"Walk people through every part of the process and take them on the journey with you, it's about effective influencing."*
>
> *"Once that sponsorship happens it is amazing how the lieutenants fall in line."*
>
> *"Having someone closely linked to the board and the development of your strategy is a smart move."*

One way of building your relationship with the board to encourage buy-in is to have someone who can act as a link between the development of the security strategy and the board itself; an ally, sponsor or champion.

Depending on the size and complexity of your organisation, you may need to go through a steering, working or operations group to get your security strategy off the ground before you take it to the board. Having a contact on such a group who is also on the board will often help you to progress the development of your security strategy.

Presenting your strategy

Once the strategic document is completed it is a good idea to give a short presentation to the board identifying the pros and cons of the security strategy. It can help to use pictures or images to present material, such as graphs instead of tables or figures.

The need to adhere to regulatory requirements (where they exist) can be very engaging because the board is held accountable for non-compliance. Therefore where appropriate build your presentation to the board around these to encourage support and buy in.

You need to ensure that you and the board are talking the same language, that there is a common understanding of what is meant by a security strategy. It is normally important to use business and not technical language with the board. Furthermore it is beneficial to state your key assumptions about the business on which the strategy is based, for example that the business will grow by 5 percent in the next 5 years. One strategy that we reviewed had an appendix, which contained all of the assumptions on which it was based, for example trends in business usage, technology, threat and attack as well as the legislation and regulation, and security and continuity assumptions.

You need to be able to demonstrate the added value that a security strategy will bring to your organisation (see Demonstrating value); this can be achieved by identifying what the board values most and building on this information. There is more guidance on how to document the added value of the strategy in the section within the toolkit (see Demonstrating value).

Key points to getting board buy-in:

- Build a good relationship with and have an open dialogue with the board
- Consider a sponsor, ally or champion on the board
- Keep the board informed of progress
- Ensure the language you are using is understood at all levels
- Demonstrate the added value of a security strategy (see Demonstrating value)
- Highlight the risks or associated costs of not having a security strategy in place

> *"We had to nail down the specifics and explain the costs and we had to get metrics and evidence."*

3.13 Consultation

This section will provide an overview of why it is so important to consult with people throughout the development of your strategy and suggest different ways that you might be able to do this.

Why consult?

In order to ensure buy in to the strategy it is a good idea to involve relevant staff in the process starting at the strategic analysis stage. It is important to remember that security touches upon the entire organisation, from the director through to the cleaners; every business activity has potential security risks. And so you will need their help in identifying new and emerging threats and to generate ideas that will help prevent them. Moreover, the decisions that you make are likely to impact upon others, and you, and they will need to know what sort of impact the strategy will have so that they can be prepared and limit the likely damage, if necessary, or enhance it as appropriate. Involving people that you predict are likely to be resistant to the strategy provides the opportunity to overcome the issues before implementation. A good way to engage people in the strategy is through consultation.

> *"Involve as many stakeholders as can be involved within reason; the more acceptance there will be from stakeholders that have participated."*
>
> *"Everyone needs to be involved in contributing to the development. [I have] 64 people working for me, all of whom are responsible for security; everyone has a part to play for the strategy to work."*
>
> *"Every part of the organisation needs to know that they have a responsibility to contribute their concerns – that will help inform the people writing the strategy."*

There are other reasons to consult; such as to identify levels of acceptance or potential rejection of security measures as well as to receive guidance on the type of language and motivation required to ensure staff actively support the emerging strategy. In other words at the earliest of stages, consultation is about trying to influence behaviour and to address the perception that security is in some way linked to penalties; restrictive rules and a cost rather than benefit to the organisation. The final reason for consultation is to assess who needs to be consulted. It is not necessary to consult with everyone but care needs to be taken to engage with a sufficiently large and representative sample.

Who to consult?

The extent and method of the consultation required will depend on the size and culture of the organisation. However key people to consider are:

- Chief Executive Officer (or similar)
- Finance Director
- Head of business units
- Heads of departments
- Security staff
- A cross section of other staff
- Key clients
- Partner organisations
- Key suppliers

> *"At management level, find out what the board want from you, you have to talk and listen to both directions, up, down and sideways."*
>
> *"Each department has a role to play."*
>
> *"Don't think you are the centre of the universe; you're a tiny peripheral part of everybody's everyday business."*

How to consult

Some of the tried and tested approaches to engaging and consulting stakeholders include:

- Running workshops with staff across all departments/divisions/ functions to discuss their perceptions of security
- Staff satisfaction surveys to gather ongoing feedback on security
- Personal one to one interviews
- Strategy away days
- Circulating a document to stakeholders for consultation

When consulting it is important to avoid using technical or security terminology as this will not always be understood. Furthermore you also need to remember that security is not a priority for all and may even be viewed negatively by some. By talking to people about what they do and any obstacles there may be to achieving their aims, it places the conversation on grounds that they are familiar with.

> *"Ask people first what they want, and you get them on board and then you can change their thinking."*
>
> *"You should have a regular set of meetings or internal workshops to discuss the strategy and the implications of what you're doing with as many departments or units as possible."*

A steering or working group

Depending on the size of the organisation it may be useful to set up one or more strategy steering or working group(s). It could consist of representatives from the board or senior management team and staff representatives including those from the security function. The group may also benefit from a representative from the Human Resources department to advise and carry out actions relating to staff management. This group would oversee the development and implementation of the security strategy, making key decisions. They could also act as "champions" within their own departments feeding back on progress.

3.14 Business continuity

Business Continuity Management, Contingency Planning & Crisis Management

When developing your security strategy, it is important to take into account business continuity management (BCM), contingency planning, crisis management, disaster management and disaster recovery. These are covered briefly in this section. It is not intended to be an extensive account but will justify the importance of including these areas in your security strategy.

What is Business Continuity Management (BCM)?

Put simply BCM means planning to ensure that your organisation can continue to function in the event of an unforeseen event, for example a natural disaster such as a flood, a fire or a terrorist attack, a technical failure relating to loss of power affecting telecommunications, or an IT system failure caused by a computer virus or a computer hacker.

The priority risks to be addressed will be borne out of the risk assessment carried out in the analysis stage (see Risk assessments) and will inform your business continuity plan. The plan focuses on how the organisation will respond if a disaster occurs and sets out risk reduction and recovery. With good contingency planning you can minimise the impact on the organisation. Furthermore there are a number of advantages of contingency planning including:

- It can reduce losses by assisting businesses to return to normal levels of business faster after the risk has occurred.
- It can protect market share by limiting the volume of business lost to competitors.
- It can protect brand integrity by reducing the chances of customers losing confidence in a business.

Effective BCM requires a suitable balance between risk reduction and recovery mechanisms. For an example toolkit regarding Business Continuity Planning please refer to: http://www.direct.gov.uk/en/Governmentcitizensandrights/Dealingwithemergencies/Preparingforemergencies/DG_176539

The BS 25999 standard sets out detailed advice on designing and implementing a business continuity plan and the actions necessary to obtain accreditation for the plan(s) that have been developed. For further information on business continuity standards please refer to the British Standards Institution website: http://www.bsi-global.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/

The plans and procedures that relate to your strategy will need to be tested and reviewed regularly and suitable training programmes or strategy rehearsals put in place to ensure all staff understand and know how to implement them. It is important that there is commitment to BCM at the senior level and that this message is cascaded from this level. BCM needs to be part of your organisational culture (see Understanding organisational culture) and staff will need to be aware of and trained on why it is so important and what to do if an unforeseen disaster strikes.

What is disaster management/disaster recovery planning?

Having identified the risks and plans to manage them, disaster management refers to putting a range of steps and plans in place to minimise the impact of a disaster, such as a natural or manmade disaster such as a tsunami, a major flood or a fire.

Disaster recovery planning focuses on the recovery processes in response to a disaster, for example preparing for the recovery or continuation of the technological infrastructure of the organisation.

What is crisis management?

Crisis management is what it says: managing the crisis and deals with how an organisation manages the wider impact of a disaster, such as a flood or terrorist attack. Crisis management deals with providing the best response to a given crisis. It is important to consider:

- a pre crisis response, in other words, minimising the risk,
- a during crisis response, which is the immediate handling of a crisis, and
- post crisis, which is the response to the aftermath of the crisis and the steps that need to be taken so that normal business is resumed.

It is important to consider the message that is portrayed to the media and customers following a crisis. If this is not handled well and the organisation is perceived to be in chaos, this could have a damaging impact on the business, not least in terms of its reputation and loss of customer confidence.

3.15 Why is it important to consider BCM?

Why is it important to consider BCM, crisis management, disaster management, disaster recovery in your security strategy?

Incorporating BCM, crisis management, disaster management, disaster recovery into your security strategy is important for a number of reasons. Having considered it; your organisation is more likely to endure the aftermath of a major incident, without it your organisation may struggle to survive. A disaster can affect any business regardless of its size or function, so it is important to develop actions and prepare recovery plans to cover all eventualities. Small businesses in particular may find it difficult to return to ‘business as usual’ after a crisis.

Getting started

Your business may already have separate strategies for business continuity, risk management, crisis management, disaster management, disaster recovery so this is your first task - find out what exists already to avoid duplication or worst still cross purposes and use this information to feed into your security strategy.

Secondly, where these strategies exist, we would encourage you to consult with each business function such as the IT department if they have a disaster recovery strategy to ensure that the roles and responsibilities of each department are understood in order to avoid duplication. This should provide you with the foundation on which to develop your security strategy.

Your security strategy should only provide a landscape view of these areas but not go into detail; moreover by considering each of these areas you should have the ingredients to shape and develop an all encompassing security strategy, developing resilience and business continuity.

How one security strategy incorporated crisis and contingency planning

The strategy has a specific objective relating to crisis and contingency planning:

> *"To establish crisis and contingency planning procedures aligned to the organisation’s business continuity processes."*

There are a number of actions that support the delivery of the objective, including:

- Strategies should exist for responding to major emergencies and disasters and should be aligned with existing business continuity processes;
- Maintain and routinely review emergency management plans, crisis communications and business continuity and recovery;
- Ensure crisis and emergency management plans are readily available and easily communicated to appropriate personnel;
- Appropriately test the effectiveness of all crisis and contingency plans; and
- Brief and train staff in their roles and responsibilities during major emergencies and disasters. Ensure that security personnel are appropriately trained and equipped to respond to, and initially manage incidents, major emergencies and disasters, including the ability to assess situations and implement procedures to notify appropriate emergency services of the nature, location and extent of the incident (facilitate the attendance of the responding services to the scene).

3.16 Writing the security strategy

This section will provide some tips on writing your security strategy and has a link to the security strategy template and some security strategy examples.

Before you start

Before you start to write the strategy it is a good idea to share the key assumptions on which the strategy is based with a member of the board (or one of its representatives) to ensure that the assumptions are valid. The last thing you want is to spend months writing a strategy based on say a particular version of the corporate strategy and then find out that it is out of date, and that had you asked you would have known that. Or, alternatively, that the organisation was already planning a venture that would greatly impact on how you would need to think about security.

Some key things to remember when writing strategy

When writing your strategy it is important to remember:

- An effective security strategy needs to be comprehensive and dynamic, with the flexibility to respond to any type or levels of security threat, whilst also allow the organisation to take advantage of new opportunities which may arise.
- It needs to be adaptable so that it can accommodate changes in key assumptions and requirements as a result of changes within the organisation or the environments.
- The strategy needs to be clear to readers and this may include very different types of audiences.
- It is a good idea to write the security strategy in business not technical terms to ensure understanding and buy in from the board and senior managers.
- It helps to define the key terms that are open to different interpretations, for example ‘risk’; this is particularly important in large multi national companies where the language may differ.
- The strategy should document the key assumptions on which it is based, for example that it is based on a specific version of the corporate strategy, or major new developments such as the organisation moving into different markets in the following year.
- The strategy should document the resources required to meet its successfully delivery; human, financial and technical.

How long should a strategy be?

We received very different opinions on this one reflecting a myriad of practices. Strategies discussed with us varied in length; some organisations will use a one page strategy map, while others have a document exceeding 50 pages. Most, agreed however, that a strategy that is relatively brief is preferable so that it can be read and understood quickly and easily. One way of achieving this is by using appendices to support the strategy, for example detailed actions which may sit better in a supporting implementation plan. It is worth noting that your first strategy may be quite long but that over time, and with each strategic review, you are able to refine it (see Step 4: Strategic Review).

> *"You can produce a big fat one to show that you have done something. But something shorter is much more valuable to shape practice."*
>
> *"In management school we say it is not the words, it is how far people buy into it that counts. When you read something you rarely say I wish this was twice as long."*

3.17 Strategy template and guidance

The template

The first step, when deciding how to structure your security strategy, is to explore whether your organisation has a standard strategy template that you could replicate, perhaps the structure used in the corporate strategy for example. In the absence of this the structure that is suggested here provides a good practice example. However, this guide is merely one possible way of framing your strategy and you may prefer to structure it in a different way and move things around according to what works best for you. The sections suggested here are not exhaustive and you may choose to add more, likewise you may feel that you do not want to include all of the different sections that have been included. Indeed in order to keep the strategy concise you may prefer to prioritise different parts of the strategy.

Furthermore you may decide to have several different versions of the strategy for different audiences, for example one for the board (see Obtaining board approval), one for you and your managers, and a brief overview to communicate the strategy to the rest of the organisation (see Communicating strategy). This should be decided on a need to know basis and you will need to remember that some contents of the security strategy may be sensitive and should not be shared too widely. This guide suggests a structure for the whole document; you may then decide to pick and choose sections to go into versions for other audiences.

- You can download a security strategy template that you can amend for your own organisation here (Security Strategy Template.doc - 80KB approx - Microsoft Word).
- There are also guidance notes to support the template which you can download in PDF or Microsoft Word formats (Security Strategy Guidance.pdf - 25KB approx - PDF format, Security Strategy Guidance.doc - 36KB approx - Microsoft Word).

Strategy examples

This guidance provides one suggested format and structure for your strategy based on a review of strategies, interviews with experts and academic texts. However, we have also provided several different examples of what other organisation's strategies looked like to help you to decide how to structure yours.

INDEX

The examples provide an overview of some of the strategies provided to us during the review, but do not go into detail in order to protect the confidential nature of the documents. They do however provide enough detail to help you to understand what they looked like and they might help you to decide what you want to include in your strategy and which format is the most appropriate for your organisation.

Example strategy 1
Example strategy 2
Example strategy 3
Example strategy 4
Example strategy 5
Example strategy 6
Example strategy 7

3.18 Key issues in strategy development

This section describes some of the key issues that you may need to consider when developing your strategy. It outlines some of the challenges you may encounter along the way and suggests ways to overcome these.

The section has been broken down into a number of key areas including:

- Being realistic about how long it will take to develop your strategy
- Understanding your organisation
- Consulting your stakeholders, both staff and customers
- Obtaining buy-in for your strategy
- Resources

Being realistic about how long it will take to develop your strategy

The first point to note is that strategy development takes time (see How long will it take?). You will need to be prepared to invest time and resources into the development process; for example you will need to allow sufficient time to consult with your stakeholders (staff and customers). You may also need to consider inviting in external advisors to conduct a security audit, to identify gaps and propose solutions. Identify some quick wins that can be delivered on the way to completing the full strategy – this is more likely to achieve buy-in of the total programme.

Understanding your organisation

Understanding your organisation is vital to the development of strategy (see Understanding the organisation). In order to understand your organisation, you need to consult your stakeholders and that includes the board, senior management, staff, customers and trade unions.

In addition to consulting with stakeholders, which is fundamental to understanding your organisation, there are also a range of tools (see Tools) which can help you, for example a SWOT or PESTEL analysis (see SWOT and PESTEL).

Consulting your stakeholders, both staff and customers

Experts that we spoke to made the point that it is important that the development of strategy is driven by its stakeholders. One way to achieve this is through consultation and including them in the strategy development process. (See Consultation)

Obtaining buy-in for your strategy

It was quite clear that in order for your strategy to be successful, you will need to obtain buy-in from the senior management team and/or the board. The section on obtaining board approval recommends ways that can help you to achieve this (see Obtaining board approval).

Resources

One of the biggest issues when developing strategy and one faced by many businesses is the cost associated with it (see Costs). It is therefore important to seek access to financial information to ensure you have a feasible and realistic budget to work with, this will in part determine the implementation of your strategy.

It is also important to have a budget allocated to the strategy so that the required resources are available. This means that the strategy will need to be agreed before the budgets are finalised to ensure that the budget is available.

Section 4. Step 3: Strategy Implementation

The next step is to implement your strategy. You will need to devise an implementation plan (sometimes known as a business or project plan) (see Implementation plan) which will document the various actions required to meet the objectives. This will also record the owners of objectives/actions and timescales for implementation. There may need to be a reallocation of resources in order to implement the strategy.

Implementing strategy is equally dependent on good communication (see Communicating strategy). For a strategy to be effective it needs to be well-communicated to staff and stakeholders.

4.1 Understanding organisational culture

This section will provide an overview of what we mean by organisational culture, why it is so important to strategy development and implementation and discuss what a positive security culture might look like. It will also provide some guidance on change management.

What do we mean by organisational culture?

Organisational culture refers to the shared culture, or beliefs and values, of the people within an organisation. Put simply, organisational culture is the 'taken for granted' way of doing things.

The organisational culture is likely to be affected by a range of factors, such as the size of the organisation, its age, the demographics and diversity of its staff or the industry and sector. For example, the organisational culture of the police is likely to be very different to that of a financial institution.

> *"This is all about how we do things around here, and so if the culture is one of supporting functions and employees then a culture of inclusiveness, where you are part of our family, is good and important. Others may be more focused on cost, not spending money and be risk adverse and not want to make changes, then that is another."*
>
> *"Ignore organisational culture at your peril."*

Organisational culture can relate to attitudes to work or authority, as well as the extent that information is documented, the level of bureaucracy and the preferred methods of communication such as emails versus telephone calls. Different departments or offices may have different cultures, for example the finance department, marketing or the legal department. Although the culture is rarely documented its impact can be seen, particularly when employing new recruits: *"I just don't think they'll fit in here" or "We have a 'can do' attitude here"*.

How are cultural differences noticeable?

Cultural differences can manifest themselves in a number of customs, for example attitudes to work, values or expectations. The culture of an organisation consists of values, beliefs, behaviours and taken-for-granted-assumptions and is shared by all of the members of the group, not just individuals. The table explains what we mean by values, beliefs, behaviours and taken-for-granted-assumptions and provides examples.

Cultural Indicators	Definition	Example
Values	Values may be very easy to identify within your organisation, they are often written down as statements such as a company vision, mission or objective. That said they can at times be vague.	To exceed our clients' expectations.
Beliefs	Beliefs are more specific, and can be distinguished in how people talk about the issues faced by an organisation.	They'll never make redundancies here.
Behaviours	Behaviours relate to how the organisation operates on a day-to-day basis.	Always using meetings to make decisions as opposed to individual decision-making.
Taken-for-granted assumptions	Taken-for-granted assumptions are the nucleus of an organisations culture. These are often what people find difficult to identify and explain. They can be referred to as the organisational paradigm defined as the set of assumptions held relatively common and taken for granted in an organisation.	For example within a local authority the paradigm may be that local governance is fundamental to society.

Other indicators of an organisational culture include routines and rituals, such as drinks in the pub on a Friday evening, symbols such as corporate logos, the dress code and the structure of the organisation, for example how hierarchical it is.

Why is organisational culture so important?

Your strategy is only likely to be effective if it fits in with the organisational culture. Furthermore if what you require of staff is at odds with their values it can cause employees to lose their motivation. In order to achieve commitment and motivation to deliver a security strategy it is important to provide opportunities for employees to feel they both understand and see the importance of what is proposed, and that they have the skills and knowledge to ensure that it is implemented and followed.

Thus, it is important that the culture of the security function aligns with that of the organisation. Some interviewees noted that this was not always the case, for example, where security procedures were a hindrance to them doing business.

Similarly, some organisations have a risk-averse culture whilst others focus on every opportunity. This clearly needs to be reflected in the security strategy.

> *"It doesn't matter what it is you are introducing, if the culture is not right you are not going to implement anything successfully."*
>
> *"Security departments have to go with the grain of the culture that's in the organisation whether they like it or not. You will drive yourself round the twist if you're not working with the grain and the company."*
>
> *"It varies from country to country and business because the culture in Europe varies from the culture in the US. Because I am in 30 countries and apart from two or three they are all high risk countries but I have to sell culturally to the leader of that business unit what I am going to do and fit that within his culture so that I am not another alarmist American."*

The country that you are working in is also likely to have a role to play in the organisational culture.

Creating a positive security culture

Not only is it important to understand your organisational culture, clearly having a positive security culture will facilitate the implementation of the strategy. Good communication can help to create this (see Communicating strategy).

Some organisations use incentives to promote a good security culture; this in turn encourages stakeholders to commit to the objectives of the security strategy. Here are some examples of how some security experts have used incentives:

You need commitment to make sure things work. Here everyone gets an incentive if shrinkage is below a certain figure; we've got it down to a really low figure. If we keep it at this level each one gets a bonus, every single person that works in the store – cashiers, guards, receivers. The global amount is split equally.

> *"Bring good people on board, pay them well, have bonuses linked to targets. We had targets such as rolling out the implementation of safes around units, or it could be linked to a reduction in crime, not absolutely but comparatively."*

However, care needs to be taken when using incentives as they can have the opposite result. For example, where incentives are offered for reporting incidents it could lead to staff committing offences in order to obtain the reward or even fabricating them.

> *"A good security culture reflects the companies' brand and values and how they represent themselves, security has to look like that otherwise it's disconnected. It needs to be embedded within the business plan. It's no good saying we want a secure environment and challenge everyone and watch them if the general populous doesn't recognise that, believe in it or understand it."*

> *"There is a history in our profession of being too secretive, if we communicate openly about what we're doing it will have a positive impact on the culture."*
>
> *"So much of whether or not a security strategy works depends on the security attentiveness of the employee population. Good reporting to the security department about problems relies on every individual that works there to make that happen. If an anti-security culture exists it can have a detrimental impact."*
>
> *"It's a continuous process of education of the workforce."*
>
> *"A good security culture is embedded in the business. Create it by aligning it with the business plan, embed it with everything the company does and aspires to do."*

Managing change

Resistance to change can be a major problem for managers wishing to introduce new ways and patterns of working. A new security strategy may bring with it necessary behavioural changes, such as requiring all staff to carry or wear an identification badge. In order to ensure that change does occur good communication is a key part (see Communicating strategy), including, where possible, explaining why the change is necessary.

Change management is a field in itself, and there is a wide range of books on the subject. The Chartered Institute of Personnel and Development have a page on their website dedicated to change management and members can access a tool designed to help plan, manage and implement change more effectively http://www.cipd.co.uk/subjects/corpstrtgy/changemmt/. There are also a number of other websites providing advice on change management, for example:

- http://www.idea.gov.uk/idk/core/page.do?pageId=5817020

INDEX

- http://www.jiscinfonet.ac.uk/infokits/change-management
- http://www.businessballs.com/changemanagement.htm
- http://www.teamtechnology.co.uk/changemanagement.html

4.2 Communicating strategy

This section refers to communicating your strategy to the relevant audiences which is paramount to its successful execution. Indeed, it is striking that a large number of interviewees emphasised this point and that without it the strategy would be ineffective. After all, security is endemic to all organisational activities. It is important that you are clear who is responsible for communicating strategy and that you have processes in place to facilitate this.

The image of the security function is important – to be effective the security function must have the approval and confidence of the organisation.

Why communicate strategy?

It is important that you communicate your strategy, as appropriate, across the organisation. Typically all staff needs to be security aware and getting buy-in to what you want to achieve will necessarily require the effective engagement of staff. Poor communication can be one reason why a strategy is not properly implemented. That effective implementation is reliant on the support of others highlights the importance of good communication.

> *"Communication is key; they are able to say this is how I contribute to it. Get them to understand it."*
>
> *"Getting people to comply is not about incentives and punishment, it is about education, it's about communication."*

Although not ideal, if you are faced with resistance, having board approval will provide your strategy with more clout (see Obtaining board approval). But if you are facing resistance it is crucial you understand why. Perhaps you have not understood the culture of the organisation or the environment in which you operate in. One security director noted that he had had to learn that making the best use of security guards required different approaches in different countries as there were many variations. For example, in some areas activities are regulated, some follow a more militaristic type of training and deployment rather than a service orientation and so on. He had faced resistance in the past because his corporate approach had not taken account of these legal, cultural and other differences.

Who do you communicate your strategy to?

Once you have developed your strategy; you will need to ensure that it is communicated to those affected by it. It is vital that you pitch the communication of the strategy at the right level to ensure that staff and stakeholders understand how the strategy relates to them, what is expected of them and their role in its delivery. It is likely that you will need to tailor the messages you wish to convey to suit the different audiences, including trade unions, staff, managers and board members.

You will need to select the relevant information to communicate to different stakeholders. For example, security staff may need to know more than those from other departments.

Ideally, the strategy should be a high level document and therefore it should not contain sensitive information. However, there may be some sections of the strategy that you prefer not to have in the public domain. Where this is the case, it would be beneficial to have a good summary of the key points readily available for all staff.

"If company staff at the operations end do not buy in you will not be successful."

"Strategy isn't only an executive function – a successful strategy execution requires the involvement of all of the people in the organisation, so that everyone knows where you're heading and what you want to achieve."

"Everyone affected by it gets a copy of the plan and objectives so that they can see what they need to do."

As well as communicating the strategy with staff it is helpful to share it with other stakeholders such as partners, suppliers and trade unions to ensure that you are all working in the same direction. For example, it is often beneficial for security providers to understand the security strategy in order to understand your priorities. Indeed, some security providers noted that they could offer a much better service if they were made aware of the broader security aims (see Managing contractors). Most security providers consider the tender stage to be the best time to share strategies.

How to communicate your strategy?

In particularly large organisations it may be beneficial to support a strategy with a communication plan.

However, it is important to remember to link your security communication plan with any others that already exist within the organisation. Selecting appropriate channels of communication to convey the strategy is very important. You can use a number of different methods to communicate your key messages. A number of organisations use their intranet site to ensure that all staff are aware of the aims and objectives of their security strategy. Other methods of communication include:

- Newsletters
- Workshops
- Posters

- Email
- Electronic bulletin board/notice boards
- Face to face communications
- Campaigns
- Staff handbooks
- Training/presentations
- Staff inductions

Another approach is to select and nominate certain individuals within the organisation to act as champions of the strategy. Using these champions to cascade the aims and objectives of the strategy may assist to converse the key strategy messages to all relevant stakeholders.

> *"You must have a proper communication plan, you must consider who you are talking to, your direct reports, then those in different departments with different compliance requirements or different needs, and then there are shareholders and stakeholders and what they get out of security. If you are top of the game you need to communicate your message to them in their language so that they want to act. The messages will be different and you need to get this right."*

4.3 The Workforce

Human Resources Issues

When devising your new strategy it is imperative to take into account the impact it will have on the organisation and this includes any implications for human resource. Things to think about include:

- Will there need to be a re-structure?
- Employees may need support to develop the skills or motivation to work in new structures or changed working practices
- It can help if employees understand the reason for any changes, for example increased security measures, this will be dependent on effective communication (see Communicating strategy)
- Management styles may need to change in order to fit the strategy
- There may need to be a programme of awareness raising, education and training.

It is important to be clear about the differences between awareness raising, education and training. Awareness raising refers to getting people interested in security, to help them understand why and how it affects them. This can be achieved in a variety of ways even through humorous messages for example. Education provides information about the security threats and vulnerabilities and what they can do to protect themselves. Training involves teaching people new behaviours, for example how to use a new access control system.

Clearly the effectiveness of any method of security is dependent upon it being used correctly. Indeed there is a lot of research currently being undertaken on the impact of human factors on the effectiveness of security. For more information on this and the differences between awareness raising, education and training go to http://www.ktn.qinetiq-tim.net/content/files/groups/humanvuln/HFWGWhitePaperfinal.pdf.

Training

If the strategy is introducing new technologies, processes or procedures it is highly likely to require staff training. This may be related to specific technology, such as an access control system, or behaviour, such as the reporting of incidents. The effectiveness of the strategy may be heavily reliant on training the appropriate people; therefore you may need to develop a training plan. This will detail who will be trained, on what and when and will support your implementation and any communication plans.

Alignment with staff objectives

In order to achieve full compliance you might want to consider aligning the strategy with staff objectives. It will certainly be beneficial among security staff. This aligning of individual staff objectives with the security strategy objectives allows staff to understand how they can contribute to the successful delivery of the strategy. This can also be tied into staff rewards and incentives such as bonus payments. For example in one organisation all of the employees received a bonus when shrinkage (the loss of products for example through theft) was below a certain level. Furthermore specific staff responsibilities or expectations can be built into the appraisal process.

> *"It's about understanding the strategy and then linking that to my role as an individual. Now I understand why I'm here it gives me purpose and links to the vision of the organisation it creates a happier work environment."*

4.4 Managing contractors

It is highly likely that contractors will, or can, play a key role in helping you to implement and execute your strategy. This section will help you to consider how best to manage contractors to ensure that they are focussed on your needs and priorities. It outlines a range of problems identified by contractors as well as security directors and presents suggestions to overcome or avoid these.

Two important issues that emerged from the research are that there is a skill to managing contracts and to getting the best out of them, and that this skill is often not properly developed in either the buyer or provider. This is as true of security as it is of other products and services. Recognising this point is a key first stage. There are real problems that result from poor management of the contractor service as two security company directors noted.

> *"Usually [we] operate in the dark, [and I] don't understand why certain decisions are taken; if I knew why it would make more sense and I could make savings for them in overall security spend."*

> *"You can't score a goal if you don't know where the net is – you can't be sure that you're doing the job they want – you can't analyse your own performance."*

There was no doubt that security providers believe that seeing their clients' security strategy helped them to provide a better service. Furthermore, some security directors noted that specifying expectations of security contractors needed to be an element of the security strategy. And others that the starting point to an effective partnership was a good strategy to guide all those involved. And 'good' meant having something written down:

> *"Some [have] got a strategy in place in their mind but [it is] not documented – [they] say this doesn't meet our strategy. It makes us disjointed and ineffective."*

Getting the most out of contractors

Contractors highlighted a number of areas where they felt specific problems arose that undermined the work they did. For them the key to strategy was to be aware of the problems and build in solutions from the start. We have listed the main points made using four separate, but broad and overlapping areas, covering procurement, management issues ensuring good performance and working in partnership.

Procurement stage

> *"A lot of companies buy so badly they don't necessarily engage with their suppliers enough until it's too late in the process... A security department might get a say but most times it's driven by procurement. In [the] absence of a board approved strategy, procurement can go off and do what it likes."*
>
> *"The more they share the better the quote we can give – it depends on who's running the bid – if it's an operational or security lead bid we get more access or knowledge. If its purchasing or finance [then] it's based around this many hours at this many sites, give me a price... You become a price driven procurement process, [it is] not about security."*
>
> *"[I] don't think they get best value the more prescriptive they are... why? Because we're just supplying on what they've asked for rather than helping and advising and working with them to come up with the most appropriate delivery performance."*

- Ensure that your procurement team has sufficient knowledge of your security requirements. Security is not something that they probably purchase everyday so they will often need advice.
- Think about what you get from a good security company that you don't get from a bad, and know the difference as it applies to your needs.
- Since different security companies have different specialisms/ abilities/ functions and geographical coverage ensure that you choose one that meets your needs, you can always check with other clients of the company. It is better if you ask them to list current clients and you choose which ones to contact.
- You may need to think through the potential conflict between paying the lowest price on the one hand and obtaining what you consider to be the best or most comprehensive service on the other; rarely does the best come cheaper. Be clear about your priorities, are you buying a product or service at the lowest possible price, or a product or service that meets specific needs?
- Security is often purchased in silos, but you need to ensure that the different elements of security fit together. There is much discussion about 'holistic' approaches, 'integration', and 'interoperability', which in different ways emphasise the need to ensure the various parts of your security function fit together. For example, you may need security officers to operate CCTV or respond to alarm alerts; these requirements need to be built into your procurement specification for security officers.
- Providers we spoke to welcomed any chance to offer their own view on how they could meet the needs of clients; consider giving them the opportunity as they may be able to do the work more efficiently and cost effectively. Be open to the possibility of thinking in different ways,

for example by using technology alongside people, by using different technologies, or to engaging say half the number of security officers but paying them twice as much.

There are two good guides that offer advice to the purchasing of contract security.

The first, 'Introduction to Purchasing Security', has been produced by the Chartered Institute of Purchasing and Supply in collaboration with Perpetuity Research and Consultancy International and can be downloaded from our website free of charge (click here for details).

The second is 'The Good Practice Guide to Procuring and Running Guarding Contracts' produced by the British Institute of Facilities Management, and is available from, BIFM, Number One Building, The Causeway, Bishops Stortford, Hertfordshire, CM23 2ER, email: psc@bifm.org.uk.

Management issues

- Ensure the person or team managing the security contractor understands what is required of the elements he or she is responsible for, and how best to get any problems solved speedily and effectively.
- Ensure that any training offered to managers is fit for purpose. Contract managers need to be capable of managing contracts and they need to understand the performance requirements and objectives of the different elements of security they are responsible for. Other skills sets that were mentioned included the need to be able to forge meaningful partnerships, and administrative competency.
- Contractors noted that a change of contract manager often results in a loss of expertise, and sometimes a good relationship as well which can take time to re-establish. Therefore any changes in staff need to be managed; a good handover period can help.
- Satisfy yourself that contractors have built sufficient management time at the different management/supervisory levels. Ultimately this is crucial to effective service delivery.
- Be clear that what appears in the contract, as agreed at a senior level, is what is required by those lower down the organisation. Conflicts created here can be difficult to resolve later.
- Ensure that any documentation that supports the contract is updated and kept up to date. For example, the risk register, and the list of assets can change, and this may impact on what you want from your security operation.
- Consider whether there are any benefits that could be derived by effective co-ordination of the security provider with other service

providers (such as a Facilities Management provider) and whether the structures in place enable this to happen.

4.5 More on managing contractors

Ensuring good performance

- It is a statement of the obvious that performance measurements always need to be fit for purpose. Yet some companies we spoke to admitted that they did not measure the most important features of a contract. Be careful you don't encourage contractors to focus on what is measured rather than what is important if the two are not exactly the same.
- Contractors generally welcomed the opportunity to show they were capable of improvement, ensure that you provide good feedback, communicate effectively, and remember to praise as well as criticise when it is appropriate to do so.

> *"[I] think culture is more important than the strategy without the culture to deliver it its dead in the water."*

- If a problem persists be determined to find out why and recognise that sometimes the solution may involve you making changes. One point made by many contractors was the importance of working in a culture where security was recognised as important (if not a priority), and where their role was recognised as being of value to the organisation. Don't forget that contractors are often a crucial part of generating and reinforcing a positive security culture (see Understanding organisational culture), so you will need to consider approaches to engage them.

Working in partnership

- There are many elements to effective partnership working, but prime amongst them is effective communication. You need to ensure that there are appropriate communication structures in place. It seems both sides can suffer from information not being delivered often enough, in sufficient detail, and in a way that makes it most easy to act upon.
- Some contractors lamented that they were not given access to a sufficient number or level of, stakeholders to understand or explain problems and co-ordinate solutions. Consider who needs to be involved in liaising (directly or indirectly) with contractors to maximise their input.
- You need to consider what information you can share and at what point. When tendering contractors make the point that the more they understand about the organisation and its risks and priorities the more accurate and focussed their tender can be, this includes the solutions they recommend and also the costs.

- Indeed, the more the contractor understands your aims and objectives the greater their potential to help you achieve them. Think about how much information you can share with your contractor. One tip suggested was to consider each bit of information in turn and ask yourself the 'why would I not share this'.
- Contractors reported that it would be very beneficial if they could see a copy of the security strategy, where this occurred they felt that they were providing a much better service to their clients. Sharing the strategy, or the relevant parts of it, can be beneficial in a number of ways:
    - It helps the contractor understand the organisation and security department's future intentions so that they can ensure that their solutions support this. This could mean the difference between recommending technology that will continue to be appropriate in the future, versus technology that will not be fit for purpose as the organisation changes.
    - It ensures that they understand your priorities so that they can help you to achieve them.
    - It helps them to identify any ways that they can adapt or improve their service delivery to meet your objectives
    - It affords the opportunity to align their performance measurement metrics with your strategic aims
    - Overall it means that they are working to ensure that your strategy is successful.
- Some contractors noted that occasionally they are viewed as a threat in that by being efficient they can make internal security personnel look weak or inadequate. Contractors noted that it was actually in their interest to make internal staff look good, and the more they understood strategic aims (and personal objectives) the more they could help them.
- To be effective contractors will often need your help. Manned guarding is an example, as the security officer works on your site you will often have a role to play in supporting officers' work. You need to be clear how you need to help, what your company needs to do (or is prepared to do) and implement a plan accordingly.

> *"The more we know the better; lots of companies are very conservative bordering on paranoid about sharing too much information."*
>
> *"[Clients] have to fully engage they have to share all of their challenges only then can a security provider provide more than just a product."*
>
> *"We work with the contractor as a partner rather than an adversarial relationship. One of the most useful things we do is that we're willing to share with him what we buy the equipment for and agree with them the margin we make. It makes the supplier relationship much better as there's a degree of trust there that isn't there otherwise."*

- Consider involving your contractor in the development or refinement of your strategy. Suppliers have a lot of knowledge of working with many clients and this can also get buy in from them to meeting your needs. Some providers felt that clients could get more from them.
- You may even want to consider including managing contractors as an objective in your strategy, for example to work closely with contractors in order to create competitive advantage.

A good reference manual

'You & Your Contractor: a manual of best practice for contract and relationship management practitioners' is a very useful reference that guides you on the tactics you need to adopt to get the most out of working Key success factors include:

- mutual trust and understanding;
- integrity, honesty, openness and good communications; and
- a joint approach to managing delivery.

It was produced by the London Centre of Excellence (LCE) & London Fire & Emergency Planning Authority (LFEPA) (http://www.lcpe.gov.uk/Library/CRMGT_Project/1288%20LCE%20You%20&%20Contractor%204b.pdf).

4.6 Implementation plan

Having a good plan that clearly states how the strategy will be implemented is important to ensure that the objectives are met. It is worth noting that evaluations of many strategies have found that they fail because of poor implementation. This section will provide a summary of what a security plan is, what it should contain, how and when to review it and some examples of the kinds of areas that it might cover.

What is an implementation plan?

Before we start to think about plans it is useful to understand how these differ from strategy or policy statement. Generally:

- A strategy means the long term direction.
- A policy statement is an organisation's standpoint on a subject documenting how it will operate and respond.
- A plan documents the actions required to meet a desired outcome or end point.

In order to ensure that the strategy is effectively implemented it will need a more detailed plan of the actions required to meet the objectives to support it. This is sometimes known as an implementation, business, project or strategic plan. The general consensus is that you cannot have a strategy without an action plan to deliver it. The plan will clearly state:

- the specific actions required to meet the objectives in the strategy,
- who is responsible, and
- the timescale for delivery.

The implementation plan

The plan of actions will feed out of the strategy although it is likely to be a separate document to avoid the strategy document itself getting too long. It often contains the plans for the coming 12 months or it might include the actions for the next two years or more.

The implementation plan should contain actions with key dates for achieving specific targets and explain who will be responsible for carrying out proposed actions. It is a good idea to explore whether your organisation has a standard method for documenting plans and use this structure. However, in the absence of this there is also a template for a security plan that you can use for your own plan here (see Implementation plan template - Microsoft Excel). In the plan we have included:

- The actions required to meet each objective

- The resources
- Whether it is a short, medium or long term priority
- The outcome or measure of success
- And the start and end dates

This is just a guide and you may not want to include all of these in your plan. Here is an example of what one organisation's implementation plan looked like (see Example implementation plan - Microsoft Excel).

When devising your implementation plan you might also want to think about:

- Milestones – These are agreed points in the implementation of the strategy where performance or progress can be reviewed. For example you may decide that you will carry out a review on completion of a significant project, such as a CCTV upgrade.
- Dependencies - These are what your actions are dependent upon and could be financial, human or other. For example, a new manned guarding contract may be dependent on the completion and sign-off of the new procurement policy.

It is important to regularly track progress against the implementation plan; you could do this at say a monthly meeting. This will help ensure it receives the support and attention that it needs.

For the implementation plan to work effectively its content needs to be consistent with the organisational culture (see Understanding organisational culture) and communicated to ensure that all those affected, including employees at every level in the organisation, understand the steps that need to be taken to implement the strategy (see Communicating strategy). Some experts have benefited from having dedicated champions in each business area/function to oversee the implementation of different work streams or action points.

It is a good idea to include quick wins which are easy to achieve. This can help to build relationships and demonstrate the ways in which security can add value to help to obtain buy in for longer term actions or projects.

Updating the implementation plan

At the same time as the strategic review (see Step 4: Strategic Review) the implementation plan will need to be reviewed and updated so that the actions for the coming year can be added and any outstanding actions identified, this should occur at least annually.

In this section:	Step 3: Strategy Implementation	4.1 Understanding Organisational Culture	4.5 More on Managing Contractors
		4.2 Communicating Strategy	4.6 Implementation Plan
		4.3 The Workforce	4.7 Example Implementation Plan Actions
		4.4 Managing Contractors	4.8 Key Issues in Strategic Implementation

4.7 Example implementation plan actions

This is a guide to the sorts of things that some of the implementation plans we saw included, however your actions will depend upon the gaps identified in your strategic analysis stage:

Technology

- Review CCTV coverage
- Upgrade to a digital CCTV system
- Ensure that each building has an access control system
- Ensure commonality of access control technology

Risk assessment and measurement

- Undertake a formal risk review of all sites
- Ensure senior management are kept continually apprised of emerging risks

Security Culture

- Draft and implement a communication plan to raise security awareness
- Identify security champions throughout the organisation to deliver key messages

Training

- Carry out a training needs analysis for all security officers
- Construct and agree a staff training plan
- Accredit all security staff

Policy and Procedure

- Ensure all documented security policies and procedures meet with recognised quality standards
- Ensure all security activities are supported by policies, procedures, checklists, aide-memoire or other terms of reference
- To develop a CCTV Code of Practice

Downloadable documents

Example implementation plan.doc (40KB approx - Microsoft Word)

Implementation plan template.xls (25KB approx - Microsoft Excel)

Example implementation plan.xls (28KB approx - Microsoft Excel)

4.8 Key issues in strategic implementation

This section describes some of the key issues that you may need to consider when implementing your strategy. It outlines some of the challenges you may encounter along the way and suggests ways to overcome these.

The section has been broken down into a number of key areas including:

- Being realistic about how long it will take to develop and implement your strategy
- Keeping your strategy up to date and in line with current risks/threats
- The role of policies and implementation plans
- Understanding your business culture
- Ensuring that employees understand the strategy and how they can contribute to it
- Sustaining focus

Being realistic about how long it will take to develop and implement your strategy

The length of time it will take to develop and implement your strategy will differ depending on the size and culture of your business; if you are a large global business you may need time to tailor the strategy to meet the needs of individual countries and different organisational cultures. For some it may take as little as three months, for others it may take up to a year. Setting realistic timescales to implement and develop your strategy will be of utmost importance (see How long will it take?).

Keeping your strategy up to date and in line with current risks

One of the main difficulties experienced by those implementing strategy is keeping it up to date as a live working document and abreast with current risks. It is important that sufficient time is allocated to review and update your strategy to ensure it remains fit for purpose. An annual review is suggested as the minimum (see Step 4: Strategic Review).

> *"Make sure the strategy is a living document and represents current external threats and the way the company is doing business. It is a living document."*

Policy statement and implementation plans

When considering strategy development and implementation, it is important that you support this with an implementation plan. This should contain information on how you are going to achieve your strategic objectives. (See Implementation plan)

You may also choose to have a security policy statement which runs alongside the strategy. This can also help to gain support for developing a security strategy, highlighting the importance of the security function. (See Security policy statement)

Understanding your business culture

Understanding the culture of your business is important when implementing your strategy. It is important that the implementation of your strategy aligns with the organisational culture (see Understanding organisational culture).

Ensuring that employees understand the strategy and how they can contribute to it

It is important that employees have a clear understanding of the strategy and how they can contribute to it. This requires good communication (see Communicating strategy) and aligning (see Alignment) the organisation to the strategic objectives.

Sustaining focus

In order to ensure that the strategy continues to be recognised as important it is a good idea to have monthly meetings to discuss progress against the strategy (see Step 4: Strategic Review).

Section 5. Step 4: Strategic Review

To ensure that the strategy is working it is important to carry out regular performance monitoring (see Performance monitoring). This will determine whether progress is being made against the action plan and whether objectives are being met.

As well as regular performance monitoring it is important to review the strategy document regularly (see Strategic review), at least annually to ensure that the assumptions on which it is based, and the objectives and mission, are still relevant and appropriate. This review will determine when the strategy needs updating or re-writing. In some cases it may be necessary to re-write the strategy before its end date, due to changes in the economic environment for example.

5.1 Strategic Reviews

This section looks at reviewing your strategy. It explains why your strategy should be reviewed, how regularly and by whom.

Why review your strategy?

You need to review your strategy on a regular basis. Regular reviews will ensure it remains current, responsive to any changing needs and threats, and is capable of meeting your organisation’s key aims and objectives even if these change. It also provides an opportunity to review targets, to ensure that they still focus on what is important to the organisation, and allocated budgets.

When to review your strategy

How often the review takes place depends on the size and complexity of your organisation and the resources that you have available, as well as the extent to which the environment in which you operate changes. Some companies like to review their strategy monthly, some every six months and some on an on-going basis.

However, at the very least you need to review your strategy annually to ensure that the assumptions and objectives are still pertinent. Some of those interviewed highlighted this is good practice in aligning strategic reviews with budget cycles to check consistency between funding and objectives. Similarly, because the security strategy needs to align with the organisation’s strategy it is a good idea to schedule the review for after the corporate strategy is agreed.

> *"It is not something that you pick up once a year and look at; you look at it all of the time."*
>
> *"If the threats change, for example 9/11, then we look at the strategy and say the threat has changed now, and therefore we need to review the strategy. It is not a case of taking it off the shelf every 12 months, it is dynamic and it changes as the threats change."*

At the time of the review you need to determine whether the assumptions and objectives are still relevant, whether the objectives have been met and whether there are any outstanding actions.

As well as the scheduled reviews you may need to review the strategy in response to changing risks and threats; for example, after a major terrorist attack or a recession.

There were many examples given. One security director noted how his hotel chain reviewed its security strategy after the incidents in India where terrorists killed innocent people.

Who should review your strategy?

The best person to review your strategy is someone who is a member of senior management. It may be the person who originally wrote the strategy or the person responsible for achieving its aims. Some interviewees argued it is preferable to have one person responsible for the strategy throughout the whole process.

How to review your strategy

When you review your strategy you may choose to go through a shortened or simplified version of the strategic analysis stage (see Step 1: Strategic Analysis). It is a good idea to tie it into any annual audits or risk assessments that you run so that the information can be fed into the strategy. Indeed, to be truly effective there is no substitute for a thorough up-to-date awareness of all your threats and the appropriateness of all your solutions. The type of questions that you will need to ask are:

- Is the strategy still relevant?
- Review your PESTEL (see PESTEL), has the environment changed?
- Are the threats and risks up to date?
- Are your means of keeping up-to-date risks and threats still robust?
- Is the SWOT still applicable (see SWOT)?
- Are the objectives still appropriate?
- Has the corporate strategy changed? If so, are the security objectives still in line with the corporate objectives?
- Are the performance measures that you have in place still appropriate or could they be improved?
- Are you on target to achieve your strategic goals or objectives?

When to write a new strategy

It is important to remember that the reviewing process should not be a one off exercise; it is an ongoing process and the strategy will evolve over time and need to be refreshed in line with changing risks and threats.

In some cases the strategy may not cover the time period for which it was written, for example if there are significant changes in the environment for which the strategy was not prepared, such as a recession. Similarly you may find that a five year strategy becomes outdated and irrelevant much earlier. This will become evident during your strategic review.

Section 6. Tools

This section contains a range of tools that can be used to help you to develop your strategy, with practical examples from the world of security. Some are basic, for example a SWOT analysis, whilst others are more complicated such as the Balanced Scorecard. What you select will depend on your skill sets (and access to resources for example of specialist expertise) as well as your requirements.

> *"I would use as many tools as possible; I think they all tend to give you different answers SWOT, PESTEL. All tools are useful."*

There are also a range of web based tools available on the internet which you can use to help develop your strategy, including strategic planning software and tools which help you to create strategy maps.

Strategic Analysis

Tool	Use
SWOT	It can help you to identify your strengths, weaknesses, opportunities and threats
PESTEL	It provides a framework through which to explore the environment in which your organisation functions
RASCI	It helps you to identify roles and responsibilities where there may be duplication or lack of clarity
ACT	This can help you to assess your relationship with the senior level of the organisation and identify what actions you need to take to improve the relationship

Strategy Development

Tool	Use
PORCORO	Can help you decide how to respond by making you think about a number of different questions in order to determine the most appropriate solution
VMOST	A simple framework that can be used to guide you through writing the different sections of the strategy

INDEX

The Balanced Scorecard	A sophisticated strategic management system
Management Frameworks	Sophisticated business management methodologies which can be used to support strategy development

Templates

Tool	Use
Strategy Template & Guidance	This provides you with a template security strategy to adapt to your own organisation and guidance on how to complete it
Implementation Plan Template	This provides you with a template implementation plan to adapt to your own organisation

6.1 SWOT

The vast majority of the security directors we consulted with used a SWOT as part of the strategic analysis phase.

This tool enables the user to explore the strengths, weaknesses, opportunities and threats to the organisation. In this way it can help you to identify the organisations' priorities and determine what the security strategy should contain and what the strategic objectives might be.

> *"A SWOT is beautifully simple; it takes complex situations or initiatives and breaks them down."*
>
> *"For the risks running a SWOT is really good to make sure you've covered them all. Pull out the strengths and weaknesses to align with the strategy going forward."*

A SWOT combines an examination of the organisation's internal environment (internal processes and structures) to establish its strengths and weaknesses, alongside an examination of the organisation's micro environment (the sector in which a business competes) and macro environment (influences such as political, economic, technological etc. which affect the whole sector in which an organisation sits). This information is used to establish an organisation's threats and opportunities which can be used to inform your strategy.

When completing a SWOT analysis:

- Keep points short and to the point, justifications should be presented separately
- Include 'soft' facts such as organisational culture and leadership skills not just 'hard' facts such as financial measures
- Put the most important points first

A SWOT Analysis

S	Strengths	These are internal to the organisation
W	Weaknesses	These are internal to the organisation
O	Opportunities	These are external to the organisation
T	Threats	These are external to the organisation

An example of a security department SWOT analysis

Strengths	**Weaknesses**
Good procedures, processes & policies such as risk assessments Senior management support Pro-security culture Good implementation of security measures Good image/reputation	Reliability of data Poor performance measurement Outdated technology Small budget
Opportunities	**Threats**
Integrated technology solutions Improve reputation More alignment with the organisation Better contract management Improve cost effectiveness	Risks – staff theft Loss of data Loss of reputation Legislation – corporate manslaughter

Whilst carrying out a SWOT analysis it is quite easy to lose focus. A technique to avoid this is to focus on the Real Strengths and the Real Threats. Real Strengths are those strengths which are also represented as an opportunity; Real Threats are those threats which also appear as weaknesses. For example:

	Opportunity	**Threat**
Strength	**Real Strengths:** Good procedures, processes & policies such as risk assessments Senior management support Pro-security culture Good implementation of security measures Good image/reputation Opportunity to improve technology	

	Alignment with the organisation Better contract management Improve cost effectiveness	
Weakness		**Real Threats:** Data reliability & performance measurement Outdated technology & staff theft Loss of data Loss of reputation Legislation – corporate manslaughter

How does this inform my strategy?

The areas that fall under your threats or weaknesses feed into your security gap, and will be the areas that you should consider addressing in your security strategy. So, using the real threats listed in the SWOT above your key strategic areas might be expressed as the following realistic and achievable actions:

- Improving data quality and performance metrics. For example by providing local managers with timely and accurate information so that they can respond to and prevent staff theft and data loss and provide comparative data so that managers are able to compare their performance with others.
- Improving technology to tackle staff theft & data loss. For example by providing local managers with procedures and technology to prevent and investigate staff theft and data loss.
- Aligning the organisation with corporate manslaughter legislation. For example by auditing operational practices that have the potential to breach emerging legislation dealing with corporate manslaughter and hold named Directors accountable.
- Identifying the threats to the organisation's reputation and the actions to tackle them.

6.2 PESTEL

A PESTEL can be used to explore and identify the various environmental factors that will influence the success or failure of your security strategy. It is useful to carry out a PESTEL analysis to inform your strategy development. The table shows what the acronym stands for as well as providing examples of the kinds of things that might fall under each heading when you do your analysis.

PESTEL Analysis

P	Political	The role of governments, local or national
E	Economics	World, UK or industry trends
S	Social	Cultural change; demographics; expectations; family change
T	Technology	Technological innovation
E	Environmental	'Green' issues: pollution and waste; cost implications; public opinion; sites and locations
L	Legal	Legislation

It is worth noting that many of the factors will be linked together. For each of the themes you will need to identify the issues that are most likely to impact upon the organisation and or the security function. For example under economic, to identify the likely impact of the credit crunch, or under environmental to identify security issues arising from public concern about climate change. The aim of the PESTEL is to identify key drivers for change, or those factors that are highly likely to have an impact on the success or failure of your strategy.

An example of a PESTEL within a security department

One rail operator found PESTEL a useful tool to inform its strategy development. Prior to carrying out the PESTEL analysis the security manager searched the internet for documents and information relevant to its sector and organisation, such as strategies, plans or available documentation for the following organisations:

- Partner agencies such as Transport for London
- Key stakeholders
- The Local Authority such as the Mayor of London

- The British Transport Police
- The Metropolitan Police
- The Department for Transport
- Transec

In addition they also reviewed CONTEST, the government's counter-terrorism strategy, as well as reviewing information on forecasted terrorist activity or threat levels. The security manager used this information to inform the PESTEL as seen in the table. For each of the themes it considers how they might impact upon the organisation or the security function.

An example of a PESTEL Analysis

Political	• How the government view the rail industry and its responsibilities to prevent terrorism • What will be the likely impact of the general and mayoral elections on the organisation and security?
Economics	• The financial constraints of a fixed fee contract versus growing passenger numbers and how this impacts upon available resources for security • Economic downturn: is this likely to lead to an increase in crime? Is it likely to lead to increased violence to avoid penalty fares?
Social	• How will changing drinking patterns affect the transport network? • The impact of an alcohol ban on transport, what do the security team need to do to respond? • The introduction of £50 penalty fare is this likely to increase staff assaults or the workload for the security team? • Increasing anti social behaviour, graffiti, trespass – how do the security team respond? • Increasing passenger numbers, what impact will this have on incidents? Does the number of security staff need to increase in response? • How will the Olympics 2012 impact the security of the transport network?
Technology	• Home Office guidelines on CCTV means that there needs to be an upgrade for the whole railway network
Environmental	• A review of events that might be targeted by environmental

	activists and how these can be tackled
Legal	• Transec and DfT legislation • The 2007 Manslaughter Legislation • The Data Protection Act and how it affects CCTV data

For each of these areas there are likely to be actions that are required by the security team and these may need to be built into the strategy, for example the upgrade of the CCTV system. At the very least a lot of the information can help to inform the strategy, for example deciding what the organisational priorities are, what the strategy's objectives should be and what actions need to be taken to ensure success. For this organisation counter-terrorism and staff assaults were deemed to be necessary priorities in the strategy.

6.3 RASCI

RASCI is a tool for identifying roles and responsibilities. Because a lot of corporate security functions overlap with other functions RASCI is a good tool to identify duplication and responsibilities. It may also be a useful tool for deciding how business continuity or IT security, for example, fit into your security strategy. It can also help to for assigning roles/ responsibilities when implementing strategy. As one Security Director commented:

> *"The RASCI diagram is the most useful for corporate security. You find a lot of security functions have a huge amount of overlap and this is a good way of highlighting in a non-aggressive way where the overlap is, the dependencies and who's responsible for what. This is key to the delivery of strategy."*

The table shows an example of how a RASCI model might be used for the preparation of a security strategy.

RASCI diagram

A security strategy

R	Responsible	Who is the owner?	Head of Security
A	Accountable	Who is the approver?	Operational Director
S	Supportive	Who plays a supporting role?	Finance Director
C	Consulted	Who needs to be consulted?	The board, senior management, security team
I	Informed	Who needs to be informed?	All staff at differing levels

The table shows an example of an alternative use of the model to identify overlap in the development of IT contingency plans.

IT contingency plans

R	Responsible	Who are the owners?	IT Director, Risk Manager, Head of Security
A	Accountable	Who is the approver?	Operational Director
S	Supportive	Who plays a supporting role?	Finance Director, Operations Director, Insurers through Corporate Secretary
C	Consulted	Who needs to be consulted?	The board, senior management, security team
I	Informed	Who needs to be informed?	All staff at differing levels

6.4 ACT

The ACT acronym can be useful to help you to assess your relationship with the senior level of the organisation and may help to identify what actions you need to take to improve the relationship. As presented here, ACT comprises three dimensions of the relationship and some tips on how you can impact on each or measure the strength or otherwise of your relationship.

Without access, credibility or trust you are unlikely to be able to influence the leaders of the organisation.

Access	Do you have access to the key decision makers? You need this to be able to understand what is important to them.	You can assess this from the number of times you are in contact with them in a business rather than social setting; the number of occasions when you have been invited to deal with specific issues and the times on which you have represented the company during external events.
Credibility	Do you have credibility with them? Without this you are unlikely to be able to influence their decision making.	You can assess this from the number of occasions on which you have successfully resolved or impacted positively upon important events affecting the business or the number of times you have been invited to be part of an internal working group or similar.
Trust	Do they trust you? They need to see you as working in co-operation with them, not undermining or competing with them.	You can assess this from the way in which you have handled sensitive information or investigations or events within the organisation.

6.5 PORCORO

PORCORO is a tool that can help with strategy development. It can walk you through a decision making process by making you think systematically, first about a number of headings, and then about some important questions under each heading. The result is intended to ensure that the strategy is relevant, achievable and realistic. The table shows the PORCORO headings and related questions.

Purpose	What is the purpose of the strategy?
Outcome(s)	What are the desired outcomes?
Resources	What resources (human, financial, technological) do you have and what do you need?
Constraints	What are the constraints, such as resources, skills or lack of support?
Options	What are the different options to achieve the desired outcomes?
Risks	What are the risks of implementing the various options?
Opportunities	What opportunities do the various options create?

The table shows an example of how a PORCORO might be used.

Purpose	To improve security across the organisation concentrating on five priorities providing the greatest savings or other benefits to the organisation
Outcome(s)	To reduce the number of serious incidents impacting directly upon the business and to reduce the fear of crime whilst at work
Resources	The security team, consultancy support to draft the strategy
Constraints	Lack of support from the board, shortage of necessary resources, access to resources when required
Options	New technology
Risks	Costs of, dependency on, and the reliability of, technology
Opportunities	Integration of existing technologies to reduce costs

6.6 VMOST

VMOST is a simple strategy framework that can be used to guide the development of strategy. It walks you through the various parts of a strategy document such as the Vision, Mission and objectives.

VMOST diagram

Vision (see Mission & Vision)	The security function's aspirations
Mission (see Mission & Vision)	The security function's overriding purpose
Objectives (see Objectives)	The specific outcomes to be achieved in order to meet the vision
Strategy	The overarching measures undertaken to meet the objectives
Tactics	The specific actions required to meet the objectives

An example of a VMOST framework for a transport operator

Vision	To be seen as the most secure transport network in the United Kingdom
Mission	Improve security across the network
Objectives	Minimise the risk of terrorist attacks; improve the use of security technologies; reduce the number of staff assaults
Strategy	Focus on reducing crime levels; increasing passengers' perception of safety; and implementing counter terrorism tactics
Tactics	To obtain the secure station's accreditation, increase the number of security staff, etc.

One security manager used VMOST to present his strategy in a business format which executive directors would recognise. He wanted to steer away from security jargon and use the language of the business to encourage buy in from the board. He reported that VMOST:

> *"…worked really quite well, I quite liked it and stuck with it. I think that has helped to achieve buy in. They recognise the format; it's [the strategy] a professional document that they would be happy to have produced."*

6.7 The Balanced Scorecard

The Balanced Scorecard[1] is a strategic management system created by Kaplan and Norton which provides a useful, well used and recognised process for managing strategy. It is a sophisticated tool and is best applied where a strategy is already in place. The Balanced Scorecard translates a company's vision and strategy into a coherent set of performance measures. The four perspectives of the scorecard--financial measures, customer knowledge, internal business processes, and learning and growth--offer a balance between short-term and long-term objectives, between outcomes desired and performance drivers of those outcomes, and between hard objective measures and softer, more subjective measures. The scorecard can be adapted to fit the needs of a security function.

Indeed Kaplan and Norton also describe how to align the security function with the overall business strategy and other departmental strategies. The framework ensures that people and processes are focused on delivering the strategy. It also provides a framework to enable you to align your supplier relationships to ensure that they understand and work to meet your strategy.

For more detail please see Kaplan, R. and Norton, D. (1996) Translating Strategy into Action: The Balanced Scorecard. Harvard Business School Press: Boston http://harvardbusinessonline.hbsp.harvard.edu/b02/en/common/item_detail.jhtml;jsessionid=W4HTQUXJKSQPUAKRGWDSELQBKE0YIISW?id=6513&referral=2340; and Kaplan, R. and Norton, D. (2006) Alignment: Using the Balanced Scorecard to Create Corporate Synergies. Harvard Business School Publishing Corporation: Boston http://harvardbusinessonline.hbsp.harvard.edu/b02/en/common/item_detail.jhtml?id=6905&referral=2340

Case Study

One security team used the Balanced Scorecard alongside their strategy as a measurement tool. Their scorecard had six themes which relate to the objectives in the strategy:

- Safety
- Customer: Quality of Service
- Commercial
- Financial
- Efficiency and Productivity
- People

[1] Kaplan, R. and Norton, D. (1996) Translating Strategy into Action: The Balanced Scorecard. Harvard Business School Press: Boston

Under each theme sits a number of performance measures, for example:

Theme	Example of performance measure
Safety	Number of assaults
Customer: Quality of Service	Number of incidents, such as theft or fraud
Commercial	The terrorist threat assessment + the current response level
Financial	Total cash loss
Efficiency and Productivity	The number of successful prosecutions
People	Sickness absence

These are measured and monitored regularly and used to determine whether the objectives that they relate to in the strategy are being met.

The Security Director commented:

"It's a means of simply articulating what could often be very complex subjects and difficult to define. A scorecard forces you to think about what you're trying to achieve, e.g. we'll put in access control etc., with the scorecard you have targets that can be measured. It enables you to evaluate strategies and ensure they have a tactical application."

6.8 Management Frameworks

Aligning with the company methods

In some cases your strategic development process will have to align with those already in place within the organisation. An example of these are the Six Sigma or Hoshin Kanri processes. Both are sophisticated methodologies encompassing strategic planning with process development and change management. They cannot, however, be applied to the security function alone, they need to be driven throughout the organisation from the senior management team or board.

Case Study

One major American investment bank used Hoshin Kanri as a tool to guide their strategy development. This is a sophisticated Japanese strategic management process or '*systems approach to management change in critical business processes*'[2]. Objectives are set from the top down which then feed throughout the organisation and its processes including budget setting and process development to create alignment throughout the organisation.

> *The bank had been using the process for at least five years. The International Security Executive described their process:*
>
> *The president or chairman sets the business objectives, of which there are three types:*
>
> 1. *Customer*
> 2. *Shareholder*
> 3. *Staff*
>
> *Based on the business objectives the corporate security department is given two to three specific objectives from which the security strategy is developed. The objectives then feed into individuals' objectives, personal development plans, training, salary and bonus payments to provide a holistic approach. Furthermore the process involves networking with each line of business and agreeing service level agreements with each of them.*
>
> *The strategy is updated annually; however the whole process is repeated every two to three years.*

The International Security Executive commented:

"…it intimately ties in the corporate security strategy to the business strategy, which is very important when you get to the practical levels of financing and measuring the strategy."

[2] Akao, Y. (Ed) 1988 Hoshin Kanri: Policy Development for Successful TQM, Productivity Press: New York

This is a simple explanation of how the Hoshin Kanri process can work within an organisation. It has to be a top down process from senior management which will apply to all functions of the organisation, including the security department. Therefore Hoshin Kanri really needs to be implemented by the board or senior management team. For more information on using the Hoshin Kanri process see Akao, Y. (Ed) 1988 Hoshin Kanri: Policy Development for Successful TQM, Productivity Press: New York.

Section 7. Glossary

Added value	The benefits, including economic and other (sometimes referred to as 'hard' or 'soft'), that the strategy will bring to the organisation.
Alignment	Ensuring that the security strategy is focused on the organisation's priorities.
Awareness raising	Getting people interested in security, to make them realise that it affects them.
Board	The Board, sometimes know as a Board of Directors, Board of Trustees, or Advisory Board, are the ultimate decision makers for the organisation.
Business continuity management	Planning to ensure that your organisation can continue to function in the event of an unforeseen event.
Business strategy	A business unit strategy, for example a subsidiary company.
Chief Executive Officer	This is the operational head of the organisation, they may also be known as the Director or Managing Director as opposed to Chairman or President.
Competencies	These are capabilities, for example defined processes or technical or subject matter knowledge.
Competitive advantage	The advantage that one organisation has over its competitors.
Consultation	Seeking information, advice or agreement from others, this can be done one-to-one or in a group setting.
Corporate strategy	The overall purpose of an organisation. The strategy for the whole organisation.
Crisis management	Crisis management deals with how an organisation manages the wider impact of a disaster, such as a flood or terrorist attack, and providing the best response to that crisis.
Dependencies	What your actions are dependent upon and could be financial, human or other.
Deliverable	A tangible or intangible object achieved as part of the implementation plan.
Disaster recovery planning	The recovery processes in response to a natural or manmade disaster, for example preparing for the recovery or continuation of the technological infrastructure of the organisation.
Education	Provides information about the security threats and vulnerabilities and what they can do to protect themselves.
Functional strategy	See operational strategy.

Goal	General statements of aim or purpose.
Hard benefits	Value added usually described in financial terms.
Implementation plan	Sometimes known as a business, project or strategic plan which will document the various actions required to meet the strategic objectives.
Milestone	These are agreed points in the implementation of the strategy where performance or progress can be reviewed.
Mission statement	Documents the overall purpose of your security function.
Objective	The specific outcomes to be achieved in order to meet the vision.
Operational strategy	How parts of the organisation deliver the corporate strategy, e.g. the security strategy.
Opportunity	Areas for potential development or improvement external to the organisation.
Organisational culture	The shared culture, or beliefs and values, of the people within an organisation.
Performance monitoring	This will determine whether progress is being made against the action plan and whether objectives are being met.
Performance targets	Targets used to measure performance, of the strategy for example.
PESTEL	A tool that helps you to analyse the environment in which your organisation functions.
Plan	The actions required to meet a desired outcome or end point.
Policy	An organisation's standpoint on a subject documenting how they will operate and respond.
Resource	These are available assets and include physical and financial assets, as well as human resources such as employees.
Security audit	An intensive review of the security function.
Security gap	The difference between the security function's capability and what it needs to be to allow the organisation to meet its long term objectives.
Security risk assessment	A review of the organisation's security risks and how they will be responded to.
Security risk/threat	Something which could have a negative impact on the security of the organisation, including its property, assets, staff, data or reputation.
Soft benefits	Qualitative added value such as increased staff morale.

Stakeholder analysis	A stakeholder analysis identifies the individuals or groups who are likely to be affected by the strategy and their requirements.
Strategic analysis	The first step of the strategy process, an analysis of the organisation and the environment that it is operating in to be able to make informed decisions.
Strategic review	A review of the strategy to ensure that it is still relevant and fit for purpose.
Strategy	The long term direction.
Strength	An organisation's strengths, these are internal to the organisation.
Tactics	The specific actions required to meet the objectives.
Threat	The threats to the organisation, these are external.
Training	Teaches people new behaviours.
Value proposition	This concisely documents what you do in terms of tangible results for the organisation.
Vision statement	Documents the security aspirations for the future.
Weakness	An organisation's weakness, these are internal to the organisation.

Perpetuity Research & Consultancy International Ltd
148 Upper New Walk
Leicester
LE1 7QA
United Kingdom
Tel: +44 (0)116 222 5555
Fax: +44 (0)116 222 5551
www.perpetuityresearch.com
prci@perpetuitygroup.com