Global Information Assurance Certification Paper

Strategic planning for information security

Robert Wentworth

GSEC (Assignment 1.4b)

Option 1 – Research on topics in information security

Abstract

This document provides a model for building a strategic plan for information security aligned to corporate business direction, from an Australian perspective.

Key elements in the model include strategic business objectives, core security functions, security objectives, constraints, strategies and initiatives.

Contents

1 Overview

Business managers expect information security to protect information in business systems and prevent the systems from being interrupted.

Information security supports the business in achieving its objectives. To begin the development of a strategic plan for security it is essential to understand the business objectives and the key elements of the information security function.

Business objectives can be analysed to identify dependencies on security. The security objectives can then be defined in terms of the business objectives.

The security objectives are then impacted on by business and environmental constraints, and by threats and vulnerabilities.

Metrics are developed to allow comparison between current security capability and the capability required to meet business requirements.

Strategies can be developed to fill the gap between current and planned capability while allowing for environmental constraints and threats.

A strategy is the direction or the approach taken to meet one or more objectives. Strategies do not have priorities: they are mutually exclusive.

Each strategy is supported by one or more initiatives. An initiative is the implementation of an operational plan that achieves part or all of the security objectives.

The overall objective is to implement a range of initiatives that collectively achieve all of the security objectives.

2 Purpose of a strategy

The purpose of a strategic plan for security is to provide management with the necessary information to make informed decisions about investment in security. The strategic plan links the security function with the business direction.

The strategy must present a business case that describes key business benefits and outcomes related to security, with recommended strategies for achieving those outcomes.

Strategies for security help achieve business objectives by identifying and addressing security requirements in business functions and initiatives, and providing infrastructure, people and processes that meet those requirements.

Although driven by business requirements, strategies must take into account other factors that may impact on the achievement of those outcomes. The strategies must be revised periodically to allow for changes in the business direction and in the constraining factors.

3 Security functions

As the strategy describes business outcomes related to security, the scope for security strategy is defined by an organization's definition, or scope, of its security function.

The security function should be defined by objectives. Security objectives are well documented in relevant standards*.

> E.g. The objective of security at <organization> is to protect information and information systems and prevent unauthorised access, unauthorised modification or damage, or interruption to business functions.

Under company law, directors are obliged to take reasonable actions to protect company assets. Reasonable action can be demonstrated by aligning an organization's security functions with industry standards.

Security functions can be strategic, tactical or operational. Security functions are implemented in terms of technology, processes and people.

Security functions should be documented with accountability against organizational roles.

Accountability for security functions may be concentrated in a single security group, or allocated to other areas that have common objectives. For example, the accountability for business continuity may be allocated to an operational support group. A security strategic plan should include objectives for all security functions regardless of where they are placed within the organization.

4 Strategic business objectives

Strategic business objectives are the highest level, or fundamental, objectives of the organization. At the conceptual level these objectives relate to the prosperity of the organization and all of its stakeholders. When enumerated by the business the objectives become more descriptive and may include the following:

- to reduce costs by efficiency gains
- to reduce potential costs through risk reduction
- to protect assets
- to create opportunities for revenue growth by
    - enhancing or creating customer services and products
        - by creating competitive advantage

---

* In ISO 19977 (1) the key functional areas defined are security policy, security organization, personnel security, asset classification and control, physical and environmental security, computer and operations management, system access control, system development and maintenance, business continuity planning, and compliance. The management of security functions is defined in AS 7799.2 (3).

        - to extend the customer base
    - enhancing or maintaining reputation in the marketplace
    - reducing time to market
    - marketing/advertising and channel management

Business objectives are implemented through a range of business strategies.

Strategies will vary greatly between organizations. Example business strategies may include the following:

- Building infrastructure to provide extended customer functions
- Joint venture or mergers to improve market position
- Outsourcing to achieve flexibility and cost reduction

Business strategies will be achieved through implementation of a range of business initiatives.

5 Strategic security objectives

5.1 Determining strategic security objectives – Method 1

Security objectives are the sub-set of the business objectives that can be achieved by application of the security functions.

To determine the security objectives, evaluate the potential for each business objective or initiative to be impacted by each security function.

For example, consider the business objective of increasing revenue through reduced time to market. The first two security functions from ISO 17799[1] are evaluated for impact on that objective.

How does security policy impact on time to market?

> Policy provides a statement of acceptable risk. If security policy does not define protection requirements for sensitive information, then development may be delayed while the risk is assessed and security controls defined.
>
> At the same time, stringent policy requirements may also delay the development of system enhancements, and may even preclude some business initiatives as excessively risky.
>
> The security objective would be to optimise between policy that defines the minimum controls - giving best time to market, minimum cost and maximum business enablement - while keeping residual risk below an acceptable threshold.

How does security organization impact on time to market?

> Security organization ensures that accountability for security functions has been allocated to organizational roles. If security functions have not been effectively allocated, delays could be incurred at any point of the development lifecycle that depends on a security function. For example, if

inadequate resources have been allocated for security assessment, there may be delays in getting approval to promote a system into production.

The security objective would be to ensure that security functions are supported adequately to prevent delays in getting products and services into production.

Continuing the evaluation to assess the impact of each security function on each business objective will produce security objectives directly aligned with business objectives.

This method may be more relevant when revenue and growth is a priority.

5.2 Determining strategic security objectives – Method 2

Method 1 starts with business objectives and identifies where security functions impact them. Method 2 should arrive at the same result from the other direction. Start with each of the security functions and create a scenario showing the potential impacts to the organization should the security fail. The security objectives for each scenario are then to implement security that prevents those impacts.

For example, consider the security function to manage access. In a scenario where access management fails, a hacker might gain access to an internal server and expose information from business partners. Information may be commercial in confidence and also contain information subject to information privacy legislation. Resulting impacts could include:

Parties whose information is exposed seeking penalties for breach of non-disclosure agreement, and also seeking to recover subsequent losses;

Customers using alternative service providers. The organization's reputation and revenue is adversely impacted;

Exposure resulting in breach of privacy legislation, litigation costs, penalties and impact on reputation.

The security objectives from this scenario could include:

to prevent hackers gaining unauthorised access to internal servers;

to ensure adequate controls are in place to reduce the risk of claims under privacy legislation should exposure result in such claims.

Scenarios should be developed to cover each security function. Multiple impacts may be associated with each function.

Further validation can be attained by including scenarios for actual losses previously incurred by the organization, or by including potential losses from risks identified in recent audits or recorded in risk registers.

In addition to event-based scenarios (e.g. failure of security controls) also consider pre-event scenarios. Using the security assurance function as an example, if customers perceive that security in a web service is inadequate they may not take it up, resulting in lost revenue.

This method may be more relevant when reducing cost is a priority.

5.3 List of strategic security objectives

Having determined the security objectives using either (or preferably both) of the methods above, the rationalised list of security objectives now describes the purpose of the security function.

Security objectives must be achievable by the security functions. Security objectives will vary across organizations. A list of possible security objectives, including how they are achieved by security functions follows:

- Objective – to reduce security events
    - Security functions can alter the likelihood and impact of security events. For example, access management can prevent unauthorised access. Reduction in security events will reduce system interruptions, reduce costs arising from business interruptions and from recovery, protects reputation and existing revenue streams, reduce information exposure and damage, and reduce legal penalties.
- Objective – to provide security infrastructure that reduces development costs
    - Security functions can implement security infrastructure (e.g. authentication services, access management and provisioning, identity management, key management) that can be re-used by multiple systems. Re-use reduces development costs and also reduces complexity.
    - Infrastructure may provide revenue-generating opportunities through product differentiation.
- Objective – to reduce operational costs
    - Security functions can reduce operation costs by increasing the efficiency of providing services, such as access control mechanisms.
    - Security functions can reduce insurance costs by reducing the risk profile of the organization.
- Objective – to reduce development costs
    - Security functions can reduce development costs by imposing minimal security controls, by providing infrastructure to reduce the cost of developing controls, by providing policy that reduces the need for risk assessments,

by providing processes that ensure security requirements are identified early in development and avoid late requirements and rework.

- Objective – to protect assets
    - Security functions can protect assets by performing risk assessments and security reviews to ensure assets are effectively protected.
- Objective – to reduce fraud
    - Security can reduce fraud by imposing access controls that limit opportunities to modify information for financial gain. Security can also impose logging and monitoring to identify unauthorised activities during or after events. Monitoring can be a deterrent.
- Objective – to achieve certification to standards for revenue growth.
    - The sales team may be able to generate more revenue when company systems and processes have a recognised security certification. The business objective is revenue growth. The security objective is to achieve certification to meet business requirements set by sales and marketing.
- Objective – to reduce legal penalties
    - Security can reduce the exposure to legal penalties by establishing policies and procedures that demonstrate due care.
    - Security can protect personnel from personal liability and damages by establishing policy and procedures that make people accountable for their own actions.
- Objective – to reduce third party claims.
    - Security functions can reduce third party claims by reducing events (as above), and by adding security requirements to contracts that avoid liability for security events.
- Objective – to provide consulting to reduce risks
    - Consulting can reduce risks by identifying vulnerabilities and risks in business processes and projects during risk assessments and security reviews.

6 Measuring security outcomes

6.1 Metrics

Once security objectives have been identified, an organization must chose methods that demonstrate when those objectives have been met or not met.

Metrics must be established that show if security is effectively achieving the security objectives.

Strategies for implementing security cannot be achieved unless their impact on security objectives can be assessed either qualitatively or quantitatively.

Typical management process includes planning for an outcome, implementing a process to achieve the outcome, measuring the results, and using the results as a measure of effectiveness to improve on the original plan.

The process for the management of security is atypical in this regard. Security assurance cannot be measured in terms of the "results" where there are none. Major security events may never occur, or occur very infrequently.

There are also limitations on assessing security in terms of the likelihood of impacts occurring.

Consider a scenario in which there is a one in a million chance in any given year that there will be a security breach resulting in a $50 million loss. The probabilistic loss rate is $50 per year. Therefore any mitigation plan to reduce the risk must cost less than $50 per year to provide a positive return.

For straight-line risk tolerance, definition of acceptable risk levels is limited by the difficulty in determining the true probability of the event and the true loss that may occur.

In practice, risk tolerance is non-linear. Organizations tend to exhibit increasing aversion to high level impacts despite very low likelihood of occurrence.

Furthermore, security events are not as simple as the product of likelihood and impact as often used. Due to the nature of security incidents they are typically based on a number of successive events. A simple vulnerability may result in a low impact event. There is a lower probability that this will be exploited into a higher impact event. Successively unlikely events will result in successively higher impacts. Therefore, a security event has a risk probability function showing decreasing likelihood with increasing impact.

Likelihood may be indicated by history of previous events if available. Typically there is no history of high impact events.

Security assurance needs to be measured in terms of the reduction in this risk probability function. Security assurance also needs to be measured in terms of each of the security objectives.

For example, metrics for the first security objective derived above (to reduce security events) are described as follows:

> Objective – to reduce security events
>
> Metric – The reduction in risk of security events can be measured in the following terms:

- Security can be measured by a system's resistance to a range of penetration and/or vulnerability tests.

- Security can be measured against benchmark implementations. For example, the security of an NT server could be measured by assessing compliance with the CIS Benchmarks [(5)]. Other industry standards include ISO 17799 [(1)], AS 7799.2 [(3)], ISO 13335 [(6)] and AS 4360 [(7)], FIPS 191 [(8)], and SSE-CMM [(9)].
- Security controls can be measured analytically. This might be done by measuring the number of Top 20 twenty vulnerabilities [(10)] occurring across critical services within the organization.

  Metrics should be customised to reflect organizational objectives and values.

This assessment should be continued to establish metrics for each security objective. This task is demanding but essential to providing the context for risk assessment.

As the requirements for security controls change rapidly in response to changes in business initiatives, legislative requirements, customer expectations and new technology, measurement of security should also distinguish between the effectiveness of existing controls, and the capability of the organization to maintain the desired level of security assurance.

Each security measure should be assessed in terms of current effectiveness, and the organizations ability to maintain that level of effectiveness.

Taking the first metric above (resistance to penetration and vulnerability testing) as an example, the capability would be measure in terms of the processes, technology and resources in place to plan, implement and respond to penetration and vulnerability tests.

One model that measures the maturity of processes is the System Security Engineering – Capability Maturity Model, or SSE-CMM [(9)].

6.2 Current security capability

Once the security metrics have been established it is possible to assess the current (point-in-time) security capability of the organization.

Each of the measures described above should be applied to the organization to produce a statement of capability. This can serve as the baseline against which enhancements and changes to security can be planned and measured.

A sanitized version of this statement of capability could be used to represent capability to customers and business partners.

6.3 Current outcomes

Current outcomes are a measure of the actual security events rather than assurance. Information is collected in regard to actual events impacting on each of the security objectives.

For example, for the objective of reducing security events, the current outcomes will be the number of recorded security breaches and the actual costs arising from that event.

For the objective of minimising litigation, the outcome would be the number of litigations raised against the organization and the actual costs arising from such litigation.

Some objectives will always be difficult to measure, such as reputation. Customer surveys may indicate levels of satisfaction in existing customers.

The current outcomes are used in conjunction with the current capability to define the baseline for security planning.

7 Security vision

The vision is the picture of the future environment, showing how people, process and technology, with work together to overcome constraints and threats, and meet all security objectives.

For example, the vision for fulfilling the security objective of reducing risk to litigation (e.g. obligation for due care under company law) will be achieved by establishing comprehensive policy, procedures and training that either reduce events of information disclosure, or transfer the responsibility to the individual.

For example, the vision for fulfilling the security objective of reducing security events (e.g. in response to increased attacks from the internet and exploitation of vulnerabilities in new technology) will be achieved by a combination of system hardening, segregation of sensitive systems, and enhanced perimeter security that will reduce vulnerabilities to an absolute minimum.

Continue the process and create a vision of the future environment that meets all security objectives.

8 Constraints

In addition to the business objectives and initiatives driving security there are also a range of constraints that inhibit or prevent the achievement of security objectives. These factors may be internal to the organization and controllable, or external and beyond the control of the organization.

External constraints

- Emerging technology (e.g. wireless networking) creates business opportunities but also brings new vulnerabilities and risks.
- Legislation (e.g. information privacy) may increase the potential costs arising from exposure of sensitive information and may create new obligations for providing controlled access to information.
- Customer requirements (e.g. increased connectivity) may increase vulnerability and complexity in internal systems.

Internal constraints

- Cost – organizations tend to vary their level of risk acceptance in response to growth or retraction in the market.
- Architecture – (e.g. authentication systems) may restrict use of strong authentication or inhibit adequate monitoring.
- Culture – organizations with a strong culture of trust may fail to recognise weak security systems. Attitude and awareness play a key role in building effective security.
- Complexity – organizations that are highly responsive to customer requirements may create solutions with increasing complexity and interdependence.

Security strategies must allow for these constraining factors.

9 Threats and vulnerability

Threats and vulnerability also impact on the organization's ability to achieve its objectives. Vulnerability is weakness in a system that can be exploited. A threat is something that may act to exploit vulnerability.

Threats to an organization should be identified and allowed for in setting security objectives. Typical threats include external hackers (script kiddies, criminal, competitors), disgruntled staff and contractors, viruses and other malicious code, and inadvertent action by authorised operators. CSI/FBI survey [(4)] reports show 40% of respondents detecting system penetration from the outside.

Typical vulnerabilities include published system vulnerabilities, poor configuration, inconsistent application of processes and untrained staff.

Security strategies must allow for vulnerabilities and threats.

10 Strategies

Strategies are the plans for moving from the current environment towards the vision. Strategies do not have priorities: they are mutually exclusive. A strategy is a direction, plan or approach to achieving the security objectives while allowing for the influence of the constraining factors.

Use the business objectives, security objectives, and measures of the current capability to identify security objectives that are not fully met. Create strategies to meet those objectives while allowing for constraints and threats.

For example:

> The business objective is to generate more revenue. The business strategy is to create additional connectivity with customers to provided value-added services.
>
> One security objective is to allow the connectivity while mitigating the risk of hacker and virus infiltration to an acceptable level.

Another security objective is to ensure that customer expectations for integrity and availability can be met.

The vision includes comprehensive perimeter monitoring and access controls. The current capability meets existing needs, but will require enhancement to protect new communication channels used to provide the planned increase to connectivity.

External constraining factors could include the technology (e.g. inherent weakness in wireless networking), and the obligation to protect customer information that is subject to information privacy legislation.

Internal constraining factors could include complexity of internal systems. Adding new connectivity may require addition resources to cover essential security monitoring.

The security strategies might be:

- to increase monitoring of external connections. This will mitigate some risk associated with increasing the connectivity.
- to increase the security "hardening" of all customer facing systems.
- to provide redundancy for critical production system components to improve availability of services.

Continue the process to identify strategies for all security objectives. Each strategy must support at least one objective. In total, all of the strategies must meet all of the objectives.

Examine each security objective and ensure that it will be fully achieved if the strategies are fully implemented. If not, further strategies are required.

11 Initiatives

11.1 Setting Initiatives

Initiatives are the operational plans for the implementation of processes, technology and people that achieve the security objectives. Each initiative must support at least one strategy.

Initiatives, if fully implemented, should completely achieve the strategy and its objectives. If the initiatives do not meet all of the objectives, further initiatives should be prepared.

For example, with a strategy of hardening all customer-facing systems, the initiatives might be:

- to configure all customer-facing servers in accordance with CIS security benchmarks [(5)];
- to replace network bridges with switches;

- to rebuild a customer application to allow the business rules to be relocated inside the organizations trusted network;

Each initiative must include assessment of the expected benefits (reduction in residual risk), costs (allocation of funding and resources to achieve changes in technology, process and people), priorities and interdependencies.

In the example above, consider if customer-facing systems will be adequately hardened when these initiatives are fully implemented. If there are further measures that can be taken to harden these systems, multiple initiatives should be identified.

Multiple initiatives provide further opportunity for senior management to determine the appropriate level of investment and acceptable risk by choosing between initiatives.

Owing to the inter-dependencies between strategies and initiatives, changes to timing or acceptance of one initiative may impact on others. For example delays to virtual private networking may impact on delivery of a single-sign-on solution using the same infrastructure (directory service and certificate authority).

Initiatives can be validated against best-practice. Cost effective outcomes may be achieved by following the approach other organizations have used in similar situations and leveraging off their experience to avoid costly errors.

Continue this process to include initiatives for all security objectives.

The strategic security plan should include a summary showing that the initiatives in total meet the strategic objectives, and also produce the future vision as described earlier.

11.2 Accountability and governance

The security function cannot be made responsible for achievement of business objectives outside of its area of control. For example, a security objective may be to provide certification to international standards so that the business can differentiate services on that basis. The security staff cannot be held accountable for revenue generation: that is the sales team's responsibility. The security team can be accountable for achievement of the certification.

When completed, the strategic security plan will have input from business areas to ensure alignment with business direction, and input from information technology, legal services, personnel and other support areas to ensure that the plan is realistic and feasible.

Governance of the security process should be included in the organizations governance process along with risk management. Security reporting should be consistent with risk reporting.

The organization's senior officers will be seeking to demonstrate reasonable care. Question that could be expected might include the following, as provided in the ISACF information security governance guidance [(11)]:

Is management confident that security is being adequately addressed in the company?

What are other people doing and how is the enterprise placed in relation to them?

Does management have a view on how much the enterprise should invest in IT security improvements?

At this point the strategic security plan should be able to answer all of these questions except for the question of the appropriate level of investment. This must be answered by senior management.

The plan provides the rationale behind each of the strategies and initiatives and allows management to invest in security based on the financial position of the organization and the level of risk considered acceptable by senior management.

Senior management will be looking for comparison of the security in their organization against organizations of similar ilk to validate the strategic plan. An approach to determining the cost of security and comparative industry costs follows.

11.3 Cost of security

The cost models for security are still evolving. Models supported by security consulting firms tend to emphasise operational costs backed up by the potential cost of disastrous events in order to generate sales of security services. Such models may understate the significance of other security objectives such as asset protection or legal risk mitigation.

Security costs can be described as being made up of planned costs and potential (risk) costs.

11.4 Planned costs

Planned costs are incurred regardless of the occurrence of actual security events and can be direct or indirect costs.

Direct costs are associated with planning, implementing, and operating security functions. This includes salaries, depreciation on security assets, and maintenance and service changes related to the supply of security functions.

Indirect costs include the cost of insurance (premiums may vary with the level of security assurance).

A strategy showing an increase in planned security spending should demonstrate a reduction in the overall risk profile to the organization, or containment of escalating risk. A reduction in security spending should be reflected in the acceptance of a higher risk profile.

11.5 Potential costs

Potential costs are only incurred if security events occur.

Potential costs are tied into the strategy as optional implementation plans. Different implementations have differing probabilities and impacts. Senior management can adjust the risk/investment balance by choosing between initiatives.

Potential costs need to take into account all of the security objectives and include security events (response and recovery, loss of business, reputation etc), interruption to operations, loss of operational data, exposure of confidential data, contract claims for non-performance, cost of litigation and legal penalties for breach of obligations regarding privacy, copyright, trades practice, company governance, etc.

11.6 Comparative costs with industry

In order to compare company costs with typical industry costs there needs to be an understanding of the elements of the costs being compared. For example, various surveys show that large companies allocate about 5% of their total IT budget on information security. Unfortunately it is difficult to tell if these costs include major elements such as business continuity or application development. Nor does the costing indicate if consistent levels of security have been achieved.

Comparatively high investment, more likely during periods of growth, may indicate a risk-averse culture, or excessive reaction to vendor hype about vulnerabilities.

Comparatively low investment, more likely during periods of reducing profit, may indicate aggressive risk taking, or a lack of awareness at the senior level of the actual level of risk being adopted by the organization.

12 Tying it all together

The overall plan is to provide enough information to the senior management to allow them to make informed decisions about investments in security. They invest to get benefits. To get the investment, security must demonstrate potential benefits, implement to get them, and then demonstrate the benefits have been achieved.

The method provided above creates a strategic security plan aligned with business strategy and direction, and responsive to changes in external constraints.

13 References and resources

1. International Organization for Standardisation
   ISO/IEC 17799:2000 Information technology
   - Code of practice for information security management.
   www.iso.org

2. Standards Australia
AS/NZS ISO/IEC 17799:2001 Information technology
– Code of practice for information security management
(Note - this is the Australian adoption of ISO 17799 [1])
www.standards.com.au

3. Standards Australia
AS/NZS 7799.2:2003 Information technology
– Information security management systems
www.standards.com.au

4. Computer Security Institute
CSI/FBI Computer Crime and Security Survey 2002
www.gocsi.com

5. The Center for Internet Security
CIS Security Benchmarks & Security Tools
Level 1 Benchmark for Windows NT v1.03 (2002, 2003)
www.cisecurity.org

6. International Organization for Standardisation
ISO/IEC 13335-1:1996 Information technology – Guideline for the management of IT security Part 2: Managing and planning IT Security
www.iso.org

7. Standards Australia
AS/NZS 4360:1999 Risk Management
www.standards.com.au

8. National Institute of Standards and Technology
Federal Information Processing Standards (FIPS)
FIPS 191 Guidelines for the analysis of local area network security (1994)
csrc.nist.gov/publications/fips/

9. Carnegie Mellon University
Systems Security Engineering – Capability Maturity Model (1997)
www.secat.com.download/pdf/ssecmm.pdf

10. The SANS Institute
SANS/FBI Top 20 List (2003, updated regularly)
www.sans.org/top20/

11. Information Systems Audit and Control Foundation (ISACF)
Information security governance
– Guidance for boards of directors and executive management (2001)
http://www.itgi.org/resources.htm