6.1 Security Needs Identification for Enterprise Assets

This is the root pattern for all enterprise security concerns. It helps resolve the issue of whether security is really needed and, if it is, what properties of security should be applied for a particular enterprise. Security properties considered include confidentiality, integrity, availability, and accountability.

Example

A new wing of a museum of gemstones is to be opened. The museum has significant previous experience handling gems, and theft is a large enough risk for the museum to want protection from the unauthorized removal of any gems. The museum also has information about the collections, and employee information, that should be protected from damage or deletion, and in some cases should be kept confidential. How can the museum determine the assets that need security protection, and which types of protection?

Context

An enterprise considers security as a significant non-functional requirement. Key business factors and assets of the enterprise are understood.

Problem

An enterprise that considers security to be important must plan for appropriate security in accordance with the overall enterprise business plans. An enterprise may need to address legacy security plans and policies for the enterprise, or develop completely

new ones. The same will apply to any information technology (IT) systems that are major assets of the enterprise. For the IT systems, the enterprise may need to adopt an existing security architecture or specify a new target architecture. To determine the most appropriate security to select and implement, the enterprise must establish its validated security needs.

How can realistic enterprise security needs be explicitly identified?

The resolution of this problem is strongly intertwined with the environment of the enterprise, which consists of the following *forces*:

- The enterprise needs to comply with laws and regulations, such as privacy laws
- It needs to handle sensitive information in a way that protects confidentiality
- It must comply with its own existing policy, especially any security policies
- It needs to provide sufficient protection for mission-critical business assets
- It must ensure that the security employed has minimum potential impact on business efficiency and efficacy—that is, it does not protect more than is necessary
- It must know when undesired events occur
- It must be able to recover from undesired events
- Overall costs need to be minimized

Solution

Systematically and explicitly identify the types of business assets that need protection and determine the types of protection they need. This activity is typically performed by an enterprise architect or strategic planner, and includes five steps:

1. *Identify the business assets* of the enterprise:
   - Information or data assets such as personnel and financial data
   - Physical assets such as personnel and buildings
2. *Identify business factors* that influence the security protection needs of assets, both external and internal to the enterprise:
   - Laws and regulations, such as privacy laws: see [DoJ02], [EU95], [EU02], and [FOIA96]
   - Enterprise partner relationships
   - Enterprise mission, goals, and objectives
   - Desire for strong enterprise financial health

- Business processes, such as accounting and ordering processes
- Sensitive business events, such as the monthly payroll processing
- Locations at which business processes and events occur

3. *Determine which assets relate to which business factors*. Examples include:

   - A privacy law may apply to employee data
   - Certain physical asset types may exist only at certain business locations
   - Selected financial data may need to be shared with an enterprise partner

4. *Identify what types of security may be needed*: see [ISO15408], [CMU03], [DCD+02], and [NSA02]. Our recommended set is:

   - Protection against inadvertent or unauthorized disclosure: confidentiality
   - Protection against inadvertent or unauthorized modification: integrity
   - Making business assets available for authorized use: availability
   - Attribution of responsibility for actions: accountability

   Confidentiality, integrity and availability are the core properties of security literature. Accountability is also important, but it has a different context. Confidentiality, integrity and availability are attributes of an asset, while accountability is not. When someone is specifying security properties of enterprise assets, it is important to identify who is responsible for security related activities, and that is where accountability comes in.

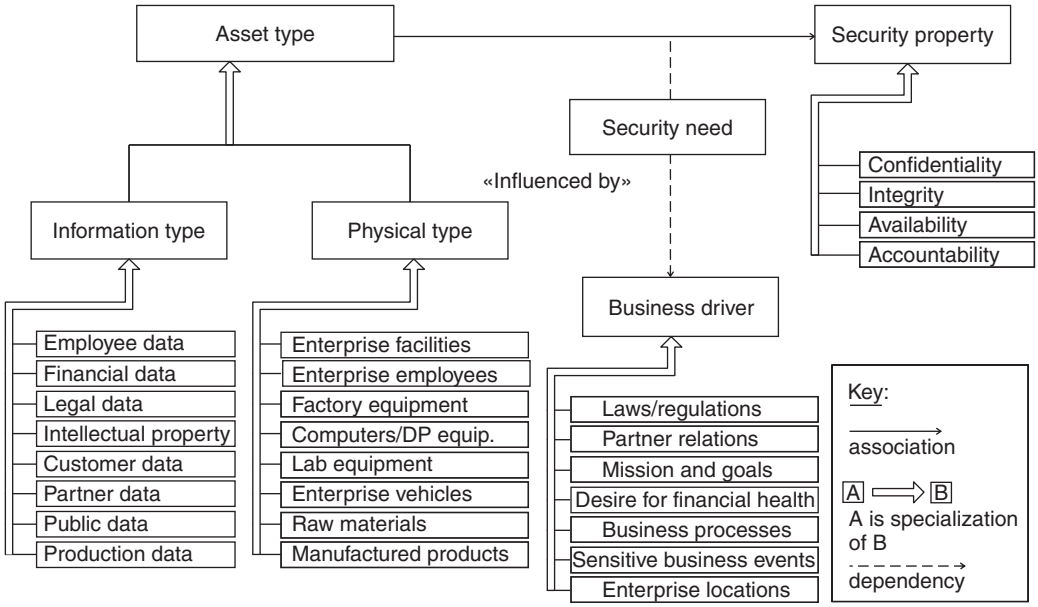
5. Based on the business factors, *determine for each asset type which types of security are needed*. The desire for security must be balanced against the resources required to achieve security in making this determination. More details about the association of common types of assets, types of security needed, and business factors are provided in the Implementation section below.

   These steps can be applied in a linear fashion, as listed, but other alternatives are also possible. The Dynamics section discusses allowable sequences.

Structure

Using the UML class diagram notation, the general relationships among assets, business factors, and security properties are illustrated in the figure below. A *security need* is an association between an *asset type* and a *security property*: each asset type needs a security property. A given asset type may need any number of security properties (0, 1, or multiple), while a given security property may be needed by any number of

asset types. *Business factors* influence security needs. The security properties are listed in the figure, as well as common asset types and business factors:

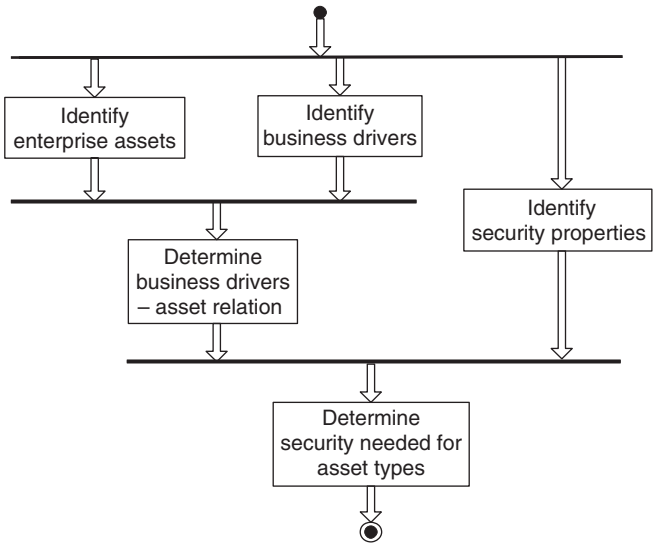


Security needs solution structure

Dynamics

Allowable sequences for performing the solution steps are shown in the figure on page 93. Identifying assets and identifying business factors are essentially independent activities, and can therefore be performed in parallel. However, both activities must be performed prior to determining relationships between assets and business factors. There is often some iteration among these three steps. Defining the set of security properties is also independent, and can be performed in parallel with the first three steps.

Defining properties can also be trivial, providing that the enterprise planner agrees with our suggested set of properties: confidentiality, integrity, availability, and accountability. Some enterprises may want to focus on a subset of these, or add related properties such as privacy, safety, or reliability. Several references discuss this issue further: see [ISO15408], [CMU03], [DCD+02], and [NSA02]. In any case, both defining properties and defining relationships must be performed prior to the last step, determining asset security needs.



Security needs solution sequence constraints

Implementation

Business factors tend to present conflicting forces regarding security. Some, such as laws and regulations, the sensitivity of certain assets, and the desire to be viewed as a secure enterprise, encourage a high level of security. Others, such as cost constraints, the need for financial health, and the desire to be viewed as open and accessible, encourage a minimum degree of security. The result of this trade-off is that assets need to be differentiated according to their importance to the enterprise.

An investment in security is needed for critical assets, while a greater degree of risk may be accepted for non-critical assets. Critical assets typically are those whose loss or damage would cause significant harm to the enterprise, such as assets whose protection is required by law, strategic plans and other assets related to competitive advantage, irreplaceable items, the reputation of the enterprise, or assets whose loss would entail significant cost impact. Non-critical assets are those whose loss or damage would cause little or no harm to the enterprise, such as easily replaceable items, or information that could be divulged with little or no effect.

In addition to criticality of asset, the types of security needed can also vary by type of asset. Confidentiality and integrity typically apply to data. Integrity and availability apply to physical assets as well. Availability applies to services and may also apply to data. Accountability applies to actions taken on assets. To some degree confidentiality conflicts with availability—the more available an asset is, the less confidential it tends to be.

In some cases, one asset or type of asset may require all types of security protection. A software program is an example:

- It may be proprietary, in which case it requires confidentiality
- It needs to be protected against unauthorized change, and it thus requires integrity
- It must be accessible for authorized users, and it thus requires availability
- Any changes made to it must be known and attributed, and it thus requires accountability.

The following tables identify typical asset categories that need protection, the type of security needed to protect the assets, the business factors that influence the need, and some explanatory discussion. The tables provide common examples from an enterprise perspective, but they should not be construed as addressing all possible asset types. Table 6.2 lists and discusses protection of information assets, while Table 6.3 lists and discusses protection of physical assets.

In using the above tables, it is important to understand, first, that the information is generated from an overall enterprise perspective, and second, that specific combinations may vary from those in the tables for a given enterprise.

An example will illustrate both of these points. Table 6.2 indicates that personnel data needs availability, while financial data does not. The reasoning is that, in a typical enterprise, availability of finance information is not needed outside the finance department and the senior officers, while availability of personnel data is needed by multiple parts of the enterprise, such as human resources, finance, training, and

Table 6.2 Common information asset categories and protections

ASSET TYPE	PROTECTION NEEDED	BUSINESS FACTORS	DISCUSSION
Personnel data (including payroll)	Confidentiality, integrity, availability, and accountability	• Privacy laws • Competition issues	Privacy law will require that personnel private information be treated confidentially. Enterprise staff will need assurance that only human resource staff can modify their information. The data will need to be available to human resource staff as needed, and to financial staff to support payroll. Changes to personnel data must be accountable within the enterprise.

Table 6.2 Common information asset categories and protections (*continued*)

ASSET TYPE	PROTECTION NEEDED	BUSINESS FACTORS	DISCUSSION
Financial data (enterprise financial data)	Confidentiality, integrity, accountability	• Reporting requirements of tax collection agency • Competition issues • Nature of the enterprise (public, private, or stock-held)	Financial laws and the regulations of government agencies must be upheld in the enterprise or legal repercussions will ensue. Such laws and regulations will require that the financial data be protected from unauthorized modifications and that when modifications occur, there is a clear record of accountability in the enterprise. No enterprise willingly provides its financial data to its competition; the confidentiality of this information must be protected.
Legal data (for example, contracts and information on legal proceedings)	Confidentiality, integrity, accountability	• Law • Competition issues	An enterprise will need to provide confidentiality under contract law that may also require confidentiality of information related to participants in the contract. The modification of such contracts should be restricted to authorized and knowledgeable personnel and there should be a clear record of accountability in the enterprise.

Table 6.2 Common information asset categories and protections (*continued*)

ASSET TYPE	PROTECTION NEEDED	BUSINESS FACTORS	DISCUSSION
Intellectual property (data and processes)	Confidentiality, integrity, availability	• Partially dependent on the nature of the enterprise (public, private, stock-held) • Some competition issues	While some intellectual information (for example, advertisements) will be for the public, others, such as sensitive business processes, will not. Sensitive intellectual property may need restricted access. At the same time, if the business process contains design specifications, it may also need to be highly available within the enterprise.
Customer and business partner data (including personal and financial data and intellectual property)	Confidentiality, integrity, accountability	• Competitive issues • Service issues if a public company	Enterprise privacy information may be contained in this data. If competitors are aware of the relationships with customers and business partners, they can cause an enterprise to lose its competitive edge. Access to all customer and partner data should be accounted for to ensure that it is not altered in unauthorized ways, and that access to the data is restricted.
Public data (product/service information, advertisements, public enterprise information)	Integrity, availability	• Service issues	Unauthorized modification of the data could result in loss of enterprise reputation and/or business share. When such public information is made unavailable, a denial of service situation arises.

Table 6.3 Common physical asset categories and protections

ASSET TYPE	PROTECTION NEEDED	BUSINESS FACTORS	DISCUSSION
Buildings	Integrity, availability	• Critical business processes	An enterprise needs to protect the buildings that provide a work environment for the enterprise from unauthorized modifications or destruction. By doing so, they also promote the availability of the buildings for the enterprise.
Employees	Availability, accountability	• Critical business employees and processes	An enterprise needs to provide environments that are safe for personnel to ensure the availability of critical personnel. In part they accomplish protecting personnel by establishing accountability for employees.
Raw materials/ durable goods/ manufactured products	Integrity, availability	• Need to minimize the cost of doing business	Raw materials and durable goods need to be available for use in business processes as required. The enterprise needs to be able to assure its client base that manufactured products will be available as required. Damage, theft, or destruction of raw materials/durable goods will make them unavailable to support business processes. Likewise, damage, theft, or destruction of products will make them unsalable to clients.

security. Clearly the finance department needs availability of financial data, but this pattern is an enterprise-level pattern, and across the typical enterprise availability of financial data is not a significant issue. In addition, this table is only representative of common associations. There may be variations for specific enterprises—each will have its own business processes that may differ.

Example Resolved

This example solves the problem identified as the problem example described earlier. The museum enterprise identifies the following asset types and business factors:

Information asset types

- Museum employee data
- Museum financial/insurance data, partner financial data
- Museum contractual data and business planning
- Museum research and associated data
- Museum advertisements and other public data
- Museum database of collection information

Physical assets

- Museum building
- Museum staff
- Museum collections and exhibits
- Museum transport vehicles

External business factors

- Insurance policy constraints
- International laws and agreements relative to on-loan materials
- Privacy laws
- Museum charter
- Goals and strategies relative to exhibits
- Loan of materials and accessions (acquisitions)
- Requirements or constraints of organizations that loan materials

Internal business factors

- Tracking of exhibit items/cataloguing
- Item data, including location and value (both a factor and an asset)
- Exhibit planning, including loan agreements, transport and installation plans and schedules, legal contracting with exhibitors

- Accession (acquisition) planning, via purchase or loan or gift
- Legal data (acquisition)
- Cost constraints, including funds available for acquisition, personnel and patron data (including donation amounts), financial data (how much depends on charter: public, private, semi-public, and so on), and cost of security
- Intellectual property, such as studies and research data, statistics and papers
- Public information, including hours and current exhibit schedules (near term) as well as brochure and exhibit publications
- Building plans
- Importance of enterprise reputation for security
- Importance of enterprise reputation for accessibility
- Sensitive business events, including accession of new items, asset transport to alternate locations, cleaning/caretaking of assets, and special temporary accession for on-loan exhibits

The planner generates a scope statement listing all the above information. The scope statement will be presented to and refined with the museum director. Together they will work to generate an asset protection list such as that shown in Table 6.4.

Known Uses

Identification of enterprise assets and their security needs is best practice, but is often done informally or as part of security risk analysis. A few examples that illustrate concepts in this pattern—and in some cases were sources for the guidance in the pattern—are briefly discussed here.

The Systems Security Engineering Capability Maturity Model (SSE CMM) [CMU03] defines capability levels of a security engineering process, associated with risk assessment. It has elements in common with this pattern:

- It addresses security across the scope of the enterprise
- It addresses coordination of security needs driven from external entities, including laws, policies, standards
- The assess impact process includes identifying and characterizing enterprise assets and the need for confidentiality, integrity, availability, accountability, authenticity or reliability.

PriceWaterhouseCoopers has a process for designing an enterprise security framework that incorporates many of the elements of this pattern [PWC01]. It tailors a security process based on the business requirements and factors of an enterprise. It includes asset inventory collection and information classification.

Mint Business Solutions has defined an approach to security in the context of best practice in enterprise information management [MBS03]. Within this broad

Table 6.4 Establishing security properties for the museum:

ASSET TYPE	REQUIRED SECURITY PROPERTIES	BUSINESS FACTOR
Museum employee data	Confidentiality (HR, management, individual) Integrity (HR, individual only) Availability (HR and management) Accountability (changes in HR)	• Privacy law • Enterprise/employee relations
Museum financial/ insurance data, partner financial data	Confidentiality Integrity Basic accounting	• Contractual obligations • Financial reporting laws
Museum contractual data and business planning	Confidentiality Integrity Basic accounting	• Museum/partner relationships • Protect acquisition and transport plans and strategies • Protect scheduling data • Insurance policy constraints
Museum research and associated data	Confidentiality (restricted to narrow group)	• Museum charter requirements • Intellectual property • Enterprise/employee relations • Enterprise/public reputation
Museum advertisements and other public data	Integrity	• Enterprise/public reputation • Museum charter requirements • Partner reputations for loan exhibits
Museum building	Integrity Accountability (for any change)	• Insurance policy constraints • Enterprise/employee relations • Enterprise/public relations
Museum staff	Availability (safety)	• Enterprise/employee relations • Laws • Enterprise/public reputation
Museum collections and exhibits	Integrity Availability Accounting	• Insurance policy constraints • Enterprise/partner relations • Costs

framework, they base their security approach on the ISO standard 17799. This standard identifies a set of controls that include:

- Organization of assets and resources, with relation to managing information security
- Asset classification and control, so that they may be identified and protected
- Information security policy
- Compliance with any criminal and civil law, statutory, regulatory or contractual obligations, and any other security requirement

These controls correspond to the identification of assets and business factors for security addressed in this pattern.

Other standards and practices, including ISO 13335 Part 3 [ISO13335-3], SANS Institute [SANSa], and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [AD01], discuss asset identification as part of the overall risk analysis process. OCTAVE is an asset-driven evaluation approach that requires an analysis team to identify information-related assets such as information and systems that are important to the organization.

Consequences

SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89) has the following **benefits**:

- It facilitates making balanced and informed decisions about enterprise security needs, by making the competing forces and business factors explicit. The tradeoffs in these factors cause a clear distinction to be made between critical and non-critical assets. The result is increased likelihood that security properties will be applied where needed. That is, protection needs will be explicitly designated for the most critical assets.
- An additional beneficial result of applying this pattern is that traceability of business asset protection needs back to the relevant business factors is produced and is available for additional use. This information offers a useful rationale to support the evolution of security needs over time. It can also be used, as indicated above, as a basis for more detailed protection requirements in ENTERPRISE SECURITY SERVICES (161).

SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89) also suffers from the following **liabilities**:

- Applying this pattern does not come free of charge. It requires an investment of resources, including the time of people who have intimate knowledge of

enterprise assets and business factors. While the benefits of applying the pattern are expected to exceed these costs, it is possible for an enterprise to assign people to this task who have less than adequate knowledge of enterprise assets and business factors, and thus to obtain results that are inaccurate or not useful.

- It is also possible for an enterprise to produce good results from this pattern, but then fail to make use of the results in succeeding patterns.

In both cases, the cost of applying this pattern can exceed the benefits.

See Also

After applying this pattern, the next step typically is to apply a set of risk-assessment patterns to further calibrate the security needs of each asset type to determine more specific security requirements. The set of risk patterns in this chapter help with asset valuation, threat assessment, vulnerability assessment, and risk determination, and assists in deciding how much protection is needed for each business asset type. While SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89) is somewhat internally focused, the risk assessment patterns include both internal and external considerations.

Following risk assessment, the next step is to assess enterprise security approaches that meet the combined security needs and requirements from this pattern and from the risk assessment.