

## 6.6 Enterprise Security Approaches

---

This pattern guides an enterprise in selecting security approaches, that is, prevention, detection, and response. Security approaches are driven by the security properties its assets require, such as confidentiality, integrity, and availability, and by assessed security risks. Security approaches also provide a basis for deciding what security services should be established by the enterprise.

---

### **Example**

A new wing of an existing museum of gemstones is to be opened. Business planning activities have provided an enterprise scope in terms of needs, concerns, and assets. Application of SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89) has identified security properties applicable to each asset type. The dominant asset type for the museum is gemstones. Gems are valuable and should not be stolen or manipulated, so their required properties are availability and integrity. Another important asset type is documentation and records of gem properties, which require confidentiality, integrity, and availability. The museum needs to determine the security approaches most appropriate for achieving these required security properties, and how those approaches should be coordinated for the museum.

### **Context**

Business assets that require protection and their required security properties (confidentiality, integrity, and availability) are understood, for example from applying SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89). Enterprise or business unit security risks (not system risks) are sufficiently understood, for example, from applying RISK DETERMINATION (137) and its closely-related patterns.

### **Problem**

To integrate security into a business model, an enterprise or organization needs to determine preferred security approaches for achieving the security properties of its assets. Planning and operational diligence are security approaches that are always necessary to ensure effective security. In contrast, prevention, detection, and response are security approaches that may be applied in different proportions to each asset type and security property combination. Some business asset/property combinations will have one preferred approach. For example, critical assets that require

the integrity property and that cannot be repaired or replaced will have a focus on prevention, since detection and response do not offer a solution to business impairment. On the other hand, assets that require the integrity property but are not critical, or that can be easily and cheaply repaired or replaced, will have a focus on detection of integrity problems and response (usually replacement).

How can security approaches be selected and integrated across an enterprise?

The forces applicable at the business model level of organization concerns are still abstract and are strongly intertwined with the business processes of the organization. The enterprise needs to resolve the following forces:

- The security properties identified for enterprise assets must be achieved.
- Security risks cannot be eliminated, but can be significantly reduced by a combination of prevention, detection, and response approaches.
- For critical assets, prevention is preferable to recovery, that is, it is better to prevent a violation of security than to have the violation occur and then try to recover from it.
- Prevention is sometimes impossible to guarantee, or is prohibitively expensive. A prevention mechanism can fail in the face of an unforeseen attack, but it can still be effective for the regular case.
- Some detection mechanisms can also facilitate prevention, especially when made obvious, such as a prominently-displayed security camera, or a motion sensor that sets off a loud alarm.
- The costs of providing security must be kept to a minimum.
- Security should have minimal negative impact on business process performance and on users (for example, vendors, clients, staff).
- Continuity of operations must be maintained even in the face of security incidents, and you want to recover in a timely and satisfactory way from security incidents that cannot be prevented (for example disaster recovery).
- It should be possible to analyze security incidents to improve your approach.

### ***Solution***

Specify an integrated set of approaches that achieve the required security protection for each asset type. The process emphasizes two perspectives, namely, the individual perspective of each asset type, and a holistic perspective of the overall organization. For each asset type, systematically and explicitly examine a set of risk criteria to determine appropriate security approaches and their suggested business priorities. Risk criteria involve the security properties for an asset type, business risk analysis results regarding criticality of the asset, and other high-level business operations information.

From a holistic perspective, ensure that the various approaches for asset types complement and reinforce each other, rather than work against each other.

The process of defining approaches is typically performed by an enterprise architect or strategic planner. The first step is to collect all the necessary information, including asset types and their security needs. Next, information on risk criteria that influence approaches is either collected or generated. Finally, approaches are selected and integrated.

### Structure

Table 6.25 shows elements of the structure of this solution. Participating elements include humans involved in defining the solution for a specific situation. Participants also include primary elements of the process of defining a solution: security needs, security approaches, and selection criteria. More details of these three primary elements are also given in the table. The Implementation section gives additional common examples of selection criteria. Multiple criteria apply to each security approach. More than one approach can be selected for each need.

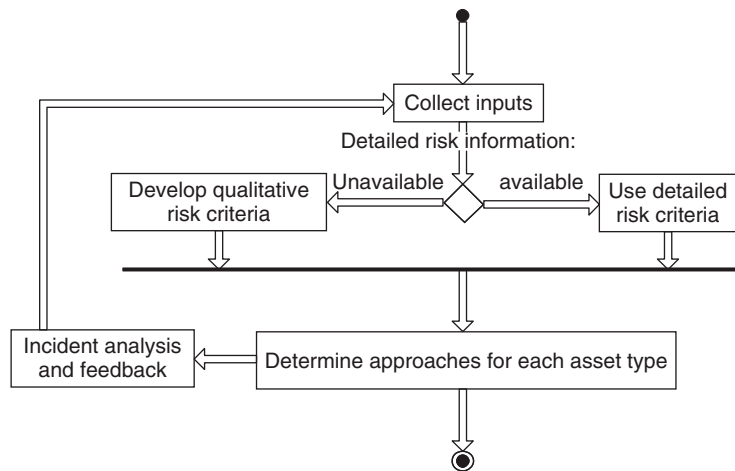
### Dynamics

The process introduced in the Solution section is illustrated in the next figure. The process comprises three basic steps: collect information, identify security risk criteria, and determine security approaches for each asset type. The second step varies depending on whether sufficient risk information is available to understand the risk

**Table 6.25** Table: elements of selecting enterprise security approaches

PARTICIPATING ELEMENT	SECURITY NEED	SECURITY APPROACH	SELECTION CRITERION
<ul style="list-style-type: none"> <li>• Business planner/controller</li> <li>• Enterprise architect</li> <li>• Enterprise security officer</li> <li>• Asset</li> <li>• Security need</li> <li>• Security approach</li> <li>• Selection criterion</li> </ul>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> <li>• Availability</li> <li>• Accountability</li> </ul>	<ul style="list-style-type: none"> <li>• Prevention</li> <li>• Detection</li> <li>• Response</li> </ul>	<ul style="list-style-type: none"> <li>• Assets are irreplaceable</li> <li>• Asset loss prevents operations of critical business processes</li> <li>• Accountability is needed in case of legal ramifications</li> <li>• Assets must be repaired/restored as soon as detection occurs</li> <li>• ... (see implementation section)</li> </ul>

criteria that affect the security approach. If it is not available, some qualitative level of criteria must be developed.



The process for selecting security approaches

The figure also shows an analysis and feedback process. Decisions must be revisited, because the world changes continuously. The figure shows feedback to the ‘collect inputs’ step, but feedback can go to any of the steps. In addition, if circumstances change sufficiently, feedback can extend beyond the scope of this pattern, to re-apply previous patterns such as RISK DETERMINATION (137).

## Implementation

This section first provides further detail on the process, then presents criteria for selecting security approaches.

### Process guidelines

1. Collect necessary input information:
  - Critical enterprise asset types
  - Basic security needs or properties for each asset type
  - Specific security risks for each asset type

Note that asset types and basic security needs might be obtained as a result of applying SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89). Similarly, specific security risk information obtained as a result of applying RISK DETERMINATION (137).

2. Identify security risk criteria that influence approaches:
  - If detailed risk information is available (for example, by applying RISK DETERMINATION (137)), those criteria can be used here to determine which approaches to use: prevention, detection, response (also planning, operational diligence).
  - If such detailed risk information is not available, qualitative risk criteria such as criticality, ease of replacement, cost of replacement, and harm to reputation can be defined and used here.
3. Determine which approaches to use for each asset type.

More details about the association of types of security needed, risk criteria, and approaches are provided below.
4. Revisit approaches for each asset type as circumstances change.
  - Decisions to revisit may be time-driven, for example annually.
  - Decisions to revisit may be event-driven. Examples are: (1) an organization makes a significant change to its business process, (2) a major law is passed that requires specific security measures, (3) an organization experiences a major security incident that calls into question its security approaches.

### Approach criteria

For each asset type, appropriate security approaches and their suggested business priorities are determined based on desired security properties and risks. If detailed risks are available, for example, from applying the risk management pattern system in this chapter, they can be used to determine approaches. If such risks are not known or available, the qualitative selection criteria shown in Tables 6.26–6.29 can be used.

For example, Table 6.26 would be used to help determine approaches. If accountability is needed for an asset type due to legal ramifications, then detection is an indicated security approach with a high priority.

In using the above tables, it is important to understand that the information is generated from an overall organization perspective. In addition, the tables are not intended to cover all situations for a given organization. The example resolved in the next section will illustrate both of these points.

The focus on security approaches is typically documented as part of a security concept of operations. A security concept of operations presents approaches for addressing security properties and how the approaches work together to address security across the organization. The result should balance prevention, detection, and response into an appropriately layered set of defences. Balance is needed among layered asset protections, such as entrances to museum spaces and gem display cases. Balance is also needed for the focus on approaches, such as prevention versus detection and response.

**Table 6.26** Criteria for approaches to achieve accountability

SECURITY APPROACH	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION OF APPROACH AND PRIORITY
Detection	High	Accountability is needed in the case of legal ramifications
	Medium	Validity of business communications and their signatures/sources must be ensured
		Validity of business process flow/ work flow (for example, chain of responsibility or signature) must be ensured
		Assets are in a single or limited number of controllable/ observable locations
Response	High	Means of unauthorized asset access must be closed immediately
	Low	Intrusion claims must be substantiated in order to pursue administrative or legal actions against unauthorized access to assets
		Information asset is non-critical and does not require accountability

**Table 6.27** Criteria for approaches to achieve availability

SECURITY APPROACH	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION OF APPROACH AND PRIORITY
Prevention	High	Asset loss prevents operations of critical business processes
	High	Asset loss could result in irreparable harm to enterprise reputation
	Medium	Asset loss severely impacts operations of critical business processes
		Asset loss could result in serious damage to enterprise reputation
	Low	Asset loss will impact business processes
Detection	High	Asset loss could result in ill will in client and/or customer base
		Total prevention of loss or alteration of assets is not possible
		Detection is cost-effective and prevention is not
		Asset can be replaced though very costly

## 154 Chapter 6 Enterprise Security and Risk Management

**Table 6.27** Criteria for approaches to achieve availability (*continued*)

SECURITY APPROACH	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION OF APPROACH AND PRIORITY
	Medium	Assets are in a single or limited number of controllable/ observable locations
Response	High	Assets must be repaired/restored as soon as detection occurs
		Alterations to assets or other asset characteristics (for example functionality for software assets) must be completely identifiable for repair/replacement
		Means of unauthorized asset access must be closed immediately
		Intrusion claims must be substantiated in order to pursue administrative or legal actions against unauthorized access to assets
	Medium	Assets are of moderate importance to enterprise functions and do not require confidentiality
	Low	Particular enterprise assets interact only with non-critical functions

**Table 6.28** Criteria for approaches to achieving confidentiality

SECURITY APPROACH	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION OF APPROACH AND PRIORITY
Prevention	High	Asset reveals highly-confidential or sensitive information.
	Medium	Asset reveals valuable information.
	Low	Asset reveals information.
Detection	Medium	Information assets can be made available in forms in which no damage can be done (for example, read-only forms, or 'sanitized' versions). Since tools to provide such forms are subject to risk, some protection is still needed.
	Low	Intrusions (that is, unauthorized attempts to read or write protected assets) denied, but awareness of them is needed.

**Table 6.29** Criteria for approaches to achieve integrity

SECURITY APPROACH	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION OF APPROACH AND PRIORITY
Prevention	High	Asset critical and non-replaceable if corrupted or otherwise damaged.
		Asset extremely costly to replace or repair.
		Asset loss could result in irreparable harm to enterprise reputation.
	Medium	Asset very significant and requires long-lead time to replace or repair.
		Asset cost to replace very high.
		Asset loss could result in serious damage to enterprise reputation.
	Low	Asset significant but replaceable.
		Asset cost to replace or repair moderate.
		Asset loss could result in ill will in client and/or customer base.
Detection	High	Permanent asset alteration will significantly impair enterprise or operation of critical business processes.
		Total prevention of loss or alteration of assets is not possible.
		Detection is cost-effective and prevention is not.
		Asset can be replaced although very costly.
	Medium	Validity of business communications and their signatures/sources must be ensured.
		Validity of business process flow/ work flow (for example, chain of responsibility or signature) must be ensured.
		Assets are in a single or limited number of controllable/ observable locations.
		Information assets can be made available in forms in which no damage can be done (for example, read only forms or 'sanitized' versions). Since tools to provide such forms are subject to risk, some protection is still needed.
	Low	Enterprise information assets need to be accurate and support any/all legal needs.



**Table 6.29** Criteria for approaches to achieve integrity (*continued*)

SECURITY APPROACH	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION OF APPROACH AND PRIORITY
Response	High	Intrusions (that is, unauthorized attempts to read or write protected assets) denied, but awareness of them is needed.
		Assets must be repaired/restored as soon as detection occurs.
		Alterations to assets or other asset characteristics (for example, functionality for software assets) must be completely identifiable for repair/replacement.
		Means of unauthorized asset access must be closed immediately.
	Medium	Intrusion claims must be substantiated in order to pursue administrative or legal actions against unauthorized access to assets.
		Assets are repaired/replaced normally within three days of problem detection.
	Low	Assets are of moderate importance to business functions and do not require integrity.
		Assets should be restored within a week, but longer periods will not impair enterprise operations.
		Information asset is non-critical and does not require integrity.
		Particular enterprise assets interact only with non-critical functions.

Business factors tend to present conflicting forces regarding appropriate balance. Some, such as laws and regulations, sensitivity of certain assets, and the desire to be viewed as a secure enterprise, encourage a high level of prevention. Others, such as cost constraints, the need for financial health, and a desire to be viewed as open and accessible, encourage a minimum degree of prevention with reliance on detection/response. In cases in which the risk is sufficiently low, a 'no action' approach may be selected, that is, the approach is to take no measures of prevention, detection, or response. For example, theft of expensive clothes from a shop can be detected by security tags that sound an alarm when the goods are taken outside. But for very inexpensive clothes, the cost of security tags may exceed the cost of a few stolen items. The shop owner therefore may decide to make no response and just write off the loss.

The process of balancing these forces requires assets to be differentiated according to their importance to the organization. An investment in prevention 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 organization, such as assets whose protection is required by law or strategic plans. Other critical assets are those that offer competitive advantage, are irreplaceable items, can impact the reputation of an organization, or whose loss would entail significant cost impact.
- Non-critical assets are those whose loss or damage would cause little or no harm to the organization, such as easily-replaceable items, or information that could be divulged with little or no effect.

Obviously, there are many possible asset value gradations between non-critical and critical assets. Balancing forces and approaches can also exploit a fact that was mentioned in the discussion of forces: some detection mechanisms can also provide a measure of prevention. These are typically cases in which potential violators are made aware of detection mechanisms and possible accountability, such as prominently-displayed surveillance cameras or loud alarms.

It is well known that many considerations are brought to bear at this level in determining an appropriate enterprise security strategy. Management may sometimes levy a requirement to address something specific for security that is realistically beyond what can be accounted for in this pattern. It is strongly recommended that such items be captured, so that when appropriate, they can be tracked through to implementation. In cases in which they are inappropriate, developers of the system model will be forewarned that these requirements will need to be revisited with management.

### ***Example Resolved***

This section outlines portions of the result of applying the solution to a museum of gemstones. Identification of museum assets and their security properties is available from the Example Resolved section of SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89). Museum enterprise architects and planners have completed a business unit risk assessment for the new wing of the museum. The architects and planners must now work to identify security approaches for which the museum will be willing to allocate the resources necessary to achieve the security properties identified.

An example outcome is summarized in Table 6.30 on page 159. The column for ‘Special notes’ has been included to show examples of special considerations and decisions that might be made by management while considering general security approaches.

Note that in the integration perspective, approaches are coordinated. For example, when prevention fails (thief grabs gem), detection and response act as a fallback (laser beam was interrupted, causing automatic doors to close before thief can leave the building).

### ***Known Uses***

The prevention-detection-response approaches identified in this pattern, and the process of associating them with risk criteria, are well-established functions in the security community. [Chu02] refers to ‘the commonly mentioned prevention-detection-response philosophy...’ In a security course description, [SANSf] states that ‘general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.’ Sometimes these approaches are included in a broader list of security functions or safeguards. [DCD+02] identifies these categories: planning, prevention, detection, diligence, and response. [ISO13335-4] states (page 44) ‘In general, safeguards may provide one or more of the following types of protection: prevention, deterrence, detection, reduction, recovery, correction, monitoring, and awareness.’ Criteria details in the Implementation section of this pattern are based on extensive MITRE Corporation experience with our customers.

### ***Consequences***




The following benefits may be expected from applying this pattern:

- The pattern fosters management level awareness: all enterprise security patterns help management better understand security as an overall issue, and gives them terminology and simple understanding of the underlying concepts without relying on details of the technology used to implement them.
- It facilitates conscious and informed decision-making about security approaches to satisfy identified security needs.
- It promotes sensible resource allocation to protect assets.
- It allows feedback in the decision process, to better adjust security approaches to the situation at hand by traceability back to business factors and security needs.
- It encourages better balance among the security, cost, and usability of an asset.
- It shows that you can combine approaches to better and more cheaply protect an asset.

The following potential liabilities may result from applying this pattern:

- It requires an investment of resources to apply the pattern. In some cases the cost of applying the pattern may exceed its benefits.

**Table 6.30** . Security approaches established for desired security properties

PROPERTIES AND APPLICABILITY	SECURITY APPROACH	BUSINESS PRIORITY FOR APPROACH	SPECIAL NOTES
Protect <i>Integrity</i> of museum data: ■ Employee ■ Contractual ■ Financial ■ Partner financial	Prevent 	High	Employee data should only be available to HR, staff, & management
	Detect 	High	
	Respond 	High	
Protect <i>Integrity</i> of all other museum data: ■ Insurance ■ Business planning ■ Public data	Prevent	Moderate	While this information is very important, modifications can be detected and emended without high consequences
	Detect	High	
	Respond	Low	
Protect <i>Integrity</i> of physical assets: ■ Buildings ■ Collections/exhibits	Prevent	High	This is a critical cost driver
	Detect	High	
	Respond	High	
Protect <i>Confidentiality</i> of museum data: ■ Financial/insurance ■ Partner financial ■ Contractual ■ Exhibit plans ■ Research and its data	Prevent	High	These are critical to business operations. Management wants a focus on prevention and detection with high quality encryption.
	Detect	High	
	Respond	Moderate	
Protect <i>Confidentiality</i> of employee data:	Prevent	Moderate	Not as critical to business operations. Restrict access to HR, staff & management
	Detect	Moderate	
	Respond	Moderate	
Protect <i>Availability</i> of museum employee data:	Prevent	Moderate	HR is only user with critical availability concerns
	Detect	Moderate	

- It requires the involvement of people who have intimate knowledge of assets, and basic knowledge of asset security needs and security approaches. These people typically have high positions in the enterprise and their time is valuable.
- It is possible for an organization to assign people to this task who have a less than adequate knowledge of assets, security needs, or approaches, because they may have more available time or are less expensive. If the people applying the pattern do not have a good knowledge of enterprise assets and their value, the pattern results may be inaccurate or not useful.
- Perception of security needs can differ throughout an organization. This may make it difficult to reach agreement on priorities of approaches. On the other hand, bringing such disagreements to the surface may be a benefit, because they can then be properly discussed and resolved.

***See Also***

After applying this solution, the next step typically is to apply ENTERPRISE SECURITY SERVICES (161) to select security services that support the approaches selected in this pattern.