

IT GLOBALSECURE'S POLICY IT ARMOR™ (PITA) FRAMEWORK

Security policies often begin with discussions of confidentiality, integrity, and availability or discussions about access controls, encryption, public key infrastructures, and other matters. Security policies are invariably kept separate from business policies, plans, and procedures – inevitably dooming them to irrelevance.

IT GlobalSecure believes that security policies begin, and end, with our client's business. Security needs to be integral to all business operations – from top-level planning down to day-to-day activities. Our security policy framework is, therefore, built from the business' mission, operations, and objectives. This has the additional benefit of improving the acceptance of the security policy as well as ensuring that security requirements are understood in terms of operational business requirements. Also, by associating security requirements with business requirements, the financial or operational impact of failing to meet a security requirement is immediately visible. Ideally, there would be no separate security documentation, rather, all business documents would reflect a sensitivity to security issues.

A security policy must be used to have value. While this is *almost* obvious, in fact, most security policies are created by technical or staff organizations and forgotten even before they are completed. Line managers and executives must be held responsible for security or failure of security – security cannot be delegated to a peripheral staff element. Measures for security are needed so that executives and managers can be provided with some means to track security performance. Unfortunately, many of the security modeling or analysis tools provide numerical scores that are not tied to business metrics. The security community has done a very poor job of providing useful tools for leaders to measure security.

TOP-DOWN BUSINESS DESCRIPTION

IT GlobalSecure's IT Armor™ Security Framework starts with a top-down analysis of a business's operation. This begins with a basic description of the organization's mission and its external relationships.

This first step is critical. Security policies tend to rapidly become mired in the specifics of technology and procedures without stepping back to determine the security needs of the organization. This creates three almost insurmountable problems:

- Scarce security resources get wasted on security projects that are technically interesting, but have little or no business value.
- Resources are not kept available for the operation, support, training, and awareness necessary for an effective security program.
- Management and staff do not feel that the security requirements belong to them, but are rather imposed in an arbitrary fashion by the security office.

This business model provides the essential foundation for the entire security process. By providing a direct and obvious connection between business operations and security requirements, frivolous security projects will not even be started, executive and management leaders will become advocates for adequate funding, and the entire

organization will be more likely to implement security procedures instead of seeking ways to bypass them.

This decomposition follows a process familiar to software engineers and program managers. It begins with the organization as an “atomic” entity and looks at its external environment. It then follows by taking each interaction and entity and breaking each down into its constituent parts. This continues until the components change from business functions and into specific systems and human procedures.

We begin the decomposition by looking at the relationship of the organization to its environment. External relationships can include customers, competitors, partners, major suppliers, peers or related organizational entities, and “utility” service providers (facilities, power, banks, and other “enabling” services necessary for an organization to function):

- Business Name**
- Mission**
- External Relationships**
 - Partners**
 - Customers**
 - Competitors**
 - Major Suppliers**
 - Utility Service Providers**
 - Peer or Related Organizational Entities**

This first level analysis is a “black box” look at the organization – an assessment that does not examine how the organization operates internally or identify individual roles, but rather looks at the organization as if it were an organism. Each External Relationship will be briefly described based on its operational interaction with the Business or Organization as well as a brief description of its goals and objectives (both independently and as they relate to the Business or Organization).

- External Relationships**
 - Partners**
 - Partner X**
 - Name**
 - Summary of Interaction with Business**
 - Goals and Objectives**
 - Goals and Objectives related to Business**
 -
 - Customers**
 - Customer Y**
 - ...
 - Competitors**
 - ...
 - Peer or Related Organizational Entities**

Once this stage is complete, each External Relationship and Peer Entity element will have its interactions specified with the Business or Organization. For each External Interaction, the External Entities will be identified as well as a description of the role of the various parties. It is best to do this analysis first from the view of the business or organization and then a second pass based on each external relationship.

- External Interactions**
 - External Interaction Y**
 - Name**
 - Description**
 - Participating Entities**
 - Roles of Participating Entities**

This process will likely need to be iterated several times as additional External Relationships and External Interactions are identified during the course of the analysis.

Next, for each External Interaction, a more detailed decomposition of the Interaction will be carried out. Process steps will be identified, key decision making functions from each participant noted, control and management will be highlighted throughout. There may be a triage to determine which external interactions are more important for further analysis at this point based on a preliminary security review. There is a risk involved in that choice, however, as certain processes may actually create vulnerabilities even though they appear innocuous.

External Interaction Z
Participating Entities
Participating Roles within Entities (including Business or organization entities)
Detailed Process Decomposition
Process Step 1
Description
Participating Entities
Participating Entity Internal Elements
Role of Participating Entities
Internal Elements
Oversight and Management Control
Possible Results of Process Step (which process steps it can lead to and why)
Process Step 2
....

This entire process can be repeated for internal entities and interactions, but these interactions are much more vulnerable to organizational and procedural changes. Note, that one may reorganize, automate, or remove a procurement department, but a procurement function is likely to always exist with modest changes in internal processes. The overall objective is to completely describe the organization's behavior – if something cannot be described or tied to an external entity or interaction, it is likely that the decomposition is incomplete.

The only exception are key internal support functions (internal utilities) such as management, accounting, staff, internal information technology support. These groups actually should show up in external interactions, but it is likely that excessive decomposition has occurred if they do (i.e., a decomposition showing internal senior staff briefings to a decision maker to close a decision is excessive decomposition or a process that shows a transaction down to the level of detail of a computer breaking down).

Internal Utility Functions
Management
Accounting
Audit
IT
...

Each Internal Utility Function should be linked to the transactions that it supports. The objective for the assessment of Internal Utility Functions is that their description not be vulnerable to changes in organization and that they are not at such a low level of detail where they could be logically grouped (separating network administration from system administration is probably unnecessary and not helpful).

Internal Utility Function X

Name
Description
External Interactions Supported
Sub-Function Identification
 Sub-Function Description
Related Internal Utilities
 Internal Utility Y
 Relationship Description

The top-down business description is complete when a series of cross-tabs are created to capture the external and internal relationships and interactions captured in this analysis.

Top-Level External Relationship X External Entity Table
Detailed External Relationship X External Entity Table
External Relationship X Internal Utility Table

An attachment to the analysis can be created that tailors the analysis to the current state of the organization. This is somewhat perilous, as organizations are vulnerable to changes for numerous reasons

It is up to the individual analyst to determine the level of detail that is necessary for this decomposition to be completed. There are alternate methodologies that can be drawn from software engineering and other sources to describe and decompose an organization's functions. The specific characteristics of an individual organization and the skills of the analysts should determine the most appropriate methodology.

BUSINESS-DRIVEN SECURITY MODEL

IT GlobalSecure's PITA Security Framework process starts with business operations because security requirements only really make sense in the context of the organization's activities. Security policies often begin with the principles of Confidentiality, Integrity, Identity, and Availability. Unfortunately, these principles really grew out of the security definitions used by the US Department of Defense efforts in the early 1980's – most notably, the "Orange Book". Even in real military environments, and certainly in business, these driving principles were not well understood nor did they map to the needs of the concerned organization. Security requirements must be stated in the language and values of the client organization. Protecting lives, dollars, property, or the integrity of operations are concrete values that can be tied directly to an organization's mission or bottom line. Thus, a \$10,000 access control system is often hard to justify if stated in terms of some "Identification, Authentication, and Authorization" requirement. But, it is very simple to justify if it is protecting a \$1 million dollars per month in transactions.

Thus, once the top-down business assessment described above has been completed, the security requirements can be identified. First, associated with the overall Mission of the business, there should be a corresponding set of security objectives that need to be supported. Then, for each major External Relationship there should be a description of what are the security objectives and where there may be a divergence on security issues:

Business Name
Mission

Mission Security Goals/Requirements

External Relationships
Partners
 Partner X
 Name
 Summary of Interaction with Business
 Goals and Objectives
 Goals and Objectives related to Business
 Shared Security Goals/Requirements
 Divergent Security Goals/Requirements

Customers
 Customer Y
 ...
Competitors
...
Peer or Related Organizational Entities

As will be seen later, by directly linking the security goals to mission objectives, it is much easier to develop metrics for security in context of the mission and to more easily value security measures. In some sense, real security policies are utterly unique to an individual organization – they should reflect the core values and objectives of that organization as well as its given circumstances and resources.

Similarly, for each External Interaction, the security analyst identifies relevant security goals and requirements. Each interaction will have its own unique characteristics and, in addition to the identification of the security goals, an assessment of the “value” of the interaction in terms of the organization's overall goals and objectives (both in terms of mission and security) must be completed:

External Interactions
 External Interaction Y
 Name
 Description
 Participating Entities
 Roles of Participating Entities
 Organizational Value (or Values) for External Interaction
 Security Goals for External Interaction

Once each external interaction is identified, the decomposition carried out previously can be used to allocate specific security objectives and requirements to process stages. When done in context of the security requirements for the specific external interaction, these security elements should be much more self-apparent. They may also result in alterations to processes to make the processes more secure rather than adding security mechanisms to structurally insecure interactions.

External Interaction Z
 Participating Entities
 Participating Roles within Entities (including Business or organization entities)
 Security Component for Each Role
 Separate Security or Oversight Roles
 Detailed Process Decomposition
 Process Step 1
 Description
 Participating Entities
 Participating Entity Internal Elements
 Role of Participating Entities
 Security Role of Participating Entities
 Security Relevant Internal Elements
 Security “Ignorant” Internal Elements

Oversight and Management Control
Security of Oversight and Management Control
Possible Results of Process Step (which process steps it can lead to and why)
Security Failures of Process Steps
Process Step 2
....
Security Failure Process Steps

Security is, itself, usually an Internal Utility Function. Thus, three additional functions need to be added to the set:

Internal Utility Functions
Management
Accounting
Audit
IT
...
Security
Security Management
Security Auditing

It is important that all three of these functions are in place. They are often, and regrettably, combined. Security is the actual security operations to support the mission of the organization. Security Management is the oversight and supervision of those actions as well as the security components of other Entities and Interactions. Finally, Security Auditing is the independent assessment to ensure that all organizations, including Security and Security Management themselves, are supporting the organization's security objectives. Auditing is an often misused term in the security community. A real audit independently generates and reviews data from multiple sources. Often, security systems generate their own "audit logs" or reports. Since these are generated by the systems under investigation, the audit is not independent and therefore cannot be relied on.

Each Internal Utility will also have its own security components that support each individual functions own requirements as well as supporting security needs for other interactions and entities:

Internal Utility Function X
Name
Description
Security Goals and Requirements
External Interactions Supported
Security Requirements for Each External Interaction
Sub-Function Identification
Sub-Function Description
Security Requirements for Sub-Function
Related Internal Utilities
Internal Utility Y
Relationship Description
Security Requirements for Relationship

The first stage in the resulting analysis will be to re-architect the External Interactions and Relationships as well as supporting security activities to simplify interactions and reduce overall complexity. This activity is likely to gain the largest security benefits – most security problems stem from activities that are complicated and poorly understood. The next stage is to allocate existing security mechanisms – specific policies, procedures, system implementations, technologies, to the lower level processes listed above.

External Interaction Z

Supporting Security Mechanisms

Participating Entities

Participating Roles within Entities (including Business or organization entities)

Security Component for Each Role

Separate Security or Oversight Roles

Detailed Process Decomposition

Process Step 1

Description

Participating Entities

Participating Entity Internal Elements

Role of Participating Entities

Security Role of Participating

Entities

Security Relevant Internal Elements

Security "Ignorant" Internal Elements

Allocated Security Mechanisms

Usage Description

Policy

Policy 1

Usage and Value

...

Procedures

Procedure 1

...

System Implementations

System Implementation 1

...

Technologies

Technology 1

...

Metrics

Oversight and Management Control

Security of Oversight and Management

Control

Allocated Security Mechanisms

Usage Description

Policy

Policy 1

Usage and Value Metrics

...

Procedures

Procedure 1

...

System Implementations

System Implementation 1

...

Technologies

Technology 1

...

Metrics

Possible Results of Process Step (which process steps it can lead to and why)

Security Failures of Process Steps

Allocated Security Mechanisms

Usage Description

Metrics

Process Step 2

....

Security Failure Process Steps

Allocated Security Mechanisms

Usage Description

Metrics

Internal Utility Function X
 Name
 Description
 Security Goals and Requirements
 External Interactions Supported
 Security Requirements for Each External Interaction
 Allocated Security Mechanisms
 Usage Description
 Metrics

Sub-Function Identification
 Sub-Function Description
 Security Requirements for Sub-Function
 Allocated Security Mechanisms
 Usage Description
 Metrics

Related Internal Utilities
 Internal Utility Y
 Relationship Description
 Security Requirements for Relationship
 Allocated Security Mechanisms
 Usage Description
 Metrics

Once again, once the security mechanisms have been allocated, it is likely that a review of the security approach will be necessary to simplify and improve security and its relationship to the External Interaction or Internal Utility Function. It is recommended that this be done as a separate step so that the changes are clearly visible to management – organizational acceptance of security relies on the ability to show demonstrable benefits and most benefits of a stronger security framework will come from process changes, not visible “reduced threat or attacks”.

The next step is to carry out a Gap Analysis comparing existing mechanisms with the level of vulnerability of relevant External Interactions or Internal Utilities. It is important to do this from a Vulnerability perspective, NOT a Threat-based model. The key reason for this is that Threat modeling is essentially a view of an organization’s understanding of the **intent** of potential adversaries. Since intent can change rapidly and organizations are not very good at reliably interpreting other entities’ intent, vulnerability based policies are much more robust. Usually, when threat is introduced into the security debate, it is the immediate predecessor of a budget cut or loss of priority for security as an organizational objective.

It is also important to carry out a “cross-tab” analysis of mechanisms relative to External Interactions and Internal Utility Functions to identify where standardization of mechanisms will improve usability and reduce costs and training.

OPERATION, OVERSIGHT, AUDITING, AND ACCOUNTABILITY

Monitoring, Oversight, and Auditing are essential to making any Security Policy valuable to an organization or business. Without these mechanisms, a Security Policy simply becomes another document filed away until someone else decides they need to update it in response to a crisis either within an organization or in the mass media.

The structure of the IT GlobalSecure PITA Security Framework has integrated management and oversight into itself. By focusing on External Interactions and Internal Utility Functions, the intent is to reduce the amount of rework or changes to the policy

due to internal reorganizations. Also, by focusing on organizational operations, when a new Interaction is created or changed, it is easier to integrate security into ordinary business processes.

Line management within an organization or business will have a day to day responsibility for monitoring External Relationships, External Interactions, and Internal Functions under their purview. They will need to create metrics for their own purposes as well as to report to their seniors.

Executive oversight of security must be integrated into ordinary management reporting. Individuals behave in response to perceived priorities. If security and accountability for security is in-place, managers will respond. If security is reduced to a slogan, it will be treated with “appropriate” seriousness by everyone.

Auditing is the final stage in ensuring accountability. It provides the independent feedback mechanism to validate ordinary reporting as well as to highlight internal and external changes that may have an impact on an organization's security posture. Independence and authority is as crucial to the security audit process as it is to a financial audit.

METRICS

The security industry lacks in basic metrics that can be easily used by organizations or businesses. On one hand, this is an expression of the security communities' lack of appreciation of accountability (and countability) by busy executives and managers. On the other hand, it is also a result of the utter specificity of security to an individual organization. Organizations should be able to express their security needs relative to their ordinary business needs and requirements. Below are several possible security metrics:

Money/Budgets – Comparing the security budget to the budget or value of the transaction provides an immediate and close correlation to the business. This can be separated into two obvious categories – developmental or acquisition budgets and operations and maintenance budgets.

External Isolation – This is the first measure of “security simplicity” – how isolated or separated is the external transaction or internal utility from other transactions and utilities. If it is very isolated, it is more likely to be secure from outside parties and also less expensive to secure.

Internal Complexity – This is the second measure of “security simplicity” – how complicated is the External Transaction or Internal Utility. If it is highly complicated, it is likely that it is not well understood and that it is not very manageable. Also, complexity will increase the cost of integrating security and the difficulty in assessing whether something is actually secure.

Other important measures are Outage times, time to restore, lost revenue, lost property, and, of course, lost lives. For security, it is usually not advisable to aggregate measures into too few values. By keeping the metrics tied to business operations, consequences of security decisions will be well understood by executives, managers, and other

leaders. Also, aggregation basically allows the aggregator to “lie with security statistics” to manipulate the results based on his or her individual biases.

Since it is difficult to quantify “what is secure” it is much more effective to build metrics around “relative security”. Therefore, any security metric should be a comparison of a baseline and a new or proposed state as opposed to any “absolute” security measure.

CONCLUSIONS

IT GlobalSecure has developed its Policy IT Armor™ Framework based on its real-world experience making security relevant to businesses and organizations. This framework focuses on the concrete value of security to business operations rather than abstract security concepts.

IT GlobalSecure uses the same methodology for its Business Information Technology Security Assessment to rapidly focus on critical security issues that affect a business, not limitations of individual products.

IT GlobalSecure uses this same approach for its product and service solutions through bundles such as its Business Protection Packages. These combinations of security solutions are grouped to allow an enterprise to quickly meet their security needs. IT GlobalSecure also recognizes that there is no such thing as “one-size-fits-all” security, so we have relationships with over 40 vendors to provide the most appropriate security solutions to meet an individual business’s needs.