Applying Critical Success Factors to Information Security Planning

Richard A Caralli, William R Wilson
Survivable Enterprise Management Team

Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense
© 2004 by Carnegie Mellon University
Objectives

Introduce the concept of critical success factors

Illustrate the use of critical success factors as a foundation for security management

Provide real world examples in developing and analyzing critical success factors
Agenda

Introduction

CSF Concepts

Applying CSFs to security

Summary
Field observation

Enterprise security strategies are ineffective in the long run when they do not focus on and align with organizational drivers.
How do we fix it?

Base organizational strategy and security strategy on the same organizational drivers

- Mission is good, but abstract and open to interpretation
- Goals are better, but more operational in nature
- **CSFs are more reliable and universal**—key performance factors that all levels of management must consider
Introduction to Critical Success Factors
CSFs defined

The limited number of areas in which satisfactory results will ensure competitive performance for the organization and enable it to achieve its mission.

Key areas of activities
- in which favorable results are necessary to achieve goals.
- where things must go right for the organization to flourish.
- that should receive constant attention from management.
CSF examples

Automobile industry
“Meet federal energy standards for automobiles.”

County government
“Deliver high-quality, low-cost citizen services.”

Educational institution
“Attract and retain high-quality faculty.”
CSFs are the glue
Characteristics of CSFs

**Sources** define the various entities where CSFs originate

**Dimensions** describe the properties of CSFs relative to perspective (internal vs. external) and function (monitoring vs. adapting)

**Hierarchy** describes the relationship between CSFs at the various layers of an organization
Five sources of CSFs

**Industry** in which the organization operates

Organization’s relationship with its **peers**

**Environmental factors** that the organization can’t control

**Temporary** barriers, challenges or problems

**Domain** of each layer of management
Sources of CSFs

**Industry CSFs:**
- Deliver on-time service.
- Move away from hub-and-spoke system.
- Monitor the legal and regulatory environment.

**Peer CSFs:**
- Continually reduce cost per passenger mile.
- Attract merger opportunities.
- Increase code share partnerships.

**Environmental CSFs:**
- Address the effects of terrorism.
- Enhance relationships with new labor leadership.

**Temporal CSFs:**
- Enhance brand image.
- Address decrease in customers due to security issues.

**Management CSFs:**
- Control airline schedules.
- Optimize crew utilization.
- Manage budgets.
Internal vs. External CSFs

Internal CSFs are within the span of control for a particular manager

External CSFs are most likely not controllable by a particular manager

An awareness helps managers actively set better goals and predict potential impacts when CSFs are not achieved
Monitoring vs. Adapting CSFs

Monitoring CSFs emphasize the continued scrutiny of existing situations

Adapting CSFs focus on improving and growing the organization

Managers almost always have monitoring CSFs

Adapting CSFs most likely to be confused with goals
Hierarchy of CSFs

CSFs exist throughout the organization at every management layer and level
The CSF Method
Five key activities

Defining scope
Collecting data
Analyzing data
Deriving CSFs
Analyzing CSFs
Organizational CSF participants

**Specific roles:**
- C-level executives
- Vice-President and director level
- Division heads
- Chief Legal Counsel
- Corporate Secretary
- VP Investor Relations, M & A, Marketing & Sales, PR
- Strategic Planners

**Unique functions:**
- Asset management
- Corporate reporting and taxes
- Risk Management
- Controller and treasurer
- Government relations
- Select Board members
- Select external personnel
Interview questions -1

What are the CSFs in your job right now?

In what 1, 2, or 3 areas would failure hurt you most?

In what area would you hate to see something go wrong?

Assume you are placed in a dark room with no access to the outside world. What would you most want to know about the organization when you emerged three months later?
Interview questions -2

What is your personal mission and role in the organization?

What are your most critical goals and objectives?

What are your three greatest business problems or obstacles?
Deriving CSFs

CSFs are pulled from supporting themes

So long as the process is followed, supporting themes should be all that is needed to derive a CSF
CSF approach advantages

Guarantee alignment with organizational drivers

Reduce organizational ambiguity

Dependable guiding force/target for the organization

Reflect current operating environment of the organization

Reflect management’s risk perspective

Course correction
Applying CSFs to Enterprise Security Management
Areas of promise using CSFs

As a tool for information security risk management

Providing impetus for managing security as a process throughout the organization

Foundation for enterprise resiliency
CSFs can enhance ISRM

Determining risk assessment scope

Selecting critical assets for assessment

Identifying and validating security requirements

Identifying risks to critical assets

Setting evaluation criteria for measuring risk

Evaluating threats and mitigating risk
Using CSFs to set scope

Most important and difficult task in risk assessment

Failure to focus a risk assessment on the right areas of the organization will not yield meaningful results

Using affinity analysis, focus on those areas that are most important to accomplishing the organization’s mission
## Scope example

<table>
<thead>
<tr>
<th>Organizational Departments</th>
<th>Critical Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Develop human resources</td>
</tr>
<tr>
<td>Human Resources</td>
<td>X (△)</td>
</tr>
<tr>
<td>Legal</td>
<td>X</td>
</tr>
<tr>
<td>Controller’s</td>
<td></td>
</tr>
<tr>
<td>Internal Auditing</td>
<td>X</td>
</tr>
<tr>
<td>Government Affairs</td>
<td>X</td>
</tr>
<tr>
<td>Research &amp; Development</td>
<td>X (△)</td>
</tr>
<tr>
<td>Information Technology</td>
<td>X</td>
</tr>
<tr>
<td>Public Affairs</td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td></td>
</tr>
</tbody>
</table>

This intersection indicates that the work of the Human Resources department is a primary factor in achieving the "develop human resources" CSF.

These intersections indicate that all departments play an important part in meeting the "maximize teamwork" CSF.

This intersection lacks a relationship. This indicates that the work of the R & D department has no apparent connection to achieving the "manage compliance" CSF.
CSFs and critical assets

Risk-based approach to information security directs resources to protecting the organization’s most critical assets

Selection of assets to protect is often left to judgment or perceived value

CSFs can aid in identifying an organization’s critical assets—those that contribute most to accomplishing the organization’s mission
## Critical assets example

<table>
<thead>
<tr>
<th>Critical Assets</th>
<th>Critical Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Develop human resources</td>
</tr>
<tr>
<td>Customer information</td>
<td>X</td>
</tr>
<tr>
<td>Payroll information</td>
<td></td>
</tr>
<tr>
<td>ERP system</td>
<td></td>
</tr>
<tr>
<td>Financial data</td>
<td>X</td>
</tr>
<tr>
<td>Widget formulas</td>
<td></td>
</tr>
<tr>
<td>EIS system</td>
<td></td>
</tr>
<tr>
<td>Skills database</td>
<td>X</td>
</tr>
</tbody>
</table>

The asset “financial data” is important for managing compliance.
CSFs and security requirements

An important component of protecting critical assets

Foundation for devising an appropriate protection strategy for the assets

Prioritization of the requirements is necessary to determine which requirement, if unmet, would impact the owner of the asset and the organization

CSFs can aid in this prioritization of requirements.
### Security requirements example

#### Critical Assets and Security Requirements

<table>
<thead>
<tr>
<th>Critical Assets and Security Requirements</th>
<th>Critical Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Develop human resources</td>
</tr>
<tr>
<td>Medical records</td>
<td></td>
</tr>
<tr>
<td>confidentiality</td>
<td>X</td>
</tr>
<tr>
<td>integrity</td>
<td></td>
</tr>
<tr>
<td>availability</td>
<td></td>
</tr>
<tr>
<td>Widget formulas</td>
<td></td>
</tr>
<tr>
<td>confidentiality</td>
<td></td>
</tr>
<tr>
<td>integrity</td>
<td></td>
</tr>
</tbody>
</table>

A violation of the confidentiality requirement impedes the ability to manage compliance.
CSFs and risk identification -1

At the core of a risk management approach to security

Two popular means:
▪ Use a taxonomy as a guide
▪ Rely upon organizational judgment

Both methods can overlook common risks or risks unique to an organization

CSFs can sharpen focus on important risks
CSFs and risk identification -2

Properly focus risk identification in the right areas

Shape and guide the knowledge or input from personnel in the organization

Validate and prioritize risks that have been identified
CSFs and measuring risk

Requires evaluation criteria

Organization-based criteria likely to reflect unique drivers, but not guaranteed

Criteria can be validated (to ensure alignment with organizational drivers) by comparison to the organization’s CSFs
### Evaluation criteria example

<table>
<thead>
<tr>
<th>Evaluation criteria</th>
<th>Critical Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Develop human resources</td>
</tr>
<tr>
<td>Reputation</td>
<td></td>
</tr>
<tr>
<td>Life &amp; health</td>
<td>X</td>
</tr>
<tr>
<td>Fines &amp; legal penalties</td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td></td>
</tr>
<tr>
<td>Productivity</td>
<td>X</td>
</tr>
</tbody>
</table>
CSFs and risk mitigation

Depends on prioritization of those risks that most impact the organization

The organization is impacted whenever its ability to conduct its normal course of business is impeded.

Comparing risks to CSFs identifies those risks that are candidates for mitigation because

▪ they interfere with the achievement of CSFs and
▪ they affect other organizational drivers (goals, etc.)
### Risk mitigation example

#### Risks to Critical Assets

<table>
<thead>
<tr>
<th>Risks to Critical Assets</th>
<th>Critical Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop human resources</td>
<td>Manage compliance</td>
</tr>
<tr>
<td>Widget formulas</td>
<td></td>
</tr>
<tr>
<td>Stolen and sold</td>
<td></td>
</tr>
<tr>
<td>Altered</td>
<td></td>
</tr>
<tr>
<td>Destroyed by flood</td>
<td></td>
</tr>
<tr>
<td>Employee records</td>
<td></td>
</tr>
<tr>
<td>Altered</td>
<td></td>
</tr>
<tr>
<td>Customer information</td>
<td></td>
</tr>
<tr>
<td>Destroyed</td>
<td></td>
</tr>
</tbody>
</table>

This risk should be considered for mitigation because it potentially impedes the “manage compliance” CSF.
Enterprise resiliency -1

Physical property of a material that allows it to spring back after deformation that has not exceeded its elastic limit [www.cogsci.princeton.edu]

“...ability to withstand systemic discontinuities” [Booz Allen]

“...ability to adapt to new risk environments” [Booz Allen]

Source: Booz Allen - Enterprise Resilience: Managing Risk in the Networked Economy
Enterprise resiliency -2
Summary and conclusions

CSFs relate to the core functions of management—planning, organizing, coordinating, directing, and controlling

CSFs are essentially a management tool for better decision making that aligns with the organization’s business drivers

CSFs show significant promise as a tool for improving enterprise security management by helping to ensure that security strategy actually enables the achievement of the organizational mission
Presentation references

