Best Security Practices: An Overview

by Guy King, Ph.D., CISSP

Information Security & Operations Center, Defense Group, Computer Sciences Corporation (CSC)

gking1@csc.com
1-703-575-5115
Agenda

- Context
- Best Security Practices (BSPs)
- Security Process Framework (SPF)
- BSP Life Cycle
- Conclusion
Context

◆ Security requirements are implemented by several means:

- **Technical**: software, hardware (i.e., IT)
- **Physical**: barriers, locks, etc.
- **Administrative**: the actions and practices of people

Best security practices (BSPs) fall under the last-named

◆ Good security practices are the *foundation* of security
A Best Security Practice (BSP) Is:

- A human practice; i.e., a repeated or customary method used by people to perform some process.

- Security-related; i.e., plays a part in protecting an organization’s information or operations.

- Shown by experience to be effective in performing some security process; the result of operational experience.

- Among the most effective of those existing practices used to perform a given security process.

- Not an IT security mechanism.

- Not a business practice, though it supports the organization’s operations.

- Not a best possible practice but a best existing practice; not the result of armchair theorizing.

- Not necessarily the single best existing practice of a particular sort.
Best Security Practices, 2

- BSP reuse leverages security knowledge
- Knowledge Management (KM) techniques apply to BSP sharing
- KM experience indicates that expert-novice interaction is needed for knowledge transfer to occur
- BSPs may be of varying levels of goodness
Security Process Framework (SPF), 1

- Facilitates the sharing and management of best practices
- Is closely related to the notion of a **security program**:
  - A comprehensive set of program areas (e.g., risk management, personnel security, security training) that together guide an organization’s actions to protect its information resources
  - Each program area is a cluster of related security sub-processes
- Together the program areas and their sub-processes provide an **SPF**—a structure of security processes used to categorize BSPs
SPF, 2: The SPF’s 10 Program Areas

- Security Program Management
- Customer Security Support
- Risk Management
- Certification and Accreditation (C&A)

Program Areas:
- Personnel Security
- Security Training
- Physical Security
- Contingency Planning
- Technical Security
- Incident Response
SPF, 3: Complications

◆ The SPF’s program areas have a life cycle
◆ Organizational security program (OSP) vs. system security program (SSP)
  ✦ BSPs useful in developing and operating an OSP differ from those useful for an SSP
  ✦ The same program areas pertain to both OSP and SSP
  ✦ The life cycles of an OSP and of an SSP are distinct: the Operate phase of the OSP life cycle guides all phases of the SSP
SPF, 4: High-Level Structure

### SPF, Part 1: ORGANIZATIONAL SECURITY PROGRAM

<table>
<thead>
<tr>
<th>Security Process Areas</th>
<th>Life Cycle Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Initiate</td>
</tr>
<tr>
<td>Security Program Mgmt</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
</tr>
</tbody>
</table>

### SPF, Part 2: INFORMATION SYSTEM SECURITY

<table>
<thead>
<tr>
<th>Security Process Areas</th>
<th>Life Cycle Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Initiate</td>
</tr>
<tr>
<td>Security Program Mgmt</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
</tr>
</tbody>
</table>
BSP Life Cycle, 1

1. Identify

2. Package

3. Evaluate

4. Adopt

5. Deliver

6. Improve
# BSP Life Cycle, 2: Packaging

## 1. Identification Data
- Number & Name
- Version
- Date Adopted
- Approving Authority
- Source of BSP
- Level of BSP
- Framework & Process Supported
- Point of Contact

## 2. What This BSP Does
- Purpose of BSP

## 3. What This BSP Is
- Requirements Addressed by BSP
- Success Stories
- Description of BSP
- Relations to Other BSPs

## 4. How To Use This BSP
- Implementation Guidance
- Resource Estimates
- Performance Goals (Metrics)
- Tools
- Training Materials

◆ Appendices
BSP Life Cycle, 3: Evaluating

◆ Preliminary evaluation criteria:
  ✦ BSP contributors are who they claim to be
  ✦ Mandatory sections are complete
  ✦ BSP seems unlikely to cause harm

◆ Evaluation criteria:
  ✦ Effective in performing some security process
  ✦ Reduces costs
  ✦ Saves time
  ✦ Is easy to implement
  ✦ Consistent with other BSPs
  ✦ Reveals no vulnerabilities
Conclusion

◆ The sharing of BSPs helps address the critical shortage of skilled security practitioners

◆ In sharing and managing BSPs:
  ✦ Use a security process framework (SPF)
  ✦ Employ a standard BSP format
  ✦ Support the six BSP life-cycle functions