Feature

Evaluating Information Security Solutions
Swapping the Cost of Failure for Success

One of the biggest budget busters for an information security program is technology solutions that are not a good match for the organization. Often, the technology is more than adequate in terms of functionality; however, other attributes of the solution may clash with the organization's needs and culture. Some acquisitions fail because there is a poor match between the solution's functionality and the capabilities required to meet the real needs to ensure the organization's security posture. Thus, it is critical to identify and evaluate security technology solutions to maximize the potential for a successful implementation.

The number of information security solutions available has grown exponentially as the marketplace for these products has matured. Much of the demand for these products has resulted from one or more of the following factors:

• Regulatory compliance requirements and legislation
• Increasing incidence of data breaches
• Increase in hacktivism
• Increasing cyberthreat landscape
• Trend toward IT consumerism, such as bring your own device (BYOD)

While the increase in solution alternatives makes it easier for an organization to find a security product that offers the perfect fit for its specific requirements, the myriad of options can be confusing for the information security manager. In addition, there is a key trend among solution vendors to merge new functionality into their core products, which previously existed as stand-alone applications, such as malware-detection capabilities in a vulnerability management suite. It can be more difficult to evaluate these hybrid solutions when seeking to fill gaps in the information security organization's toolset.

SYMPTOMS AND COSTS OF A POOR FIT BETWEEN ORGANIZATION NEEDS AND SOLUTION

The consequences of a poor fit between the actual needs of the organization and a security solution may surface as the following symptoms:
1. Consuming too many resources and too much time
2. Requiring extensive technical and product expertise
3. Necessitating extensive customization
4. Purchasing supplementary solutions to augment missing functionality
5. Extensive manual workarounds

In addition to creating frustration for staff and customers, a bad match between the solution and the organization can waste budget resources. For example, an organization purchased a data loss/leak prevention (DLP) solution for US $250,000, only to replace it with another equally costly solution within a few years. The advantages of wrapping a more extensive solution evaluation process around the product acquisition would have increased costs on the front end, but the benefits would exceed the expenditure and include:

• Diminishing the need for do-overs or premature replacement of a solution
• Decreasing costs associated with excessive consulting, customization or training due to incompatibilities with the infrastructure or organizational culture

COMMON MISTAKES IN EVALUATING SECURITY SOLUTIONS

One mistake that information security managers seeking security solutions to fill a gap in their tools portfolio or replace an existing product make is to develop a set of selection criteria that mirrors a solution with which they are familiar. The disadvantages to using this approach for the creation of solution criteria include:

• May lead to single-sourcing because no other vendor offering meets overly specific criteria

Kerry A. Anderson, CISA, CISM, CGEIT, CRISC, CCSK, CFE, CISSP, CSSLP, ISSAP, ISSMP, is an information security professional with more than 17 years of experience in information security and compliance. She is an adjunct professor in cybersecurity at Clark University (Worcester, Massachusetts, USA). Anderson is the author of numerous articles in professional journals and the book, The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture, and has been a speaker, panelist, moderator and chairperson at many professional conferences. She can be reached at kerry.ann.anderson@verizon.net.
• Limits exploration of other options or solutions
• Discourages performing an assessment to determine specific needs to be filled by a solution

The information security manager or individual responsible for performing a needs analysis may omit this step and jump to vendor selection. Often, the outcome can be summed up as “if it does not fit, I will make it fit” because the information security team attempts to make a solution work. The result is a subpar solution that may require premature replacement. Insufficient product evaluation prior to purchase could potentially result in a solution with capabilities that are inconsistent with the sales pitch or the organization’s security needs.

OPTIMIZING ACQUISITION USING A STANDARD EVALUATION PROCESS

A standard evaluation process allows potential solutions to be assessed based on an agreed-upon set of criteria designed to meet the identified needs of the organization. At its essence, it allows an apples-to-apples comparison of essential features. Additionally, it avoids the potential for undue vendor or other internal influences on the purchasing decision by vetting all possible solutions against a common set of criteria. The objective of this process is to narrow the possible set of alternatives down to a few—perhaps two or three—potential solutions for further assessment:

1. Document key requirements and restrictions. Start by determining the specific needs and requirements the organization must fill to increase its security posture. This is a list of must-haves that are generally nonnegotiable. While this might seem obvious, the information may not be documented and functionality that is cool or nice-to-have may overshadow the original purpose for seeking a security solution. Before proceeding with seeking potential vendors, the following needs to be recorded and agreed upon by stakeholders:
   • What need(s) will the solution fill? The needs should be concise and ideally written in vendor-neutral language.
   • Are there any specific restrictions or requirements, such as operating systems, compatibility with other solutions or other architectural issues, that must be taken into consideration?
   • Does a budget exist for this purchase? If so, what is the upper limit in terms of initial purchase price?
   • In addition to the solution, what other costs need to be taken into consideration related to the acquisition, such as training and consulting?

2. Use the Goldilocks Principle. The Goldilocks Principle states that a solution to something must fall within certain parameters rather than going to extremes in terms of offering too little or too much functionality. The most successful solutions provide a “just right” balance in terms of benefits received, security needs met and resources required for support.

Additional features outside the scope of an organization’s needs, rather than providing potential extra value, can add costs because unwanted functionality cannot be disabled easily, becomes reactivated in successive releases or requires additional workarounds. This may be true when a feature such as monitoring functionality runs contrary to the organizational culture. To simplify, an organization would be paying for something it cannot use, and that is a waste of money.

3. Avoid “analysis paralysis.” Without specific criteria to provide guidance to identify appropriate solutions, an information security team may cast too wide of a net in its search. The result could lead to analysis paralysis with the consequences of additional purchasing costs and longer acquisition times.

4. Consider total cost of ownership. When evaluating a security solution, it is important to consider the total cost throughout its life cycle. Rather than focusing on the immediate acquisition costs, estimate the total expenditures required to implement and support the solution throughout its expected life cycle. Implementation of innovative technology or

Enjoying this article?

• Learn more about, discuss and collaborate on information security management in the Knowledge Center.

www.isaca.org/topic-information-security-management

The most successful solutions provide a ‘just right’ balance in terms of benefits received, security needs met and resources required for support.
unfamiliar solutions can require extensive consulting beyond basic setup fees included in the purchase price. According to Fred Brooks, author of *The Mythical Man-Month*, the costs of support and maintenance may be up to 90 percent of an initial technology investment.\(^1\) It can be tempting to believe some of these costs, such as consulting and training, are optional and do not need consideration in preparation of an initial cost estimate. However, for many solutions involving complex technologies, these expenditures are necessary for a successful implementation and adoption of the product. Some components of the total cost of the solution may include:

- Training
- Testing
- Consulting
- Legal
- Required infrastructure upgrades
- Hiring additional staff

5. **Develop use cases.** Use-case diagrams\(^2\) are a simple way to document requirements. They are graphic representations using stick figures (actors) and ovals (use cases) with lines documenting their interactions. Use cases provide a way to document the required processes from the point of view of the users. A complete use case consists of diagrams and textual descriptions. Use cases offer some clear benefits to evaluating candidate solutions, including:

- Providing a mechanism to allow stakeholders to walk through a process with the inclusion of different solution alternatives. This answers the question: How would this work with solution X?
- Identifying any potential issues.

Use cases do have a limitation in regard to documenting requirements. Use cases are an effective technique for capturing and documenting functional requirements. However, functional requirements are only one type of requirement. Other types of requirements include legal and compliance requirements, architectural strategy, usability, reliability, and performance requirement. Therefore, it is important to identify the relationship between the functional requirements captured in the use cases and other types of requirements.

### USING SWOT AS AN EVALUATION TOOL FOR SECURITY SOLUTIONS

After the possible field of contenders has been reduced to a maximum of two or three, the evaluation process may require a deeper dive to assess each alternative. One method is to perform a strengths, weaknesses/limitations, opportunities and threats (SWOT)\(^3\) analysis of each solution option. SWOT analysis is designed as strategic planning to provide information for matching the organization’s resources and competencies to the environment in which it runs. However, it is readily adaptable to evaluation and selection of other alternatives, such as a strategic technology investment. As such, it is instrumental in strategy formulation and selection. As a strategic evaluation tool, SWOT considers the strengths, weaknesses, opportunities and threats involved with the different options. It involves identifying the internal and external factors that are favorable and unfavorable to achieve the objectives of a project (**figure 1**):

- **Strengths**—The solution’s strengths are its capabilities that increase its ability to meet or exceed the objective of the acquisition. Examples of such strengths include:
  - Innovative technology
  - Start-up vendor, hungry for opportunities
- **Weaknesses**—In some cases, a weakness may be the other side of strength. A weakness is any attribute that might prevent the achievement of the acquisition’s objectives. For example, each of the following may be considered weaknesses:
  - Unproven technology/limited performance history
  - Start-up with limited financial history

<table>
<thead>
<tr>
<th>Internal Factors</th>
<th>External Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
<td><strong>Opportunities</strong></td>
</tr>
<tr>
<td>Multilayered browsing protection against web-based attacks</td>
<td>Provides security-in-breadth by providing heterogeneous antimalware product environment</td>
</tr>
<tr>
<td>Smart updates provide frequent automatic updates</td>
<td>Provides protection against malware for remote and network devices</td>
</tr>
<tr>
<td>Uses a combination of reactive blacklists and proactive content analysis</td>
<td></td>
</tr>
<tr>
<td><strong>Weaknesses</strong></td>
<td><strong>Threats</strong></td>
</tr>
<tr>
<td>No central console manager</td>
<td>Potential that users might experience some minimal performance drop</td>
</tr>
<tr>
<td>No automatic distribution mechanism</td>
<td>Attack software that could potentially disable application</td>
</tr>
</tbody>
</table>

Source: Kerry A. Anderson. Reprinted with permission.
Opportunities—An external factor that is capable of increasing or optimizing the value of an acquisition. Some examples include:
- Single, secure authentication mechanism across all platforms and devices
- Use of two-factor authentication decreasing potential for security breaches

Threats—An external factor that is capable of decreasing the value of an acquisition or diminishing the chance of achieving the acquisition’s objectives. Some examples of such threats include:
- Meeting compliance requirements
- Untested technology

BENEFITS OF USING SWOT ANALYSIS TECHNIQUE IN SOLUTION EVALUATIONS
Using the SWOT technique can offer insights into the strengths and weaknesses of a solution candidate, its ability to achieve business and technical objectives, and the ability to exploit the solution to support the business strategy. The primary advantages of conducting a SWOT analysis are that it costs very little and can be performed quickly. Additional benefits include:
- Concentrates on the most important factors affecting how a solution might affect a business
- Showcases the solution’s weaknesses and strengths
- Offers the potential to identify external opportunities available as well as possible external threats to the organization
- Compares the specific environmental factors of the organization against the candidate solution to determine a potential fit between the two

LIMITATIONS OF USING SWOT ANALYSIS TECHNIQUE IN SOLUTION EVALUATIONS
The results of a SWOT analysis could be misleading if inadequate or incorrect data are used in the analysis. In addition, the resulting analysis could be biased if internal teams wish to sway the purchasing decision toward a particular solution. Additionally, the following are some limitations of the SWOT technique:
- Covers only issues that can positively be considered as a strength, weakness, opportunity or threat
- Does not factor in other issues and nuances with the potential to affect the success of a particular solution within a specific organization
- Does not prioritize issues

A SWOT analysis should not be the sole tool used in the decision-making process. For complex or strategic acquisitions, it may be necessary to conduct additional in-depth analysis.

CRITICAL SUCCESS FACTORS
Critical success factors (CSFs) are influential factors in the success of a project or function. They are required for ensuring the success of an organization. In the evaluation of multiple options available to carry out an initiative, CSFs may appear equally capable of achieving the objectives of the project. However, on closer inspection, specific attributes of one potential solution may present a better fit for the organization.

That solution may offer tangible or intangible benefits more aligned with an organization’s culture, mission or direction. Therefore, these factors need to be weighted more heavily in recommending the best alternative to pursue for a specific organization and project. CSFs are elements that are essential for the success of any project or strategy. They propel it forward and can make or break its outcome. Project failures often have their root causation in neglecting to consider CSFs, including:
- Organizational culture
- Ease of use
- User profiles (technical proficiency, backgrounds, job tasks performed)
- Degree of customization possible
- Long-term support requirements

KEY PERFORMANCE INDICATORS
Key performance indicators (KPIs) define and chart progress toward a business or project objectives. KPIs are objective measurements that should reflect the CSFs. Candidate solutions should be evaluated against their ability to meet CSFs and perform against the agreed upon KPIs. Common KPIs include:
- Performance
- Security
- End-user support
- Solution support and maintenance
- Ongoing infrastructure support
- Appropriate functionality
- Ease of modification
SWAPPING THE COST OF FAILURE FOR SUCCESS

The tactical approaches discussed in this article have the objective of optimizing the outcome of the solution assessment by identifying the most cost-effective or fulfilling organizational needs. Each tactic mentioned serves one or both of these purposes when mapped against a matrix of these two benefits. However, it is the combining of these tactics into a comprehensive framework that allows for the achievement of the maximized benefit and for the solution selection process to be optimized (Figure 2).

Fully evaluating a list of possible solutions against an agreed-upon set of technical and business criteria increases the opportunity for successful implementation. While common sense says that one should identify what is needed before seeking a solution, in many instances, the order of activities is reversed. Solution selection may be overly influenced by a vendor’s persuasiveness or a stakeholder’s bias toward a specific product. This consequence may be a poor fit between the product and the organization. Often, the fault for less than successful technology investment is attributed to one or more of the following causes:

- The vendor, sales representative or product itself
- Prior management that made the acquisition
- Lack of senior management support
- Project team

While some of the reasons cited in this article may also be partially true, often the root cause is a poor fit between the solution and the organization. Identifying the best fit between a security solution and a specific organization is analogous to finding the correct piece in a complex jigsaw puzzle. To find the right piece, it is necessary to look at all aspects of the piece itself, as well as the surrounding pieces. If there is a failure to make an appropriate survey of both the piece (solution) and the puzzle (organization), a mismatch may result. Each organization is unique because of a fusion of its culture, mission, vision and individuals. An organization’s security solution portfolio must be designed with a custom-made approach to optimize its value.

ENDNOTES

1 Brooks, Fred; The Mythical Man-Month, 2nd Edition, Addison-Wesley Professional, 1995