How to Validate Your Security Program: Part Two

By Ray Bernard

This is the second of a multi-part series that provides 15 important perspectives from which to validate your Security Program. If this is the first article you have seen in this series, please read at least the introductory article below before launching into the validation steps.

Introduction: *Top 5 Reasons to Validate Your Security Program*.

How to Validate Your Security Program Series: *Part One*.

Validation Attribute: Defensible

Definition: 1. that can be defended in argument; capable of withstanding attack.

The overall mission of security is to reduce security risks to acceptable levels, at an acceptable cost. The defensibility of any particular security program element consists of knowing exactly what is being done, why it is being done, and how its costs are acceptable to the alternatives of not doing anything or to doing something else.

This is why there are two things that seriously undermine the defensibility of a security program:

- lack of documentation that includes the *rationale* for the security program elements
- lack of record-keeping that shows the *value* of the program in action

This validation action addresses the first of the two: the rationale for each security program element.

The rationale is the business case for why the security program elements are needed. It is important to be able to articulate to the decision-makers and stakeholders what the business value is for individual security program elements. Security practitioners who have documented the rationale for their security program elements, and have developed very simple plain-language talking points around them, have reported that they subsequently encountered many opportunities to casually engage stakeholders on the subject. They were able to easily give the stakeholders insight into the business value behind some of the security program elements. *It is likely that such opportunities existed earlier, but—not having been prepared to discuss them—the opportunities weren't obvious to the practitioners.*

An additional benefit reported, and which occurs without necessarily having shared any information, is an increase in confidence that manifests itself in the demeanor of the practitioner.

Identifying Security Program Elements

In physical and corporate security programs it is common to have documentation for procedures and tasks, as well for job responsibilities, but these typically do not contain two important items: their rationale and performance criteria.

IT departments are usually more mature than physical or corporate security departments in their utilization of documentation. However, IT is sometimes weak in establishing the rationale behind the various aspects of security programs, and often don't establish performance criteria that directly speak to the program's value for the organization.

Security functions that apply security standards are guided by the standards to give appropriate thought to the design and structure of the security program, and to documenting the rationale behind each program element as well as its implementation plan. Sources for standards include the ISO/IEC standards, ANSI/ASIS standards, NIST, and security associations relevant to the business sector your organization operates in.

Regardless of the state of security program documentation, it is always possible to identify and document the rationale for the program and its individual elements. Without having clearly established the rationale for security program elements, and the language articulating them, the security practitioner's mindset is missing a critically important element.

Points of Defensibility

The points of defensibility for a security program can include:

- Security concerns reported by management
- Standards and guidelines
- Business sector commonly found risk factors
- Discovered/reported vulnerabilities

Validation Steps

Many security practitioners find that they can easily perform the validation steps for most of their security program elements—but for some their rationale has never really been expressed in writing.

Step 1. *Outline your security program.* If you your program is well-documented, you can easily extract a list of security program elements. If the documentation you have is in the form of an org chart, position or job descriptions, along with roles and responsibilities—you can identify security program elements under which the roles and responsibilities fall.

Step 2. *Make notes about the rationale for each element.* Remember that what is obvious to you may not be obvious to non-security personnel or even security staff. For each program element, provide the reason why that element is important to the business. A simple format is "The purpose for [name of security element] is to [describe what the element accomplishes]. If the element were not in place, [these bad things] are very likely to occur." It's not necessary to follow that format exactly, but however you present the rationale, it must be understandable from the perspective of management and the people outside of your security function who have responsibilities for ensuring the security measures or controls are followed or are in use. Another way to think of it is that you are describing the category or group of risks the element addresses, and identifying example risk impacts that are being prevented or minimized. Keep in mind that the rationale needs to answer the question. "Why is this important?"

Step 3. *Create a Security Program Chart.* Create a table or chart in a word processor or spreadsheet document that contains these columns:

- **Name:** the name of security program element
- **Date:** the approximate date the program element was initiated
- **Rationale:** a concise statement of the program element's rationale
- **Stakeholders:** the stakeholders who have an interest in the security element

Fill in the chart based upon the notes you made earlier, and any new thoughts you have while doing this exercise.

Step 4. *Reality Check.* Run these by a few non-security people to make sure that the statements make sense to them, and to catch any terms that aren't well known outside of your security function.

Step 5. *Staff Update.* For any direct reports you have, either individually or as a group, brief them or engage them in discussions about the information in the chart.

Step 6. *Stakeholder Check.* Who would or should care about each program element and why? The answers to this question identify the stakeholders.

Step 7. *Knowledge Capture and Follow-Up.* In the course of performing these steps, you may learn things that you did not expect to, or discover ideas (good or strange) that have existed about your security program elements. Be sure to document what you have learned and follow as appropriate where additional action is needed.

Ray Bernard, PSP, CHS-III is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities (www.go-rbcs.com). Mr. Bernard has also provided pivotal strategic and technical advice in the security and building automation industries for more than 28 years. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788. Mr. Bernard is also a member of the Subject Matter Expert Faculty of the *Security Executive Council* (www.SecurityExecutiveCouncil.com).