How to Validate Your Security Program: Part One

This is the first of a multi-part series that provides 15 important perspectives from which to validate your Security Program. The introduction the series is: Top 5 Reasons to Validate Your Security Program. Be sure to read the introduction first before jumping in to the validation details below.

Validation Attributes

As introduced in the previous article, the *validation attributes* that we apply to security programs are listed below in alphabetical order:

- accepted
- authoritative
- defensible
- effective
- justifiable
- official
- proven
- qualified
- relevant
- robust
- substantiated
- successful
- viable
- well-supported
- well-founded

We have found these to be key attributes of a sound security program. Validating your security program is an important exercise in beginning or continuing the transition from a mostly reactive security program to a mostly proactive security program.

Your Program's History

The vast majority of CSOs, security directors and security managers find themselves in the position of inheriting the security program established by their predecessor, and having to improve, correct—or in the worst case replace—that program. *All security programs are developed over time, as you can't do everything at once.* And always there is a lot to do, but not always the time and resources available to do it. This is why some things fall through the cracks, some things backslide, and most security programs are in the position of playing "catch-up" to business changes and changes to the risk picture.

The more you have inherited, the more important it is to validate your security program. If you have significantly changed what you have inherited, then it is just as important to validate your entire program, as the state of program documentation and the degree of business alignment will vary across the various program elements, depending upon how long they have been in force.

The Central Element in Your Security Program

Whatever your program's history is, and whatever improvements you have in mind, reviewing the current situation helps ensure that all steps going forward are well-placed steps. More importantly, it provides a baseline against which you can evaluate your managerial and supervisory role and the burden that role places upon you operationally. If the burden is excessive, that must be corrected before you embark on any significant improvements.

Going forward, security program improvements must be designed to make your job easier. **That's not selfishness, it's necessity, for three reasons.**

First, you are the central element in your security program. Without you—well, you know what's likely to happen.

Second, if each improvement to the security program increases the burden on you, it won't be long before a breaking point is reached.

Third, the pace of change for the business and to its risk picture are increasing for the foreseeable future. So even as you work to decrease your burden, external factors work to increase it. That's why now is the best time to gain the insights and perspectives you gain from validating your security program.

Validation Priorities

The order in which to address these validation points is not alphabetical. It is the order in which practitioners have found to **increase the stability of their own position**, and to make the **most orderly progress** out of stabilizing and advancing their security program implementation.

Because the central element in your security program is you, your role is the first priority. *This is why the first step in validating your security program starts with aligning your role within the business, and ensuring that the right stakeholders have the right idea about your role. It is seldom that stakeholders sufficiently aware of the critical importances of the security practitioner's role. Just as seldom are security practitioners aware of the misimpressions that key stakeholders have.*

Purpose of a Security Program

The overall mission of security is to reduce security risks to acceptable levels, at an acceptable cost. This is the job of a security program, according to the scope and objectives assigned to the program. Each and every one of these security program attributes is directly related to the capability of the security program to sufficiently address risk in the context of the organization to which it belongs.

Validation Attribute: Authoritative

Definition: 1. having due authority; having the approval of or weight of authority;

It is surprising how many times security assessors find security program elements or security actions that *exceed the actual authority* of the individual implementing or overseeing them. This is one reason why job descriptions are important. Rarely does an assessor find a security practitioner's job description to be a fair match to the practitioner's assigned authority and responsibility. This is relatively easy to fix, as most companies would prefer to change the job description rather than cancel operational security program elements.

As an added benefit, an accurate job description allows Human Resources to perform a valid market analysis of your pay level. **Without an accurate job description, you could be underpaid** while HR considers that you are overpaid! Don't take this validation step too lightly. Most practitioners report valuable and often surprising results from doing a thorough job on this particular action.

There are two rare situations for which an additional step of preparation can be needed:

- Your job description, *unlike those of your peers*, is minimalist and vague.

- Your job description *and those of your peers* are similarly minimalist and vague.

For first case, an unusually minimalist and/or vague job description, you should be able to work with your boss and HR to get example job descriptions so that you can get an idea of how to bring yours up to speed to what is commonly done in your organization.

For the second case, which I encountered once, HR intentionally wanted job descriptions to be "very high level and not detailed". I can't repeat the rationale that was being followed, but in that case we created the detailed kind of job description that would have been ideal to have, and worked with HR to for the validation steps, and for the first time the security practitioner's boss had a very clear picture of what went on in the security function, which was very beneficial.

If your job description has been recently created or updated, it can still be very beneficial to walk through these steps because unless you wrote the job description yourself, it may not be a sufficiently accurate summary of your actual responsibilities.

Validation Steps

Step 1. ***Gap Check.*** Review your job description to identify any item that you are not doing full justice to, then make notes on what should be improved, and add somewhere in your security improvement planning.

Step 2. ***Job Description Scope Check*****.** Study your job description closely, word-for-word, checking it against the combined scope of all the elements in your security program. Make notes about what needs to change in the job description.

Step 3. ***Job Responsibilities Check*****.** Most security programs evolve bit by bit, and it can be surprising how what you are doing can grow beyond the scope of your job description. Go over your job description again, this time checking it against the quarterly, monthly, weekly and daily actions that you take. Include all managerial and supervisory roles that you perform. Make additional notes about what needs to change in the job description.

Step 4. ***Advancement and Leadership Check.*** If you have security certifications that require continuing education, add continuing professional education as one of your responsibilities. If you act as a mentor or an on-the-job trainer for your peers or subordinates, include that as well. If you participate in cross-collaboration with another security function, incorporate that, too. If you sit on any committees, task forces, or working groups—add those roles as expected contributions of your position.

Step 5. ***Job Description Update*****.** Update your job description based upon the results of Steps #1 and #2.

Step 6. ***Talking Points Development.*** You should *be prepared* to discuss your job description update with the relevant stakeholders: your immediate boss, any security sponsors, any peers with whom you have a close working relationship, and last but not least Human Resources/Personnel. You may not end up saying much about the new job description, or you may end up sharing it fully. Regardless of how much you share the job description itself, your ability to articulate what you and your security department are doing will come in handy many times.

Here are some reasons that other practitioners have identified for updating their job descriptions:

- Changes to the organization's security needs
- Changes to the organization's risk picture
- Security function has evolved over time
- Responsibilities of the department head have increased

When communicating about the job description changes, it can be helpful to provide some specific examples of changes, especially risk-related changes. In describing the changes, remember that security improvements are not driven by your personal desires or those of your people, but by the organization's need to improve its risk picture. Or in some cases where cost-saving changes were made, simple fiscal responsibility.

You already know that, but the people you are talking to may not. **So ensure the message they receive is the one you intend them to receive.** For example, instead of saying "I wanted to . . . ", it is usually more accurate to say "the company needed us to . . ." and include a mention of the business reason for the change. Something else that helps is to reference the role from which you realized a change was needed. Instead of saying "I" or "me", you can reference yourself as the department head, or as a mentor. "I realized that the effectiveness of our personnel would be improved by incorporating [specific responsibility] at the department head level." That's easy to do in writing, but may take just a little bit of practice to get comfortable saying it verbally.

To be prepared for any discussions, write down at least one bullet point reason for each job description change, keeping in mind that you are referencing a business need and not just a personal desire.

Step 7. ***Job Description Communication.*** Prepare a simple explanation of why you updated your job description, including an interesting thing or two that you learned in the process. Submit the updated job description to your boss, explaining that it represents what you have been requested to do and what you have found necessary and important to do. With the understanding and approval of your boss, submit your new job description to HR (or have your boss submit it).

At some point in this validation step, it may happen that you get valuable feedback from your boss and/or HR. If that occurs, take the feedback to heart and let your boss (and HR, if appropriate) know about any follow-up that you may have done as a result of their feedback.

About the Author

Ray Bernard, PSP, CHS-III, has been writing for *Security Technology Executive* magazine for more than 20 years and is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities. Ray is also a subject matter faculty member of the Security Executive Council. Follow Ray on Twitter: @RayBernardRBCS. For more information on RBCS see: www.go-rbcs.com. Ray's Elsevier book is available on Amazon: *Security Technology Convergence Insights*.