RBCS
Ray Bernard
Consulting Services

Advancing the Mission of Security:

Reduce security risks to acceptable levels,
at an acceptable cost.

Security Ladder of Involvement

“People’s attitudes toward security in general and your organization’s security program in particular tend to fall into one of six categories, which we’ve put on what we call our ‘ladder of involvement’ in security.

- Ownership
- Participation
- Compliance
- Apathy
- Avoidance
- Subversion”

—Carl Roper, Dr. Lynn Fischer, and Joseph A. Grau, from page 75 of their book Security Education, Awareness and Training.

Many of us think of **security education** as a campaign or project that involves posters, slogans, policy reminders and perhaps a live or online security training class or two. That is a very narrow view, as the authors explain:

> *“Security education is everything we do to enable people in our organization to carry out their roles in our security program effectively and reliably, plus everything we do to influence them to do just that.”*

One-on-one education for key stakeholders who influence and direct others can be more important and effective than some of the typical “poster awareness programs” that have no supporting education and training elements.

Enabling and Influencing

My two favorite words in that statement are “**enable**” and “**influence**“. It doesn’t make much sense to try to **influence people** to carry out a role **if we don’t first enable them** with **the knowledge and the means** to do so. This provides a **good yardstick** against which to measure the current situation.

Moving Stakeholders Up the Ladder

Here is an **excellent exercise** for **security practitioners**:

1. **Make a list** of the **categories of security stakeholders** in your organization. For example, Purchasing Stakeholders, Business Unit Managers, Budget Decision-Makers, Risk Assessment Collaborators, ID/Access Badge Holders, and so on.

2. **For each category**, identify **where you want them to be** on the security **Ladder of Involvement**.

3. **Make your best estimate** based upon evidence and intuition, as to **what percentage of stakeholders** in each category are at **each level**.

Regardless of the scores, see **how your thinking has now changed** with regard to your **objectives for security education and awareness**. Where the results are not to your liking, consider what education, training and awareness elements would help improve the picture. One-on-one collaborative discussions with individual stakeholders to influence and direct others can be very effective in making changes amount the broader audience whom they influence and manage.

Helping security stakeholders understand their role, and enabling them to fulfill it, is **definitely not a "one-shot" action**. Depending upon your starting point and also how much happens to be on each stakeholder's plate at any time, helping the stakeholders could be a series of conversations and supporting actions that take place over a period of months. It's easier and often more effective to start with small steps, as each action can build on the previous one.

Basic Steps with Stakeholders

The following numbered **questions** below can server as the **underlying basis** for a **conversational discussion with security stakeholders.**

1. What is **your security role**?
2. Are you **fully empowered** for it?
3. If not, **what would it take to fully enable you** in that role?

Those questions capture the ultimate issues that you want to address. However, the questions are a bit to direct and are usually a bit of a leap for someone to consider, if they have no assigned security role or aren't aware of or disagree with their assigned role. (Sometimes a role exists in policy, such as is common with information security, but in practice is not given the attention it deserves and can become completely forgotten.)

Any manager or executive has at least a role in seeing that the personnel in his or her charge apply security policy and procedure and report about any security weaknesses or any over-burdensome security practices. *The most effective perspective is not one of "compliance"*—which is the historically common approach to security roles—*but one of "helping protect the critical assets and critical processes"* of the individual's business unit or functional area. **This small shift in attitude can make a very significant difference in the effectiveness of a security program.**

This is why you wouldn't ask these key questions directly, but would find good success with related sub-questions or discussion points like those shown below each question. The idea is to get the stakeholder's thinking going in the right direction. At the same time, you'll have an opportunity to discover the stakeholder's current concept about security and his or her relationship to it based upon job position or business unit risks.

The stakeholder group that is furthest away for your objectives for them is a suitable candidate group for your next initiative. **Remember that anything you do or say**–no matter how small–**has value** if it helps to **enable or influence** them to better fulfill their role.

Obviously these are example questions, and you'd have to determine what kind of discussion is appropriate to have given the security stakeholders in your organization, and the current state of information, physical and corporate security as it affects them.

Here are some example questions for a business unit manager or executive who has no specifically assigned security role.

1. What is **your security role**?

    a. How do you think most managers at your level feel about security in general? Too much, not enough, or something else?

    b. Are there any security policies or procedures that should be changed or improved to be less burdensome or more effective?

    c. Can you think of any ways in which security could or should support your business unit more or better?

    d. Could I ask you to take on the role of letting me know if at any time you think Security should be doing more or doing something differently?

    e. In the future, we may be doing (or updating, if they have already been done) some risk assessments around the critical assets and functions within the company. Before we start that initiative, I'll circle back and touch base with you about exactly what we have in mind at that time, and provide you with some idea of what our objectives are and what possible approaches might be effective. The idea is to minimize any interruption to your time or that of any of your key personnel.

    Note that in the initial conversation you wouldn't even address questions 2 and 3 below, as these would come later since the person has just been introduced into their security role.

Here are some example questions for a business unit manager or executive who does have an officially assigned security role, but hasn't been giving it the attention it requires.

1. What is **your security role**?

    a. In assessing our security program effectiveness, it appears that we haven't been giving some of our managers (or executives – as the case may be) the support they should be getting for their security-related managerial roles. For example, according to our business planning (notice we didn't say "company policy") we should be providing some guidance and assistance to mangers to help them annually assess the criticality of the information they depend upon, to make sure that our business continuity plans are sufficient to keep the business units at low risk from operational interruptions. *Over the past few years, do you recall receiving any guidance or communication about this particular managerial role?*

   b. Have the results of our last business unit information assessment been made easily available to you?

2. Are you **fully empowered** for your role?

   a. Have you been hampered in any way in accomplishing any information protection objectives that you have for your area?

   b. Do you have any current concerns about the current state of business continuity planning for your area?

   c. Is there anyone to whom you have delegated responsibilities in relating to information classification, protection or business continuity planning?

3. If not, **what would it take to fully enable you** in that role?

   a. As soon as I have talked to most of the other managers and executives, I'd like to circle back with you and let you know what the general status is across the business units, and what approach we are considering to close the information protection gaps. *Between now and then, would you let me know if you have any thoughts or questions on this topic?*

   b. We're thinking of establishing an Information Protection Council for the managers at your level, who would meet once a year, and to whom Security would report progress on initiatives that we undertake. We might have one or two ad hoc meetings throughout the year prior to undertaking any initiatives, or if we want to explore the potential impacts of any new security threats that appear on the horizon. The purpose would be to keep the managers from being blindsided by any new threats, and to provide a channel for feedback to Security regarding the efficiency and effectiveness of our programs. I guess I could describe this as a small but critical partnership between Security and the business unit managers. *Does that make sense to you? Is that likely to address any concerns that you might have now or in the future about the sufficiency of information protection in your area?*

Although information security has been used as the subject area above, this same approach could be applied to protection of critical materials and areas, such as copper storage, clean room manufacturing areas, warehouses, R&D materials, federally regulated materials, and so on.

Ray Bernard Consulting Services (RBCS, Inc.)
23600 El Toro Road #D-367 | Lake Forest, CA 92630
Office: 949-831-6788 | Direct: 949-472-8295 | Fax: 949-544-0414
E-Mail: RayBernard@go-rbcs.com | Follow on Twitter: @RayBernardRBCS