Measure/Rank/Evaluate/Grade Your Efforts!

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for October 2007 CSI Alert

Grades Indicate Improvement Needs As Well As Strengths

When I was growing up there was a trend in many schools to not give grades, but instead just give a "pass" or "needs improvement" mark in an effort not to damage the "delicate self-esteem" of children. My father, who taught and was also school superintendent for a few decades, believed that was hogwash. If you don't show how well students are doing in a subject for their age and grade level, how will you be able to know where improvement is necessary? How will you be able to know the specific areas in which a student needs to student more, or differently, to understand the subject better? How will you be able to know where curriculum needs improvement? How will you be able to tell if a teacher may not be living up to the standards established if you see all students are either doing very poorly, or if they are all doing exceptionally well across the board? As you can probably tell, we definitely had grades, including the minuses and pluses, within our school.

While a notable portion of the population would rather not establish any manner of measuring how well someone is doing, or how well some initiative is performing, in order to spare feelings, not measuring effectiveness is not good business. If you do not measure where your organization is at compared to where it started (your benchmark), or how close it is to meeting goals, you will not be able to clearly show how much change has occurred as a result of implementing certain business processes. This also applies to information security and privacy programs. If you do not establish some measurements, rankings, ratings, evaluations, metrics, key performance indicators (KPIs) or whatever label you want to use, you cannot demonstrate to your business leaders the value of your efforts to the business.

There has been a large amount of disagreement lately about what the correct "term" for the various types of evaluations should be called. It doesn't really matter whether or not a specific international evaluation term exists. What does matter is how you define the evaluations you are making within your organization, that you clearly communicate those definitions and then consistently follow them.

To demonstrate the need for evaluating program effectiveness I'm going to focus on measuring the effectiveness of information security and privacy awareness and training initiatives. These same concepts can be used for other types of initiatives.

Business Drivers for Evaluating Effectiveness

The goal of information security and privacy awareness and training should ultimately be to change personnel work habits so that they work in a more secure manner and protect the privacy of personally identifiable information (PII).

On 8/22/2007 the European Network and Information Security Agency (ENISA) released a study, "Information security awareness initiatives: Current practice and the measurement of success." It provides nice documentation validating this need to measure the effectiveness of information security education efforts to improve business.

It details the awareness methods that have worked and not worked, and the various experiences of a wide range of organizations.

There are many business drivers for maintaining documented measurements to track the effectiveness of your information security and privacy program. Documented measurements:

- Point out where you need to make improvements within your program.
- Highlight what is working well within your program.
- Show how much you have improved within specific areas of your program.
- Validate to stakeholders the value of information security and privacy initiatives.
- Demonstrate the need to invest in information security and privacy.
- Demonstrate due care processes are in place and are actively being followed to meet compliance requirements.
- Raise the awareness of information security and privacy issues.
- Highlight information security and privacy risk areas.
- Facilitate making better business decisions.

Components for Successfully Evaluating Effectiveness

There are many methods that can be used to evaluate the effectiveness of information security and privacy program initiatives. Don't get stuck only looking at the very specific, narrowly scoped technical measurements. While these types of metrics are useful, you also need to look at the big picture; your business enterprise.

How are information security and privacy initiatives and efforts impacting your business? You must always keep in mind that information security and privacy exists within your organization to support and protect your business and customers. Create and communicate your evaluations and measurements in terms of your business whenever possible.

When you are contemplating and planning for how you will perform your evaluations, be sure to include and document the following components:

- Evaluation topics
- Evaluation areas
- Evaluation methods
- Tangible benefits
- Intangible benefits

Don't get carried away and have too many measurements, though. After you brainstorm and document all your possible measurements, determine the ones most important for your business. You don't want to overwhelm your business leaders with too many measurements or they will not pay attention to any of them. Determine the ones that will resonate most with business.

Also determine how often to take the measurements. You will need to choose what is most appropriate for each of the topics. Some measurements will be appropriate to do once a year, and others will need to be done once a week to be meaningful.
You will also need to regularly re-evaluate the measurements you've chosen and fine-tune them, replace them, or completely do away with them. As your business changes

over time as a result of your training and awareness efforts, your metrics will also need to be modified.

Evaluation Areas For Your Awareness Program

It is important to know, and demonstrate to your business leaders, that your information security and privacy awareness efforts are valuable and are making an impact on the way your personnel do business. Before you can create measurements, grades or effectiveness ratings, though, you need to identify the areas within which you will be looking for these metrics. The following is largely an excerpt from my book *Managing an Information Security and Privacy Awareness and Training Program* (Boca Raton, FL: Auerbach, 2005), but I've updated it to provide more detail.

Verduin and Clark identified eight areas of evaluation for learning (*Distance Learning*. San Francisco: Jossey Bass, 1991); access, relevancy, quality, learning outcomes, impact, cost effectiveness, knowledge generation, and "general to specific." I find them useful when measuring the success of information security and privacy education efforts. Tailor them to facilitate the evaluation of your own organizational education programs by considering the questions listed with each area.

By answering the questions for each of these areas you will be better able to identify the types of metrics you should create to answer the questions, as well as focus better on how to communicate those metrics. I will not cover how to generate the metrics in this paper; that is a big topic and will be best discussed in a future article.

1. *Access.*
   - What groups are you targeting for your education efforts? List the groups that handle personally identifiable information (PII), use your networks, communicate directly with your customers, and so on. Check with other areas in your organization; use your information security and/or privacy oversight group if you have one. Ask them, are there groups missing?
   - Are all members of the target groups participating in the training offered to them? Why or why not? Are all personnel participating in awareness events? How many of the personnel have access to attend the awareness events? Are all personnel reading awareness communications? Do all personnel have access to awareness communications?
   - Are you providing appropriate delivery methods for your target audiences? Can all your target audience access your training and awareness materials and participate in your delivery methods?

2. *Relevancy.*
   - Is your education program relevant to your organization's business goals and expectations? Do your information security education messages have a clear link to the business goals? Do you explain how your privacy efforts support business efforts?
   - Are your training and awareness messages and information relevant to the participants' job responsibilities? Do you clearly communicate where information security actions occur within the normal execution of business transactions? Do you relate how privacy can be impacted by misuse of PII?

- Does your education program have a noticeable impact on business practices? How have personnel changed the way they handle and protect PII as a result of training and awareness? Is your training content appropriate for your target participants? Does your training cover information security and privacy regulatory and policy requirements?

3. *Quality*.
   - Does the quality of your information security and awareness materials effectively deliver the intended message? Do your communications capture the attention of your personnel throughout the training period? Does the quality of your training materials contribute to your learners' success?
   - Do your trainers and teachers deliver quality education? Do they know how to interactively adjust to the abilities and experiences of their learners? Do they have enough background and understanding of information security and privacy to be able to answer the learners' questions?
   - Were the conditions right for learning? Were the learners encouraged by management to participate in training? Did the learners indicate that, in their subjective opinion, they were satisfied with the quality of the training?

4. *Learning outcomes*.
   - Is the amount of time allowed for learning appropriate for successfully understanding the message? What do your learners say about the usefulness and effectiveness of your training and awareness activities? Do you speak to the learners about the expected outcomes of your education activities?
   - Do you tell the learners how their job activities should change as a result of taking the training? What did the learners actually learn, as evidenced through observable actions or through feedback from quizzes or follow-up surveys? Did your learners indicate they truly learned something from taking the training?

5. *Impact.*
   - What is the impact of your education program on your entire organization? Were security and privacy activities and habits noticeably changed in a positive way following training and awareness activities?
   - Were more information security incidents reported following training and awareness activities? Do personnel ask the information security and privacy areas more questions?
   - What are the long-term impacts? Did the training methods promote the desired information security and privacy skills? Did job performance improve? What was the trend related to noticeable personnel work changes following each training session?
   - Do you assist managers with determining their own workforce performance changes? Do you provide managers with communications to make them aware of the personnel changes they should notice and document following the training? Do you create related statistics to support and validate training and awareness funds?

6. *Cost effectiveness*.

- What time requirements is involved? Is the length of time necessary to take the training appropriate for not disrupting business work? How much time do your awareness activities take? Are education activities offered during normal work hours, during lunch, before and after work, and so on?
- What are the costs of the materials? Are the costs within budget? Are there ways in which cost can be reduced by partnering with other departments, or using donations from outside entities?
- How many people are in your targeted groups? How was training delivered? Did it allow for all personnel within the targeted groups to attend?
- Are you using inside or outside training and awareness resources, or both? What is the value of the method of awareness activity or training session you used compared to other awareness and training options?

7. *Knowledge generation*.
   - Do you understand and document specifically what is important for your personnel to know about information security and privacy? Do you understand and document specifically what is important for your managers to know?
   - Do you understand what works and what doesn't work within your education program? Are you actually utilizing your evaluation results?
   - Do you account for all types of learners; visual, audio and kinesthetic (hands-on)? Do you provide effective multi-media training methods? Do you provide awareness communications to account for all types of learners?
   - Do you assist employees in determining their own performance success for implementing the information they received? Do you compile trend data to assist instructors in improving both information security learning and teaching?

8. *General to specific*.
   - Do your instructors give learners enough information to allow them to evaluate their own success in implementing what they learn?
   - Are learners told overall goals for information security and privacy, along with the specific actions necessary to achieve them? Are information security and privacy goals and actions realistic and relevant to the business?
   - What is the necessary prerequisite general and specific information security and privacy knowledge for your personnel?

Measurements can be developed within each of these eight areas to demonstrate the value of information security and privacy activities for your business.

Consistently Measured Evaluations

Some believe that unless you can assign an exact number to your measurements, your measurements are not meaningful. Poppycock! There are many ways in which you can measure your effectiveness; through metrics, percentages, ratings, rankings, KPIs, grades and any other type of label you want to use. The most important consideration to make them truly useful is that they need to be consistently measured and applied.

Some argue that meaningful evaluations should not be subjective. Yes, there are many methods of evaluating effectiveness that can and should be objective. Specific measurements, such as the cost in dollars, the number of hours used, the numbers of

questions correctly answered, and so on, are valuable. However, there are also some very valuable measures that are necessarily subjective. Consistent and useful measurements can be obtained if your subjective measurements are clearly defined, and examples provided.

For example, it is important to know that the management in each of the departments are supporting awareness and training efforts. However, trying to measure this with an objective numerical value is hard, if even possible, to do. Management support is not a mathematically accurate concept. But you can determine a measurement for management support based upon clearly observable management characteristics and actions. Some possible measurements for information security and privacy education management support include the following:

1. **Unacceptable**. Management did not make awareness communications available to staff. Management did not send staff to available and applicable information security and privacy training sessions. If you want a value assigned instead of the "Unacceptable" label, use the value "1."
2. **Needs Improvement**. Management sends some, but not all, staff to information security and privacy training sessions. Management occasionally, but inconsistently, provides awareness communications to the staff. If you want a value, use "2."
3. **Satisfactory**. Management consistently sends most staff to information security and privacy training offerings. Management consistently gives staff access to awareness communications. Use the value "3" if you want.
4. **Better Than Expected**. Management sends all staff to training offerings regularly and always to usually returns training evaluation forms. Management actively and visibly encourages all staff to participate in awareness events. The value "4" would correlate with this label.
5. **Role Model**. Management has incorporated information security and privacy training into staff job requirements and performance appraisals. Management urges staff to create information security and privacy awareness communications tailored to their own areas, along with participating in corporate awareness activities.

Subjective evaluations can tell a lot about awareness efforts in addition to other metrics if they are consistently applied.

Your Measurements Are Unique To Your Organization

Effective use of information security and privacy measurements can have a profound impact on your business. As you gain a better understanding of your business and move closer to achieving important goals, your day-to-day work will become easier and your staff will be more accountable for the measurements that matter. You'll make sound information security and privacy decisions based upon consistently generated measurements that are created in the context of business.

I see too many organizations try to use a cookie cutter approach to establishing information security and privacy measurements. I see too many vendors pushing their cookie cutter metrics onto organizations, only to subsequently have the organizations realize they are trying to measure something that isn't applicable to them.

The axiom generally attributed to Peter Drucker holds true for information security and privacy efforts, “You can’t manage it if you can’t measure it.” You also cannot be successful in your efforts if you do not maintain measurements. Organizations must establish metrics based upon their own unique organizational characteristics. They can use ideas obtained from others, but their ultimate metrics must be customized to fit their organization.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She just released the quarterly employee awareness tool, “Protecting Information” (Information Shield) and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.