Preface

I hope that what you read here sounds and feels familiar. If the result of reading this gives voice to some of your own experiences, or provides new ideas that contribute to your success, then I have succeeded. At times, you will hear strong recommendations around proprietary products and processes. I make no apologies, for I would do all readers a disservice if I failed to disclose with great passion those interventions that can change your company. At the same time, I provide guidelines and suggestions on how to create your own versions of these solutions.

As you take your own journey, I would like to hear from you. I invite you to email me with your questions and stories of your victories as you chart your own change path. (mguenther@cox.net)

A common thread of those that had success with security awareness efforts all talked about giving people clear direction and immediately enlisting their energies in creating that future.

I have accepted positions in academia, Fortune 100 and small businesses, and found myself in a variety of situations with one constant. People. Regardless of presenting issues, whether occurring in associations, institutions, or corporations, profit or nonprofit, success ultimately boils down to meeting a challenge, solving a problem, or forging a better future. And it takes people to accomplish these feats. Even if you define change as implementing technical solutions, such as a Firewall or automatic update installations, ***technology doesn't work unless people decide to make it work.***

Getting people involved in the process - because people are the ones who make changes work - is key. ***"Organizations don't change – people change. And then people change organizations."***

SETTING THE GOAL

Before beginning to develop the content of a security awareness program, it is essential to establish the objective or goal. It may be as simple as "all employees must understand their basic security responsibilities" or "develop in each employee an awareness of the IT security threats the organization faces and motivate the employees to develop the necessary habits to counteract the threats and protect the IT system."

Some may find it necessary to develop something more detailed, as shown here: Employees must be aware of:

- Threats to physical assets and stored information
- How to identify and protect sensitive (or classified) information

- Threats to open network environments
- How to store, label, and transport information
- Federal laws they are required to follow, such as copyright violations or privacy act information
- Who they should report security incidents to, regardless of whether it is just a suspected or actual incident
- Specific organization or department policies they are required to follow
- E-mail/Internet policies and procedures
- AUP (Acceptable Use Policy) adherence

When establishing the goals for the security awareness program, keep in mind that they should reflect and support the overall mission and goals of the organization. At this point in the process, it may be the right (or necessary) time to provide a status report to the Chief Information Officer (CIO) or other executive members.

I use a tool with Executive Teams to create a dialogue (shared meaning) regarding security Awareness. The exercise entails facilitating a working session where the participants identify a minimum of 4 Levels of SA and then define the characteristics of each level.

The end result is a tool that can be used throughout your project to communicate visible results. The benefits derived from the process, however, are priceless because it articulates a clear direction and immediately enlist the executive teams energies in creating that future.
A sample of the text for the tool is attached at the bottom of this paper. I use a more graphic version because I use it as a mental model for the duration of each assignment.

EVALUATION

All management programs, including the security awareness program, must be periodically reviewed and evaluated. In most organizations, there will be no need to conduct a formal quantitative or qualitative analysis. It should be sufficient to informally review and monitor whether behaviors or attitudes have changed.

Rather than suggest a “Best Practice” approach with SA metrics and Evaluation, framing ***Effective*** SA Evaluation and Metrics effort is much more realistic. There are to many things that influence the SA program, i.e., culture, threats and vulnerabilities, varying regulatory drivers, centralized vs. decentralized environment, etc. Because of these differences, evaluation of programs is not a one-size-fits-all effort. Rather, the following provides a few simple options to consider:

1. **Distribute a survey or questionnaire seeking input from employees.**
   If an awareness briefing is conducted during the new-employee orientation, follow up with the employee (after a specified time period of three to six months) and ask how the briefing was perceived (i.e., what do they remember, what would they have liked more information on, etc.).

2. **Walk-about's.** While getting a cup of coffee in the morning, ask others in the room about the awareness campaign. How did they like the new poster? How about the cake and ice cream during the meeting? Remember that the objective is to heighten the employee's awareness and responsibilities of computer security. Thus, even if the response is "that poster is silly," do not fret; it was noticed and that is what is important.

3. **Track the number and type of security incidents that occur before and after the awareness campaign.** Most likely, it is a positive sign if one has an increase in the number of reported incidents. This is an indication that users know what to do and who to contact if they suspect a computer security breach or incident.

Putting metrics in perspective – A Case Study

Four years ago my organization determined that one of our key areas for security focus was viruses and worms. We had two main goals. First, to reduce the number of lost work hours in the organization due to virus/worm infection and effort required trying and preventing virus/worm infections. The second was to reduce or eliminate secondary infections of our business partners. Our organization has over 1100 employees and we have a business partner who has access to our networks and receives hundreds to thousands of emails from us daily. We obviously made some technical changes (automatic signature distribution, controls between us and the partner, etc.) and they helped reduce the problems in the first year or so after introducing them. After that we reached a plateau. So we introduced an awareness program. It consists of an Intranet website dedicated to virus problems, security bulletins for new virus/worm outbreaks and regular, monthly security awareness articles. We have not changed our technical controls whatsoever since that point except to upgrade them as our vendors released new versions, etc.

Here's what happened:

Then - 6,000 hours expended annually to control virus/worm outbreaks in 2000
Now - Less than 2,000 hours in 2003

Then - 5 significant virus/worm outbreaks in 2000

Now - 2 significant virus/worm outbreaks in 2003

Then - Out of a typical 25 new helpdesk requests per business day, four of them dealt with virus/worm problems
Now - New helpdesk requests per day has increased to 28 on average, virus/worm requests have dropped to less than 1 per day

4. **Conduct "spot checks" of user behavior.** This may include walking through the office checking if workstations are logged in while unattended or if sensitive media are not adequately protected.

5. **If delivering awareness material via computer-based delivery, such as loading it on the organization's intranet, record student names and completion status.** On a periodic basis, check to see who has reviewed the material. One could also send a targeted questionnaire to those who have completed the online material.

6. **Have the system manager run a password-cracking program against the employee's passwords.** If this is done, consider running the program on a stand-alone computer and not installing it on the network. Usually, it is not necessary or desirable to install this type of software on one's network server. Beware of some free password-cracking programs available from the Internet because they may contain malicious code that will export one's password list to a waiting hacker.

Keep in mind that the evaluation process should reflect and answer whether or not the original objectives/goals of the security awareness program have been achieved. Sometimes, evaluations focus on the wrong item. For example, when evaluating an awareness program, it would not be appropriate to ask each employee how many incidents have occurred over the last year. However, it would be appropriate to ask each employee if they know whom to contact if they suspect a security incident.

Baseline Program Recommendation

1. Review the methods being used to monitor control effectiveness and employee compliance.
2. Review the effectiveness and attendance of the awareness sessions.
3. If used, review incident reports, their effectiveness, and the methods used to follow up on them. Also, check if employees are using incident reports to describe ineffectiveness of management controls or technical controls.
4. Review methods used to provide rewards and recognition to employees and groups that effectively protect information and comply with controls. Where recognition is not effective, determine why.

Baseline Incident Data

The next area provides areas that potentially relate to security/privacy awareness. It is recommended that you track responses for the period covering the last six (6) months.

How many virus outbreaks has your organization experienced? _____
How many mobile devices (such as laptops, PDA's, cell phones) have been stolen or compromised? _____
How many calls does your IT help desk receive due to forgotten passwords? _____
How many incidents of password theft have been reported? _____
How many intrusion incidents to your network have been detected? _____
a. How many required investigation by your technical staff? _____
b. How many required outside or criminal investigations? _____
How many of the intrusions cited in previous question
a. Were due to the exploitation of weak passwords? _____
b. Were due to the exploitation of application vulnerabilities? _____
c. Were due to social engineering? _____
d. Were from insiders? _____
e. Were from an external source? _____
Physical Theft
a. How many incidents of physical theft have occurred? _____
b. What percentage of these thefts would have been prevented by encryption, shredders, laptop locking devices, etc.? _____%
15. Of all Incidents your organization has experienced:
a. How many incidents were classified as workplace violence? _____

Business Impact Data:

What dollar amount was lost due to:
a. Legal fees? $_____
b. Resources to resolve incorrect billing? $_____
c. Paying for fraudulent calls/phone fraud? $_____

What dollar amount was lost due to security breaches?
a. Weak passwords? $_____
b. Social engineering? $_____
c. Employee-lost or stolen data? $_____
What dollar amount of new business/lost sales were impacted as a result of a security breach?
What dollar amount were impacted to your need to comply with one of more regulatory requirements (SLBA 1386, GLBA, HPAA, etc.)/

What dollar amount was lost due to lost productivity from chain letters and/or SPAM? $_____

What dollar amount is associated with inappropriate/miss-use of Internet surfing? $_____

What dollar amount is associated with the inappropriate/miss-use of email? $_____

Does your organization have insurance to cover security breaches (yes/no)? _____

If your answer was yes, did the existence of a Security Awareness Program reduce your insurance premium? $_____

a. Weak passwords? $_____
b. Social engineering? $_____
c. Employee-lost or stolen data? $_____

Have there been any positive business impacts as a result of the Security Awareness Program? If so, what are they?

Role of Uncertainty / Things we Missed:

What percentage would you use as a confidence factor about the responses given in this survey? Where 100% equals certainty. _____%

Are there any noteworthy anecdotes or incidents that you can share with us?

Benefits Are Difficult to Measure in the Short Term

The benefits of a training program are not tangible in the short term and can be difficult to measure in the long term. One can attempt to quantify potential benefits by revisiting both of the very real incidences that have occurred. For example, in a scenario in which the laptop computers were stolen, the losses are calculated as follows:

From this example, part of the loss is quantifiable.

If $20,000 had been spent on a SA&TP or procedures development, the thefts may not have occurred. Tangible savings to the organization are estimated to be $18,000.

5 laptops @ $3500	= $17,000 (tangible loss)
Consulting rework (200 hours @ avg. $100/hr)	= $20,000 (tangible loss)
Administrative staff to order, configure and distribute new PCs	
PCs (30 hours @ avg. $50/hr)	= $1,500 (tangible loss)
TOTAL TANGIBLE LOSS	**$38,500**

Client information	= Unknown (intangible loss)
Potential lawsuit from mishandling sensitive and confidential client information	= Unknown (intangible loss)

From this example, part of the loss is quantifiable. If $20,000 had been spent on a SA&TP or procedures development, the thefts may not have occurred. Tangible savings to the organization are estimated to be $18,000.

Summary
Tangible loss $38,000
SA&TP investment $20,000
Tangible savings $18,000

When an SA program is in place, it is difficult to know what would have happened if the SA program had not been in place. It is difficult to measure what has not yet occurred. Loss estimates can be formulated on previous incidences or potential incidences that are caught quickly and rectified due to proactive procedures. Comparisons can be made to incidences involving the competition within the same enterprise. If the incidence has occurred at a competitor, then more likely than not, it is a realistic threat and proactive measures should be taken to keep it from happening within one's own organization.

Goals-Based Evaluation
(Are you programs achieving your overall, predetermined objectives?)

Goal-based evaluations are evaluating the extent to which programs are meeting predetermined goals or objectives. Often programs are established to meet one or more specific goals. These goals are often described in the original program plans.
Questions to ask yourself when designing an evaluation to see if you reached your goals are:

- How were the program goals (and objectives, is applicable) established? Was the process effective?
- What is the status of the program's progress toward achieving the goals?
- Will the goals be achieved according to the timelines specified in the program implementation or operations plan? If not, then why?
- Do personnel have adequate resources (money, equipment, facilities, training, etc.) to achieve the goals?
- How should priorities be changed to put more focus on achieving the goals? (Depending on the context, this question might be viewed as a

program management decision, more than an evaluation question.)

- How should timelines be changed (be careful about making these changes - know why efforts are behind schedule before timelines are changed)?

- How should goals be changed (be careful about making these changes - know why efforts are not achieving the goals before changing the goals)? Should any goals be added or removed? Why?

- How should goals be established in the future?

Process-Based Evaluations
(Understanding how your program really works, and its strengths and weaknesses)

Process-based evaluations are geared to fully understanding how a program works -- how does it produce that results that it does. These evaluations are useful if:

- Programs are long-standing and have changed over the years,
- Stakeholders report a large number of complaints about the program,
- There appear to be large inefficiencies in delivering program services and
- They are also useful for accurately portraying to outside parties how a program truly operates (e.g., for replication elsewhere).

There are numerous questions that might be addressed in a process evaluation. These questions can be selected by carefully considering what is important to know about the program. Examples of questions to ask yourself when designing an evaluation to understand and/or closely examine the processes in your programs are:

- On what basis do members decide that products or services are needed?

- What is required of members in order to deliver the product or services?

- How are members trained about how to deliver the product or services?

- How do members come into the program?

- What is required of members?

- What is the general process that members go through with the program?

- What do members consider to be strengths of the program?

- What do board members consider to be strengths of the product or program?

- What typical complaints are heard from members?

- What do members recommend to improve the product or program?

Outcomes-Based Evaluation
(Identifying benefits to stakeholders)

Program evaluation with an outcomes focus is increasingly important for behavior change and asked for by stakeholders, especially those that are funding your efforts. An outcomes-based evaluation facilitates your asking if your organization is really doing the right program activities to bring about the outcomes you believe (or better yet, you've verified) to be needed by your members (rather than just engaging in busy activities which seem reasonable to do at the time).

Outcomes are benefits to stakeholders from participation in the program. Outcomes are usually in terms of enhanced learning (knowledge, perceptions/attitudes or skills) or conditions, e.g., increased incident reporting, increased security, decrease virus or Trojan attacks, etc. Outcomes are often confused with program outputs or units of services, e.g., the number of clients who went through a program.

The United Way of America (http://www.unitedway.org/outcomes/) provides an excellent overview of outcomes-based evaluation, including introduction to outcomes measurement, a program outcome model, why to measure outcomes, use of program outcome findings by agencies, eight steps to success for measuring outcomes, examples of outcomes and outcome indicators for various programs and the resources needed for measuring outcomes. The following information is a top-level summary of information from this site.
To accomplish an outcomes-based evaluation, you should first pilot, or test, this evaluation approach on one or two program interventions s at most (before doing all interventions).
The general steps to accomplish an outcomes-based evaluation include to:

- Identify the major outcomes that you want to examine or verify for the program under evaluation. You might reflect on your mission (the overall purpose of your organization) and ask yourself what impacts you will have on your stakeholders as you work towards your mission. For example, if your overall mission is to provide opportunities to report a security incident, then ask yourself what benefits this will have on those that report if you effectively provide them processes and information needed to report and other services or resources.

- As a last resort, you might ask yourself, "What major activities are we doing now?" and then for each activity, ask, "Why are we doing that?" The answer to this "Why?" question is usually an outcome. This "last resort" approach, though, may just end up justifying ineffective activities you are doing now, rather than examining what you should be doing in the first place.

- Choose the outcomes that you want to examine, prioritize the outcomes and, if your time and resources are limited, pick the top two to four most important outcomes to examine for now.

- For each outcome, specify what observable measures, or indicators, will suggest that you're achieving that key outcome with your clients. This is often the most important and enlightening step in outcomes-based evaluation. However, it is often the most challenging and even confusing step, too, because you're suddenly going from a rather intangible concept, e.g., increased security incident reporting, to specific activities, e.g., supporting stakeholders to report incidents, etc. It helps to have a "devil's advocate" during this phase of identifying indicators, i.e., someone who can question why you can assume that an outcome was reached because certain associated indicators were present.

- Specify a "target" goal of clients, i.e., what number or percent of clients you commit to achieving specific outcomes with, e.g., "increased incident reporting (an outcome) for 70% of all (company employees, campus constituents, etc.) as evidenced by the following measures (indicators) ..."

- Identify what information is needed to show these indicators, e.g., you'll need to know how many individuals in the target group reported incidents, how valuable the information reported was perceived to be, any benefits obtained as result of that incident reporting, etc. If your program is new, you may need to evaluate the process in the program to verify that the program is indeed carried out according to your original plans. (Michael Patton, prominent researcher, writer and consultant in evaluation, suggests that the most important type of evaluation to carry out may be this implementation evaluation to verify that your program ended up to be implemented as you originally planned.)

- Decide how can that information be efficiently and realistically gathered (see Selecting Which Methods to Use below). Consider program documentation, observation of program personnel and clients in the program, questionnaires and interviews about clients perceived benefits from the program, case studies of program failures and successes, etc. You may not need all of the above. (see Overview of Methods to Collect Information below).

7. Analyze and report the findings (see Analyzing and Interpreting Information below).

Overview of Methods to Collect Information (by Carter McNamara, PhD; last revision: Feb 16, 1998)

The following table provides an overview of the major methods used for collecting data during evaluations.

Method	Overall Purpose	Advantages	Challenges
Questionnaires, surveys, checklists	When need to quickly and/or easily get lots of information from people in a non threatening way	-Can complete anonymously -inexpensive to administer -easy to compare and analyze -administer to many people -can get lots of data -many sample questionnaires already exist	-Might not get careful feedback -wording can bias client's responses -are impersonal -in surveys, may need sampling expert - doesn't get full story
Interviews	When want to fully understand someone's impressions or experiences, or learn more about their answers to questionnaires	-Get full range and depth of information -develops relationship with client -can be flexible with client	-Can take much time -can be hard to analyze and compare -can be costly -interviewer can bias client's responses
Documentation review	When want impression of how program operates without interrupting the program; is from review of applications, finances, memos, minutes, etc.	-Get comprehensive and historical information -doesn't interrupt program or client's routine in program -information already exists -few biases about information	-Often takes much time -info may be incomplete -need to be quite clear about what looking for -not flexible means to get data; data restricted to what

			already exists
Observation	To gather accurate information about how a program actually operates, particularly about processes	-View operations of a program as they are actually occurring -can adapt to events as they occur	-Can be difficult to interpret seen behaviors -can be complex to categorize observations -can influence behaviors of program participants -can be expensive
Focus groups	Explore a topic in depth through group discussion, e.g., about reactions to an experience or suggestion, understanding common complaints, etc.; useful in evaluation and marketing	-Quickly and reliably get common impressions -can be efficient way to get much range and depth of information in short time - can convey key information about programs	-Can be hard to analyze responses -need good facilitator for safety and closure -difficult to schedule 6-8 people together
Case studies	To fully understand or depict client's experiences in a program, and conduct comprehensive examination through cross comparison of cases	-Fully depicts client's experience in program input, process and results -powerful means to portray program to outsiders	-Usually quite time consuming to collect, organize and describe -represents depth of information, rather than breadth

Planning Your Outcomes Evaluation: Analyzing/Reporting Preparation

Strongly consider getting evaluation expertise now to review, not only your methods of data collection mentioned above, but also how you can analyze the data that you collect and how to report results of that analyses.
Before you analyze your data, *always* make and retain copies of your data.

Analyzing Your Data
For dealing with numerical data with numbers, rankings:
-- Tabulate the information, i.e., add up the ratings, rankings, yes's, no's for each question.
-- For ratings and rankings, consider computing a mean, or average, for each question.
-- Consider conveying the range of answers, e.g., 20 people ranked "1", 30 ranked "2", and 20 people ranked "3".
To analyze comments, etc. (that is, data that is not numerical in nature):
-- Read through all the data
-- Organize comments into similar categories, e.g., concerns, suggestions, strengths, etc.
-- Label the categories or themes, e.g., concerns, suggestions, etc.
-- Attempt to identify patterns, or associations and causal relationships in the themes

Reporting Your Evaluation Results
- Level and scope of information in report depends for whom the report is intended, e.g., funders, board, staff, clients, etc.
- Be sure employees have a chance to carefully review and discuss the report before sent out
- Funders will likely require a report that includes executive summary – the summary should highlight key points from the evaluation, and not be a Table of Contents

Example of Evaluation Report Contents
Title Page (name of the organization that is being, or has a product/service/program that is being, evaluated; date)
Table of Contents
Executive Summary (one-page, concise overview of findings and recommendations)
Purpose of the Report (what type of evaluation(s) was conducted, what decisions are being aided by the findings of the evaluation, who is making the decision, etc.)
Background About Organization and Product/Service/Program that is being evaluated
-- a) Organization Description/History
-- b) Product/Service/Program Description (that is being evaluated)
-- -- i) Problem Statement (in the case of nonprofits, description of the community need that is being met by the product/service/program)
-- -- ii) Overall Goal(s) of Product/Service/Program

-- -- iii) Outcomes (or client/customer impacts) and Performance Measures (that can be measured as indicators toward the outcomes)
-- -- iv) Activities/Technologies of the Product/Service/Program (general description of how the product/service/program is developed and delivered)
-- -- v) Staffing (description of the number of personnel and roles in the organization that are relevant to developing and delivering the product/service/program)
Overall Evaluation Goals (e.g., what questions are being answered by the evaluation)
Methodology
-- a) Types of data/information that were collected
-- b) How data/information were collected (what instruments were used, etc.)
-- c) How data/information were analyzed
-- d) Limitations of the evaluation (e.g., cautions about findings/conclusions and how to use the findings/conclusions, etc.)
Interpretations and Conclusions (from analysis of the data/information)
Recommendations (regarding the decisions that must be made about the product/service/program)
Appendices: content of the appendices depends on the goals of the evaluation report, e.g.:
-- a) Instruments used to collect data/information
-- b) Data, e.g., in tabular format, etc.
-- c) Testimonials, comments made by users of the product/service/program
-- d) Case studies of users of the product/service/program
-- e) Logic model
-- f) Evaluation plan with specified outcomes, sources to collect data, data collection methods, who will collect data, etc.

Summary

“What does not get measured, does not get done,” or at best, ‘does not get done right.’ Because, how do you know it got done right if we do not have measurements of anything? That is why effective Security Awareness programs uses measurements and bench-marking techniques to track the quantity and quality of communication, its impact, and the degree to which it achieved its objectives.

As you start developing your SA Plan, keep the idea of measurement in mind. In formulating any goal, think of how you will measure it. Ask, “How we will know when we have achieved this goal?”

Then incorporate the measurement right into the goal design. For example, instead of a general goal statement like: ‘our goal is to enhance the security our organizational information,” use a goal that states, “To increase the security of organizational information by 5% over the next two-year period.”

But to increase the security of security information by 5% you must have a measurement of the security of information before you start and then again at the end of two years. Once you start measuring, you will have a benchmark to which to compare future efforts.

If you do not have measurements already established for your past efforts, you might want to take the opportunity of developing your SA Plan to start this benchmarking process. Measurements do not have to be complex and do not have to require a degree in statistics to conduct or understand.

Too complex a measurement system often defeats its own purpose by being more subject to errors. In addition, when it is too complex to understand, people stop trying to make sense of it, and therefore it becomes practically useless. What is needed is a simple, yet effective, measurement system that gives you benchmarking to facilitate future references and measurements.

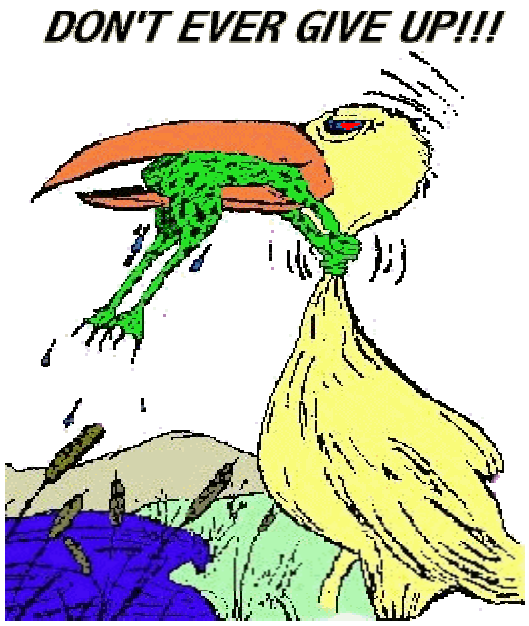
By deploying benchmarking and measurements you will be speaking a language senior management understands and uses all the time. By using measurements, your efforts will be seen as an important management process that achieves tangible results for the organization.

I do recognize, however, that measurements often take time and money to do. Some organizations, or Security departments, might not be able to invest too much time or money in this process. In such case, you can still produce an effective SA process to communicate the organization's strategy and goals to its constituencies without measurements. Many organizations do this and are satisfied with the results.

Conclusion

This SA campaign ought not be an end,*
Replacing what within we might achieve.
After all, the good that we intend
Does much to serve the good that we receive.
Underneath the mask of a decree
A person must perform with just the skill,
The knowledge and the art that he or she
Internalized through pluck, hard work, and will.
On what we are will rest what we become,
Nor do we have much else to draw upon.
Thomas Tallis

*"SA campaign" inserted



Sample Metrics and Benchmark Tool
Which of the following best describes your security/privacy awareness program?

Level _____

Level 1
Complacency.

Information Security Policies & Standards are minimal and may or may not be documented.
Information Security Incidents are viewed as someone else's problem. Security/Privacy is viewed as a technology problem.
No Awareness program or interventions are in place.

Level 2
Acknowledgement.

Realization that existing Security processes are fragmented.
Security/Privacy is seen as a business enabler.
Realization that a focused Information Security/Privacy Program & Organization is needed.
Efforts are compliance based only and are driven by regulatory triggers only (HIPPA, GLBA, Federal Sentencing guidelines, etc.)
No metrics in place to measure effectiveness of security interventions.

Level 3
Integration.

There is a general acceptance of organization-wide standards based on Information Security Infrastructure.
There are effective communication tools in place to ensure all employees are familiar with Security policies and procedures.
Employees are aware of the alignment of the Policy & Procedures and their specific jobs.
Some security/privacy awareness and accountability is anchored.
Technology, Operations and Awareness/Education/Training applied as security solutions.

Level 4
Common Practice.

The Security Infrastructure is established. The integration of Security programs and services in the business units is complete. Security is brought in at the onset of every new project and program. Management actively and visibly participates in the Security programs and services. Incident reporting is fast and effective. Security/Privacy Awareness is mandatory for all employees, and all employees sign Annual Acceptance of Responsibility Statements.

Level 5
Continuous Improvement.

Threats are continually reevaluated based on changing threat population and security incidents. The practice of Security/Privacy is considered a component of the corporate culture and accountability is apparent and measurable. Security/Privacy awareness is measured on individual performance reviews. Employees understand the need for security and know their individual responsibilities are the best protection we can have!