9

Establishing a Metrics Management System

Don't work harder—work smarter.—Ken Blanchard

CHAPTER OBJECTIVE

This chapter, "Establishing a Metrics Management System," is designed to provide basic guidance necessary for the development of a metrics methodology to understand what, why, when, and how InfoSec can be measured. Using the fictitious company (IWC) and functions that were previously described, a metrics system will be developed. It includes a discussion of how to use the metrics to brief management, justify budget, and use trend analyses to develop a more efficient and effective CIAPP.

INTRODUCTION

Some of the most common complaints ISSOs make are that management doesn't support them, and—as the famous comedian Rodney Dangerfield is known for saying—"I get no respect." Another complaint is that the cost and benefits of InfoSec cannot be measured.

As for the first two, you get support because you are being paid—and these days, more often than not, quite handsomely—and you have a budget that could have been part of corporate profits. Furthermore, respect is earned. Besides, if you want to be popular, you are definitely in the wrong profession.

One often hears management ask:

- "What is all this security costing me?"
- "Is it working?"
- "Can it be done at less cost?"
- "Why isn't it working?"

That last question often comes right after a successful denial of service attack or some other attacks on the corporate systems or Web sites. Of course, many ISSOs respond by saying that it can't be measured. That is often said out of the ISSO's ignorance of processes to measure costs or because the ISSO is too lazy to track costs.

The more difficult question to answer is, "What are the measurable benefits of a CIAPP and InfoSec functions that provide support under the CIAPP?" Of course, one could always use the well-worn-statement, "It can only be measured as a success or failure depending on whether or not there have been successful attacks against our systems." The truth is that many attacks go unnoticed, unreported by the users or IT people. Furthermore, separating attacks from "accidents" (human error) is usually not easy; however, metrics can help in the analyses.

What Is a Metric?

To begin to understand how to use metrics to support management of a CIAPP, it is important to understand what is meant by "metrics." For our purposes, a metric is defined as *a standard of measurement using quantitative, statistical, and/or mathematical analyses*.

What Is an InfoSec Metric?

An InfoSec metric is the application of quantitative, statistical, and/or mathematical analyses to measuring InfoSec functional trends and workload—in other words, tracking what each function is doing in terms of level of effort (LOE), costs, and productivity.

There are two basic ways of tracking costs and benefits. One is by using metrics relative to the day-to-day, routine operations of each InfoSec function. These metrics are called level of effort (LOE) and are the basic functions noted in the ISSO's charter of responsibilities and accountabilities. Examples would be daily analyses of audit trail records of a firewall; granting users access to systems; and conducting noncompliance inquiries. In more financial terms, these are the recurring costs.

The other way of tracking costs and benefits is through formal project plans. In other words, if the tasks being performed are not the normal LOE tasks, then they fall under projects. Remember that functions are never-ending, daily work, while projects have a beginning and ending date with a specific objective. In more financial terms, these are the nonrecurring costs.

So, in order to efficiently and effectively develop a metrics management program, it is important to establish that philosophy and way of doing business. Everything that an ISSO and staff do can be identified as fitting into one of these two categories: LOE or project.

What Is InfoSec Metrics Management?

InfoSec metrics management is the managing of a CIAPP and related InfoSec functions through the use of metrics. It can be used where managerial tasks must be supported for such purposes as backing the ISSO's position on budget matters, justifying the cost-effectiveness of decisions, or determining the impact of downsizing on providing InfoSec service and support to customers.

The primary process to collect metrics is as follows:

- Identify each InfoSec function[1];
- Determine what drives that function, such as labor (number of people or hours used), policies, procedures, and systems; and
- Establish a metrics collection process. The collection process may be as simple as filling out a log for later summarization and analysis. The use of a spreadsheet that can automatically incorporate InfoSec statistics into graphs is the preferred method. This will make it easier for the ISSO to use the metrics for supporting management decisions, briefings, etc.

The decision to establish a process to collect statistics relative to a particular InfoSec function should be decided by answering the following questions:

- Why should these statistics be collected?
- What specific statistics will be collected?
- How will these statistics be collected?
- When will these statistics be collected?
- Who will collect these statistics?
- Where (at what point in the function's process) will these statistics be collected?

By answering these questions for each proposed metric, the ISSO can better analyze whether or not a metrics collection process should be established for a particular function. This thought process will be useful in helping explain it to the InfoSec staff or management, if necessary. It will also help the ISSO decide whether or not the ISSO should continue maintaining that metric after a specific period of time. Since the IWC ISSO had

[1] It is assumed each function costs time, money, and use of equipment to perform.

begun with an analysis of InfoSec requirements (drivers) that led to identification of an ISSO charter that led to the identification of InfoSec functions with process flowcharts, the task of developing metrics will be much easier. That is because each step noted in the InfoSec functions' flowcharts can be a point of quantifying and qualifying costs of performing that specific function.

All metrics should be reviewed, evaluated, and reconsidered for continuation at the end of each year, or sooner—when a requirement changes, a function may also change. Remember that although the collection of the metrics information will help the ISSO better manage the InfoSec duties and responsibilities, a resource cost is incurred in the collection and maintenance of these metrics. These resources include:

- People who collect, input, process, print and maintain the metrics for you;
- Time to collect, analyze and disseminate the information; and
- The hardware and software used to support that effort.

When using these metrics charts for management briefings, one must remember that the chart format and colors are sometimes dictated by management; however, which type of chart is best for analysis or presentation to management is probably up to the ISSO.

The ISSO should experiment with various types of line, bar, and pie charts. The charts should be kept simple and easy to understand. Remember the old saying, "A picture is worth a thousand words." The charts should need very little verbal explanation.

If the ISSO will use the charts for briefings, the briefing should only comment on the various trends. The reason for this is to clearly and concisely present the material, and not get bogged down in details which detract from the objective of the charts.

One way to determine whether the message of the charts is clear is to have someone look at each chart and describe what it tells them. If it is what the chart is supposed to portray, then no changes are needed. If not, the ISSO should then ask the viewer what the chart does seem to represent and what leads them to that conclusion. The ISSO must then go back to the chart and rework it until the message is clear and is exactly what the ISSO wants the chart to show. Each chart should have only one specific objective, and the ISSO should be able to state that objective in one sentence, such as "This chart's objective is to show that InfoSec support to IWC is being maintained without additional budget although the workload has increased 13%."

The following paragraphs identify some basic examples of InfoSec metrics that can be collected to assist an ISSO in managing a CIAPP and briefing the management on the CIAPP and the InfoSec organization. By the way, when establishing a briefing to management where the metrics

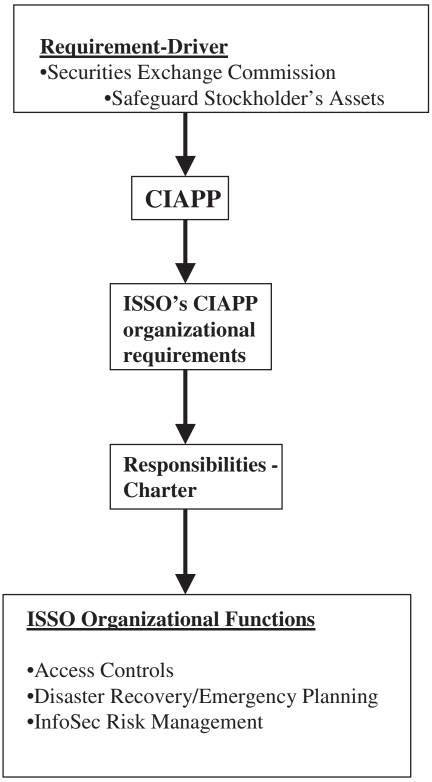

Requirement-Driver
•Securities Exchange Commission
•Safeguard Stockholder's Assets
CIAPP
ISSO's CIAPP organizational requirements
Responsibilities - Charter
ISSO Organizational Functions
•Access Controls
•Disaster Recovery/Emergency Planning
•InfoSec Risk Management

Figure 9.1 An example of tracing a requirement to a specific function.

charts will be used, a chart similar to Figure 8.1 (as shown in Chapter 8) should be used to start off the briefing. That chart tracks the requirements (drivers) which can be traced to each function. One may also want to provide more detailed charts tracking specific requirements to specific functions (Figure 9.1).

Of course, as the ISSO, you would want to get more specific and track to a more detailed level of granularity. In fact, the InfoSec staff responsible for leading a specific function should be tasked with developing this chart or charts. That way, the staff will know exactly why they are doing what they do. The next step would be for them to track their workflow, analyze it, and find more efficient ways to do the job. At the same time they would also look at current costs and cost-savings as more efficient ways are found to successfully accomplish their jobs.

The ISSO must remember that the use of metrics is a tool to support many of the ISSO's decisions and actions; however, it is not perfect. Therefore, the ISSO must make some assumptions relative to the statistical data to be collected. That's fine. The ISSO must remember that metrics is not rocket science, only a tool to help the ISSO take better-informed actions and make better-informed decisions. So, the ISSO should never get carried away with the hunt for "perfect statistics," or become so involved in metrics data collection that "paralysis by analysis" takes place.[2]

The spreadsheets and graphs used for metrics management can become very complicated with links to other spreadsheets, elaborate 3-D graphics, etc. That may work for some, but the ISSO should consider the KISS (Keep It Simple, Stupid) principle when collecting and maintaining metrics. This is especially true if the ISSO is just getting started and has no or very little experience with metrics. One may find that the project leads who are developing an "automated statistical collection" application are expending more hours developing the application—which never seems to work quite right—than it would take to manually collect and calculate the statistical information.

It is also important, from a managerial viewpoint, that all charts, statistics, and spreadsheets be done in a standard format. This is necessary so that they can be ready at all times for reviews and briefings to upper management. This standard is indicative of a professional organization and one that is operating as a focused team.

ISSOs who are new to the ISSO position, or management in general, may think that this is somewhat ridiculous. After all, what difference does it make as long as the information is as accurate as possible and provides the necessary information? This may be correct, but in the business environment, standards, consistency, and indications of teaming are always a concern of management. Your charts are indicative of those things.

The ISSO has a hard enough job getting and maintaining management support. The job should not be made more difficult than it has to be.

Another negative impact of nonconformance of format will be that the attendees will discuss the charts and not the information on them. Once "nonconformance to briefing charts standards" is discussed, management has already formed a negative bias. Thus, anything presented will make it more difficult to get the point across, gain the decision desired, and meet the established objective of the briefing.

It is better just to follow the established standards than to argue their validity. It is better to save energy for arguing for those things that are more important. After all, one can't win, and the ISSO does not want to be seen as "a non-team player" more than necessary.

Of course the number, type, collection methods, etc., that the ISSO will use will be dependent on the environment and the ISSO's ability to cost-effectively collect and maintain the metrics.

[2] Dr. Kovacich had used approximately 47 metrics charts at various times to assist in managing several large CIAPPs and InfoSec organizations.

METRICS 1: INFOSEC LOE DRIVERS—NUMBER OF USERS

There are two basic InfoSec LOE drivers within an organization, that is, those things that cause the InfoSec workload to be what it is, increasing or decreasing. The two basic drivers are:

- The number of systems which fall under the purview of the CIAPP and ISSO's overall responsibility for protection; and
- The number of users of those systems.

A question that must be asked is: Why are these metrics worth tracking? They are worth tracking because they drive the InfoSec workload—the LOE—which means they drive the number of hours that the InfoSec staff must expend in meeting their InfoSec responsibilities relative to those systems and users.

As the number of users on IWC networks changes or the number of systems changes, so does the workload; therefore, so does the number of staff required and the amount of budget required—time to do the job. For example, assume that IWC is downsizing—a common occurrence, which ISSOs will eventually face in their InfoSec careers. If the ISSO knows that IWC will downsize its workforce by 10%, and assuming that the workforce all use computers, which is not unusual in today's corporations, the workload should also decrease about 10%. This may cause the ISSO to also downsize (lay off staff) by approximately 10%.

However, the downsizing, whether it is more or less than the IWC average, should be based on the related InfoSec workload. The InfoSec drivers are metrics that can help the ISSO determine the impact of the IWC downsizing on the CIAPP and InfoSec organization. The metrics associated with that effort can also justify downsizing decisions to IWC management—to include possibly downsizing by 5% or 12% instead of 10%. For example, more layoffs may mean more CIAPP-related infractions, which means an increase in noncompliance inquiries, and thus an increase in the workload. Massive layoffs would also mean more work for those who are responsible for deaccessing employees from the systems prior to employment terminations. The metrics can show this work increase and make a case to management for not laying off InfoSec staff until after the other major layoffs have occurred.

Charting LOE through Number of System Users

As an ISSO, you decided that it would be a good idea to use the driver's metric that is used for tracking the number of system users. You have gone through the analytical process to make that decision based on answering the why, what, how, when, who, and where questions.

Why Should These Statistics Be Collected?

The driver's metric which tracks the number of system users for which the ISSO has InfoSec responsibility is used to assist in detailing the needed head-count budget for supporting those users. As an example, the following functions are charted based on the number of IWC system users (Figure 9.2):

- Access control violations;
- Noncompliance inquiries; and
- Awareness briefings.

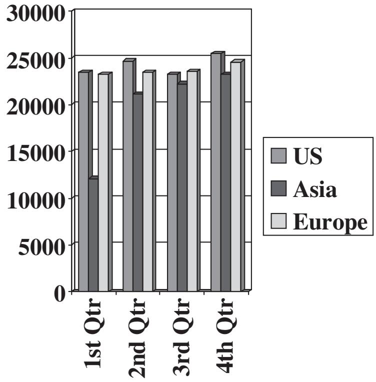
What Specific Statistics Will Be Collected?

- Total users by location and systems; and
- Total systems by location and type.

How Will These Statistics Be Collected?

- The total number of users will be determined by totaling the number of userid's on each network system and adding to it the number of standalone systems. It is assumed that each standalone system has only one user.
- Standalone microcomputers and networked systems (which will count as one system) will be identified and totaled using the

Total Users of IWC Networks World-Wide - 2002



- Number of users **increasing** at all locations
- Average **increase** in users per quarter is **11%**
- Number of access violations have **increased** at a rate of **13%**
- Number of awareness briefings have **increased** at a rate of **10%**
- Number of non-compliance inquiries have **increased** at a rate of **17%**
- **No increase in InfoSec staff**
- **InfoSec functional productivity improvement kept headcount steady while handling increased workload without a decline in service quality**

Figure 9.2 Use of a metrics chart to show how the ISSO and staff are performing their jobs in an efficient manner without a loss of quality service and support.

approved system documentation on file within the InfoSec organization on the approved systems database. At IWC, all systems processing sensitive IWC information, falling within the categories previously identified at IWC for identifying information by its value, must be approved by the ISSO (designated InfoSec staff members). Therefore, data collection is available through InfoSec organization's records.

When Will These Statistics Be Collected?

The statistics will be compiled on the first business day of each month and incorporated into the Metrics 1, InfoSec Drivers graph, maintained on the InfoSec department's administrative microcomputer.

Who Will Collect These Statistics?

The statistics will be collected, inputted, and maintained by the project leaders responsible for each InfoSec function, such as system accesses and system approvals.

Where (at What Point in the Function's Process) Will These Statistics Be Collected?

The collection of statistics will be based on the information available and on file in the InfoSec organization through close of business on the last business day of the month.

Of course the number of system users affects all InfoSec functions; however, Figure 9.2 is just an example of how the ISSO may want to depict the InfoSec workload. Follow-on charts would show the workload relative to the other InfoSec functions that are affected. The bold fonts are used to highlight important facts that the ISSO wants to emphasize—management's eyes are naturally drawn to bold fonts.

Significance of the System Users Chart

The number of system users is also a driver of InfoSec workload because the InfoSec functions' level of effort (LOE) and some projects are based on the number of users. They include the following:

- The InfoSec staff provides access controls for users;
- The number of noncompliance inquiries will probably increase based on the increased number of users;
- The number of noncompliance inquiries may actually increase when IWC downsizes because of more hostility among the employees (a metrics charts showing caseload may help in defending ISSO staff

from more drastic layoffs than may have been required by management);

- The time to review audit trail records will increase as a result of more activity because of more users; and
- The number of awareness briefings and processing of additional awareness material will increase as a result of an increase in users.

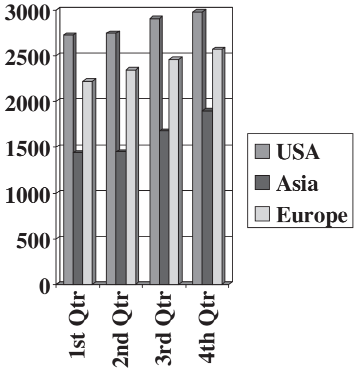
Remember that as an ISSO you are also an InfoSec "salesperson" and must effectively advertise and market information and systems protection to IWC personnel. The chart noted in Figure 9.2 and similar charts can be used by the ISSO for the following:

- Justify the need for more budget and other resources;
- Indicate that the CIAPP is operating more efficiently because the budget and other resources have not increased although the number of systems has increased; and
- Help justify why budget and other resources cannot be decreased.

The "Total Users of IWC Networks World-Wide—2002" chart (Figure 9.2) is one of many that can be used to brief management on systems' users, and also for the ISSO to use internally to manage the InfoSec organization. A similar chart (Figure 9.3), related to Figure 9.2 and showing InfoSec LOE systems, is also useful for briefing management,for example, on head count and budget matters.

When deciding to develop metrics charts to track workload, efficiency, costs, etc., of that function, always start at the highest level and then develop charts at lower levels (in more detail) that support the overall

Total Number of IWC Systems World-Wide - 2002



- Number of systems **increasing** at all locations at average of **8.5%**
- InfoSec workload **increasing** at a rate of **2.3%**
- Non-Compliance Inquiries **increasing** at a rate of **.17%**
- **InfoSec manpower remains the same due to productivity gains with no decrease ion quality of service**.

Figure 9.3 The number of IWC systems, a main InfoSec budget driver.

chart. This is done for several purposes. The ISSO may have limited time to brief a specific audience, and if it is an executive management briefing, the time will be shorter, as usually their attention span is short when it comes to InfoSec matters. So, the "top-down" approach will probably work best. If you have time to brief in more detail, the charts are available. If executive management has a question relative to some level of detail, then the other charts can be used to support the ISSO statements and/or position in reply to the question of the audience. Other systems' users-related charts flow from the main chart (Figure 9.4).

Granting Users Access to Systems

A major InfoSec service and support function is to add new users to systems and to provide them new access privileges as directed by their management and information owners.

As part of that service and support effort, the ISSO wants to ensure that these users are given access as quickly as possible, because without their access or new access privileges, the users cannot perform their jobs.

If users cannot gain expeditious access, then the CIAPP is costing IWC in terms of lost productivity of IWC employees or even possibly lost revenue in other forms.

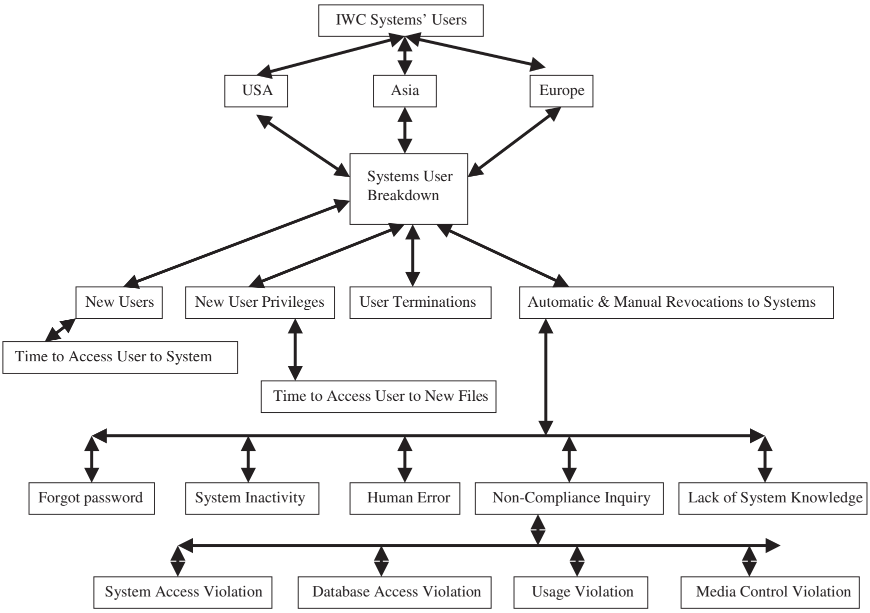


Figure 9.4 The flow of metrics charts related to the system users chart (Figure 9.2). Each box identifies a potential additional metric chart.

The ISSO, in coordination with the InfoSec staff responsible for the access control function, evaluated the access control process and determined that users should be given access within 24 hours of receipt of a request from management.

The ISSO decided to track this process because of its high visibility. Nothing can damage the reputation of the ISSO and staff faster than a hostile manager whose employees cannot get systems access to be able to do their work, leading, for example, to increased costs due to lost department productivity caused by the slowness of accessing employees to systems. In order to develop a metrics chart, one should first create a flowchart of the function. Then the ISSO can identify statistical collection
1 points for metrics management charts (Figure 9.4).

> Anything worth doing does not have to be done perfectly—at first.—Ken Blanchard

EXAMPLES OF OTHER METRICS CHARTS

There are numerous metrics charts that can be developed to support the various needs of the ISSO. The following are examples of some of those charts.[3]

The ISSO may also use this information when budget cuts are required. The chart can be shown to management and modified to show what would happen if the staff were cut one person, two people, etc. In other words, the average users' initial access to systems in terms of turnaround time would increase. Management may or may not want to live with those consequences. The cost can be quantified by taking the average hourly wage of the employee, identifying how much productivity time is lost with access coming within 1 business day, and comparing that to time lost if access, because an access control person has been laid off, takes 2 business days.

For example, an employee earns $15 an hour. The employee shows up at the desk of an access controller at the start of the business day, 8 A.M. That employee is authorized system access by 8 A.M. the next day. This loss of at least 8 hours of productivity at $15 an hour would be the normal cost of the InfoSec function of access control, or $120 per employee. However, if the access were not authorized until the day after, the costs per employee would be $240.

The chart can show the ISSO where staff cuts can be made and still meet the expected goals. The ISSO can also use this information when

[3] The reader should try developing other metrics charts and also, using the examples, determine how they could be used to support ISSO requirements; to determine successes and failures of the CIAPP; and to support briefings.

deciding to reallocate resources (transfer a person) to another function where the goals are not being met, and where the fastest way to meet the goal is to add head count. A word of caution here—adding or decreasing head count is usually considered a fast, simple solution. However, it is not always the answer.

> Sometimes when the numbers look right the decision is still wrong!—Ken Blanchard and Norman Vincent Peale

Many project leaders and ISSOs have found over the years that projects and level-of-effort problems are not always solved by assigning more bodies to solving the problem. One should first look at the process and at systemic problems. This is usually a more cost-effective approach to solving these types of problems. For example, using the example of the newly hired employee getting first-time system access, suppose a way was found to cut that time down to 1 hour. The costs saving would be from the normal $120 to $15, or a saving of $105 per new employee. Such charts can be used for management briefings and will show specifically how the ISSO and staff are lowering InfoSec costs, at least for that particular InfoSec function.

Samples of Noncompliance Inquiry Charts

Examples of this kind of chart are given in Figures 9.5 through 9.7.[4] These charts typically show infractions by individual departments (Figure 9.7). That means each department's vice president will internally compare his or her department against the others, thereby causing a covert competition to begin. Vice presidents do not want their departments to look bad, and because of their competitive nature, the vice-presidents will push to have a "zero" for each month. Each will want to know exactly what the individual NCIs were for. The ISSO must be prepared to answer them—using individual charts per department. Is this a lot of work? Yes. However, the benefits are that each department's vice-president will be pushing to have zero noncompliance inquiries conducted, which means the vice presidents will be overt supporters of the CIAPP and will push their staff to follow the CIAPP.

It also often leads to the ISSO joining the staff meetings of the departments' vice presidents and presenting the individual analyses of each department and sub-department. The ISSO should also then be in a position to explain what can be done to minimize these infractions, as well as minimize the loss of productivity, and thus dollars, caused by each

[4] Although these and all charts are published in this book in black and white, it is assumed that the ISSO's charts would be in color.

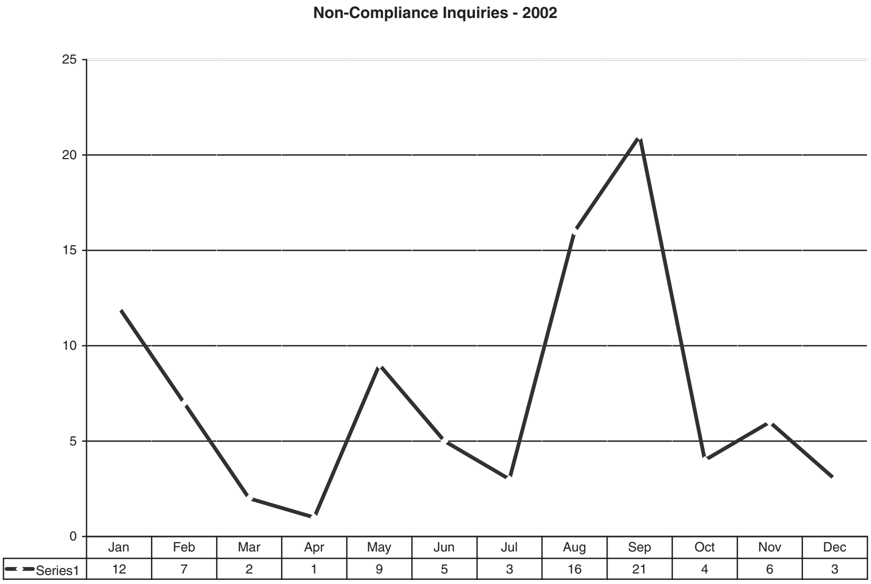


Figure 9.5 The total number of noncompliance inquiries conducted by month for the year 2002.

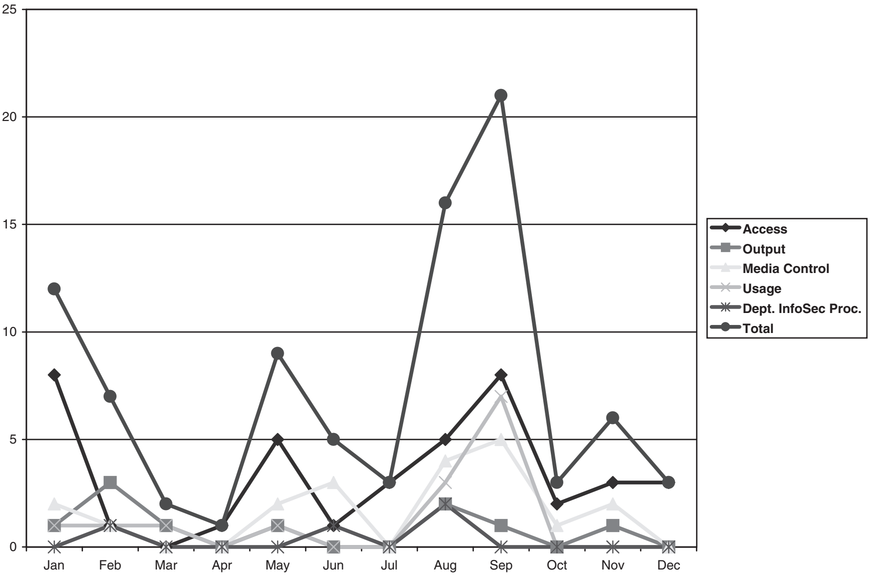


Figure 9.6 The total number of noncompliance inquiries conducted by type for the year 2002.

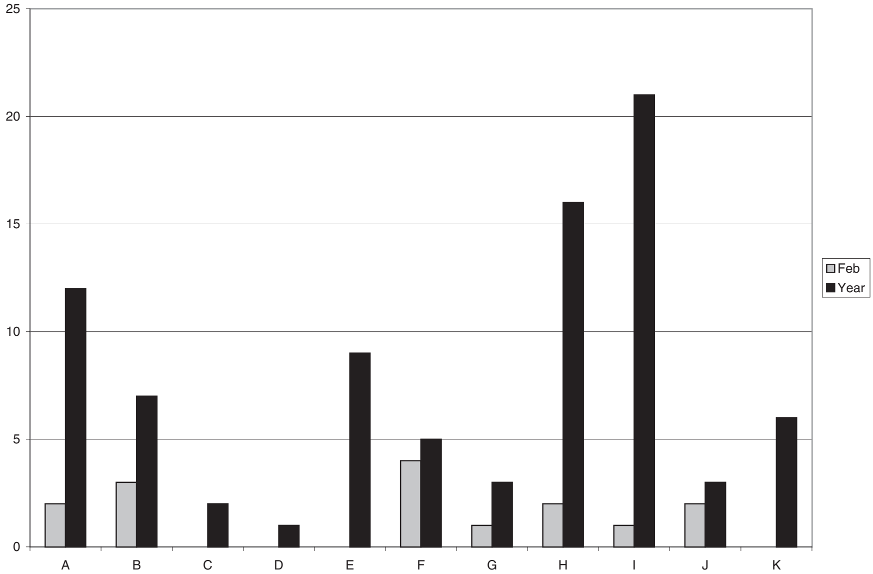


Figure 9.7 The total number of noncompliance inquiries conducted by each IWC department for the month of February, and the total of all departments for the period January and February 2002.

infraction. Showing the cost in lost productivity in hours per noncompliance inquiry will have a major impact on the staff. This can then also be linked to losses in terms of budget using an average IWC salary or hourly wage, which can often be gotten from the Finance or Human Relations staff.

The ISSO should also take to these briefings one or more of the InfoSec staff who have some responsibility for the information presented. This lets the staff members see how their work affects IWC department personnel. It also helps them become part of the entire process of working the InfoSec issues—and it is an opportunity for the ISSO to show confidence and support for InfoSec staff. By no means should they be used as a scapegoat or allowed to be the target of abuse by managers defensively rationalizing that a noncompliance inquiry was groundless, should not have been conducted, or the like. The ISSO should at all times take the blame and give the credit to InfoSec staff members. Furthermore, the ISSO must keep the focus of the meeting on the material being briefed and must discuss the numbers. The meeting should never be allowed to become a "finger-pointing" and inquiring report critique. This is not often easy to do as the department managers try to defend themselves. The meeting objective and ground rules for discussion should be stated in advance by the ISSO if the vice president does not so state.

The primary use of a chart like the one in Figure 9.8 is for the ISSO to understand the workload of one of the InfoSec functions. By looking at the number of inquiries opened, closed, and pending per month, the ISSO can, for example, determine whether the staff member conducting the inquiry requires additional staff support. The turnaround time of these inquiries is important—the sooner an inquiry is completed, the sooner, the employee's manager, in concert with IWC Human relations staff, can take whatever action is deemed appropriate. This is crucial if the person may be subject to termination or if the employee's system access had been suspended pending completion of the inquiry and the adjudication process.

As with all metrics charts, a decision must also be made whether to collect the data monthly, quarterly, semiannually, annually, or somewhere in between. The time period will depend on several factors. These include, but are not limited to:

- What they will be used for, such as monthly or annual executive briefings;
- Budget justifications;
- InfoSec staff functions resource allocations, and
- The objectives of each chart.

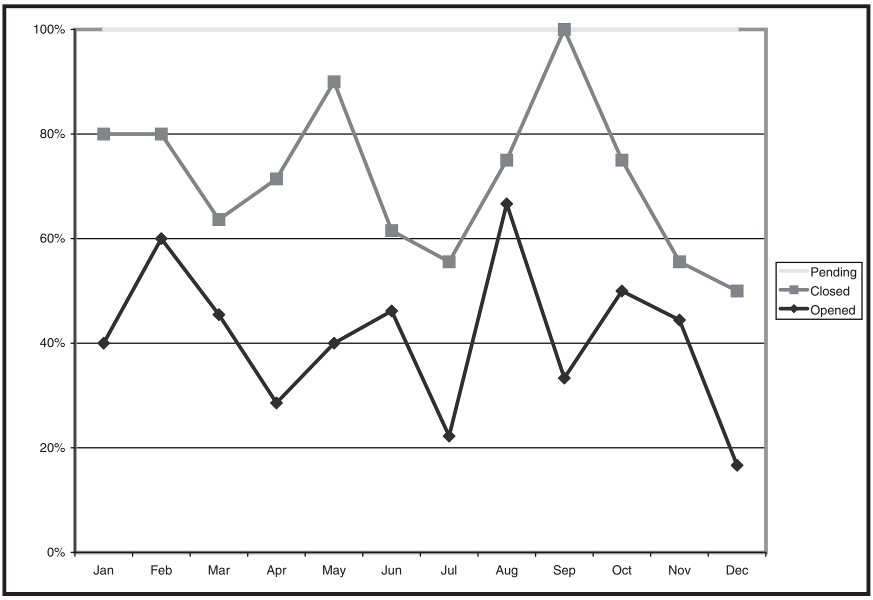


Figure 9.8 The total number of noncompliance inquiries opened per month, closed per month, and pending per month.

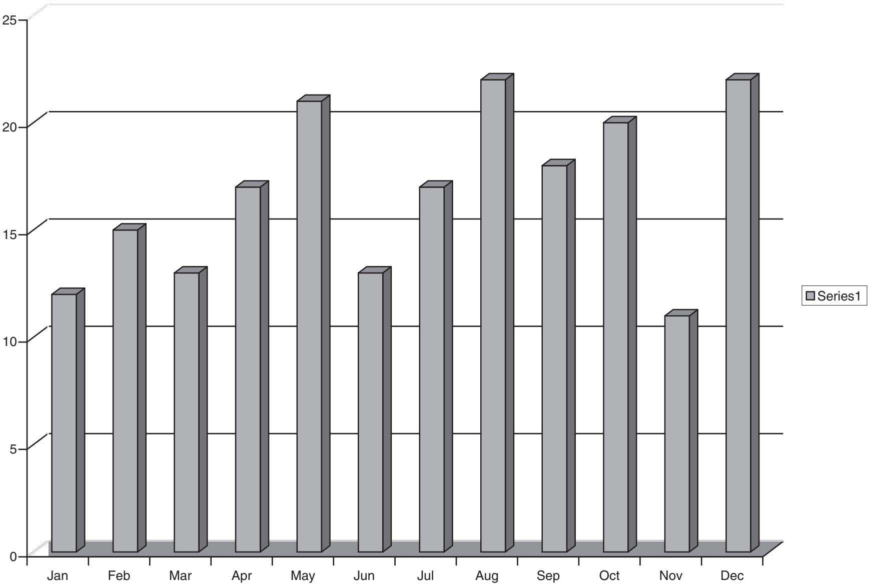


Figure 9.9 The average time spent in hours per noncompliance inquiry.

A subchart of this chart may be the average time spent per type of inquiry (Figure 9.9). Once the time elements are known, they can be equated to productivity gains and losses, as well as budget, such as money, equipment, and staff.

InfoSec Tests and Evaluations

The ISSO decides to establish a process that will provide guidelines on the need, establishment, and implementation of metrics charts. The ISSO uses an InfoSec function to develop the process—the methodology—with the following results:

- IWC InfoSec will conduct security tests and evaluations (ST&E) as prescribed by IWC InfoSec policies and procedures.
- Results of IWC InfoSec ST&E will be charted.
- Each chart will be evaluated to determine whether a pattern/trend exists.
- Patterns/trends will be evaluated to determine how effectively a function is being performed
- Results and recommendations will be presented, in accordance with InfoSec policies and procedures, to the applicable managers.

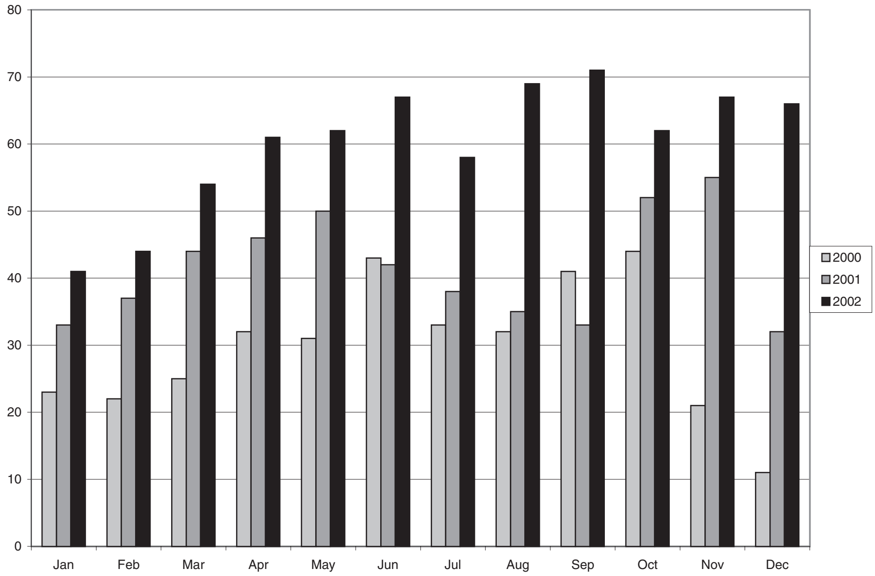


Figure 9.10 The total number of ST&Es conducted over the past 3 years.

Another InfoSec function that provides opportunities for using metrics management techniques is the function of InfoSec ST&E. The charts in Figures 9.10 through 9.12 are samples of metrics management charts that may be of use to an ISSO.[5]

Figure 9.10 is a useful chart in that it shows an increase in workload over time that can be compared with staffing for that function over time. The ISSO may consider a reallocation of staff because of the increased workload. Also to be considered is whether or not to change the ST&E process. One consideration is to conduct fewer ST&Es. If one does that, it would be important to monitor the number of noncompliance inquiries, as they may go up. For example, fewer ST&Es may result in increased systems vulnerabilities, which may in turn lead to more successful attacks, and thus to more noncompliance inquiries. Another factor the ISSO may consider is doing more ST&Es using automated InfoSec software to replace some currently manual testing.

One can also consider providing training to IWC department staff so they can do their own ST&Es and provide reports to the ISSO. This is usually not a good idea, as the objectivity of the testing may be question-

[5] For those readers trying to match numbers between charts and subcharts, you might as well know now that the numbers for each chart are arbitrarily assigned and do not reflect any consistency throughout. They are given as samples only. If you are looking for "real" numbers, you are missing the point of this chapter—the process and thinking behind metrics management of InfoSec functions.

able. For example, they may find vulnerabilities but not report them, because they do not want to incur the costs in time and budget to mitigate the risks identified by these vulnerabilities. In addition, as far the IWC as a whole is concerned, one is only passing on the costs in terms of allocation of resources to conduct the ST&Es to another department and not decreasing overall IWC CIAPP costs.

Remember that IWC is a global corporation with plants and offices on three continents. Since the ISSO has overall CIAPP and InfoSec functional responsibility for all locations, a process must be put in place for metrics management at all locations. The CIAPP-InfoSec functional leads at all the locations would provide the statistics and charts for their locations (Figure 9.11).

These statistics would be indicators in establishing InfoSec functional resource allocations based on the "worst" locations (Figure 9.12).

The issue that will often come up when designing charts is what type of charts to use—bar, line, pie, etc. The choice should be to use the format that meets the chart's objective in the most concise and clear way.

An ISSO sometimes comes across numbers that are out of balance with each other, e.g. 135 satisfactory ST&E ratings, 13 marginal. If the chart

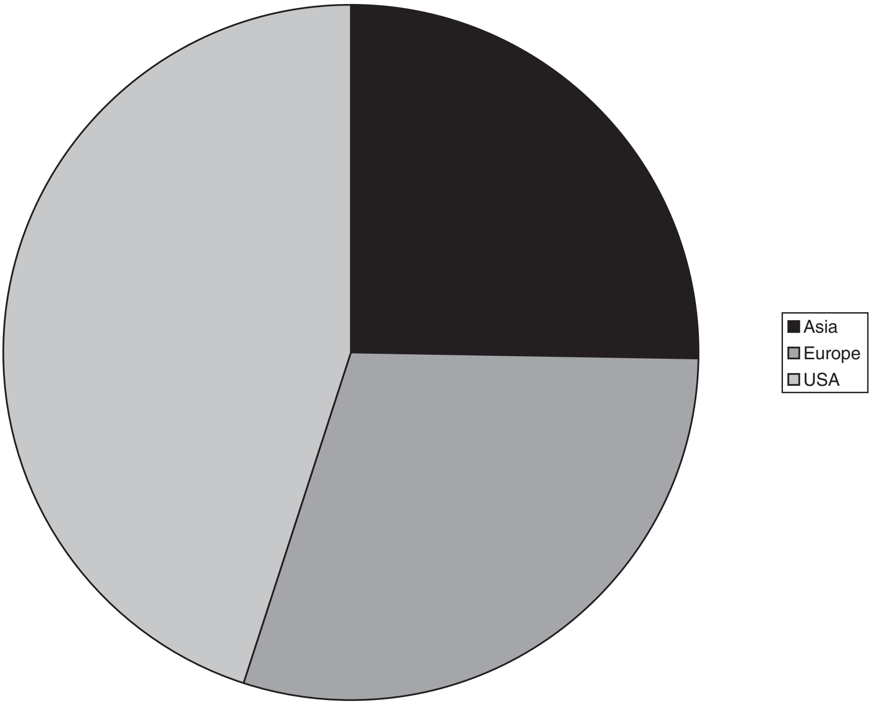


Figure 9.11 The number of ST&Es conducted per location in 2002.

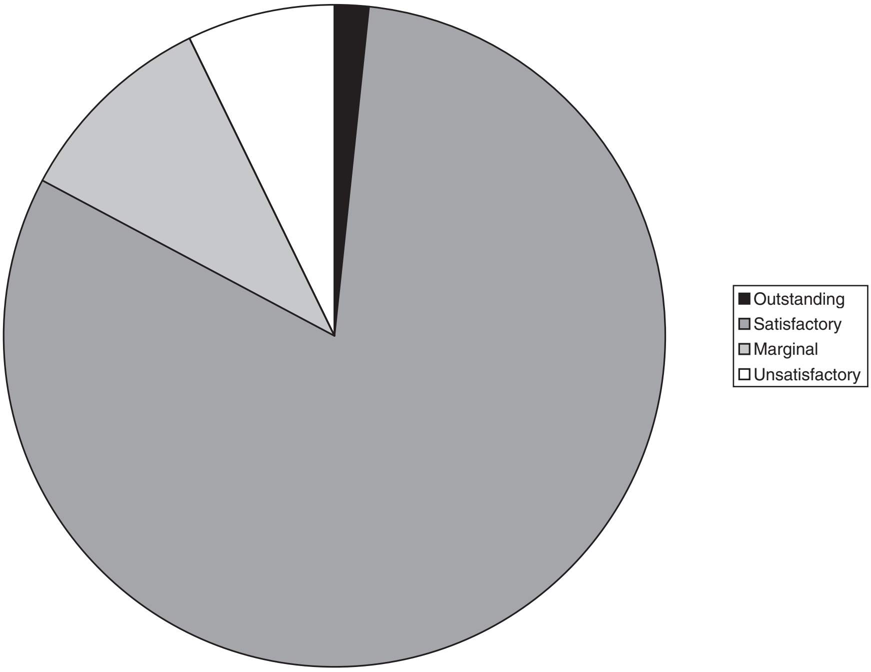


Figure 9.12 The ratings (Outstanding, Satisfactory, Marginal, Unsatisfactory) of ST&Es conducted within the corporate office in the year 2002 by department.

chosen were a line chart or a bar chart, the smaller number would so dwarfed as to be unreadable. In this case, the pie chart may be the solution.

The other solution may be to label each point in the chart with its number. For example, the bar or line designating 13 marginal ratings would have the number 13 over that point in the chart. This may give the perception that the marginal ratings were somewhat meaningless. However, as an ISSO, you are aware that is not the case, and in fact, indicates increased vulnerabilities to successful attack on those systems. The pie chart, on the other hand, shows that the number is small, but it at least appears large on the graph. The audience will see that number as being at least more significant than the same number shown on a line or bar chart.

InfoSec Education and Awareness Training

The CIAPP's InfoSec Education and Awareness Training Program (EATP) is one of the major baselines of the CIAPP. It follows that it is an integral part of the ISSO's InfoSec organization. It doesn't matter whether briefings, training and such are given by an InfoSec staff member, the IWC Training Office, the Director of Security's security training personnel, Human Resources new-hire briefings, or a combination of any of these organizations. It is a CIAPP, and therefore an InfoSec cost, and it should be metrics-managed.

For the purposes of this chapter on metrics management, let us assume that one of the ISSO's InfoSec staff is responsible for the EATP. At least two major metrics charts should be maintained (Figures 9.13 and 9.14).

Let's assume that to be somewhat cost-effective, the goal is to have at least 15 employees on average attend each briefing. That being the case, this metrics chart or another like it would show not only the number of briefings and the total attendees, but also the average number of attendees per briefing. In addition, a straight line could be included at 15 so that the average attendees per briefing can easily be compared against the goal of 15 employees per briefing. Lost? OK, let make it easy. See Figure 9.14.

If the goal was not being reached, as the ISSO, you might want to discuss the matter with your InfoSec leader for the EATP. Certainly if the goal is not being met, you can't and obviously shouldn't ignore it. There is nothing worse than setting a goal, metrics managing to attain that goal, and then ignoring it when it is not being met. Furthermore, as an ISSO you shouldn't just wait until the end of the year to attempt to correct the

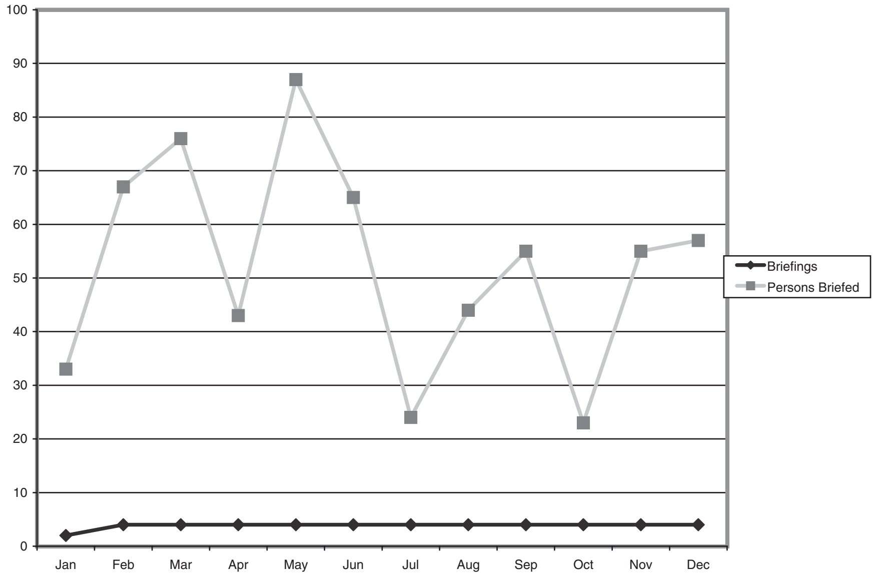


Figure 9.13 The number of briefings given and the number of personnel per briefing.

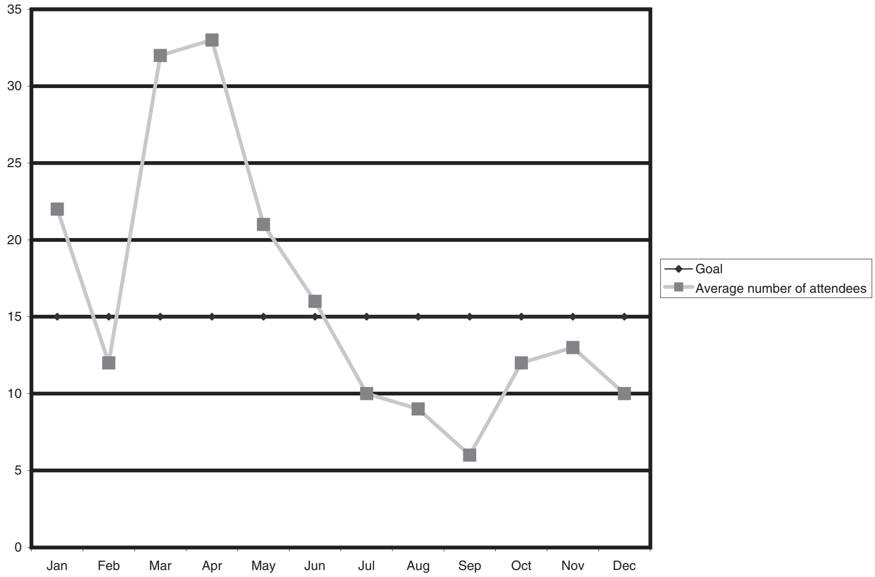


Figure 9.14 The average number of attendees per SEATP briefing measured against the goal of at least 15 personnel per briefing.

matter in discussion with your EATP lead, and then zap that person in their year-end performance evaluation.

Let us assume that employees must attend an annual briefing relative to the CIAPP and their duties and responsibilities. Assume that they prepare to attend the briefing and walk to the briefing room, and that it takes 15 minutes. They attend a 1-hour briefing and return to their place of work for a total time of 90 minutes. At an average employment rate of $15 per hour, each employee's time (and lost productivity, since they are not performing the work for which they were hired) for the annual briefing is $22.50. Let's also suppose that IWC employs 100,000 people worldwide and all of them must attend the annual briefing. That means that the annual briefing program, excluding the time the InfoSec specialist takes in preparing the updated material each year and other expenses, costs an astounding $2,250,000!

Figure 9.15 shows one type of category; however, there are others. For example, the ISSO may want to track the number of personnel briefed by such categories as InfoSec systems custodians, general users, subcontractors, Asian offices, European office, and U.S. offices.

One can argue that the briefings are necessary, they save money in the long run because valuable IWC is protected, and all that. However, that does not change the fact that this is a rather costly program. In fact, there is no indication that the cost–benefits have ever been validated. Yet, every

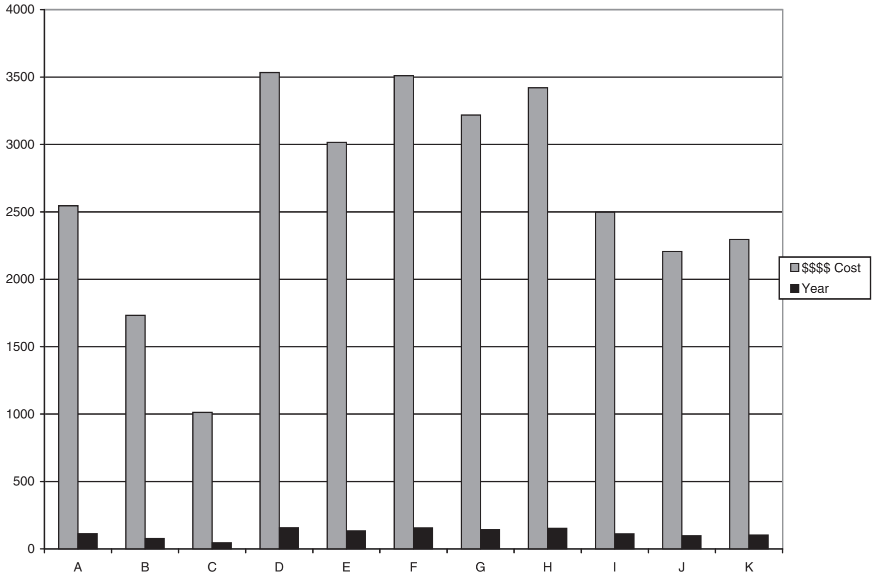


Figure 9.15 The number of personnel briefed by IWC departments and the costs of the briefings in each department, such as lost productivity equated to dollars of time.

ISSO knows that employee awareness of the threats, vulnerabilities, and risks to information and information systems is an absolute necessity. So, what can be done to lower the cost of such a program?

Using the project team approach the ISSO should establish a project team to look at the costs, benefits, and risks of not having an annual briefing and other methods for providing awareness to employees. Possibly the use of e-mails, online briefings, and other electronic means could eliminate the need for the employees to physically attend a briefing. Possibly briefings could be eliminated or online bulletins used.

Cost Avoidance Metrics.

As an ISSO, you may want to use the metrics management approach to be able to quantify the savings of some of your decisions. For example, when analyzing your budget and expenditures, you note that a major budget item is travel costs for your staff. This is logical, because staff, as well as you, must travel to the various IWC offices to conduct InfoSec tests and evaluations.

Again, using the project management approach, you lead a project team of yourself, staff members, and a representative from the Contract

Office and Travel Office. Your goal is to find ways to cut travel costs while still meeting all the CIAPP and your charter responsibilities. A representative from the Contract Office will advise the project team on contractual obligations and way in which they can be met with less travel, but without violating the terms of the contracts. The Travel Office will give advice on ways to cut travel costs. For example, because many trips are known well in advance, flights and hotels can also be booked in advance.

The project team came up with some valid changes in the processes the InfoSec staff uses as part of their travel budget. Figure 9.16 was developed to track the savings based on the process changes.

Metrics Management and Downsizing

All ISSOs at one time or another in their careers face the need to downsiz—that is, lay off, fire, or terminate—InfoSec staff. However, if you are operating at peak efficiency and have not built any excess staff into meeting your charter responsibilities, you may be able to make a case for not terminating staff, or terminating fewer personnel.

Many managers, and ISSOs are no exception, tend to forget that they are hired to do a job, and that job is not to build an "empire" or bureaucracy. The key to success is getting the job done efficiently and effec-

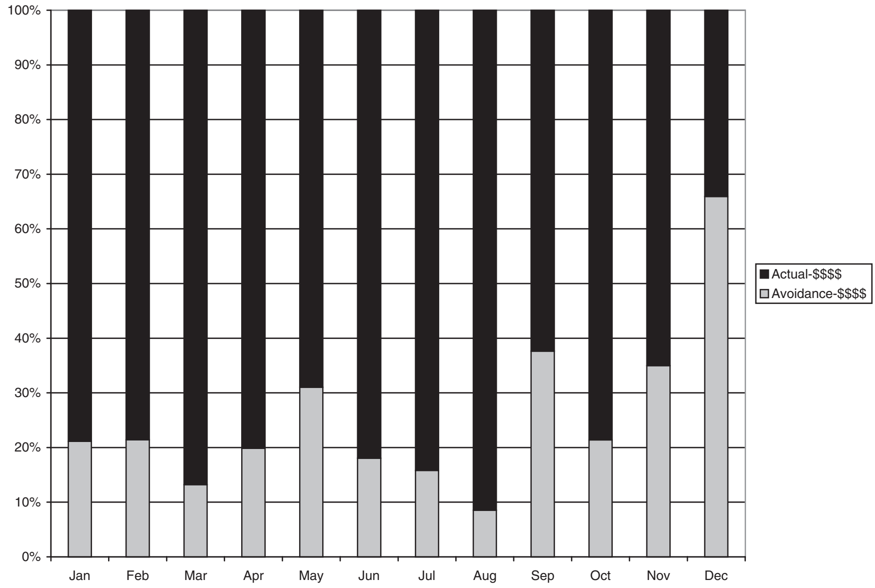


Figure 9.16 The costs and cost avoidance of InfoSec staff travel.

tively—as we said before, good and cheap. Besides, the more staff members and the larger the budget you have, the more people problems you will have and the harder the financial people will try to take some of your budget. So you are constantly battling to maintain your large budget.

If, on the other hand, you have a small staff and a smaller budget, you have a better chance of protecting what you have, because it is the minimum needed to get the job done. That approach coupled with metrics management techniques and periodic briefings to executive management will help you continue to get the job done as you deem appropriate, even though other organizations are losing staff.

Let's look at some figures showing various ways of presenting information based on metrics management's data collection efforts:

The LOE versus project support chart in Figure 9.17 clearly shows that the InfoSec organization has been supporting the projects of other IWC departments and that the workload is not "nice-to-have" projects. These are projects that require the support of the ISSO and InfoSec staff. It also shows that the ISSO and staff are an integral part of major IWC projects and are functioning as part of their service and support duties.

Taking this chart as an example, similar charts can then be developed using the same template but showing the workload per function versus budgeted hours for each function, such as SEATP and ST&E.

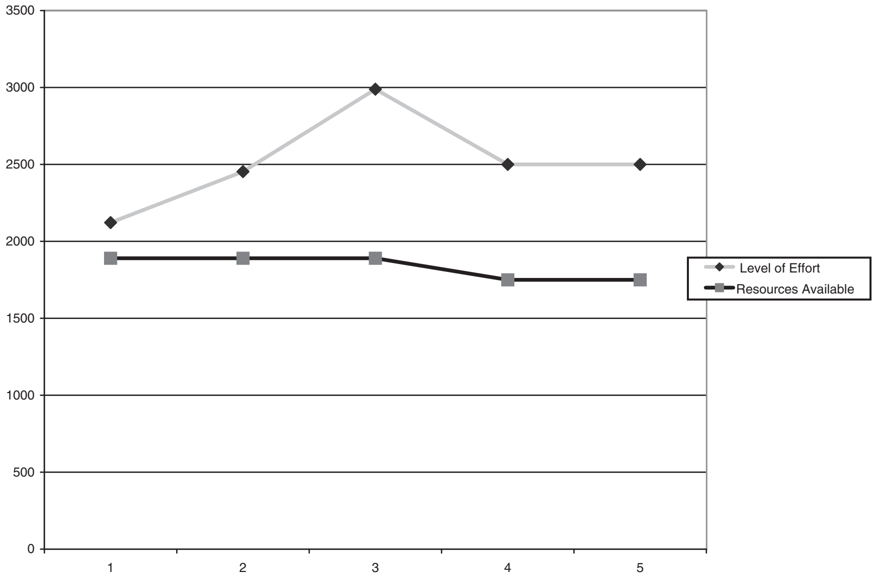


Figure 9.17 A 5-year period tracking the level of effort in hours of work of the InfoSec staff per year, per individual, compared to the hours of work that must be accomplished to support the IWC departments.

Another chart that is important for briefing management is one that shows the LOE versus the hours available for the InfoSec staff (Figure 9.18). The difference between LOE and time available can be shown to be part of a briefing on work backlog or used to show the difference is overtime being worked. A subchart may show details on the amount of backlog and its impact on the cost of doing business. It can also show the overtime costs being paid, and perhaps a comparison of that cost with the cost of hiring one or more additional staff. Seeing this comparison would help in making decisions as to which is cheaper, paying overtime or hiring more staff.

These charts must also be accompanied by others showing productivity and drivers of workload, as in some of the charts shown earlier. This is necessary because management will ask why you must do the things you do, and why must you do them in the way you are doing them. This quest for productivity and efficiency gains will be a constant chore for the ISSO. It is a challenge, but one that can be supported by metrics charts.

Layoffs are a fact of life in business, and metrics charts can help the ISSO justify head count and work, as shown by some of these charts. Other charts may also help, such as that shown in Figure 9.19. The chart can show measurement in terms of head count or hours that are equivalent to head count.

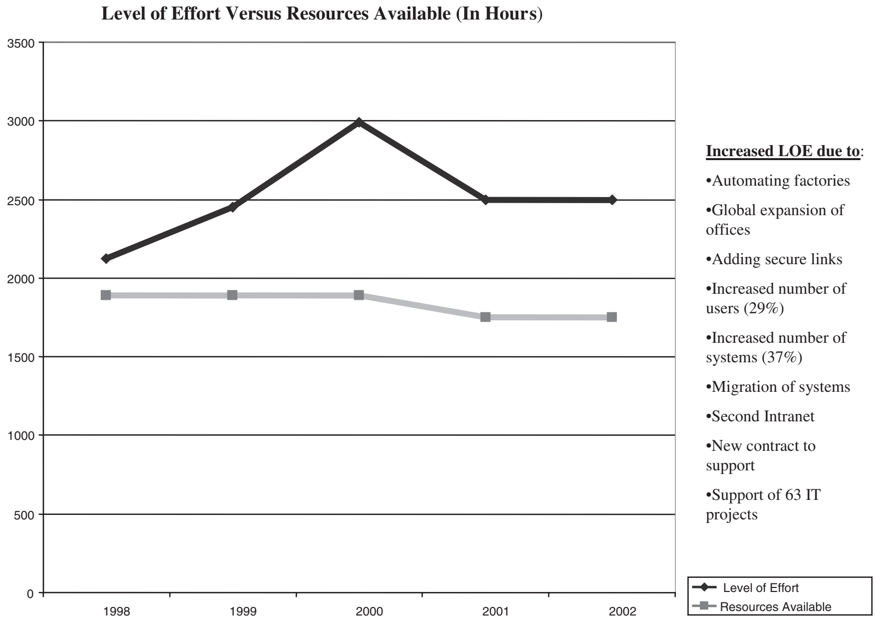


Figure 9.18 The LOE versus the hours available to do the work.

Generally, when management decides to cut costs, they lay off employees as the easiest method. They also usually direct each manager to cut a certain percentage of staff, say, 20%. However, although this may the easiest way, it is not the best way; sometimes it would be cheaper to keep some of the staff, because their loss caused delays costing millions of dollars worth of production, sales, etc. As we all know, executive management often takes a short-term, "what's in it for me now" approach to managing their parts of the business.

Metrics management can help the ISSO plead the case to not cut 20% of staff. One word of caution: The ISSO should do this objectively and based on providing effective and efficient service and support to the IWC departments. It should never, ever be based on keeping a large staff and bureaucracy for the sake of status, power, ego, or other nonbusiness reasons.

Along with the chart shown in Figure 9.19, the ISSO would include information relative to the impact of both IWC's directed layoff numbers and those of the ISSO. This must be objectively done based on a business rationale. This information would include the following, identified as increasing the level of risks to information and information systems:

- *Contingency planning*: Contingency, emergency, and disaster recovery testing and plan updates will be delayed. The result will be any-

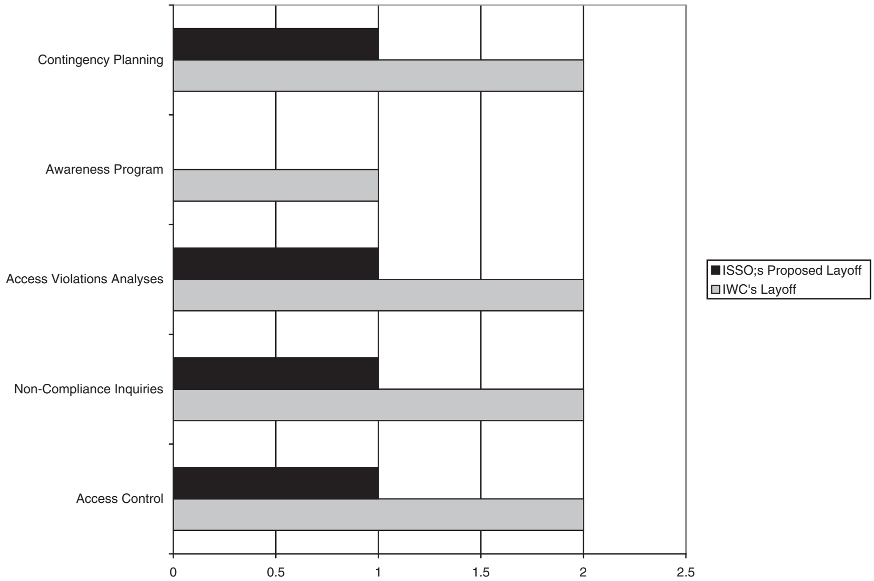


Figure 9.19 Comparison of IWC executive management requested layoff versus a counterproposal by the ISSO.

thing from no impact to not being able to effectively and efficiently deal with an emergency.

- *Awareness program*: Employees may not be aware of their responsibilities, thus leaving the systems open to potential attack or an increase in the potential of the loss of sensitive information.
- *Access violations analyses*: There will be delays of between 48 and 72 hours in the analyses of audit records. Thus, an attack against IWC systems would not be known for at least 48–72 hours. During that period, information could be stolen. However, something like a denial of service attack would be known when it was successful. The opportunity to identify the initial attempts at these attacks over a period of time would be lost, and with it the chance to mount defenses before the attacks were successful. The result will be systems, possibly production systems, that are down for an unknown period of time.
- *Noncompliance inquiries*: The average time it would take to complete an inquiry would increase by more than 2 weeks. Thus, no action to adjudicate the alleged infraction would be possible until the report was delivered to management. Furthermore, the alleged infraction may have called for the revocation of system privileges of the employee or employees who are the subject of the inquiry. Thus, their ability to be productive employees during that time would be negated.
- *Access control*: It is assumed that the number of new employees hired would be drastically reduced, and that could mitigate some of the level of effort expended by the access controllers. However, employees requiring changes in privilege would have those access changes delayed an additional 48–72 hours from the present average of 8–12 hours. This may adversely affect their productivity. To allow departments to do their own employees' privilege changes was evaluated under a previous project and found to not be realistic: The information to which the employees needed access did not belong to that department; most often it belonged to another information owner. These information owners did not want others to access their information without their approval. In addition, this change would just a transferring of costs and would not save IWC any additional resources.

The foregoing is a small example of how metric management techniques can be used when the need for budget cuts occurs. The example provides some insight into how metric management techniques help mitigate the risks of budget and staff downsizing when such downsizing will hurt the CIAPP and IWC. Metric management techniques can help the ISSO make a case to executive management. Furthermore, if the ISSO, supported by the metric management approach, has been periodically briefing management of the CIAPP and ISSO's projects and level of effort, the ISSO will have gained the confidence of management as a reliable manager who gets the job done as efficiently and effectively as possible.

PROJECT MANAGEMENT

As previously discussed, there are two basic types of work performed by the ISSO and staff: (1) level of effort (LOE) and (2) projects. We have discussed LOE and have provided some examples of process and metrics flowcharts relative to LOE.

It has been stated several times, but bears repeating: Projects are established where some tasks related to the CIAPP and/or InfoSec functions must be completed but they are not ongoing tasks. It is imperative that the ISSO be intimately familiar with and experienced in project management—as well as time management.

Remember that whether or not some task should be a project depends on whether it has the following:

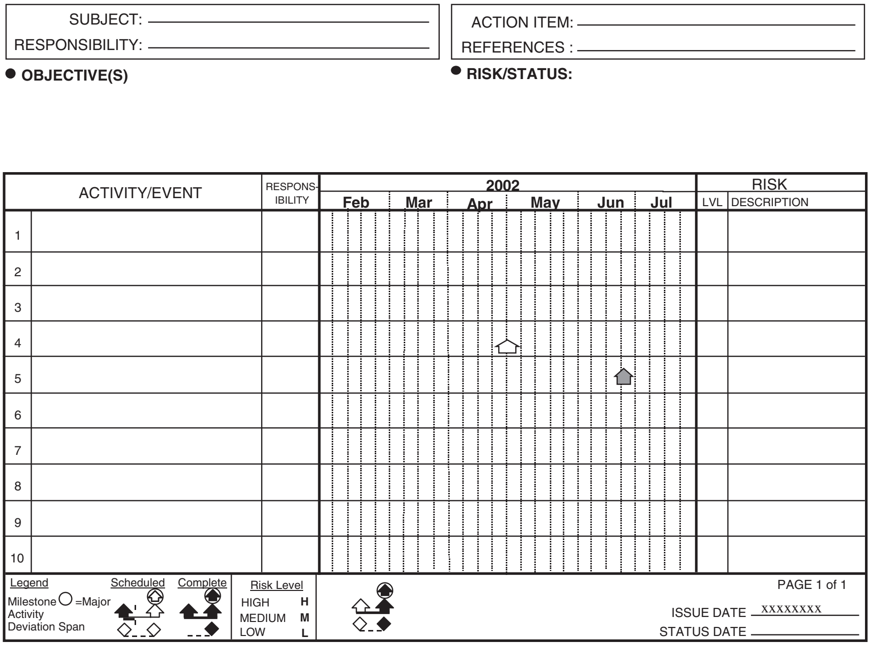
- A stated objective (generally in one clear, concise and complete sentence);
- A beginning date;
- An ending date;
- Specific tasks to be performed to successfully meet that objective;
- A project leader; and
- Specific personnel to complete each task and the time period when the task will be completed.

Let's assume that the CIO sent a memo to the ISSO based on a conversation that the CIO had with the Director of IT. It seems that they had a meeting and during the meeting the discussion turned to IT projects related to their projects of upgrading systems, such as hardware, software, and their general maintenance. The CIAPP policy called for such upgrades and maintenance efforts to ensure that the information environment is maintained in compliance with the requirements set forth in the CIAPP. The Director stated that the IT staff didn't know if that was always the case when they made changes to systems. Consequently, the Director suggested that members of the ISSO's organization be part of the IT project teams with responsibility for determining whether the changes kept IWC's information environment secure. The CIO agreed and sent the ISSO a letter to that effect. When the ISSO received the memo, the ISSO discussed the matter with the Senior Systems Security Engineer. It was decided that a project be developed in order to establish a process and function to comply with the request from the CIO and Director of IT.

As an ISSO, you should be able to identify several issues that the ISSO must resolve apart from initiating this project. First, the Director of IT and the ISSO should be working closely together, and by doing so, they could have dealt with this matter without involving their boss, the CIO. In addition, the fact that the CIO sent a memo to the ISSO, instead of calling or meeting personally with the ISSO, indicates that the communication and working relationship between the CIO and ISSO must be improved. The ISSO must take action to immediately begin improving the communication and relationship with the Director and CIO.

That aside, using Figure 9.20 as an example, let's develop a project and fill in the blanks for major portions of the chart:

- SUBJECT: The project name: Security Test & Evaluation Function Development
- RESPONSIBILITY: The name of the project leader: John Doe, InfoSec Senior Systems Security Engineer.
- ACTION ITEM: What is to be accomplished:. IT requires ISSO support to ensure that information and systems protection are integrated into IT systems' integration, maintenance, and update processes.



SUBJECT: ______
RESPONSIBILITY: ______

ACTION ITEM: ______
REFERENCES : ______

● OBJECTIVE(S)

● RISK/STATUS:

	ACTIVITY/EVENT	RESPONSIBILITY	2002 Feb	Mar	Apr	May	Jun	Jul	RISK LVL	DESCRIPTION
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Legend
Scheduled
Complete
Milestone ○ =Major
Activity
Deviation Span
Risk Level
HIGH H
MEDIUM M
LOW L

PAGE 1 of 1
ISSUE DATE xxxxxxxx
STATUS DATE ______

Figure 9.20 A basic project management chart that can be used to track CIAPP and InfoSec functional projects.

- REFERENCES: What caused this project to be initiated. For example: "See memo to ISSO from CIO, dated November 2, 2002."
- OBJECTIVE(S): State the objective if the project: Maintain a secure information environment.
- RISK/STATUS: State the risk of not meeting the objective(s) of this project: Because of limited staffing and multiple customer projects being supported, this project may experience delays as higher priority LOE and projects take precedence.
- ACTIVITY/EVENT: State the tasks to be performed, such as "Meet with IT project leads."
- RESPONSIBILITY: Identify the person responsible for each task. In this case, it is the Senior Systems Security Engineer, John Doe.
- CALENDAR: The calendar could be a year-long, monthly, quarterly or 6-month calendar with vertical lines identifying individual weeks. Using the 6-month calendar, the Project Lead and assigned project team members would decide what tasks had to be accomplished to meet the objective. The arrows and diamonds identified in the legend would be used to mark the beginning and ending dates of each task. The arrows are filled in when the task is started and when the task is completed; the diamonds are used to show deviations from the original dates.
- RISK—LVL: In this space, each task is associated with the potential risk that it may be delayed or cost more than allocated in the budget for the task. Using "High," "Medium" or "Low" or "H," "M" or "L," the Project Lead, in concert with the person responsible for the task, assigns a level of risk.
- RISK—DESCRIPTION: A short description of the risk is stated in this block. If it requires a detailed explanation, that explanation is attached to the project plan. In this block the Project Lead, who is also responsible for ensuring that the project plan is updated weekly, states "See Attachment 1."
- ISSUE DATE: The date the project began and the chart initiated goes in this block.
- STATUS DATE: The most current project chart date is placed here. This is important because anyone looking at the project chart will know how current the project chart is.

Other types of charts can also be developed to show project costs in terms of labor, materials, and the like. A good, automated project plan software program is well worth the costs for managing projects.

In the case of project charts, the ISSO uses them to brief management relative to the ongoing work of the InfoSec organization and states of the CIAPP. The ISSO receives weekly updates on Friday morning in a meeting with all the ISSO's project leaders, where each project lead is given 5 minutes to explain the status of the project—for example, "The project is still on schedule" or "Task ##2 will be delayed because the person assigned the task is out sick for a week; however, it is expected that the project completion date will not be delayed because of it."

The ISSO holds an expanded staff meeting the last Friday of each month. All assigned InfoSec personnel attend these meetings, which last 2 to 3 hours. At these meetings, 1 hour is taken for all project leads and InfoSec functional leads to brief the status of their LOE and projects to the entire staff. The ISSO does this so that everyone in the organization knows what is going on—a vital communications tool. Also during this time, other matters are briefed and discussed, such as the latest risk management techniques, conferences, and training available.

QUESTIONS TO CONSIDER

Based on what you have read, consider the following questions and how you would reply to them:

- Do you use formal metrics management techniques?
- If not, why not?
- If so, are they used to brief management?
- Are each of your InfoSec functions documented not only in work instructions but also in process flowcharts?
- Do you use similar charts to document the InfoSec functional LOE?
- What other charts would you develop for each of the ISSO functions?
- Do you have at least one metrics chart to track costs of each InfoSec function?
- How would you use metrics management charts to justify your budget requests?
- How would you use metrics management charts to justify the number of your staff?
- How many charts, by function and description, would you want to use as an ISSO?

SUMMARY

Metrics management techniques will provide a process for the ISSO to support InfoSec- and CIAPP-related decisions. The ISSO should understand the following points:

- Metrics management is an excellent method to track InfoSec functions related to LOE, costs, use of resources, etc.
- The information can be analyzed, and results of the analyses can be used to:

Identify areas where efficiency improvements are necessary;

Determine effectiveness of InfoSec functional goals;

Provide input for performance reviews of the InfoSec staff (a more objective approach than subjective performance reviews of today's ISSOs); as well as

Indicate where InfoSec service and support to IWC requires improvement, meets its goals, etc.