Gathering Security Metrics and Reaping the Rewards

Dan Rathbun

Gathering Security Metrics and Reaping the Rewards

GIAC (GSLC) Gold Certification

Author: Dan Rathbun, dan.rathbun@aecom.com
Advisor: Lori Homsher

Accepted: October 7th 2009

Abstract

This paper deals with the importance of using objective measurement to manage security improvements and to steer an information security program. It outlines the best way to design and produce a comprehensive security metrics program. It also describes how to leverage that effort within an organization to achieve improved decision-making, to increase visibility, to perform benchmark comparisons, and to demonstrate the value of the Information Security department.

Far from being another treatise on detailed metric formulas or data analysis techniques, this is a practical roadmap for initiating a brand new metrics program or strengthening an existing one. We will discuss what security metrics are; the value they bring; what to measure; where to get the raw data; how to produce useful metrics and the importance of presenting them in a visually compelling and logically persuasive way. Without objective measurement leadership is nearly impossible, so join us as we consider the benefits of a well-designed security metrics program.

Introduction

Imagine you have just accepted the challenge of creating an information security function for your organization. Until this point security had been baked-in to everyone's job and was an unspoken expectation. But that approach was inefficient and provided uneven results. Your mandate is to bring order to the chaos and to steer the ship. Where do you head first? What do you focus on? Security metrics can inform your decisions.

Or maybe you are pitching a security initiative to management and they want formally defined success factors. What exactly will your project accomplish? Is this the right priority? How will they know if the project is successful? Security metrics can provide you with objective answers.

Perhaps your Board of Directors has been funding information security as a priority for several years now. They want to understand whether that decision has helped the organization to achieve a competitive advantage. Are they spending enough on security, or are they spending too much? Can you demonstrate the return on investment? Has your security improved in the past year? How does the organization compare with its peers? Security metrics can answer these questions and many more.

Each of these scenarios highlights the need for objective answers. In many organizations such answers are hard to come by, but it doesn't have to be that way. Most computing environments are rich with sources of statistical data in the form of log files and dashboards. This wealth of information simply needs to be mined and then used to generate business measurements known as security metrics. As we explore the art of security metrics we will teach you how to leverage this valuable tool to support the goals and objectives of your organization.

1. Why should I be interested in security metrics?

Gathering available data and turning it into useful performance measurements sounds like a lot of work, and it's likely that nobody is explicitly asking you to do it. So let's make

sure we are clear about the benefits you can expect to achieve if you invest the time to produce a metrics program.

- **Security metrics will help you communicate performance**
  Without taking consistent and objective measurements how can you expect to demonstrate the performance of your organization in matters of security? Conversely, when you do take the time to quantify the effectiveness of your security processes and present that information in easy to digest morsels, you will find that your efforts are better understood and even better appreciated. Increased visibility for the security function is a delightful byproduct of having a metrics program.

- **Security metrics will help drive performance improvement**
  It has been said that "what doesn't get measured, doesn't get managed", but what may not be as obvious is the motivating influence your metrics program can exert on the performance of your organization in executing its security operations responsibilities. When visibility is increased people tend to be more diligent. Don't underestimate the power of this truism. Use security metrics to shine a light on your organization and then watch the improvement.

- **Security metrics measure the effectiveness of your IT controls**
  Are your controls producing the expected results? For instance, are there fewer cases of non-compliant anti-virus software since you instituted a monthly audit control? Are more computers coming under the care of your patch management program due to the technology controls you instituted? Is the business unit where you administratively locked down the endpoints suffering less malware infection per user than your more loosely managed divisions? Security metrics can provide proof positive of whether your best laid plans are succeeding or not.

- **Security metrics can help to diagnose problems**
  With objective data to support your conclusions it becomes relatively easy to determine where the weak links are in your security posture, and what your priorities need to be going forward. The right metrics can serve to quickly diagnose problems and pinpoint vulnerable threat vectors.

- **Security metrics provide effective decision-making support**
  Where are the greatest areas of opportunity for you to address as a matter of priority? What would be the expected result if your organization invested in a specific security project? More than just providing assistance with budget justification, a metrics program can facilitate objective data-driven decision-making.

- **Security metrics provide increased accountability**
  By shining a light in the dark corners of your organization, a widely circulated security metrics report can increase the resolve of your Information Technology team. By comparing the results of each business unit to an agreed upon baseline or, even more effectively, to their peers within the organization, a high level of commitment and enthusiasm can be achieved. This can dramatically increase motivation and improved results will follow.

- **Security metrics can guide resource allocation**
  Being able to gauge the level of risk throughout the organization based upon relevant and objective measurements can make requests for additional resources more defensible.

- **Security metrics can demonstrate the state of compliance**
  Demonstrating compliance with internal security policies, established governance frameworks, or regulatory requirements becomes a little simpler with a security metrics program in place. When stakeholders throughout the organization can

each review the same report card each month, that visibility will drive you toward achieving your compliance goals.

- **Security metrics can be used to facilitate benchmark comparisons**
  How effective is your security program when compared to peer organizations within your industry or sector? How does your security spending compare, and are you getting better results than your competitors? A well structured security metrics program holds the promise of making such comparison possible.

2. So what exactly is a security metric?

A clear definition of what constitutes a security metric is not easily found. Security metrics are more frequently defined by how they are used, or by the characteristics or attributes that make them useful.

One practical definition states that "*Metrics* is a term used to denote a measure based on a reference and involves at least two points, the measure and the reference. Security in its most basic meaning is the protection from or absence of danger. Literally, security metrics should tell us about the state or degree of safety relative to a reference point and what to do to avoid danger." (Brotby, 2009)

When we talk about security metrics we are referring to objective measurements that tell us about our current level of safety and show us how to achieve our goals. One author artfully distilled it all down to this statement. "The primary goal of metrics is to quantify data to facilitate insight." (Jaquith, 2007)

2.1. What is not security a metric?

If security metrics can be defined by how they are used or by their dominant attributes, that picture can be brought into clearer focus by also considering how they are misused and how some data is altogether mislabeled as a security metric.

One frequent misapprehension regarding security metrics is the use of security taxonomies as a framework for the metrics program. While standards such as ISO-17799 and COBIT provide a good overview of the issues a security program should be concerned with, they direct us toward producing more subjective measurements. As we will soon see this is not a recipe for effectiveness.

Another common mistake is to produce a metric that answers a question nobody is asking, or a metric which fails the "so what" test. If a metric does not specifically meet the needs of an interested consumer then why produce it? If it is not immediately obvious what action that individual should take based upon the metric then it fails the "so what" test and again we need to question its worth.

With this broad definition in mind let's see if we can add some clarity by considering what attributes make a metric successful.

2.2. What makes a good metric?

"Good metrics facilitate discussion, insight, and analysis; bad metrics prompt furious arguments about methodology." (Jaquith, 2007)

We have argued above, and common sense would confirm it; some metrics are good and some are not. So how can we ensure that our metrics program is based upon measurements that will be useful and will provide value to our organizations?

Fortunately, good metrics all have some things in common. Good metrics are:

- **Necessary to satisfy a specific business requirement** – the first question to ask before even considering how to produce a given metric is whether it communicates information that someone needs to know. If there is no compelling business need for the information why would you deliver it?

"Any discussion of metrics must first and foremost consider the constituency."…"What information is needed by whom? The issue can be summed up by the question, "Who needs to know what when?" (Brotby, 2009)

If you have not identified an interested consumer with a defined need for information then you are just adding to the noise.

- **Consistently measured** – A metric can't be compared to anything, not even to itself, if it is not produced in a consistent and uniform fashion. In fact, once you have developed the process for producing a given metric you would be well served to place it under rigid change management controls to protect its integrity.

- **Cheap to produce** – If a metric takes too much time to gather then it becomes less effective to produce it. At some point you face the realization that time is better spent taking remedial action on the issues already identified than in gathering data to support excessively arduous metrics. Ideally an automated means of gathering data and producing metrics should be the goal.

- **Must yield quantifiable information** – The product of a metric formula must be a quantifiable value, and preferably a cardinal number or percentage. Again, we should prefer a cardinal number, one that counts how many of something there is. Using a more subjective expression such as a rank-ordered list or the classic red-green-yellow traffic-light rating makes it impossible to compare the data in any meaningful way.

  Furthermore, choosing a percentage or ratio to express the measurement can normalize the data when other variables fluctuate dramatically. For instance, reporting 1,500 vulnerabilities in your environment one month and 2,500 the next might lead you to draw the wrong conclusion unless you are aware that the number of computers doubled during that timeframe. It is much more useful to report on the percentage of computers with a critical vulnerability, or even the

average number of vulnerabilities per computer. These measurements allow for meaningful comparisons even when other factors vary wildly.

- **Expressed using at least one unit of measure** – In addition to being expressed as a number, a metric should be presented using a unit of measure that describes the thing you are counting; for instance "average critical vulnerabilities per computer" or "number of application security defects". Andrew Jaquith offers some valuable wisdom on this often overlooked characteristic.

  "The single unit of measure for the "number of application security defects" metric makes it hard to compare dissimilar applications on an apples-to-apples basis. But if one unit of measure is good, two are better. For example, a better metric might be "number of application security defects per 1,000 lines of code," which provides two units of measure. By incorporating a second dimension (dividing by 1,000 lines of code), we have constructed a metric that can be used for benchmarking." (Jaquith, 2007)

- **Only repeatable information security processes should be measured** – numbers generated by an IT process must only be gathered if the procedure is stable and there is consistency in the way it is executed. While technical statistics are abundant and in many cases simple to gather, statistics produced by manual procedures can be inconsistent or subjective. Protect the credibility of your metrics program by ensuring any procedures you measure are repeatable and that the resulting measurements are defensible.

- **Contextually specific** – each metric you produce should matter to someone and should provide clear, actionable intelligence to that consumer. If a measurement is met with indifference or confusion as to what it means then it either needs to be refined or retired.

3. Which metrics should I produce?

At this point you are ready to start developing your own metrics program, and so the question of where to begin must be considered. Several options present themselves:

- You could produce an inventory of available data sources and let that dictate which metrics you produce.

- You could consult reference materials on security metrics and compile a list of potential measurements, finally choosing the ones that are most easily within reach.

- Or you could interview the stakeholders in your organization, learn what measurements are important to them, and devise a way to produce that information.

While there are arguments to be made for all three approaches, we are always wise to remain focused on producing the information that is most useful to our audience. Remember "Metrics…exist only to provide decision support. They serve no other purpose. The information they provide is only useful to the extent it serves that purpose." (Brotby, 2009)

It may help to facilitate the discussion with your stakeholders if you have a list of potential metrics in hand when you approach them. While your list may not contain the exact measurements they are looking for, it may spark a productive discussion that will lead you in the right direction.

One effective way to create such a compendium is to leverage available reference materials, gathering potential metric definitions and compiling them into a menu of possibilities. The '*References*' section at the end of this essay is a great place to start. Once we understand the needs of our organization we can begin formulating ways to meet those needs.

However, in spite of our thoroughly vetted ideas and the best of intentions, there can be many limiting factors which prevent us from being able to meet consumer demand. "The maturity of an organization's information security program determines the type of measures that can be gathered successfully. A program's maturity is defined by the existence and institutionalization of processes and procedures. As an information security program matures, its policies become more detailed and better documented, the processes it uses become more standardized and repeatable, and the program produces a greater quantity of data that can be used for performance measurement." (Chew, 2008) For this reason you will generally find that technical metrics are more readily produced than process or program oriented measurements, especially in a less mature security organization.

It is sensible at this point to identify which potential metrics on your list are able to be produced given the data sources available. Once this has been determined, you can cross-reference those metrics with the list of the requirements provided by your metric consumers and a set of initial priorities should come quickly into focus.

It is also important to review the metrics that you cannot produce to determine if any of them represent key performance indicators that are of substantial value to your audience. If so, then an analysis should be performed to determine the amount of investment required to produce those metrics.

When developing program-oriented metrics, wisdom would direct us to work closely with the business to ensure that our metrics program aligns with stated business objectives. A good place to begin is with the organization's mission statement, annual report, or any other documentation from which you can learn organizational goals and the preferred language used to express them. As much as possible we should employ this terminology as we develop our program. This will help to make the link between our measurements and the organization's goals patently obvious even to the most casual reader. It may also help to capture the attention of senior managers and others with an interest in corporate governance; which is never a bad thing for a security program.

One word of caution is to avoid the temptation to bury your organization in metrics just because you can. The following sage advice is well worth heeding (Herrmann, 2007):

- If there are no pre-stated objectives on how results will be used, there should be no measurements. You have to know the question before you can supply the answer.

- Establish pragmatic goals for the metrics program from the outset. Start small, grow slowly, manage expectations, and be realistic.

- Balance the desire to provide value to metric consumers with the overhead of the metrics program. Do the best you can with the information that is available today, and then improve upon it tomorrow.

- Use common sense. Do not think that people will be more impressed if you inundate them with mounds of metrics. Instead of impressing people, this will trigger an extra level of scrutiny.

3.1. Where do I get these metrics?

Raw data for use in producing security metrics is available in abundance in most IT shops. In fact we are generally drowning in data which is one reason that most of the time it sits there without being reviewed and without adding any value. Our mission is to harvest the most useful pieces of that data, and to do it in a repeatable way. We will use it to produce information, something which is of infinitely greater worth than mere statistics.

However, before we begin collecting data we need to decide what to collect and have a good idea why we want it. This is where starting off with an ounce of planning can prevent us from gathering a pound of frustration. A good plan for data collection and validation is necessary. Such a plan will consider the following questions and details (Herrmann, 2007):

- **What?** – Simple enough. You must begin by determining specifically what data you will gather.

- **Why?** – This is a critical question to answer. Why are you collecting this data and what will be done with it? If there isn't a clear answer to this question, then you should move on to the next metric and leave this one behind.

- **How?** – How will the data be collected? For technical data the focus should be on automation whenever possible. It just makes more sense to spend your staffing dollars remediating problems uncovered by a metrics report than to spend them producing the report. For process-oriented data a repeatable method should be followed in order to establish consistent measurements.

- **When?** – How frequently will each piece of data be retrieved and what time period will be measured? This is a point worth considering. Comparative analysis can be negatively impacted by overlooking this detail. For instance, comparing the total number of events occurring in February (28 days) vs. March (31 days) will be difficult at best. Also, if your organization has locations in multiple time-zones it can complicate time-bound data collection. Take the time right up front to make these determinations and be specific.

- **Where?** – What sources of raw data will you tap? Most organizations find they have an over abundance of resources when they really stop to think about it.

- **Ensure Data Integrity** – What type of data is allowed for use and what type is forbidden? For instance are detailed records required or can summary or historical information be used? How will the data be preserved after gathering to ensure its integrity?

- **Derive True Meaning** – define how the information will be analyzed and interpreted.

Producing Technical Metrics

Much of the data you require can probably be gathered from existing sources within your environment. The following list includes some tools that are likely to provide raw data in support of technical metrics:

- Anti-malware
- Firewalls
- Managed Security Services
- Intrusion Detection/Prevention
- Anti-SPAM
- Asset Management
- Patch Management
- Vulnerability Management
- Unified Threat Management
- Application Security Scanners
- Databases
- Website Statistics
- Network Access Control
- System Integrity Checking
- Operating Systems
- Data Leakage Protection
- Configuration Hardening
- Secure Web Gateways
- Web Application Firewalls
- Mobile Data Protection
- Media Sanitization
- Governance, Risk and Compliance Management
- Storage Encryption
- SIM/SIEM

Producing Process-Oriented Metrics

Numerous IT processes can also yield data that is interesting for our metrics program, especially when we are measuring the overall health of the security function. Just remember to take caution with these numbers. Make certain that the data is consistently produced and gathered, and that it paints an accurate picture. Nothing will bog down a metrics program quicker than wasting time explaining and defending your collection methodology. It is much more profitable to focus on interpreting what the data indicates, and then taking action on that information.

Having stated that concern, you should investigate the following IT processes which are common sources of rich statistical data:

- Change Management
- Help Desk
- Identity & Access Management
- Incident Response
- Security Awareness Training
- Disaster Recovery & Business Continuity

3.2. What do I do with these metrics?

Having gathered the raw data and turned it into valuable information, now you need to take steps to publish a report. It is vital that this report be both relevant and persuasive. It's not enough to present pertinent information; but you must also portray that information in a visually striking and logically compelling way. Experience has shown that nothing will surpass the power of an attractive visual design to ensure your report is widely read.

Data Visualization

One way to guarantee your design hits the mark is to adhere to the best practices of data visualization as taught by various thought leaders in this field. Edward Tufte has produced some of the more remarkable books on this topic. I highly recommend any of his works, especially *Envisioning Information* and *Beautiful Evidence*. Tufte can frequently be found on the lecture circuit as well and I am told he is a passionate and gifted speaker.

In dealing with the topic of data visualization, a practical piece of advice which has proven invaluable comes from Jaquith's book which is accurately described as a modern classic. "…because photocopies of good exhibits…tend to proliferate mysteriously into unforeseen hands, get into the habit of printing all exhibits in black and white *first*, before finalizing designs. By "proofing" exhibits this way, you can catch potential reproduction problems before they become an issue." (Jaquith, 2007)

Striving For Quality

You can avoid a lot of confusion regarding the meaning of your metric if you interpret it for the consumer. One highly effective method for doing this is to accompany each exhibit with descriptive text explaining what it intends to communicate. Furthermore, by including such documentation you afford yourself an opportunity to editorialize or to explain any anomalies that appear in the data. This opportunity is too valuable to ignore.

It is essential to document your metrics definitions and place them under strict change management control. This step is imperative to guarantee the processes and formulas used to produce each metric remain constant. It is the best way to make certain that your metrics allow for trustworthy data comparisons over time.

Once you settle on a design for your metrics report and begin publishing it, you must make certain it is well cared for and strive to continually improve it. Nothing will discourage faithful reading faster than a stale or poorly maintained report. Regularly take the time to solicit and review feedback from your consumers. Be quick to respond with any changes that seem to be called for. A useful exercise is to show the report to those who have never seen it before and ask them to explain what the information means. You should strive for sufficient clarity to allow even the uninitiated to instantly understand what your exhibits are communicating.

Strategic Measurements

Something you will want to give careful consideration to is how to organize the information included in the report. Sometimes the same raw data can be presented in multiple ways, each of which serves a different purpose and achieves a different result. A brief example will be useful in explaining this concept.

Let's use the example of a metric which measures the '*percentage of computers with current anti-virus definitions*'. In '*Exhibit A*' we are shown a holistic view of this information measured on a monthly basis. This metric might be interesting to the CISO, the CIO and perhaps the CEO (from a regulatory compliance perspective); but it is not actionable in any way and will not serve as a meaningful diagnostic tool. It can certainly give us a sense of the overall health of anti-virus defenses at this organization. And we may also find value in being able to observe trends over time.

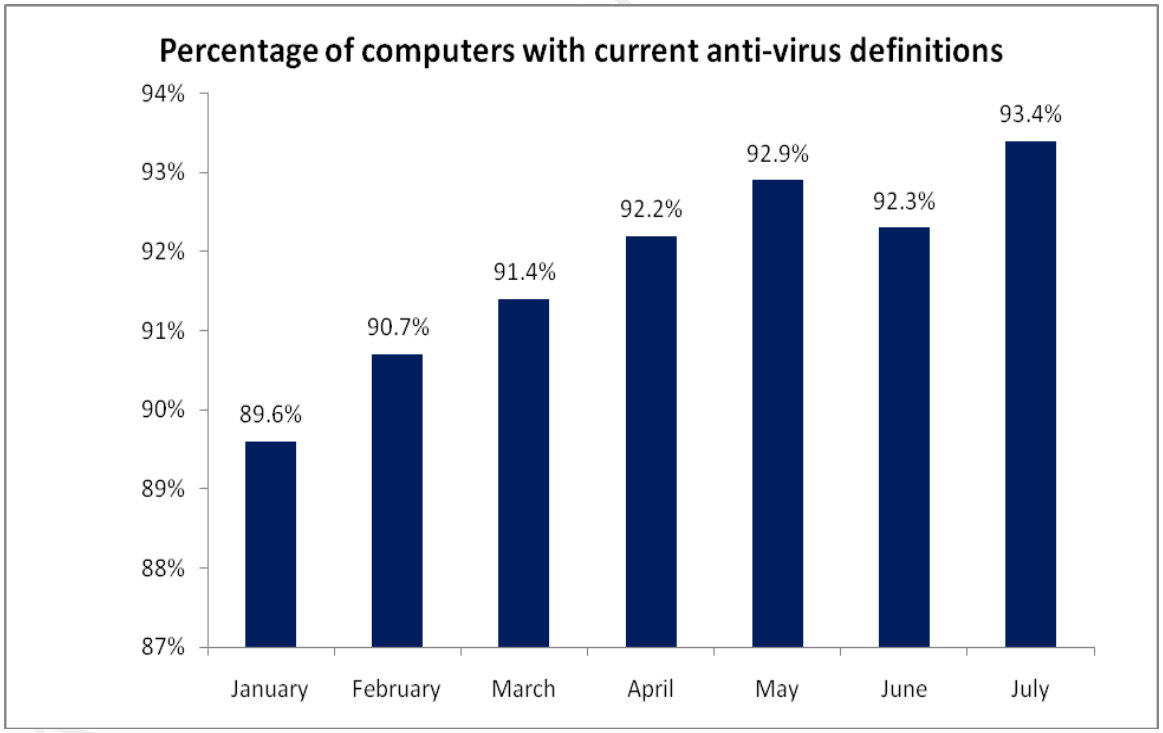

Exhibit A

But now contrast '*Exhibit A'* with '*Exhibit B*' which displays the very same measurement. However, this time instead of presenting a top-level view the information is divided along business lines. By drilling down into the data we can begin to understand which business units are struggling with this activity. This in turn will help us choose where to focus in order to improve the performance of the organization. This kind of actionable intelligence is valuable and it can really drive performance improvement.

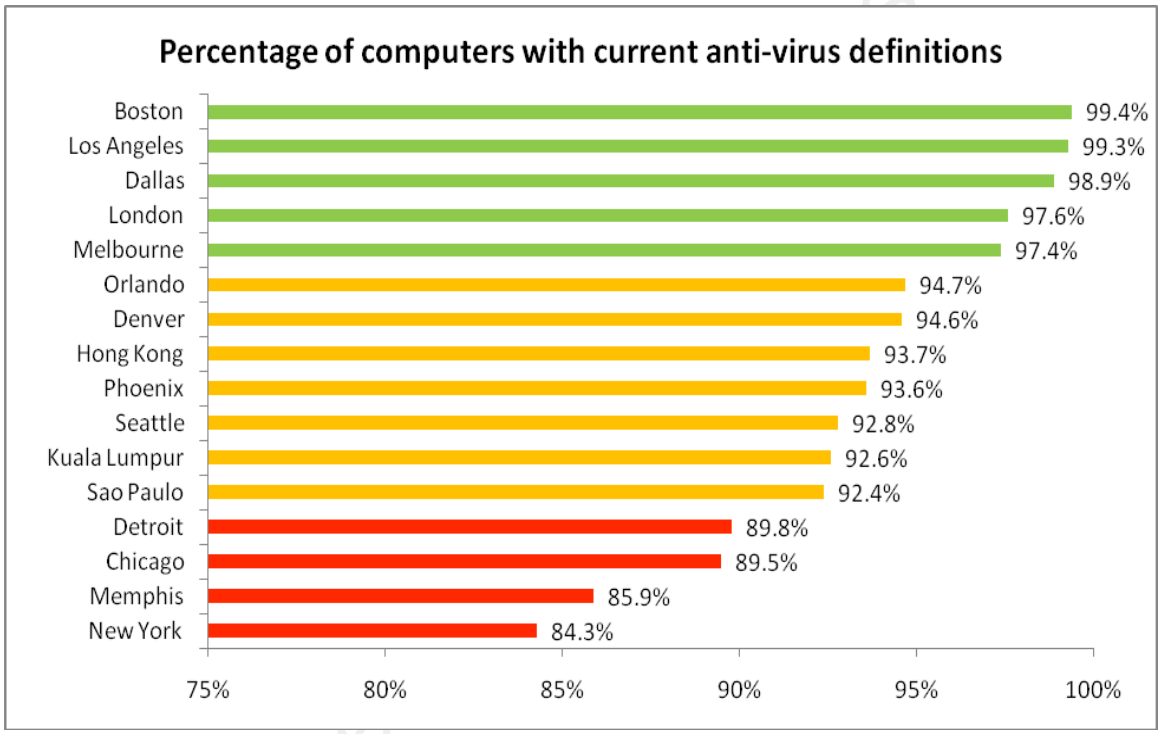

Exhibit B

But let's not be in a hurry to move on, because this example demonstrates another principle well worth learning. By presenting information in a sufficiently granular way we can inject business relevance into our exhibits. In effect this produces a benchmark of our business units, which is an especially powerful approach to performance improvement. Frequently this level of visibility will spark a competitive fire in those being measured. Professional pride will drive most people to make sure they are found among the high performers on your report. But even when it doesn't generate this response, you provide IT leadership with a helpful motivational tool. Management is simply easier when your team has an explicit and measureable goal to achieve.

Consumer Relations

Endeavor to socialize the metrics program throughout your organization, acting as an evangelist when the opportunity presents itself. Be quick to share a copy of the latest report when appropriate. The more widely read it becomes the richer the feedback will be that you can expect to receive. Regularly circulating these reports will also increase awareness of the value being produced by the security function.

Finally, with a copy of the report in hand, ask potential metric consumers what measurements *they* would like to see. Often times a tangible example that demonstrates the various possibilities will stimulate their thinking, and you will discover new ways for your metrics program to add value.

3.3. Conclusion

Many substantial benefits can be derived from initiating a security metrics program, and there is little reason for delay. At the onset it requires only a meager investment comprised mostly of the time spent planning, gathering data and producing each report. This makes a security metrics program an intriguing project, especially in economically challenging times when funding can be tricky to secure.

If you remain focused on satisfying the business needs of the consumer, and follow the basic guidelines presented here, you can have a positive impact on the performance of your organization. Furthermore, by equipping management with objective measurements you are demonstrating the increased maturity of your security program and the likelihood of its success.

4. References

Brotby, W. K. (2009). *Information security management metrics: a definitive guide to effective security monitoring and measurement.* Boca Raton, FL: Taylor & Francis Group, LLC.

Center For Internet Security - Security Metrics. (n.d.). Retrieved October 10, 2009, from Center For Internet Security: http://www.cisecurity.org/securitymetrics.html

Elizabeth Chew, M. S. (2008, July). *NIST Special Publication 800-55 Revision 1.* Retrieved from NIST Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resiliance, and ROI.* Boca Raton, FL: Auerbach Publications.

Introduction To ISO 27004 - Information Security Management, Measurement And Metrics. (n.d.). Retrieved October 10, 2009, from The ISO 27000 Directory: http://www.27000.org/iso-27004.htm

Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt.* Upper Saddle River, NJ: Pearson Education, Inc.

SecurityMetrics.org (n.d.). Retrieved October 26, 2009, from securitymetrics.org: http://www.securitymetrics.org

Security Metrics: On-Demand (n.d.). Retrieved November 04, 2009, from metricscenter.net: https://www.metricscenter.net/