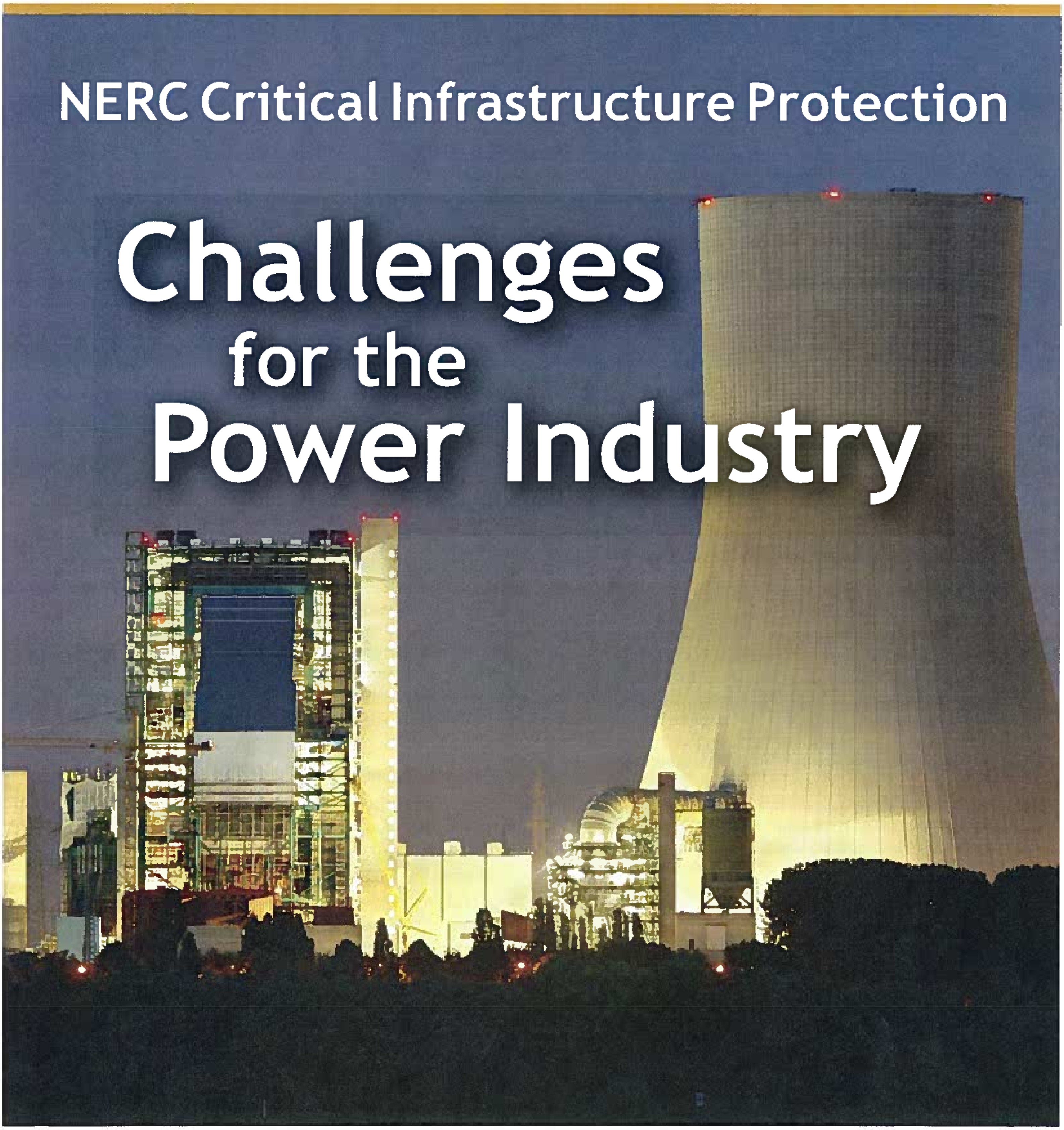
The ISSA Journal

July 2012
Volume 10 Issue 7

The Case for Compliance Regimes

Are There More Security Breaches?
Or Are We Just Reporting Them Now?

Data Needs for Network Security Metrics:
A Measure and Manage Approach



NERC Critical Infrastructure Protection

Challenges for the Power Industry

Information Needs for Cost-Effective Network Security Decisions

Data Needs for Network Security Metrics: A Measure and Manage Approach

By Soumyo D. Moitra

This article reviews the data needed to make effective decisions on planning for network security, particularly with respect to acquiring and deploying network sensors systems.

Abstract

This article describes the data that is needed to evaluate the benefits from network security systems such as sensors. The needs have been identified on the basis of modeling and analyses done to estimate these benefits. The data items are described in detail, and the rationale for collecting them is also discussed. The article describes how the data can be used to help improve managerial decisions regarding network security.

Good decisions require the right information. This is especially true in operations where decisions often have to be made quickly, and the decisions makers therefore need to have the data on hand. This article reviews the data needed to make effective decisions on planning for network security, particularly with respect to acquiring and deploying network sensors systems. Sensor systems are a critical component of network security since they monitor the traffic and help security analysts to detect and respond to cyber attacks. The term *sensor system* will be used in a broad sense to include not only the sensing device but the supporting systems that process the data from sensors as well. Thus the data needs discussed will apply more generally to network security systems; the term *sensor systems* will make the arguments more concrete.

A project was undertaken at CERT/Software Engineering Institute at Carnegie Mellon University to develop metrics to evaluate network sensors (Moitra, 2010). A key finding of the project is that the data needed to estimate the benefits of sensors (and network security in general) for managerial decisions are largely unavailable (Pfleeger, et al., 2006). However, they have been identified in the course of the project, and it is essential that this data be collected since it will help with these very important decisions, such as justifying investments, determining the appropriate level of expenditures, allocating security resources across multiple needs, and deploying security systems effectively. This article reports on the data needed to assess the value of sensor systems so that network security decisions can be more accurate, objective, and comprehensive. This measure-and-manage approach ensures the best security for a given budget (Gordon and Loeb, 2006). The data will lead to more informed and cost-effective decisions on network security management. The scope of this article is a review of the information needs only. For the interested reader, further details may be obtained from the references cited or from the author.

Cyber threats and incident handling

The following variables are needed to assess the threat scenario and the response process:

- Rate of cyber attacks against the organization by attack category (N)
- Probability of detection of an attack with current security infrastructure (p)
- Probability of detection of an attack with better (newer) detection systems (p1)
- Probability of prevention of damages after detection (q)

- Probability of some protection or mitigation after detection, even though the damage could not be totally prevented (r)
- Degree of mitigation (on the average) (M)

As with all the variables discussed, there are significant challenges in measuring these, but they are essential for assessing the performance of network defense. It is well known that for any network alerting system, we should estimate the true positives (TP), the false positives (FP), the false negatives (FN), and the true negatives (TN). The first three variables above (N, p, p1) are related to these. However, these are difficult to measure in practice. These values can only be reliably measured from carefully designed exercises (such as cyber blue team/red team exercises, or with high quality penetration testing) and, importantly, only when detailed data are collected from these exercises. From such empirical data, it is possible to get reasonable estimates of the first three variables by calibration with respect to a given organization. The last three variables have to be estimated at the individual organizational level.

These data items are necessary to assess the benefits from sensor systems (Arora, et al., 2004; Brotby, 2009; Soo Hoo, 2000; Johnson, 2008). The disaggregation by attack category is particularly important since both the incidence rate and the impacts vary greatly by category. These data items can help answer a number of important managerial questions about the detection and incident handling process and can thus help information assurance (IA) managers to improve their cyber defense operations. Currently very little reliable data are available, so even reasonable ranges will help improve operations.

There are some special challenges in measuring these variables. In reality, attacks can involve many steps and multiple alerts may have to be correlated to identify an attack. Responses and their impacts are very complex and cannot be quantified easily. Also, false negatives are extremely difficult to count except in planned exercises. Other challenges to data collection will be discussed later. For now, the emphasize is that *if the data were available*, it would greatly improve managerial decisions regarding network security.

Damages and losses from cyber attacks

Very often, organizations do not have accurate assessments of the damages (or losses in monetary terms) that can be caused by cyber attacks (CSI, 2011). Related to that, they may not have good estimates of the reduction in damages that can be expected as a result of having sensor systems and an incidence response process. However, this information is essential to estimate the effectiveness of and benefits from network sensors (Jensen, 2009). The following variables are needed for this analysis:

- The potential damage that could be done by type of damage and by different attack categories (the A/D matrix described below)
- The degrees of mitigation given detection: for example: almost no damage control; some damage control; complete damage control
- Probability of success of an attack in spite of no hindrance/detection

Thus, we need to know the potential damages that can be caused by cyber attacks without a sensor system and then with the sensor system in place. Only then can we measure its impact. Similarly we need to know the degrees of mitigations (m – if there are several degrees of mitigation) that can be achieved through incident handling and response with and without the sensor system. Finally, many cyber attacks do not succeed even if they are not detected. There can be many reasons for this, such as lack of time or resources on the part of the attacker or mistakes by the attacker or lack of skills. This is a non-trivial aspect of network defense, and each organization should know this probability.[1]

This information is essential to estimate the benefits from having a sensor (Hayden, 2010; Herrmann, 2007; Jaquith, 2007; Paquet and Saxe, 2004). Information assurance managers will have a much better basis for making security decisions at the organizational level. In addition to better decisions based on data, the quantification and clarification of the concepts of threats, vulnerabilities, and risk that will result from the exercise of collecting this data will provide many insights into the risks and defenses of the organization.

The primary challenge is estimating the data on damages and losses. It involves a lot of data: damage estimates by attack category and type of damage. The data can be represented by a matrix (the A/D matrix) where attack categories could be along the rows and the damage types along the columns. Each cell in the matrix then represents the potential damage (by type) a given attack category can cause. The data may involve a lot of uncertainty, and of course there will be considerable variability across organizations that might make calibrations and comparisons difficult. For some losses, such as losses from data compromise, estimates can vary even among experts. For this reason (and because losses from data compromise may be critical) we are developing a separate methodology to estimate the value of sensitive information.[2] In some cases, $-values for damages may be difficult to estimate, and ratings of damages may be used instead. Finally, the degrees of mitigation are actually along a scale, but to make the problem tractable we may need to consider only discrete cases, such as no mitigation, some mitigation, and complete mitigation.

[1] This is, of course, a simplification of the real situation. In reality there are many complexities and time-related intermediate observations. However, in practical terms, it is too complicated to analyze the situation in its full detail before making decisions. Also complete data is almost never available. Therefore a balance is proposed between complexity and tractability.

[2] The paper is under preparation and it is expected to be published in the open literature in the near future.

Sensor system characteristics and how they can be useful

Metrics for a sensor should include a component that reflects its characteristics and how its usage affects its value for network security. These factors help in facilitating detection and response to cyber attacks. There are three general dimensions to this: a) features, functionalities and (extent of) facilitation, b) intensity of monitoring, and c) effectiveness of response. Therefore, information on three sets of variables is needed:

- Rating of the features, functionalities and (extent of) facilitation of a sensor system ($\mathcal{S}$)
- Rating of the intensity of monitoring of network traffic with the system ($\mathcal{M}$)
- Rating of the effectiveness of response and incident handling given detection ($\mathscr{R}$)

This information is used to measure the usefulness or effectiveness of the sensor system. These variables are intrinsic to the sensor system and its usage. The first rating takes into account the extent to which the sensor system facilitates the incident handling by the security analysts. It is independent of the nature of the network or location where the sensor is deployed. These ratings can be combined through as set of importance weights for these three factors to give an additional metric for the sensor. This metric can have a number of uses. For example, it gives an indication of how valuable the sensor might be. This can help in determining the fit of a sensor at a particular location. This metric can also help in estimating the probabilities of detection, prevention, and mitigation if that senor is deployed.

This is a new approach that has been developed and one of the challenges is to ensure that the ratings are validated. Judging the value of these three variables (and the importance weights) can be difficult and initially there may not be a consensus among experts. However, after some iterations of using the metric, a standard methodology and consensus can be expected to evolve. The other challenge is to incorporate its use among decision makers for network security. The benefit of this metric is that it integrates the technical issues of sensors with the managerial issues in network defense.

Value of sensitive information

This project considered the various types of damages and losses that could be caused by cyber attacks. Analysis of available data indicated that compared to other type of damages, such as damage to hardware or software or communications ability, the potential loss from compromise of sensitive information could be far higher than other losses, and could dominate the total loss from cyber attacks. On the other hand, there is no methodology to estimate this loss with any reliability. Secondary data and media reports cite amounts that are often guesses and exhibit great variability. In the absence of any standard algorithm for computing these values, it is difficult to arrive at estimates that would be meaningful for decision making. Therefore a new methodology was developed to estimate the value of sensitive information (VOSI). Losses from sensitive information are now well-recognized as a very important issue, and the methodology represents a comprehensive and systematic approach to assess the value of the sensitive information that resides in any organizational network. It is planned to publish this methodology, and then it will be generally available.

The following describes the variables on which we need information as identified by the method to evaluate VOSI. The method is based on assigning an item of information to an "order" in a classification scheme. The order of the information directly and uniquely determines the value of that information. The loss to an organization, if that kind of information is compromised, is also dependent on the type of misuse of that information. The data to be collected are the values in the cells of a matrix defined by the orders and misuse types. That is, we need to get the loss ratings (by order and misuse) from IA experts. This is a one-time exercise.[3] Then the total loss can be assessed by weighting this rated loss by the amount of that information that is compromised. We also need the probabilities of any misuse given a compromise, and the probabilities of different kinds of compromise. The details are also available from the author.

The information required by this model is the set of values of the following four variables:

- The potential loss ($-values or ratings) resulting from compromised information by the type (or order) of the information and by type of misuse – for all orders and misuse types; the data will be in the form of a matrix we shall call $|Z|$
- The amount of information by type (order) in each item of information on the host ($|x|$); this will be on a scale of 1 to 5
- The probabilities of different kinds of compromises (q_c)
- The probabilities of different types of misuse of the sensitive information ($p[m|c]$)

In summary, the model to estimate VOSI considers the loss from compromise of sensitive data as a function of the type of compromise, the kind of misuse given the compromise, the sensitivity (order) of the information compromised and the amount of that information that is compromised.

Given this data, we can estimate the maximum potential loss (value at risk or VAR) and the expected loss to an organization given probabilities of compromise and misuse. To develop effective and efficient strategies for network defense, we need this data to estimate VOSI. This is a novel approach that captures a metric that is very important. The metric is along a scale. If uniformly applied, the metric can be used to compare organizational networks and to establish the relative values of sensitive information. With such a metric, network defense strategists will be able to consistently prioritize targets

[3] This data is independent of any organization. It is related to the intrinsic nature of sensitive information.

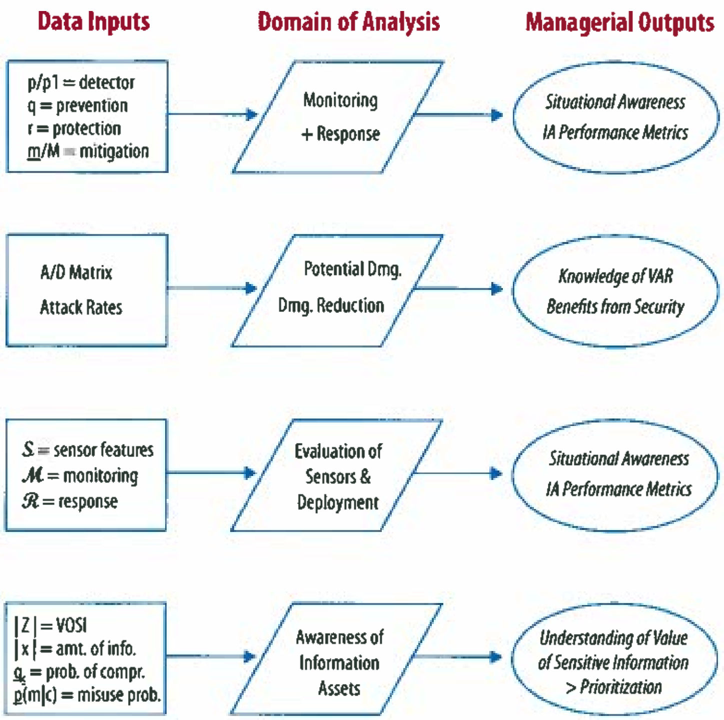


Figure 1 – Data throughput from input data to managerial outputs

by the value of information residing in them. Information assurance managers will be able to apply the metric to devise more effective cyber defenses by allocating security resources in proportion to the value of what is to be protected.

The flow of data and information is summarized in figure 1. The various kinds of data that have been identified as essential for effective security decisions are given in the first column, according to the terminology used earlier. These data items are then used as input for the respective domain analyses as shown in the second column. The results of the analyses will help in various areas of managerial decisions for network security as shown in the third column.

The current challenge in implementation is that the concepts behind this metric are new and have to be validated. In order to validate them and do case studies to establish the methodology, it has to be socialized among potential users, and that would be the other challenge. However, as discussed above, there would be significant payoffs if the data were collected and applied.

Information gathering issues

While the information discussed here may not be currently available, it is not difficult to collect. Some items may be collected already by some organizations. Once a comprehensive collection process is started, it should be relatively easy to maintain the momentum. The benefits of having this data set will be substantial, as already noted. Some data items may be collected from surveys among IS/IA analysts. Some survey instruments have already been developed at CERT/SEI to elicit some of this information. Parts of these surveys can also be fielded by organizations depending on their areas of interest. Red/Blue team cyber exercises can play a crucial role in collecting some of the data described here, and the data will always be valuable in planning cyber defenses. The key requirement is that they should be carefully planned and the data should be meticulously collected. A systematic data collection process needs to be incorporated into the information assurance policies of all organizations in any case, and this article has identified the key items to be collected. Then a comprehensive, uniform, and consistent methodology can be applied to evaluating the benefits from sensors or any network security measure.

The overall schema for addressing the data needs for managing network security is shown in figure 2. The initial model identifies the parameters to be estimated and this defines the data needs. The data is then collected and stored in a repository. This data is used for modeling and analysis to estimate the benefits of security systems and the effectiveness of the systems. The results will help develop appropriate recommendations for decisions. The analysis will in general also reveal new data needs and scenarios to be explored further. This will give rise to new data needs. Similarly, with experience there will be learning and resulting requirements for modifications. These in turn will also lead to new data needs. Figure 2 represents the whole cycle of analysis and decision making for security management.

The overall challenges in this effort are:

- The data collection can be difficult initially

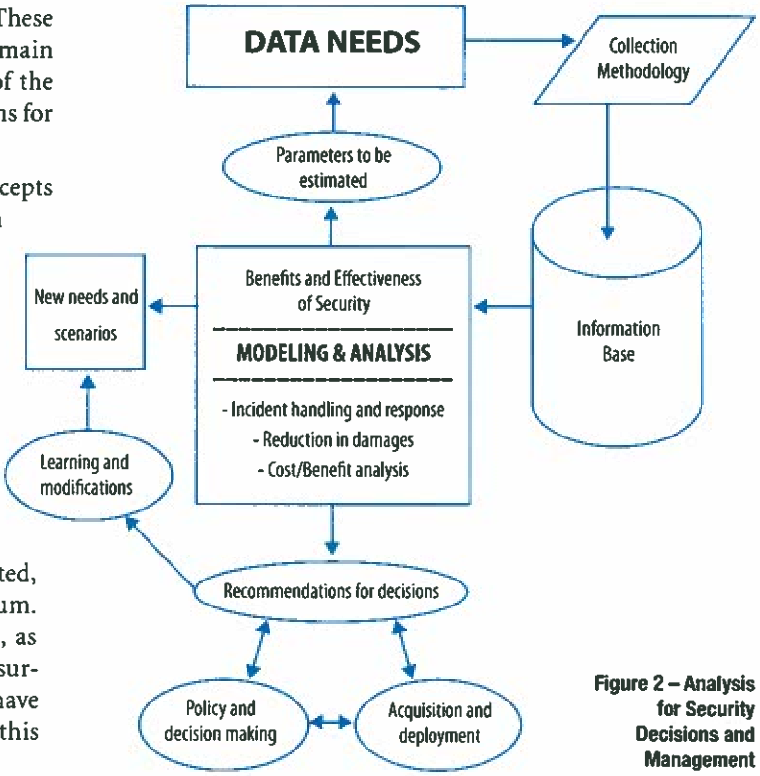

DATA NEEDS
Collection Methodology
Parameters to be estimated
Information Base
New needs and scenarios
Benefits and Effectiveness of Security
MODELING & ANALYSIS
- Incident handling and response
- Reduction in damages
- Cost/Benefit analysis
Learning and modifications
Recommendations for decisions
Policy and decision making
Acquisition and deployment

Figure 2 – Analysis for Security Decisions and Management

- Interpreting data from cyber exercises can be complicated and translation from one situation to another may not easy
- The variables concerned have high degrees of uncertainty, are sometimes intangible, and there can be a wide diversity of estimates even among experts and professionals
- Resistance to data collection and analysis: There are views that some of these variables are simply not measurable, that they are too intangible, and even if we could assess them it would be too expensive to make it worthwhile
- There can be a general skepticism about the economics of security benefits

Quantifying the returns from security investments is hard. However an attempt needs to be made to help in the expenditure decisions (Hubbard, 2010), since investments in security must be made now and in the foreseeable future. Real dollars are being spent on sensors, network security, and security in general. We need both to justify them and to determine the appropriate amount. The data described here is essential for good security decisions.

Summary, benefits, and conclusions

This article has described the major items of information needed for network security management decisions related to sensor acquisition and deployment in particular. The information will be valuable in any case as it will help inform better tactical and strategic plans for network defense under budget constraints, an issue that is of crucial importance since resources are always limited and may become even more constrained in the future. Currently there is a lack of data on cost-effectiveness and benefits from investments in the area of network security; therefore, even approximate metrics will be an improvement. The data will help implement new approaches to evaluate incident handling and sensor characteristics and to measure the value of sensitive information. Analyzing this data will additionally help to clarify concepts and assumptions related to cyber security in general.

The main advantage is that with this information and its analysis, we can arrive at concrete estimates (costs or losses on a well-defined scale) of the risks that computer networks face. Network managers will have valuable information at hand that will help reduce possible biases and errors in the assessment of damages from cyber attacks. This will improve managerial decisions regarding sensors and network security measures. Better and more effective decisions will lead to greater security for the expenditures incurred. The data will help justify acquisitions, help in deployment decisions, and help prioritize needs of different organizational networks. Many of these operational decisions have to be made regularly and quickly. If the information is systematically collected, that will facilitate quicker decisions and might assist in automating some of the decision-making processes.

To conclude, the information will support a methodology that integrates technical and managerial perspectives into network security decision making. Without the data and information discussed here, security decisions will have more guesswork than necessary and may not be as efficient or effective. This article has identified the key information items to help managers develop strategies to collect them. If they do not know what to collect, they will not be able to develop the strategies. In particular, the data discussed here are directly relevant to many of the issues such as data protection, returns on security investments, and prioritization of network defense measures that are major concerns of all organizations today.

References

—Arora, A., Hall, D., Pinto, C.A., Ramsey, D. and Telang, R. (2004) Measuring the risk-based value of IT security solutions. *IT Professiona* , Vol.6, No.6, 35- 42.

—Brotby, W. K. *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Management.* CRC Press, Boca Raton. 2009.

—CSI *Computer Crime and Security Survey.* Computer Security Institute, 2011.

—Gordon, L.A. and Loeb, M.P. *Managing Cybersecurity Resources.* McGraw-Hill, New York, 2006.

—Hayden, L. *IT Security Metrics.* McGraw-Hill, NY, 2010.

—Herrmann, D. S. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI.* Auerbach, Boca Raton, 2007.

—Hubbard, D. W. *How to Measure Anything: Finding the Value of "Intangibles" in Business.* Wiley, Hoboken, 2010.

—Jaquith A. *Security Metrics: Replacing Fear, Uncertainty and Doubt.* Addison-Wesley, 2007.

—Jansen, W. "Directions in Security Metrics Research," NISTIR7564-2009, NIST.

—Johnson, M.E. *Managing Information Risk and the Economics of Security.* Springer, 2008.

—Moitra, S. D. (2010) CERT Annual Research Report.

—Paquet, C. and Saxe, W. *The Business Case for Network Security: Advocacy, Governance and ROI.* Cisco Press, 2004.

—Pfleeger, S. L., Rue, R., Horwitz, J. and Balakrishnan, A. (2006) Investing in Cyber security: The Path to Good Practice. *Cutter IT Journal*, Vol. 19, Issue 1, 11- 18.

—Soo Hoo, K. J. (2000) How Much Is Enough? A Risk-Management Approach to Computer Security, working paper, CRISP .

About the Author

Soumyo Moitra is a Senior Member of Technical Staff in the Network Situational Awareness Group at CERT, at the Software Engineering Institute, Carnegie Mellon University. He has applied operations research models in a number of areas including policy analysis, telecommunications and technology management. He is currently working on various aspects of network sensors, network traffic analysis and work flow models. He can be reached at smoitra@cert.org.