Security Metrics
Unit-IV

IPR

Intellectual property laws include patent, copyright, trademark, and trade secret laws, which typically protect IP rights. Patents, copyrights, and trademarks are creations of statute, where the government recognizes and enforces the public expression of an original idea for a limited period of time. Trade secrets, established by common law, can protect IP through contractual and tort remedies. Copyright laws generally protect creative and artistic works such as books, movies, music, paintings, photographs, and software. Patents, trademarks and trade secret laws are used more often to protect industrial properties, as they are generally created and used for industrial or commercial purposes.

International intellectual property law, with the exception of trade secrets, is governed by federal and international treaty legislation. In the era of globalization, with the worldwide internet and the subsequent ability for proprietary data to be copied and appropriated, IP rights need to be protected and regulated at an international level.

Copyright Law

Copyright is a set of exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work. Copyright does not protect ideas, only their expression. In most jurisdictions copyright arises upon fixation and does not need to be registered. Copyright owners have the exclusive statutory right to exercise control over copying and other exploitation of the works for a specific period of time, after which the work is said to enter the public domain. Uses covered under limitations and exceptions to copyright, such as fair use, do not require permission from the copyright owner. All other uses require permission. Copyright owners can license or permanently transfer or assign their exclusive rights to others.

Patent law

Patent law is a specific area of law that encompasses the legal regulation, jurisprudence, and enforcement of specific intellectual property rights known as *patent rights*. A patent is a government issued right granted to individuals or groups that protects their original inventions from being made, used, or sold by others without their permission for a set period of time. While patents can be legally obtained without the use of an attorney, an attorney who specializes in patent law can help ensure that their client's patent is enforceable by law. Because patent law pertains to intellectual property, which is like any other property in that it can be legally sold, exchanged, traded, or abandoned, the finer points of patent law are frequently amended as technology changes. This is another reason why an attorney specializing in patent law is of significant use to those seeking a patent.

Security Metrics

- A widely accepted management principle is that an activity cannot be managed if it cannot be measured. Metrics can be an effective tool for security managers to discuss the effectiveness of various components of their security programs, and he security of a specific system.

Defination

- It helps to understand what metrics are by drawing a distinction between metrics and measurements. Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time.3 Measurements are generated by counting; metrics are generated from analysis.4 In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data.

- Good metrics are those that are SMART,

specific,

measurable,

attainable,

repeatable,

time-dependent

The Value of Security Metrics

- Metrics help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions.
- they may be used to raise the level of security awareness within the organization.
- through metrics, security managers can better answer hard questions from their executives and others

such as:

- Are we more secure today than we were before?
- How do we compare to others in this regard?
- Are we secure enough?

Why Metrics Generation Is Difficult?

- security manager needs to look beyond the organization's security incident record for indicators of security strength. There are further complications they need to keep in mind, however, in their search for meaningful metrics.
- asset value, threat, and vulnerability are critical elements of overall risk and are (or should be) weighed in most decisions having to do with security. Each of these elements poses difficulties when trying to incorporate them into a useful security metric.
  - Asset value is the easiest of these three elements to measure. (It is quantify metrics.)
  - Threat cannot be measured at all, since it is the potential for harm, although survey results and other information gathered from external sources could be useful in quantifying threat at a high level.
  - Progress is being made in objectively measuring vulnerability, at least for specific types networked computer devices.
  - Measurements of vulnerability, such as degree of understanding of security issues among computer users, remain somewhat subjective.

Contd…

- Security metrics are also hard because the discipline itself is still in the early stages of development. Those pursuing the development of a security metrics program should be prepared to adjust strategies as experience

Building a Security Metrics Program

- To facilitate understanding and acceptance at all levels of a new security metrics program, it is advisable to ground the program in process improvement frameworks that are already familiar to the organization.

Regardless of the underlying framework, the seven key steps below could be used to guide the process of establishing a security metrics program.

1. Define the metrics program goal(s) and objectives
2. Decide which metrics to generate
3. Develop strategies for generating the metrics
4. Establish benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it, and
7. Establish a formal program review/refinement cycle

The seven key steps

This seven-step methodology should yield a firm understanding of the purpose of the security metrics program, its specific deliverables, and how, by whom, and when these deliverables will be provided. The steps are briefly described below, and outcome examples, where appropriate, are provided.

Step 1: Define the metrics program goal(s) and objectives

Because developing and maintaining a security metrics program could take considerable

effort and divert resources away from other security activities, it is critical that the goal(s) and objectives of the program be well-defined and agreed upon up front. Although there is no hard and fast rule about this, a single goal that clearly states the end toward which all measurement and metrics gathering efforts should be directed is a good approach.

Contd…

A goal statement might be, for example:

Provide metrics that clearly and simply communicate how efficiently and effectively our company is balancing security risks and preventive measures, so that

investments in our security program can be appropriately sized and targeted to meet our overall security objectives.

Contd…

Statements of objective should indicate high-level actions that must be collectively accomplished to meet the goal(s). An action plan should be directly derivable from these statements. A few objectives for the goal above, for example, might be:

a. To base the security metrics program on process improvement best practices within our company.
b. To leverage any relevant measurements currently being collected.(formal apparch to record)
c. To communicate metrics in formats custom-tailored to various audiences.
d. To involve stakeholders in determining what metrics to produce.

Step 2: Decide which metrics to generate

Any underlying corporate framework for process improvement, as discussed at the

beginning of this section, could dictate what metrics are needed. For example, a “Six Sigma” approach would focus on security processes for which defects could be detected and managed, and Step 2 of building a metrics program would, therefore, be to identify those specific security processes. In this case, Step 2 would identify those standards for which compliance should be tracked.

Contd…

In the absence of any pre-existing framework, a top-down or a bottom-up approach for determining which metrics might be desirable could be used. The top-down approach starts with the objectives of the security program, and then works backward to identify specific metrics that would help determine if those objectives are being met, and lastly

measurements needed to generate those metrics. For example:

Top-Down Approach

TOP-DOWN APPROACH	
a. Define/list objectives of the overall security program	Example objective: To reduce the number of virus infections within the company by 30% by 2002
b. Identify metrics that would indicate progress toward each objective	Example metric: Current ratio of virus alerts to actual infections as compared to the baseline 2000 figure
c. Determine measurements needed for each metric	Example measurement: Number of virus alerts issued to the organization by month Example measurement: Number of virus infections reported

Bottom UP Approach

The bottom-up approach entails first defining which security processes, products, services, etc. are in place that can be or already are measured, then considering which meaningful metrics could be derived from those measurements, and finally assessing how well those metrics link to objectives for the overall security program. To illustrate:

Contd…

BOTTOM-UP APPROACH	
a. Identify measurements that are/could be collected for this process	Example measurement: Average number of Level 1 vulnerabilities detected per server by department using our xyz scanning tool
b. Determine metrics that could be generated from the measurements	Example metric: Change in number of critical vulnerabilities detected on servers by department since last reporting period
c. Determine the association between the derived metrics and	Example objective: To reduce the level of detectable vulnerabilities

Contd….

The top-down approach will more readily identify the metrics that should be in place

given the objectives of the overall security program, while the bottom-up approach yields the most easily obtainable metrics. Both approaches assume that overall security program objectives have already been established. If they have not been, defining these high-level objectives is obviously important and a prerequisite.

Step 3: Develop Strategies for Generating the Metrics

what is to be measured is well understood, strategies for collecting needed

data and deriving the metrics must be developed. These strategies should specify the source of the data, the frequency of data collection, and who is responsible for raw data accuracy, data compilation into measurements, and generation of the metric.

a formal risk assessment is one method for collecting some of the data that might be needed, experts disagree on its value for generating metrics.

Early on there were few automated tools available to make data collection, analysis, and reporting cost-effective, but in recent years products have been introduced into the marketplace to make these activities more viable.

Step 4: Establish benchmarks and targets

In this step appropriate benchmarks would be identified and improvement targets set. Benchmarking is the process of comparing one's own performance and practices against peers within the industry or noted "best practice" organizations outside the industry.

Benchmarks also help establish achievable targets for driving improvements in existing practices. A security manager should consult industry-specific data resources for possible benchmarks and best practices, but also may find national and global metrics provided by SecurityStats.com, and other services and publications helpful.

Step 5: Determine how the metrics will be reported

no security metrics efforts are worthwhile if the results are not effectively

communicated. While conventional management wisdom on disseminating information of this nature should prevail, current security metrics literature does reveal some guidance in this area. One analyst, for example, cautions that over-simplification in the name of clarity is a mistake. Executives are accustomed to dealing with financial and other trend lines, so complex security-related data can be valuable to this group if presented well. Graphic representations are particularly effective

Some metrics may be meaningful only to the security manager and staff and should not be distributed further. Security managers may, however, use other metrics to help trigger needed remedial actions with the organization.

Step 6: Create an action plan and act on it

It is time to get the real work done. The action plan should contain all tasks that

need to be accomplished to launch the security metrics program, along with expected completion dates and assignments. As mentioned in Step 1, action items should be directly derivable from the objectives. Documenting the linkage of actions in the plan to these objectives is useful, so that no one will lose sight of why a given action is important.

In the same manner that software should be developed, it is critical to include a testing process in the plan. Deficiencies in collected data may, for example, prove some metrics unusable and require re-examination of what is to be measured and how.

Step 7: Establish a formal program review cycle

Formal, regular re-examination of the entire security metrics program should be built

into the overall process. Is there reason to doubt the accuracy of any of the metrics? Are the metrics useful in determining new courses of action for the overall security program? How much effort is it taking to generate the metrics? Is the value derived worth that effort? These and other questions like them will be important to answer during the review process. A fresh scan of security metrics standards and best practices within and outside the industry should also be conducted to help identify new

developments and opportunities to fine-tune the program.

Conclusion

The task of developing a security metrics program may seem daunting to some, but it need not be. The seven-step methodology can guide development of very simple metrics programs, as well as highly ambitious ones. In fact, some individuals with experience in security metrics recommend that simple starts be made. They advise managers to do what is easy, cheap, fast, and leverage existing measures and metrics.

The important thing to keep in mind is that the metrics generated should be useful enough to drive improvement in the overall security program and to help prove the value of that program to the organization as a whole.

The purpose of this guide is to provide an overview of the current state of security metrics as well as suggestions for developing a metrics program.

Assignment-4

1. What are security metrics? What are the benefits of security metrics?
2. What do you understand by information security?
3. Explain:
    1. Patent law
    2. Copyright law
4. How can you build security into software life cycle.
5. What do you understand by ethics? What are the various ethic issues? Explain ethical issues in IT.
6. What is data privacy? What are the various types of cyber crime?

Note: This assignment should be submitted till 20 April.