Measuring Risk Using Existing Frameworks

Edwin Covert and Fran Nielsen

This article focuses on risks to information technology (IT) systems. Technically speaking, risk to an IT system is a function of the likelihood that some threat will attack, or exploit, some vulnerability in the system and a calculation of the potential impact resulting from these attacks or exploitations.

Two ways exist to calculate risk to an IT system: quantitatively and qualitatively. Each approach has its strengths and weaknesses. Quantitative risk assessment attempts to calculate some “regret for loss,” as Case and Smith describe it. This is usually expressed in monetary terms. On the other hand, a qualitative risk assessment expresses risk in abstract terms such as high, medium, or low.

Calculating risk, however, is not the same as measuring risk, nor is it the same as creating risk metrics. Calculating risk is about a single issue, or a single threat and vulnerability pairing. Measuring risk — or risk metrics — is about monitoring risk over time.

THE PROBLEM

We calculate risk to determine levels of exposure to particular threats. Perhaps the most well-understood threats are technical flaws resulting from unpatched systems. Alternately, a threat could be as “simple” as account password configurations that are in conflict with policy mandating password lengths of more than ten-character alphanumerics.

Despite how disparate, both of these threat categories can be used to calculate risk in either a quantitative or a qualitative manner. Using both simple and more complex threats when calculating risk, however, forces a system owner to aggregate a group of technical risk levels for “point problems” when trying to glean meaningful insight into the overall risk exposure to a system. While potentially addressing certain risky areas, the overall, or “big risk picture,” remains unclear. The aggregation process is not holistic enough to predict — and thus measure — future risk.

In essence, point solution calculation assumes an ability to foretell the future. This involves looking at impending threats and assuming that future threats will be similar or just as likely. With IT, however, the crystal ball is always changing shape (e.g., the warp-speed of technological innovation, the warp-speed of technological innovation, the warp-speed of technological innovation, the warp-speed of technological innovation).
product cycles, and hacker-to-hacker correspondence). Past threats may or may not be an indication of future problems. At the very minimum, to gain insight into the next technical threat facing IT systems, a risk analyst would need to monitor and track worldwide hackers over long periods of time, watching them practice for new ways of cracking systems and then analyzing the information obtained from this surveillance. Informed decisions about which risks to accept, mitigate, or transfer (e.g., via insurance) can only be made with meaningful information generated over the long term.

Risk metrics can enable this “fortune-telling” expertise. Simply examining point technical concerns, however, cannot lead to meaningful metrics. That is, the old models for calculating risk do not lend themselves to the broader picture of information assurance.

**A PROPOSED SOLUTION**

Rather than calculating risk against a point solution, a better method is a *due diligence* approach over the life of the system. We propose to measure the application of best practice controls in a broad range of categories (management, operational, and technical) over time. This proposal adds to an organization’s body of knowledge about security metrics and offers a consistent approach for gathering that information. By measuring successful mitigation against these three categories of controls, organizations gain a better understanding of the risks they face beyond those threats that are purely technical in nature. For example, an organization that monitors employee Internet usage without having a policy on Internet use for employees is open to problems. Without the procedures for dealing with Internet usage infractions, an organization could be thrust into a legal crisis.

Using a best practices, or regulatory requirements, approach — such as a certification and accreditation process or a Federal Information Systems Management Act document — offers an organization the ability to track more than simple technical concerns.

This approach forces consideration and measurement of other potential security hotspots, such as the physical location of the system, the system’s (or organization’s) business continuity plan of action, or the management of the system. The approach also covers the more straightforward security testing of technical controls such as password policy implementation and best-practice router configurations.

Several best-practice frameworks exist. Most of them categorize security controls into three major functional areas: (1) management controls, (2) procedural controls, and (3) technical controls. One widely used framework, the National Institute of Standards and Technology Special Publication 800-37 (NIST SP 800-37), calls the functional areas management, operational, and technical controls, but the premise among the many frameworks remains the same. Differences among the control types must be taken into account to understand — and thus, to manage — risk.

Management controls are those functions that govern the operation and use of the system. Operational controls are the implementation of those management ideas. Technical controls are the technological specifics that give meaning to the operational controls. An example of this architecture is a system that has its high-level information system security policy (management control) directing that the system will be managed in a secure manner. The policy is then translated into standard operating procedures (procedural control) that dictate the actions to take during particular or specific events. Technical controls contain the configuration details of certain system devices to ensure the called-for actions.

While the certification and accreditation (C&A) process is meant to provide a means for organizations to examine the adequacy and effectiveness of their security policies and controls, we propose that C&A is useful for devising risk metrics. Using a certification process to provide risk metrics solves the issues addressed previously regarding
calculated risk and the use of “point” solutions to address non-enterprise risk levels. Most often, risk is calculated as high, medium, or low. These labels are derived either quantitatively or qualitatively and are created by aggregating many point risk levels. Typically, they are also technical in nature.

However, risk should be considered first across multiple aspects of the system. For example:

☐ How well is the IT system’s physical plant protected against a natural disaster or terrorist attack?
☐ Does the system administrator know whom to contact in the event of problems with the system?
☐ How quickly can the system recover in the event of an attack, or if a natural disaster occurs?
☐ When was the last time the business resumption plan was tested?
☐ Do the system administrators have the necessary resources to properly maintain the system?
☐ Are software fixes and security patches tested in a controlled environment prior to implementation on the production system?
☐ Do the administrators have opportunities to increase their skills through training?

After questions such as these are answered, then the technical controls can be reviewed with a detailed security test and evaluation plan. This plan should list the test objective, the test procedures, the expected results, and the actual results (when completed). From these combined processes, a baseline level of meaningful risk can be identified.

With such a baseline established, system owners and management need to reexamine each risk factor periodically. This should be accomplished every quarter to be effective. While this frequency looks onerous at first, when placed in the context of threats that attack vulnerabilities in nanoseconds, benefits of frequent reviews can be clearly shown. Baselining and subsequent tracking calls for an effective management process. Another requirement is a “many eyes” look; that is, the review should be performed by a team of security professionals, not merely by one person in a backroom somewhere. Management buy-in is required as well (as with any worthwhile project).

Each time the risks are reviewed (using the repeatable process outlined previously), management is able to determine not just where their IT system risks are, but also whether or not improvements in minimizing the risks have occurred. The information gathered also enables them to better deduce which risks they simply cannot accept or mitigate and, therefore, must transfer (e.g., via insurance or another mechanism). Over time, management and system owners can depend on their risk metrics to demonstrate their organization’s dedication to both strong technical controls and strong enterprise controls.

AN EXAMPLE

As stated previously, several models exist for measuring the application of security controls. The key is capturing the implementation over time. As an example, the authors chose to create a risk metric framework model using the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). In this example, three areas are examined: (1) system architecture, (2) network interfaces, and (3) system life cycle. In each area, metrics are created from the tables from Appendix Two of the DITSCAP documentation. This is merely an example; other metrics and areas of concern can be added to this model to make it more specific to a system’s needs.

For the system architecture area, the example model has five metrics. Each metric is assigned a weight value (the higher the weight value, the greater the importance of the metric); responses to the metric are obtained; and then a score is calculated, based on the responses provided. Table 1 demonstrates the process and the resulting information. (Note that while the weight
values are the opinion of the authors, they are considered valid. Each organization, however, can assign an “importance” value based on its own criteria, such as organization mission or other factors.)

Each percentage value is multiplied by the weight to arrive at a numeric value. Once the score is determined for each metric, these values are summed and then divided by the total possible score (in this case — 9; 6.03/9 = 67 percent). Thus it is determined that the system architecture score is a 67 percent.

For the other two scoring areas, the process is the same. Results are shown in Tables 2 and 3.

From these scores, a baseline can be established. Then, if each of these scores is measured over time, as shown in Table 4, progress can be charted.
Another pictorial view of the example is given in Figure 1.

**CONCLUSION**

The old approach to risk through review of technical point solutions does not work. A new solution is required; and, the new answer can use existing tools and frameworks. Using a security control compliance model to measure risk over time encourages improved security and, ultimately, will result in return on investment. This model of measuring risk over time allows executive management an opportunity to manage and control risks, making the difference between a business getting ahead or just getting by.

**Bibliography**

