SC Infosec Opinionwire

July 2003

Network & Security Technologies

A Balanced Approach to Performing a Security Assessment

by Adam Lipson

Fundamentally, there exist just two basic approaches to performing security assessments: vulnerability priority and asset priority.

While these two approaches will eventually (if taken to their ultimate conclusion) converge to the same result, it is rare for an organization to hold the line and make the investment required to follow the process to its finale. More commonly, IT and business managers will request a more cursory review to identify the 'low-hanging fruit' – those observations that represent the most egregious of security problems. In this real-world scenario, the selection of the assessment methodology becomes paramount, since it will greatly affect the types of problems identified.

The two approaches

The vulnerability priority security assessment probably represents the most common approach today. It certainly is the best recognized. The consultant assembles a list of well-known weaknesses in common security controls. While these can include both technical and procedural controls, the focus is usually on the former. In this case, the list is captured in the operational base of a computer security evaluation tool or suite of tools. The consultant acts as an expert operator of the vulnerability scanner.

Often the interpretation of the results is automated – if a particular security weakness is identified the tool provides descriptive text and standard recommendations for correcting the problem. These tools can be very effective at locating implementation or configuration flaws in technical security controls. Less well understood is the process for 'scanning' procedural security controls for flaws. In fact, few security firms offer a 'procedural vulnerability assessment' for just this reason.

The asset priority security assessment takes a wholly different tack. It starts with an inventory of information assets. The consultant will generally compare the inventory to a generic business model to ensure all assets are identified. (For example, every business must have a roster of employees, so this must be included in the inventory to make it complete.) The inventory assigns a value to each asset and determines how it is used throughout the organization – a sort of mapping of information flow. Once the asset inventory is complete, the consultants can begin their review of security controls. As with the vulnerability priority assessment, this process is seldom run to exhaustion. Rather, the consultants focus on the most sensitive or critical assets.

Combined methods

Many companies make the mistake of assessing risk by choosing only one of these two approaches. However, they are not mutually exclusive. Indeed, the higher value lies in a well-balanced combination of both asset priority and vulnerability priority methodologies.

The strength of the asset priority assessment is that the review doesn't have to end when the list of known weaknesses is completed. The consultant can determine the (written or tacit) policy for handling the information asset. Then, stepping through the information flow, the consultant will identify missing or weak controls that do not conform to the policy. These will include technology controls. But they will also include procedural controls often overlooked by the vulnerability priority assessment.

Conversely, the vulnerability priority assessment adopts the viewpoint of a particular class of attacker, for example, an internet-based hacker. In this way the consultant can quickly determine the probability that such an adversary will succeed. The approach narrows the scope of the assessment to expedite the identification of weakness. On the other hand, the asset priority assessment produces a more fundamental picture. Its strength lies in determining the adequacy of a security program for protecting the organization's most valuable assets from all perils.

The best approach combines both of these approaches for its various security assessment offerings. For example, a high value assessment includes vulnerability scanning as part of an ISO 17799 security assessment, but places greater emphasis on an asset priority methodology. This approach tracks well with the 10 domains specified in the ISO 17799 Security Standard while cost effectively providing your organization with a clear snapshot of your overall security posture.

Modeling to the industry

A sound approach begins with a survey of the 'critical' cyberassets of the company. The baseline business model should use tracks that have been identified during numerous other engagements with clients in the same industry. This model will differ from a generic business in that it should capture the unique qualities of the business. During the data-gathering phase of the assessment, consultants collect as much information as possible about the policies and procedures in use. Many of these are written, while others are often 'traditions' or 'collective wisdom' possessed by the operators and maintainers of the systems – rules that are not broken.

Once the inventory is created, you must compare the various security controls – both technical and procedural – to those found in other companies. Drawing on experience inside and outside the industry under review, you must evaluate the controls for sufficiency and cost-effectiveness. These include the procedures and people charged with the operation, maintenance and protection of the critical cyberassets. The controls span from the physical layer to the database, including network, system and application.

Critical to this process is having people who understand that the most 'cutting edge' technical control may not be appropriate for all applications. This is especially true for any industry where there exists decades-old equipment that is difficult or impossible to retrofit. Thus, for example, we recognize where a good

physical security procedure may supplant the need for a much more costly network intrusion detection system (IDS).

An effective ISO 17799 Security Assessment applies the asset priority methodology to identify gaps to the ISO 17799 standard. But, it does so in a rational manner. It supplements the asset priority methodology with vulnerability priority assessment techniques when they represent the most expedient manner of evaluating security controls. The final product will inform management of the most cost-effective method to both meet the requirements of regulators while properly protecting their valuable cyberassets that are key and critical to the profitability of their business.

Adam Lipson is president and CEO at Network and Security Technologies (www.netsectech.com), a provider of digital security consulting solutions.
