**1. Identify Assets**

Most IT security models have between five

and 10 steps, but they all start with the same

one: identify the asset or system. From that

point, you can identify the threat and its possible

impact, as well as develop a mitigation

plan. Unfortunately, this process usually occurs

at only two distinct points in time during the

system life cycle: first, as the system is

deployed in the organization, and, second, during

a predetermined interval based on regulations

or internal policy. The problem with this

is that the threat landscape is always changing.

New vulnerabilities and exploits are released

daily, and a single review of a system’s

threat profile every few years might not be

sufficient to keep that system and its data protected.

This is probably the most common problem

seen in the risk world, and it only highlights

the need for a continuous risk assessment

life cycle.

Data classification is one of the most critical,

and difficult-to-implement, steps in the asset

identification and classification process. The

most common mistake that companies make

is that they try to push classification from

upper management or IT security groups into

the business units. You can avoid this by

creating a data classification program that provides

structure and guidance, but places the

classification in the hands of the data owners.

They are the closest to the data and will likely

have the most insight into the impact a compromise

to that data would have on the overall

**2. Identify Threats**

The next crucial step is to use the data

discovered during your asset profile creation

to determine what threats may exist for any

given system. Here, it’s important to understand

how the notions of “threat” and “vulnerability”

connect. A threat (specifically in the IT

security world) is the potential for an attacker

to take advantage of a given vulnerability.

It is also important to understand the idea

of a threat source. Threat sources in IT security

usually fall into two broad categories: internal

and external.

You can think about the flow this way: threat

source (such as a hacker)→threat (such as

hacking into a server)→vulnerability (such as

SQL injection)→risk realized (such as the loss

of confidential data).

Based on the data from the profiles you have

built, you can identify certain specific threats to

your organization’s systems. The identification

of these threats usually involves the way in

which an attacker would likely interact with a system.

**3. Identify Vulnerabilities**

Identifying vulnerabilities is probably one of

the most challenging aspects of the IT security

risk assessment process. It is challenging

not because it is particularly hard to execute,

but because of how thorough the process

must be and how often it must be performed.

Many companies rely on automated tools

such as network scanners, application scanners

or remote agents to programmatically

crawl over the enterprise footprint and identify

vulnerabilities. This is certainly a great way

to rapidly identify vulnerabilities across the

organization, but it should not be relied on as

the sole method. There are many vulnerabilities

that can be detected only by human According to the Verizon Business 2012 Data

Breach Investigations Report, 97% of breaches

in 2011 were avoidable by using simple or

intermediate controls. This only underscores

the need for a comprehensive vulnerability

assessment program within the organization.

This includes looking to outside sources for

information on vulnerabilities. Indeed, in many

cases, vulnerabilities will be discovered by

third parties. Companies should have a proactive

review process in place to check for vulnerabilities

that would affect the organization,

as well as to coordinate the process by which

patches from vendors are deployed.

**4. Develop Metrics**

While IT security risk assessment can be a

complicated, and often subjective, exercise, at

some point organizations must get to the

point at which they can use a relatively simple

formula to assess their risk. In short, asset multiplied

by threat multiplied by vulnerability

equals risk (or A \* T \* V = R

**5. Calculate Cost**

Using the impact severity matrix, we can

establish a certain risk and apply that to the

cost factors previously discussed. Let’s take

SQL injection, for example. Since we know

that SQL injection in most cases is levied

against Web interfaces with database back

ends, we can apply this risk formula to a system

identified as a Web application and a

database.

If we have 1,000 records of sensitive data in

our database, and a SQL injection vulnerability

exists, we can conclude that our financial

risk might be as follows:

If we determine that the threat likelihood is

medium (0.5) and that the threat impact is

high (1), and if we have 1,000 records and that

the cost per record is $194, then:

(0.5 \* 1) \* ($194 \* 1,000) = current monetary

risk

In this case, the current monetary risk would

be $97,000.

While this method does make a number of

assumptions, this figure can be used to

compare cost of risk mitigation with cost of

risk realization — information that can then

be shared with management in order to,

among other things, secure funding for security

protections. For example, it may cost

$5,000 to pay a developer to close the SQL Injection

vulnerability. When compared with the

potential loss of $97,000, the $5,000 looks

more than reasonable. (Dollar signs have a

much more profound meaning to executive

management than an arbitrary risk rating.)