How to Conduct an Effective IT Security Risk Assessment

Assessing an organization’s security risk is an important element of an effective enterprise security strategy. It’s also a key way to justify future security spending to upper management. In this Dark Reading report, we recommend how to conduct an IT security risk assessment — and how to translate the results into terms that make sense in dollars.

By Brad Causey
How To Conduct An Effective IT Security Risk Assessment

3 Author’s Bio
4 Executive Summary
5 Conducting An Effective IT Security Risk Assessment
5 Figure 1: Threat Matrix
6 1. Identify Assets
6 Figure 2: Components of Risk Management
7 2. Identify Threats
8 3. Identify Vulnerabilities
8 Figure 3: Analysis of Malicious or Criminal Attacks in 2011
9 4. Develop Metrics
9 Figure 4: New Threat Flow Model
10 5. Consider Historical Breach Data
10 6. Calculate Cost
11 7. Perform Fluid Risk-To-Asset Tracking
12 Related Reports

ABOUT US

*InformationWeek Reports*’ analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience. To contact us, write to managing director *Art Wittmann* at art.wittmann@ubm.com, content director *Lorna Garey* at lorna.garey@ubm.com and research managing editor *Heather Vallis* at heather.vallis@ubm.com. Find all of our reports at reports.informationweek.com.
Brad Causey is an active member of the security and forensics community worldwide. Brad focuses his time on Web application security as it applies to global and enterprise arenas. He is a member of the OWASP Global Projects Committee and president of the International Information Systems Forensics Association chapter in Alabama. Brad is an avid author and writer, with hundreds of publications and several books to his name. Brad also holds dozens of industry-recognized certificates, including CISSP, MCSE, C|EH, CIFI and CGSP.
Assessing an organization’s security risk is a key element of an effective enterprise security strategy. Such assessments can mitigate the impact of a security breach or, more to the point, prevent such a breach from happening in the first place. Done well and used correctly, an IT security assessment can also be an invaluable tool for justifying future security spending. The CEO and other business executives may not understand the technical underpinnings of vulnerabilities, hacks and the security tools used to keep organizations safe, but they will understand the dollars and cents involved when systems, networks and data are compromised.

In this special report, Dark Reading offers an in-depth look at the risk assessment process, the potential means and practices for conducting an audit, and the strengths and pitfalls surrounding a security risk assessment. We also offer some insight into how to measure and convey risk parameters so that they can be understood and used by upper management.
Many security and compliance projects begin with a simple idea: assess the organization’s risk of vulnerabilities and breaches. Indeed, implementing an IT security risk assessment is absolutely critical to the overall security posture of your organization. An effective security risk assessment can prevent breaches, reduce the impact of realized breaches and keep your company’s name from appearing in the spotlight for all the wrong reasons. Regular IT security risk assessments also enable organizations to build up a cache of historical data that can be used to effectively gauge and communicate monetary impact related to risks — and, hopefully, convince upper management to take decisive action to reduce the organization’s threat surface.

It’s important to note that not every IT security risk assessment is alike — or even remotely close. Indeed, there are many ways to perform IT security risk assessments, and the results may vary widely depending on the method used. It should also be noted that performing a risk assessment is a very small part of the overall risk management process.

There are basically three risk management components:

1. Evaluation and assessment, to identify assets and evaluate their properties and characteristics.
2. Risk assessment, to discover threats and vulnerabilities that pose risk to assets.
3. Risk mitigation, to address risk by transferring, eliminating or accepting it.

The presence of these three high-level processes is constant in all risk assessment methodologies, although what they are called may vary. Our primary focus in this report is to discuss the assessment itself, but we will also touch on key elements of risk evaluation and assessment, as well as risk mitigation.

Traditional risk assessment includes general

### Threat Matrix

Breaking down complicated assessment data into simple formulas can help quantify potential risk and the resources needed to mitigate that risk.

<table>
<thead>
<tr>
<th>Impact severity</th>
<th>Impact Low – 0.1</th>
<th>Impact Medium – 0.5</th>
<th>Impact High – 1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood of risk realization</td>
<td>0.1</td>
<td>0.5</td>
<td>1.0</td>
</tr>
<tr>
<td>Likelihood High – 1.0</td>
<td>0.1</td>
<td>0.5</td>
<td>1.0</td>
</tr>
<tr>
<td>Likelihood Medium – 0.5</td>
<td>0.05</td>
<td>0.25</td>
<td>0.5</td>
</tr>
<tr>
<td>Likelihood Low – 0.1</td>
<td>0.01</td>
<td>0.05</td>
<td>0.1</td>
</tr>
</tbody>
</table>

Source: InformationWeek Reports
IT-related issues such as accidental outages, hardware failures and uptime. Security risk assessment, on the other hand, is just what it sounds like — analysis of the issues relating directly to security threats. However, many organizations lump these two types of assessments together, applying more generic risk models in the more dynamic world of IT security. That’s a problem.

In many cases, the data compiled about a given asset and its risk is created with great care, but is not updated in a timeframe that would enable security pros to address the changing threat landscape. This leads to Band-Aid-style fixes such as hard reassessment intervals every one or two years. Ultimately, this will leave gaps in security for months at a time.

Following are the steps required to perform an effective IT security risk assessment.

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 security posture of the organization.
Data classification is just one aspect of the overall asset classification, however. You will need to have a reasonable understanding of the technologies that a given asset would utilize and what possible vulnerabilities exist for those technologies.

Take a basic Web application, for example. Most enterprise Web applications are built on a framework such as Ruby on Rails or Microsoft Silverlight. These frameworks should be part of the asset’s risk profile. Since most Web applications also utilize database back ends, databases also should be included. Other factors, such as access vectors (is it exposed to the Internet or just internally accessible?) and existing protections, should be considered. Implementing a well-configured Web application firewall, or WAF, can significantly affect the risk profile of an asset and should be included in its profile development.

It is obviously much easier to gather this information when an asset is being deployed within the organization, but retroactive review of existing assets will surely be required. Once you have created a profile that details an asset’s threat portfolio (including the classification of the data therein), you can create an asset “value.” This value is used in combination with threat and vulnerability information to establish an overall risk rating.

An easy way to do this is to use a 1-to-100-point scale based on data classification. This scale will allow you to quickly determine an asset’s importance as it relates to risk. (To make things less complicated, you can change the point range to whatever works for your organization.) Be sure to include any control analysis in your point-scale evaluation. The basic idea behind control analysis is taking into consideration the existing mitigating factors surrounding the risk you have identified on a particular asset. As an example, a risk might be a HIPAA violation, but an existing mitigating factor of policy adherence or complex passwords may be a control that already mitigates that risk. Control analysis should take into consideration items such as multifactor authentication or firewalls that may help improve the security posture of the asset for which you are building your profile.

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. In our Web application example, customer data would be at risk of Web- and database-based attacks. Access to that customer data would be a threat; a vulnerability (SQL injection) combined with a threat source (hacker) would be a realization of that threat.

One important aspect to threat identification is the impact that a realized threat may have on the CIA triad: confidentiality, integrity, and availability. Each of these three pillars is extremely important when placing importance on a given threat. For example, if your data must be available at all times, then a website defacement or distributed denial-of-service attack would be a significant threat. However, a DDoS attack doesn’t typically affect the integrity or confidentiality of data, so that risk might be negligible.

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
interaction or manual review.

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).

Let's look at the example of the website

Figure 4

New Threat Flow Model

By organizing your risk management responses by threats, you can more easily formulate metrics and mitigation.

Source: InformationWeek Reports
hosting sensitive personal information, and say we assigned it an asset value of 90 (on a scale from 1 to 100) from a risk impact perspective. Using the table in Figure 1, we can determine the risk to this asset.

If we consider the threat to have a medium likelihood with a high impact, the risk would have a 0.25 rating.

When a vulnerability exists in the wild for this threat, we would rate it as well. Let’s give it a 1.0, or high rating.

\[
\text{Asset (90) } \times \text{ threat (0.25) } \times \text{ vulnerability (1)} = \text{ risk rating (22.5)}
\]

This metric has immense value to security, audit and risk teams because it allows for a consistent scale that gauges the mathematical risk of a given vulnerability as it is applied to an asset. However, the number 22.5 might not mean much to upper management. So you will have to take it a step further.

(Hint: Money talks, which we will discuss later in the report.)

5. Consider Historical Breach Data

We have all seen those headlines regarding massive breaches and huge losses of data. Although the current risk assessment process is effective, we spend a lot of time and effort in the IT security arena addressing risk that may never be realized. While this is the nature of the game, so to speak, it is not always ideal from the IT security perspective.

It can be extremely useful to take the lessons regarding cost and impact from past breaches at other organizations and apply that to your risk formulas. Fortunately (and unfortunately) there is no shortage of examples here.

According to PricewaterhouseCoopers’ 2012 Information Security Breaches Survey, 70% of large companies were attacked in 2011. When that information is combined with the average cost per breach of $5.5 million and average cost per compromised record of $194 (according to Symantec), things can get a little costly — and scary.

Although we cannot know all of the details associated with the breaches in question, you can apply the cost values to risk metrics. This should give you an idea of what your costs would be, should a similar breach occur in your own organization.

Based on the data from Symantec’s annual Cost of a Data Breach study, we can identify that viruses and SQL injection are obvious candidates for a technology solution and could be easily applied to most organizational risk plans. Technology solutions are easy to implement because they involve a very specific implantation of a given technology and allow for a more simple cost analysis. An example of a technology solution would be a programming fix for an application flaw or the installation of a Web application firewall to protect from Web threats.

6. 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 backends, 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:

\[(0.5 \times 1) \times ($194 \times 1,000) = \text{current monetary risk}\]

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.)

### 7. Perform Fluid Risk-To-Asset Tracking

Security risk assessment must remain fluid, continuing to take into account the ever-changing threat landscape. One way of doing this is to use a method of tracking threats called fluid risk-to-asset tracking. This is counter to the traditional method of assigning threats to assets, but the model helps security managers assess the constant change of threats in the wild.

Let’s take a closer look at how this might work.

First of all, rather than asking the question, “I have an asset — what are the threats?” you need to ask, “There is a new threat — what assets does that threat create risk for?”

In most cases, the assets will change less than the threats do. Once you have gone through the process of establishing the profile of an asset, that part of the work is done, and that asset can be placed into a “risk category.” Doing this will allow you to base your risk portfolio on real, existing threats, and to update this information easily as new threats emerge.

Continuing with our SQL injection example, let’s look at how we could use this methodology.

Let’s say that a popular Web framework is found to be vulnerable to SQL injection. Since we have classified our Web asset as being in the two threat categories, database and Web, we can quickly identify that this new vulnerability may pose a risk to assets that are classified as both Web and database threat categories.

Once we make the determination that the vulnerability does in fact exist on our system, we can immediately apply our monetary risk formula and metrics to determine what our exposure is based on that new vulnerability.

There are a number of different ways to implement this, but the important thing is to
Want More Like This?

*InformationWeek* creates more than 150 reports like this each year, and they’re all free to registered users. We’ll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you’ll find:

**Avoid Risky Business by Analyzing Threats:** Risk management is all the rage for handling security today, but it’s a practice fraught with misconceptions and challenges. In this special retrospective of recent news coverage, *Dark Reading* takes a look at best practices, new technologies such as whitelisting, common missteps — and the added risks associated with the cloud and mobile devices coming in and out of the enterprise.

**A Security Pro’s Guide to GRC:** Organizations challenged by meeting the requirements of multiple regulatory mandates are increasingly looking at the alignment of governance, risk and compliance under a unified framework, GRC. In this report, we examine where the security professionals figure into the mix and recommend the steps organizations should take to align IT GRC with existing security programs and processes.

**Measuring Risk: A Security Pro’s Guide:** One of the biggest challenges facing IT today is risk assessment, a task that is increasing in importance and complexity as IT systems expand across organizations. Risk measurement and impact assessment are not exact sciences, but there are tools, processes and principles that can be leveraged to ensure that organizations are well-protected and that senior management is well-informed. In this report, we recommend tools for evaluating security risks and provide some ideas for effectively putting the resulting data into business context.

**PLUS:** Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek 500* and the annual State of Security report; full issues; and much more.