

Risk Assessment Tools: A Primer

By Tari Schreider

Performing a risk analysis, either at the logical or physical level in and around the information technology (IT) enterprise, is a complex and often confusing endeavor. Arriving at an accurate risk profile is equally difficult, but needed to identify one's risk and subsequently manage or mitigate the threats and vulnerabilities that create the risk. However, the process of identifying, quantifying and associating risk to assets falls just short of rocket science for most people. There is an art (and science) to performing risk assessments, which may explain why so few organizations conduct them well, or at all. However, calculating risk is no different from programming an application to perform a prescribed function. Also, using incorrect threat and vulnerability assumptions to determine one's risk profile and posture can be costly in terms of money and lives.

The results of a risk assessment will never exceed the quality of the data used as input to the process. Programmers understand the concept of garbage in, garbage out (GIGO) and this universal truth applies to risk management equally, if not more. There are, however, software products that provide a methodology and structure to the entire risk analysis process. This article looks at these tools, creates a framework of understanding and provides insight into the world of automated risk analysis.

To understand how a risk assessment tool can assist in the process of identifying and quantifying risk, it is important to first understand what a risk analysis is. It simply is the process of identifying the potential for possible harm to occur to a particular set of assets or processes and determining the impact. There are, of course, varying degrees of risk analysis, with each providing differing views of an organization's risk posture.

The two primary types of risk analysis processes are:

- **Qualitative**—A simplified process of identifying the major threats to which an enterprise is exposed. For example, if one's IT enterprise is located within "tornado alley," there is an implied threat of a tornado occurring that could subsequently cause an impact to assets or processes. Further, if the assets or processes are located in a hardened facility, then the actual vulnerability to the threat of a tornado could be mitigated or dramatically reduced. Basically, one must qualify which risks are worth protecting against. This process is more intuitive and generally can be accomplished in an abbreviated fashion by answering three basic questions:

- 1) What could happen?
- 2) How likely is it to occur?
- 3) What is the impact?

Qualitative answers to one or more of these questions usual-

ly can provide sufficient information to allocate resources and dollars to protect an enterprise's assets or processes. More complex enterprises or those with limited budgets require a more advanced form of risk analysis.

- **Quantitative**—Today's risk management requires a direct correlation to the value of the assets that require protection. Organizations increasingly want to know what the cost/benefit is to protecting an asset or process. CFOs also want to know what the return on investment (ROI) is for investing in risk reduction/mitigation strategies. To find this information, an advanced risk analysis technique, known as a quantitative approach, is used to provide statistical insight to risk prediction and impact. This method requires that one establish a monetary value for the assets and processes, estimate the probability of a threat occurring, and determine the ROI for implementing safeguards to reduce the impact caused by that threat occurring.

Using the previous example of an enterprise's location in tornado alley, one would examine the threat further by researching the threat frequency to determine the probability of occurrence. So qualitatively one knows that an asset is worth US \$1 million and that a tornado could occur at some point in the future. Now quantitatively it is determined through research that tornadoes only occur once every two years within the enterprise's proximal risk zone.¹ This yields an annualized frequency expectancy (AFE) of .5. Additionally, because the asset is located in a hardened facility, the impact of a tornado would be less than 100 percent. For this example, a 20 percent loss will be assumed. Qualitatively and quantitatively, all the necessary data are available to produce a credible risk assessment statement.

The results would be expressed in the following manner:

| (X) Asset Value: | Threat: | (Y) Single Expectancy (SLE): | Frequency Occurrence: | (Z) Annual Rate of Occurrence: | Annual Expectancy (ALE): |
|------------------|---------|------------------------------|-----------------------|--------------------------------|--------------------------|
| US \$1 million | Tornado | 20% or US \$200,000 | Once every two years | 0.5 | US \$100,000 |

The calculation would look like this:

$$(X) \$1,000,000 \times (Y) 20\% = \$200,000 \times (Z) .5 = \$100,000$$

The importance of the quantitative portion of the risk assessment is in knowing that the potential for loss is US \$100,000 versus US \$1 million. The concept is based on the precept that no asset faces 100 percent risk, 100 percent of the time. Adding the quantitative component to a qualitative risk assessment ensures that the safeguards deployed are commensurate with the value of assets or processes at risk.

Risk Assessment Tools

The risk assessment tools market is relatively small and is comprised of approximately a dozen companies, of which seven (see **table 1**) appear to garner the majority of the market share. These tools range in cost from as little as a few hundred US dollars to more than US \$25,000. The total number of risk assessment tools in active use today is less than 12,000 worldwide.

Table 1—Risk Analysis Tools

| Product | Company | Focus |
|------------------|---|--|
| CRAMM | Insight Consulting Ltd. www.insight.co.uk/cramm/ | Government, Public Sector |
| CORA | International Security Technology Inc. www.ist-usa.com | Telecom, Logistics, Government, IT |
| COBRA | C&A Systems Security Ltd. www.security-risk-analysis.com | Enterprise |
| Risk Check | Norman Security Solutions www.norman.com | Enterprise |
| RiskPAC | CSCI Inc. www.csciweb.com | Business Continuity |
| RiskWatch | RiskWatch, Inc. www.riskwatch.com | HIPAA, DITSCAP, NIACAP |
| The Buddy System | Alion Science & Technology Inc. www.buddysystem.net | IT |

The companies that provide these products are relatively small with most having fewer than 20 employees. This is a boutique industry where the companies generally are headed by an acknowledged expert in the field of risk management and have been in business for 10 years or more. The 2003 worldwide revenue for risk management software tools that specifically address the IT community is projected at US \$35 million.

These products are more widely accepted in Europe. However, as a result of the US Health Insurance Portability and Accountability Act (HIPAA) and the events of 11 September 2001, they are growing in acceptance throughout the US. All the companies within this industry primarily distribute their products through distributors and/or consulting organizations.

Risk Analysis Functions

All of the tools perform the same basic functions; however, they perform these functions differently. Each product is questionnaire-based and requires the user to answer myriad questions about their organization, technology, environment, geography, asset value, etc. In some cases, there are more than 500 individual questions that must be answered to produce a risk profile. The more sophisticated products also allow one to import or link to data from penetration tests, intelligence reports or other risk-gathering formats. Questionnaires also can be allocated across numerous external locations with the results rolled into a composite risk profile.

The next major function of these products is to perform calculations to determine risk probability and ultimately rank risks by their level of importance. The ability for a risk assess-

ment tool to calculate loss estimates, such as ALE, and financial metrics, such as cost of risk mitigation and ROI, is an indication of its comprehensiveness. Risk analysis tools need to be able to measure the potential for loss that a threat could have on an organization. Not all of the products noted provide ROI modules as this is a relatively recent development in the science of risk management.

Each product adheres to one or more of the industry accepted risk standards, BS7799, ISO, DOD, HIPAA, etc., for identifying risks and suggesting safeguards. In fact, many of these products sell versions or templates to address specific risk areas, such as HIPAA, the Gramm-Leach-Bliley Act, etc. It is best to evaluate which product most closely aligns to each organization's risk management philosophy.

These products also have extensive databases of threats and vulnerabilities that are aligned to occurrence probability estimates. This significantly reduces the amount of time required to research baselines for ALE calculations. Safeguard databases also are provided to map to the identified vulnerabilities. One must be careful to recognize that not all of these will provide sufficient information to make an informed decision on selecting an appropriate risk mitigation strategy.

Additionally, many of these products have been written by software programmers, as opposed to risk experts, and their quality of recommendations in safeguards, threats and vulnerabilities sometimes reflects a sophomoric approach to sophisticated risk management. One also must be careful that the product selected is more than just an automated checklist of regulations.

Reporting is an area that separates these products in their approach to providing a customized method for presenting a risk profile. While some provide comprehensive charts and graphs, others provide limited "canned" reporting. When evaluating these types of products it is best to consider how the data are presented once the analysis has been completed. While most of these products offer impressive graphic user interface (GUI) front ends, getting the data out in a usable format can be difficult at best.

Although most of these products are quite difficult to use without two to three days of training from the vendor or distributor, they can offer a substantial savings in time and resources when performing an enterprise-level risk analysis. It is important to select a product that uses industry-accepted ALE calculations, as opposed to proprietary models that are not as easily understood. And one also must understand that the end product of the risk analysis will be commensurate with the quality of the input and accuracy of the answers to the questionnaires.

Conclusion

Organizations with a serious commitment to an infosec program should have one of these products incorporated within their risk management methodology to facilitate a uniform approach to identifying, reducing and managing risk. The time savings in baseline ALE calculations easily can justify the cost of one of these products alone. However, one must remember that these products have their limitations and cannot replace sound risk management judgment or experience.

Endnote

¹ An area in circular radius to an enterprise's location where threats could occur.

Tari Schreider

is the practice director for security solutions at Extreme Logic Inc. in Atlanta, Georgia, USA. He is responsible for the development of highly secure and sustainable applications and infrastructure. Prior to joining Extreme Logic, Schreider was

the vice president of global service delivery at Internet Security Systems Inc. In that role, he was responsible for an international presence of seven security operations centers. He also spent several years with the Sprint Corporation as its practice principal for disaster recovery and security. He has appeared on CNN, NBC, ABC and CBS and is the author of *The Encyclopedia of Risk Disaster Recovery, Security, & Risk Management* as well as numerous articles and white papers on the subject of risk management.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. Information Systems Control Journal does not attest to the originality of authors' content.

© Copyright 2003 by Information Systems Audit and Control Association Inc., formerly the EDP Auditors Association. All rights reserved. ISCA™ Information Systems Control Association™

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the Information Systems Audit and Control Association Inc., for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org