Risk Assessment as a Business Process

Caroline Ramsey-Hamilton

Security Risk assessments are widely understood to be the cornerstone (or even the foundation) of any security program. The risk assessment is a classic process, originally developed by the Defense Department, to not only assess the risk of SOMETHING – a process, a facility a data center, a system; but to also detail cost effective solutions to whatever problems are uncovered and rank those potential solutions by Return On Investment.

Here's a definition of a risk assessment: ***A process to determine what controls are necessary to protect sensitive or critical assets both adequately and cost-effectively.*** Cost effectiveness and Return On Investment (ROI) are required elements of a risk assessment.

It is NOT a site survey. It is NOT a vulnerability scan. It is not a democratic process where the most popular answer wins. It is not consensus driven. Instead, it is a business process that manages a security function. Security is very process centered. Because security often consists of many different elements which are critically important, such as managing network access, it makes sense to manage it as a process.

According to the statistics, risk assessments are way up in popularity in 2009. Maybe it's economics – maybe it's the general unrest with the economic downturn, but the requirements for risk assessments have never been broader or there have never been more of them than there are now. Here's a partial list:

ISO 27001
HIPAA
Joint Commission
NIST 800-66
FFIEC – Authentication
Bank Secrecy Act (BSA)
NIST 800-53A
FISMA
Red Flags Identity Theft
NCUA 748
NERC (North American Electric Reliability Council)
FERC (Federal Energy Regulatory Commission)
OSHA 3148
FEMA 426
FEMA 428

In the current environment, many security professionals are becoming intimidated by risk assessments? Is it because they seem overwhelming with their arrays of lists and categories? (At last count – I categorized over 1.572 million combinations of the 44 asset categories, 58 threat categories, 55 vulnerability categories, 7 loss categories and 160 control categories)!

Part of the trepidation of managers tasked with a risk assessment is that they are anxious about making key assumptions and assigning importance to different areas of the business or agency. Of course, part of this is partly political – the risk analyst has the power to build up the importance of one part of an organization and reduce the stature of another – or negatively or positively effect the budget!

In practice, however, it seems like the exercise of doing a risk assessment affords a level of protection which is related to how many other people actually contribute to the risk

assessment results. Using the compliance survey as a participatory measure takes the onus of absolute responsibility away from the manager and distributes it throughout the organization where it belongs.

At a time when a recent survey shows insider theft on the increase – it is even more important to do quarterly risk assessments. According to a new McAfee study, laid-off employees are the biggest IT security threat created by the economic recession. The same study warned that cybercrime could cost businesses worldwide more than $1 trillion.

The study surveyed 1,000 IT decision makers from 800 companies in eight countries. The study says that laid-off employees may steal intellectual property from their former employer in order to sell the information, improve their chances of getting hired with a competitor, or start a company of their own. In addition, acquisitions can leave IT workers unsure of how to report security problems or who to report them to. Finally, workers who are unsure about their job security and the job security of their colleagues may be more hesitant to report security problems. Ignoring these problems can be costly. McAfee CEO Dave DeWalt says companies lose an average of $4.6 million in intellectual property during a security breach and have to spend about $600,000 to correct the problem.

"We don't have the good risk models and as a result people are taking risks," says Purdue University computer science professor and study contributor Dr. Eugene Spafford. He says the frequency of security breaches will increase as a result of the recession as companies try to cope by cutting their information security expenses.

Obviously people are a critical component of information security. In a risk assessment, people are also critical because they are able to report what's going on in their workplace every day. How can one analyst know enough to do the entire risk assessment by themselves? They would have to be everywhere at once – in the morning, late at night, on the weekends, and also be able to channel the work of everyone from the newest tech

support person to the director of the data center. And the inclusion of a variety of individuals adds weight and power to the risk assessment.

No one would think of using a paper questionnaire any more. Paper surveys are laborious and difficult to aggregate, automated questionnaires now exist which allow risk analysts to interview users electronically. Survey questions start with a Control Standard which outline the official policy of the organization. Questions should be set up to validate compliance against published policies, guidelines and directives. There is little point to asking questions unrelated to requirements, because the organization would find it difficult to enforce compliance if it was not a requirement.

The risk analysis manager is the analyst in charge. However, there may be other individuals in the organization who can make major contributions. According to the audit guidelines for risk assessment, the more people you interview, the more likely you are to find a vulnerability. Individuals should not be asked to answer more than 50 questions, which are directly related to their job. For example, a network user might answer questions related to whether they use their passwords, whether they log off their terminals when they leave their station, or whether they have attended basic data security training. A database administrator will answer a few general questions, but also more specific questions related to their job. A facilities manager may get questions about the site, the disaster recovery plan, and the physical access control.

Employees may initially be nervous when they are asked to answer questions related to how they perform their jobs. It is important to make sure that these individuals understand that the risk assessment is a scientific process, and that any data gathered in the risk assessment will be seen by only one individual (the risk analysis manager), and that their comments will not be reviewed by their supervisor, nor will they end up in their personnel file.

Random surveys are often used to predict election results, from local precincts in a particular city, to federal elections, where the network news teams are able to predict

the final results from a profile of only a few key states. In these examples, random samples are usually less than 1%. In a risk assessment, a random sample is not desirable. Instead, the objective should be to question as many people as possible. The more individuals you question, the better the chances that you will discover a vulnerability.

The true value of the risk assessment is in the cost benefit analysis, which details what controls need to be implemented, how much they cost and how much they would protect the organization by either prevent threats from occurring or by mitigating the impact of the incident if it occurs.

The cost benefit analysis combines information from the vulnerability assessment along with relevant threat data and asset information such as present day replacement values, criticality, integrity and availability of the information contained in the system under review, as well as how completely safeguards are currently being implemented.

While the analysts may be accountable for the reporting or analysis of potential risk, the responsibility for any action that needs to be taken is up at the C level, or with the Board of Directors. In fact, in the FFIEC IT (Federal Financial Institutions Examination Council Information Technology)Handbook, they spell out, "The Board is responsible for holding senior management accountable". Often we have found that the actual President of a bank or credit union doesn't always KNOW that he is going to be held responsible – this information is down another level in the organization.

The analyst should not be afraid of making assumptions in the risk assessment; auditors make assumptions all the time. One could say that the world runs on assumptions. So making an assumption about how long it would take to replace the personnel or web applications of a specific part of the organization is not too difficult. Always remember that each component of the risk assessment can be vetted before with relevant management so that senior management does take the responsibility for validating the choices the analyst makes.

I advocate getting management to sign off, in writing, on the assumptions they accept, in the course of completing the risk assessment – and of course, on the final reports. Areas where senior management can review and approve include:

- Calculation of asset values, including the value of the organization in total
- The potential costs of implementing different controls, singly or in combination.
- Validating which controls are currently in place and how well they are working.
- The conclusions from the draft report, and the final report.

The analyst is just the messenger, doing the work of assembling the risk elements and calculating their potential results. But senior management makes the final decisions on each element. There's nothing like a signature on a piece of paper to foster a climate of accountability**.**

No wonder that in a recent survey done by the Aberdeen Group in February 2008, after gathering responses from more than 800 global organizations, **42% of those surveys said they needed more help with risk assessment and management,** compared with 34% who wanted an automated process for identifying, measuring, and monitoring operational risk and 32% who needed assistance in aligning IT Policy, risk, operations management with business initiatives.
Risk Assessment is a business process that elevates the security function from widget-management to a true corporate management role. It allows the organization to use the critical security elements to increase the value of the entire corporation.

Information about the author:

Caroline Ramsey Hamilton is a risk assessment expert and futurist, building risk models to solve complex problems. Hamilton served on the NIST Model-Builder's Workshop on Risk Management and the National Security Agency's Network Rating Workshop. In addition, she was a member of the U.S. Department of Defense's Defensive Information Warfare Risk Management Model and has worked on a variety of risk assessment and risk management groups, including the ASIS Information Technology Security Council and the IBM Data Governance Council, created by Steven Adler.

Hamilton also received the Maritime Security Council's Distinguished Service Award and the Anti-Terrorism Certification Board Lifetime Achievement Award in 2011.

She currently works with some of the world's largest hospitals, government agencies and corporations to create better ways of performing fast and accurate risk assessments for both information security and physical security, including workplace violence.

Currently based in South Florida and south Lake Tahoe, California, Ramsey- Hamilton is a graduate of the University of California and is certified as an Expert in Anti-Terrorism and Homeland Security.