Integrating IT Security Risk Metrics

Into an Enterprise Risk Management Program

By Mark Moore

Two of the hottest topics over the past year in the information security arena have been governance, risk and compliance (GRC) management and security metrics. These concepts will likely continue to gain momentum in 2009, especially in financial service companies. Events over the past year, specifically the "mortgage crisis" and ultimately the collapse of several of the largest financial institutions on the globe, have demonstrated the effect improperly managed risk in one business unit can have on the entire organization. To prevent the same scenario from occurring again, leading financial service institutions (FSIs) will be strengthening their enterprise risk management programs. In many instances, these efforts will include integrating information security and privacy risk into the overall risk management profile.

Know the Enemy

At the core of a functional enterprise risk management (ERM) program is the risk analysis process. Risk analysis is the identification of risks to which an organization is exposed and the assessment of the potential impact of those risks on the organization. In most ERM models, risk analysis is used to develop the organization's risk profile. Its purpose is to inform business decision makers by identifying and measuring the risks associated with different courses of action. Common risk analysis techniques include sensitivity analysis, probability analysis, simulation, and modeling. The key to successful ERM is the analysis of risk before business and investment decisions are made. This is true regardless of a firm's risk appetite. A firm's risk appetite is based on the amount of risk they are willing to accept, which requires risk analysis to make informed decisions.

Metrics is the term most commonly associated with the data used in the risk analysis process. A "metric" is simply a measurement against a standard. In some scenarios, metrics have been developed into highly effective predictors of risk. For example, actuary tables have been used in the insurance industry for decades to calculate the premiums for policies. These tables have been developed through statistical analysis of centuries of empirical data, and hence are the "standard" that the insured is measured against. Actuary tables are an example of quantitative metrics which are typically represented as a numeric value. For this reason, quantitative metrics are preferred in ERM programs, as numeric values can be integrated into complex equations to calculate an overall risk value.

The second form of metrics commonly used in risk analysis is qualitative metrics. Qualitative metrics present the characteristics of the standard being measured in a descriptive manner, such as "high", "medium", and "low". This is the type of metrics frequently used to present the findings of a technical risk assessment. While subjective in nature, qualitative metrics are still very valuable to the risk management process.

So how does any of this help IT risk management and security integrate with an ERM program? Detailed empirical data on IT security is more difficult to obtain for risk calculations as compared to actuarial tables used by the insurance industry. New threats and vulnerabilities appear daily. Furthermore, technology evolves at such a rapid pace that what works to manage risk effectively today may be obsolete tomorrow. And exactly what

Continued on page 9

Continued from page 8

standard is the correct one to develop metrics against? The financial industry is already heavily regulated, with compliance to Sarbanes Oxley, the Graham Leach Bliley Act, and the Payment Card Industry Data Security Standard measured annually. FSIs spend millions of dollars annually on technology and resources to maintain compliance with these regulations. Doesn't that demonstrate that risk is being managed effectively?

Debunking the Myths

Unfortunately, the answer is no. While most FSIs have state-of-the-art technology to manage their IT risk compliance and security operations, the data collected is typically not suitable for integration into an ERM program. There is value in knowing that the current environment is compliant with the general "best practice" security definitions as described by regulators; and that virus signatures are up to date on 87% of the servers; and an average of 1125 ping sweeps occurs every week. But none of these data points is sufficient to provide "predictive" metrics in an ERM program. To get with their firm's ERM program, IT risk management and security must first debunk two long-standing myths about information risk.

The first myth is that all IT risk can be defined in technology-centric terms. For decades, IT risk management and compliance, along with the IT security teams, have focused their efforts on testing the current configurations of servers, networks and other technology assets to find the latest vulnerabilities. The common belief being that if these assets are safe, then risk is being managed effectively. While these efforts are critical, information risk management and security efforts cannot stop at the technology. The "assets" that are key to the ERM program are the data and services provided by technology to support business processes. Risk must be defined in terms of these assets so as to be understood and used effectively by business decision makers.

Fortunately for most FSIs, overcoming this myth will not require significant investment in technology or resources. As stated earlier, nearly all large FSIs have invested in advanced technology to manage their compliance and security programs. These systems contain vast amounts of data that, aligned appropriately, can form the basis for true predictive metrics.

Easy as 1-2-3

Developing program metrics for an enterprise risk management effort can be accomplished in three steps:

Step 1: Ask what the ERM program needs to know. While this seems simple, it is often overlooked and results in too little or too much information being provided. Once the types, format, and frequency of metrics required by the ERM program are understood and documented, it will be much easier to know how to collect / derive the remaining data.

Step 2: Classify or characterize your technology assets to align with business processes and functions. It is recommended to start with business process definitions and mapping data, people, and technology to the processes. Starting with data or technology first becomes a "boil the ocean" exercise that has failed at nearly every large organization. A business process-based classification will allow for correct identification of critical risk metrics that can be quantified for reporting to the ERM program.

Step 3: Share. It is often the case that IT risk management is a function of a compliance or internal audit group, and information security is a function of IT. While there are reasons for separation to maintain independence, remember that the overall goal is to effectively manage risk. Combining compliance data with operational data will go a long way to creating viable ERM program metrics. However, there is another part of the organization that has a stake in effective risk management: business management. Involvement of the business units to understand how data and services are prioritized in their respective business processes will be vital in developing the standards for ERM metrics.

The second myth that has to be addressed it the belief that information risk can be effectively managed using a "test and fix" methodology. "Test and Fix" assumes risk can only be addressed through technology. Furthermore, risk cannot be identified until some audit or "test" is performed, and findings are presented. Once the "test" has occurred, the "fix" phase of the methodology is initiated to address the findings. The "fix" efforts continue until all issues are addressed or the next "test" cycle happens.

Continued on page 12

Integrating IT Security Risk Metrics Into an Enterprise Risk Management Program

Continued from page 9

This approach is neither predictive nor preventative, yet it is the most common approach today for managing IT risk. To make matters worse, multiple annual regulatory requirements create a permanent test cycle with duplicate and redundant findings. Compliance initiatives are undertaken in a stovepipe manner resulting in enormous resource costs.

Finally, Analyze Before Action

To be effective, risk analyses must occur before business decisions are made. Failing to provide the necessary information risk metrics into the organization's ERM program prevents those decisions from being made with the best data, puts the company at higher risk that cannot be mitigated, and costs millions every year.

Mark Moore is a Director of Risk Management at Acumen Solutions, a business and technology consulting firm with offices in the U.S. and Europe. He can be reached at mmoore@acumensolutions.com.

CONTRACTS and Risk Management

Continued from page 10

liability limitations effectively limit the SP's liability to pretty close to 0 if it does not perform, but put no limits on the customer's responsibility to pay invoiced or other charges.

Some Thoughts on Form Contracts

We will close with a comment on the special concerns presented by form contracts. Almost without exception, such forms do an excellent job of protecting the party that drafted them but offer few protections for the other side. That does not make the party who wrote the form bad; it just means that its lawyers are doing their jobs by seeking to manage the party's business risks to the fullest extent possible. This is more of a problem for customers than providers, because most sourcing transactions start with the provider's form. The good news is that reputable vendors will cooperate to negotiate changes to their standard forms to reasonably divide risks between the parties. The cautionary point is that it is a really bad idea from a risk point of view to accept an off-the-shelf standard form just because the account rep is a great guy and you are in a hurry to get the deal done. Instead, make sure the contract language reflects the good will and fairness pledged by the SP when it was trying to retain or win your business.

Hank Levine (WSTA's General Counsel) and Mark Johnston are partners in the law firm of Levine, Blaszak, Block & Boothby, LLP, which specializes in the representation of enterprise customers negotiating network and IT agreements with major suppliers. This article is a general and hypothetical discussion, and is not the provision of legal advice on which a reader can rely in a specific fact situation. For further information please go to www.lb3law.com.