Microsoft

Risk Management Frameworks

Effective Security Practices Series

Driven by a wave of security legislation and regulations, many IT risk management frameworks have surfaced over the past few years. These frameworks attempt to help the enterprise identify risk, prioritize risk, manage risk, and identify processes and tools to help defend the enterprise. In theory, these frameworks are versatile and facilitate business-oriented risk decisions. In practice, they can be awkward, opinion-driven, and limited in scope. In this paper, we look at effective practices for implementing risk management frameworks. Through interviews and discussions with Chief Information Security Officers (CISOs), we identify the key challenges and success factors for adopting risk management frameworks.

Herbert H. Thompson, Ph.D.
Chief Security Strategist, People Security

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Preface

Information security is a very dynamic field: legislation keeps changing, technology keeps evolving, and the attacker community continues to become more sophisticated. This turmoil has forced security practitioners to think creatively to address some very difficult problems. Much of this innovation has been locked away within corporations as they have made isolated progress on issues like security metrics, security risk management frameworks, and security policy. In order to address this discrepancy, Microsoft commissioned a whitepaper series to share key security innovations. Whitepaper topics came from participants in Microsoft's CSO Council - a semi-annual gathering of security executives from leading global organizations who serve as advisors to Microsoft's Trustworthy Computing Group.

Our goal is to share practices "from-the-trenches" that address some of the toughest problems in security. After numerous interviews, discussions, and debates with these though leaders, a collection of effective practices emerged. While much remains to be done, we hope that these whitepapers fuel the discussion and help facilitate further sharing in the field of IT security.

The Situation

The National Institute of Standards (NIST) defines "IT Risk" as "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."[1] Looking at this definition through the lens of modern business, the definition of vulnerabilities must include both tears in the fabric of IT systems and also mismatches between how systems operate and the regulations and policies that govern the business.

Most modern businesses are critically dependent on a range of IT processes, and with any process, there is risk of failure. Risk management has long been an integral part of business operations. In recent years, IT risk management has become a more formalized and structured activity driven by legislation and standards.

For some business processes, the role of information technology has been to automate or expedite. In these cases failure may simply mean a degradation of service as manual (redundant) mechanisms take over. The "risk" in this case may be service disruption. For other business processes, software and technology may be so critical, so intertwined into that process's success that an IT failure may be devastating.

Beyond traditional "failure," a particular piece of software may be trusted by other systems outside of its functional role and the impact of a security compromise could be felt diffusely in a company. Compromising a publicly-facing web server for example may give one access to a company's internal financial database server, payment processing system, or email server. These process risks have to be identified, assessed, and managed.

Most large organizations have begun to formalize IT risk management processes; and frameworks like NIST's "Risk Management Guide for Information Technology Systems", ANZ-4360 from Standards Australia and Standards New Zealand, and the Information Security Forum's Information Risk Analysis Methodology (IRAM) have emerged. These frameworks try to factor IT risk into overall business risk by identifying risks, assessing the likelihood of a negative event, estimating the potential impact of a negative event, and offering a plan for mitigation. While these standards are a good starting point for managing IT risk, they offer little advice or metrics in some specific areas. As an example,

[1] G. Stoneburner, A. Goguen, and A. Feringa "Risk Management Guide for Information Technology Systems" p. 8, National Institute of Standards (NIST) Special Publication 800-30, 2002.

consider the assessment of software security, which may represent a significant source of risk for IT. Applying one of these frameworks, could, for example help one identify potential attackers, the sensitivity of data being processed by a particular application, the compensating (security) controls that are part of the network, the potential impact on the organization of data being compromised or a system/process being incapacitated. While all such factors are *necessary* to determine business risk they are not *sufficient* to make remediation spending decisions because – according to the framework - the "vulnerability" or "susceptibility" of software boils down to a checklist of security controls or a penetration testing of a system. Assessing the security of software is a much more involved task and these results may offer little insight into the true risk this software introduces into the environment.

A View from the Trenches

In preparing this paper we talked with several members of Microsoft's CSO council along with other information security executives responsible for managing IT risk in large enterprises. Most respondents had not found a risk management approach that worked well for them out of the box. Many used home-grown solutions and added components from the Information Security Forum's IRAM, frameworks from the National Institute of Standards and Technology NIST, or the International Organization for Standardization (ISO) frameworks. IRAM (and IRAM-based tools) was the most common base framework used. Risk from data leakage and exposure was the most commonly cited area for concern. Several respondents had adopted Data Loss/Leakage Prevention (DLP) solutions to help track down structured data (such as credit card numbers and Social Security numbers) but still felt that the risk from data exposure, especially unstructured data, was severe.

One of the biggest frustrations that respondents had was a lack of guidance on estimating the probability of occurrence for a negative event. In many of the frameworks used by respondents, the process of assessing risk came down to first quantifying the impact of a particular threat if it were to materialize. In most frameworks this equates to establishing bands of impact, such as Low, Medium, and High and then associating a particular dollar loss range to those bands. Figuring out where a particular risk fits in is usually a collaborative exercise where stakeholders come together in a room and talk through best guess estimates of impact.

In many cases, risks must be categorized for which there is no prior data and where the probability of occurrence is small and difficult to define. For these cases in particular, respondents expressed concerns that certain risks were being under-represented or overly addressed. The biggest concern for many respondents was around legally protected information. Several had invested significantly in technologies (such as DLP and laptop hard disk encryption) to help reduce the risk of data leakage in the enterprise. While most felt there was significant work to still be done in the classification and monitoring of sensitive information, there were other areas of risk for which they felt there was not enough information to properly manage it. One such area was insider threat. Another was unsanctioned consumerization – using personal devices without company approval or oversight.

Some respondents expressed optimism for the future of risk management frameworks, pointing to the growing amount of data breach information in the market place, particularly in the wake of new breach notification laws in the U.S.. This sharing of data may help to refine future risk assessment, particularly when a company discloses the mechanics of a data breach.

Applying risk management frameworks has become particularly important during tough economic times where there is increased pressure to thoroughly assess IT investments. Many saw risk management as a flashlight, illuminating the potential pitfalls of a new process or technology that on its surface appeared to have a high value proposition. In one particular example, a respondent discussed the temptation to move a critical business processes to a 3rd party cloud service provider for cost savings and improved efficiency. Application of a risk assessment quickly showed the risks associated with this move, the most critical of which being an audit requirement that could not be met by the service provider. In a few other cases, risk management frameworks have helped respondents determine the terms and conditions needed for 3rd party Service Level Agreements (SLAs) which are of particular importance as some processes move to clouds managed by 3rd parties.

While there were a number of home-grown risk management approaches, most respondents indicated that there was something useful to be gleaned from many of the larger risk management frameworks (such as IRAM). The greatest benefit reported was that a risk management framework allowed them to more uniformly invest in defenses. Given that security is a weakest link problem – any weak component in a process may compromise the entire process – it is crucial that defensive resourced be spread according to true risk. To this end, the frameworks allowed them to communicate risk in a more palatable way to business stakeholders.

Conclusion

During discussions with the information security executives on risk management frameworks two things became clear. First, the process of applying a risk management framework has value in both visualizing and communicating risk. Second, there has been significant innovation in risk assessment and management within enterprises that is not widely known or shared. While the general frameworks have matured over the past few years, the insular innovation within enterprises is substantial. Sharing these insights and experiences in forums like Microsoft's CSO Council and security conferences is essential for growth. Our hope is that this paper begins some of those discussions.

Appendix 1: Survey Questions

In preparing this whitepaper, we spoke with several members of Microsoft's CSO council. Respondents were leaders in the field of IT security and hold operational responsibility for security in their organizations:

Do you currently use any of the standard risk management frameworks (ISF, NIST, etc.)?

If not, do you have a home-grown IT risk assessment approach? Can you share with us what drove you to create it?

What features of the risk management approach (or standard methodology) that you use now do you think work well?

What areas of these frameworks do you wish were better addressed (software security, insider threat risk, etc.)?

How does the output of your risk management exercise tie back to metrics you can communicate with stakeholders?

Do you feel like your risk management approach allows you to do good relative assessments (meaning is *area a* stronger/weaker than *area b*)?

Which areas of risk do you feel you are able to measure most effectively?

Which areas of risk do you feel are not being measured?

Appendix 2: Acknowledgements

The Information Security Forum (ISF) is an independent, not-for-profit international association of leading organizations from around the world. It is dedicated to investigating, clarifying and resolving key issues in information security and developing best practice methodologies, processes and solutions that meet the business needs of its members. By harnessing its world-renowned expertise and the collective knowledge of its members, the ISF delivers practical solutions including authoritative research reports, risk methodologies and benchmarking tools such as the IRAM tool mentioned in this report, to overcome wide-ranging security challenges impacting business information today.

ISF members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organizations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that members are able to adopt leading edge information security strategies and solutions.

For further information on any aspect of the ISF or its services please contact:

Steve Durbin
Vice President, Sales & Marketing

Information Security Forum
10-18 Union Street
London
SE1 1SZ
United Kingdom

Mobile: +44 (0)7785 953 800
Tel: +44 (0)207 213 1745
E-mail: isfinfo@securityforum.org
Web: www.securityforum.org