

IT Security Risk Management

By Mark Gerschefske

Risk Analysis

How do you predict the total cost of a threat? Is it only the cost to restore the comprised system and lost productivity? Or does it include lost revenue, customer confidence, and trust of investors? This paper provides an overview of the risk management process and its benefits.

Risk management is a much talked about, but little understood area of the IT Security industry. While risk management has been practiced by other industries for hundreds of years, little historical data exists to support qualitative analysis in the IT environment.¹ The industry approach has been to buy technology without really understanding the potential underlying risks. To further complicate matters, new government regulations create additional pressure to ensure sensitive data is protected from compromise and disclosure. Processes need to be developed that not only identify the sensitive data, but also identify the level of risk posed due to noncompliance of corporate security policies. Verizon has developed security procedures based on industry standards that evaluate and mitigate areas deemed not compliant to internal security policies and standards. Through the use of quantitative analysis, Verizon is able to determine areas that present the greatest risk, which allows for identification and prioritization of security investments.

Risk Mitigation Process

The Risk Mitigation Process (RMP) is a part of risk management that addresses how to reduce exposure to an identified risk. A solution to mitigate the risk is developed and modeled to determine the level of reduced risk versus the cost to implement. If the solution provides an acceptable level of reduction in risk for the associated cost, then it is considered successful and the process is complete.

The RMP can be thought of as a spiral model that allows a user to complete the process and then review the results. If the risk mitigation process was successful, then the process stops at the end of the post-mitigation task. If the risk or cost is not acceptable, then the entire process is repeated to determine if it can be improved. Each time the process cycles through the model, the overall procedure can be adjusted to incorporate lessons-learned. Figure 1 shows the four steps of this process: Risk Analysis, Pre-Mitigation, Review Solution, and Post Mitigation. If the level of Risk Exposure (RE) is reduced to a low level on the Risk Assessment Chart at an acceptable cost (see Figure 3), then the mitigation can be considered successful and the process is terminated. If the RE still ranks in the high to medium range, then a new technical solution will have to be developed and the cycle repeated.



Figure 1: Risk Mitigation Process

Risk Domains

The first step of the RMP is risk analysis – this includes reviewing all documentation and determining where attack surfaces reside. Is the vulnerability internal to the corporate trusted infrastructure? Is it in the corporate DMZ? Does it reside in the Internet? Is it located at an enterprise’s location or some combination of all of these? To identify where the risk areas are located, Figure 2 shows the Risk Domains and the interrelationships that can exist. Vulnerabilities that reside in the DMZ are at greater risk than the same vulnerability located in a private trusted network.

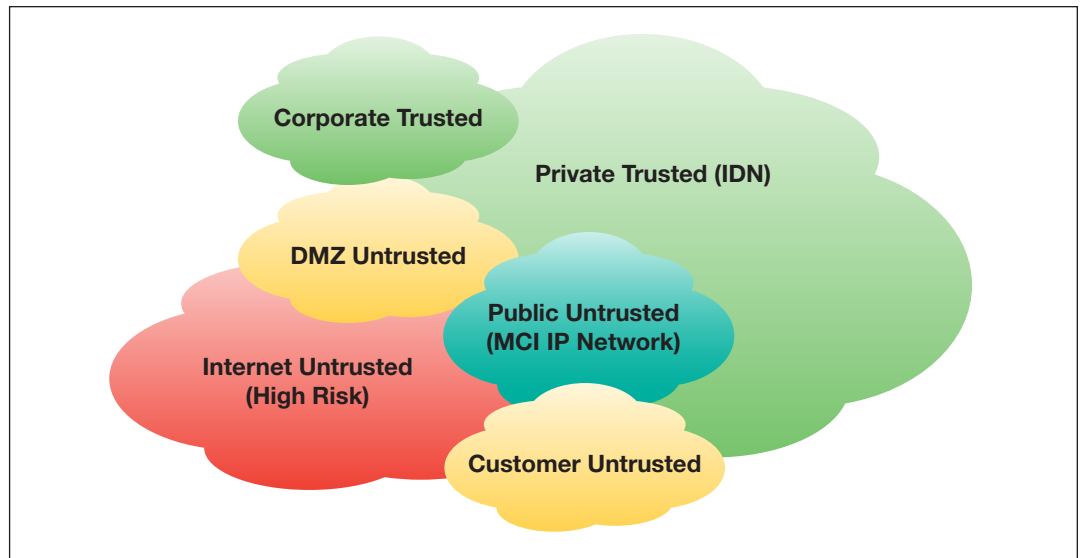


Figure 2: Risk Domains

The value of the Risk Domain chart is that it can be used to determine where the primary attack surfaces reside, as well as the source of the attacks, any secondary attack surfaces, and which domains might be affected by secondary attacks. In the case of the Code Red Virus, the RE was only medium-to-low, but the secondary impact on the IP network was high. To understand the relationship between the domains and the cause-and-effect an attack can have, it may be necessary to break a single vulnerability into multiple scenarios and model each one separately to understand the full impact.

Risk Exposure

The RE process is used to determine the RE, defined as the criticality of the system in relationship to the likelihood an attack could occur against a known system vulnerability. This analysis is fairly complex and is based on five categories that identify:

- Potential exploit threat
- Skill level required by the attacker
- Probability of occurring
- Level of risk to asset
- Value of asset(s) to the business.

The RE provides a weighted analysis that calculates the risk exposure for a given threat or known vulnerability.² This differs from the standard risk model that only attempts to take into consideration the Threat x Vulnerability x Cost and does not consider the critical impact of the at-risk system. The resulting risk exposure analysis provides a category rating of high, medium, or low based on the severity of the exploit, the probability of it occurring, and the value of the asset as depicted in Figure 3.

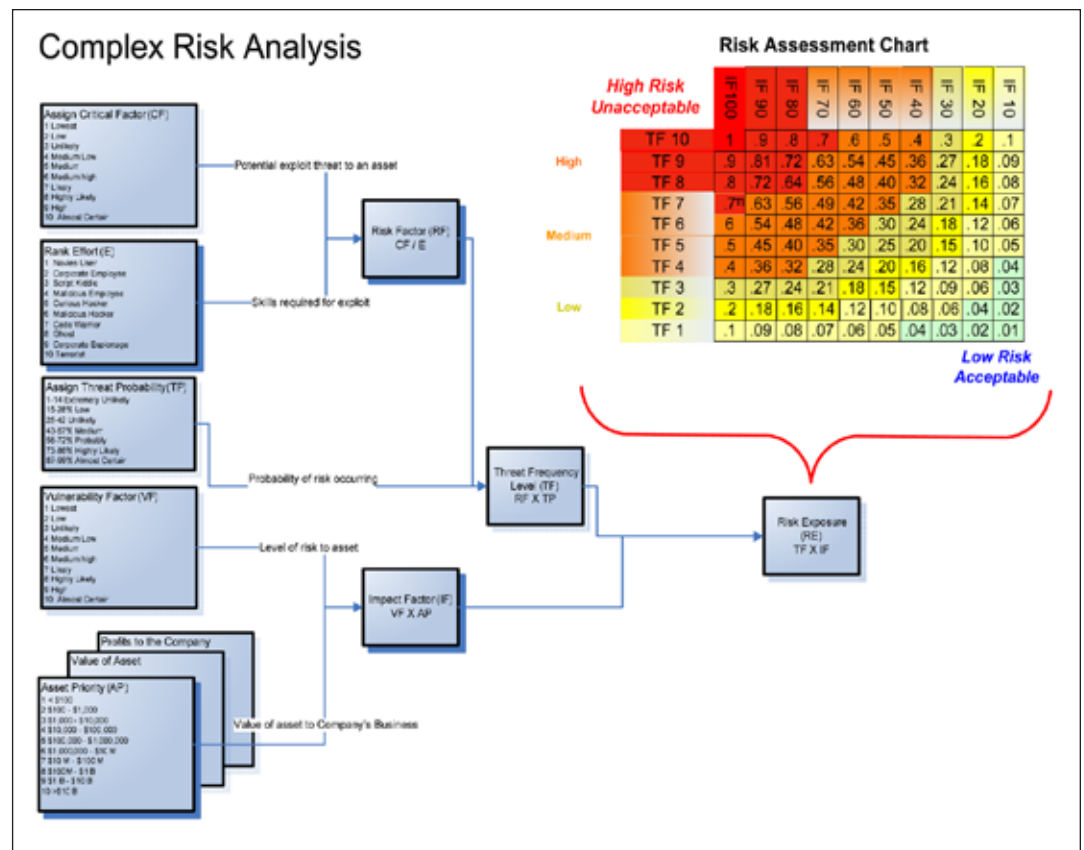


Figure 3: Risk Exposure Process

Risk Analysis

To meet corporate and regulatory requirements, a process needs to be implemented that allows for mitigation based on available solutions, financial exposure, and value to mitigate. After analyzing the problem, a detailed-level process is developed that provides an end-to-end method for risk mitigation, determines the financial exposure, and evaluates the mitigation solution to aid in reducing the financial exposure. (See Figure 4.)

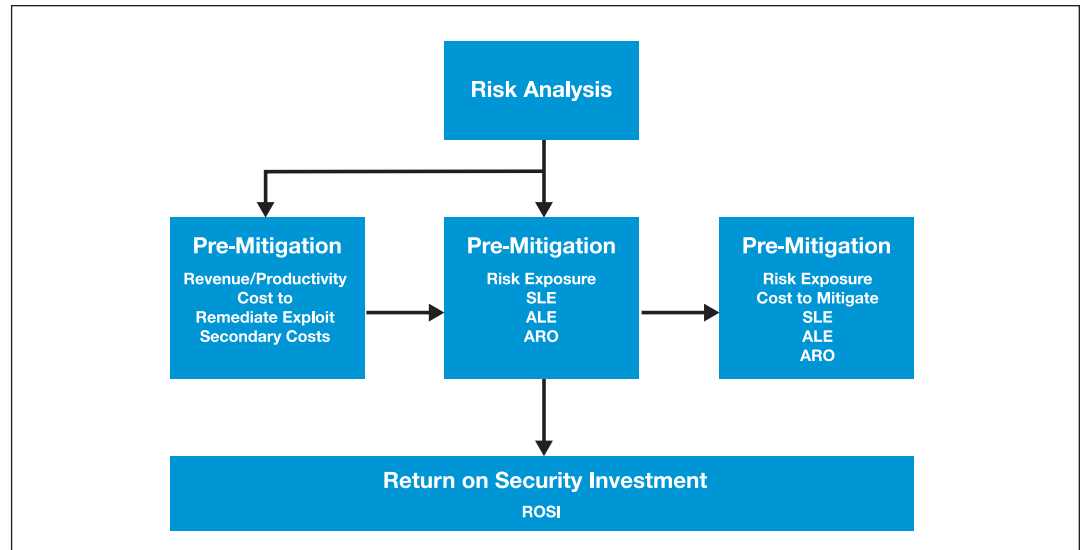


Figure 4: Risk Management Process

The process depicted in Figure 4 provides an end-to-end view of the flow and relationship of each of the individual RMP sub-processes. The process begins with Risk Analysis where all the requested documents are reviewed. The Risk Domains are evaluated along with the Threat Source/Actions, Threat Impact Trees, and Threat Probability from both industry and internal sources.^{3,4}

Asset Value (AV), RE, and Annualized Rate of Occurrence (ARO) are parallel processes. The RE is determined for the pre-mitigation scenario and is used with the AV to compute the Single Loss Exposure (SLE). The SLE is used with the ARO to determine Annualized Loss Expectancy (ALE).⁵ Other factors included in the SLE are impacts to business processes, customers, revenue, and other financial impacts.⁶

While the initial RE is being analyzed, the search for the existence of an Off-the-Shelf Technical Solution (OTSTS) is employed. If one is discovered, then the process flows into the post-mitigation analysis with the RE calculation based on this OTSTS. This is used to calculate ALE (Post)—Post-Mitigation—which is then compared to ALE (Pre)—Pre-Mitigation—to provide the Return on Security Investment (ROSI). If an OTSTS does not exist, then a Mitigation Plan (MP) that provides a custom, technical solution is required. Afterward, the MP is used to calculate the ROSI using the previously described process. If the MP does not produce an acceptable ROSI, the MP is rejected. At that point, the determination to repeat the process in hopes of finding a better solution must be made. If a better solution is technically impossible, then a business decision must be made either to accept the risk or remove it from the network.

Return on Security Investment

The ROSI process provides the basis for meaningful cost-benefit analysis of the risk reduction measures. ROSI is computed by subtracting the delta of ALE (PRE) and ALE (POST) cost exposures from the initial cost of the countermeasure (including annual recurring costs). This provides a measure that shows how effective mitigation was in respect to the cost versus the reduction in financial exposure. If the cost to mitigate exceeds the financial exposure, then the mitigation motivation becomes business-driven or regulatory in nature.

Quantitative Analysis

Quantitative analysis is used to determine risk versus cost and benefit of pending security enhancements. The risk, ROSI, and financial exposure are used to determine the security cost-benefit for proposed security upgrades. While no single area gives an overall assessment of the risk, when viewed collectively they provide an interpretation that gauges the overall risk assessment. To support this analytical approach, a third variable is modeled along with the traditional two-dimensional X and Y axis (see Figure 5). This allows for the financial exposure to be compared to the risk and ROSI of mitigation. This not only depicts the comparison and prioritization of exceptions, but provides a quick analysis to show where the best return on corporate resources can be achieved.

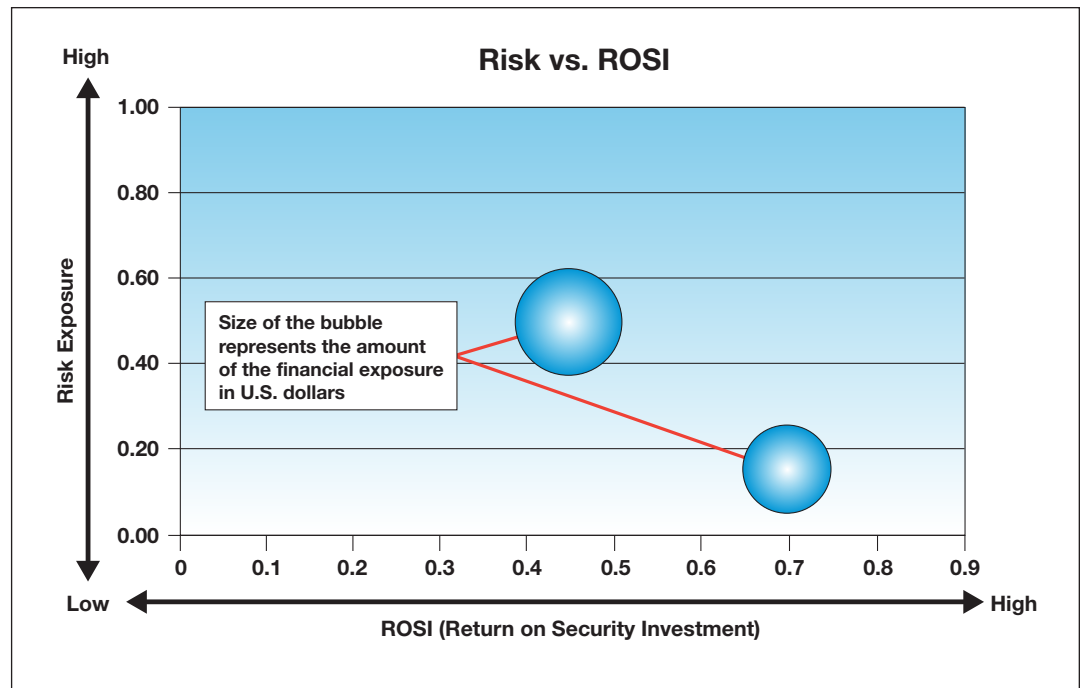


Figure 5: Risk vs. ROSI Analysis Chart

Conclusion

The risk management process discussed in this paper builds on industry-accepted practices to identify and capture the different elements that represent the total risk model for any system or network threat. The objective is to address not just traditional IT systems, but to include IT development that has extended to provide innovated solutions to business needs. These non-traditional IT systems are least understood and present the biggest challenge when trying to quantify financial exposure. Other considerations are the type of data processed, data stored, or data transported by the compromised systems and what impact(s) a threat could present. From preliminary reviews, this model addresses the fundamental risk elements as they are known. The complicated part of the analysis may be identifying multi-level risks as an exploit propagates through a network creating various cause-and-effect circumstances. In some cases, the secondary effect may be greater than the primary effect (e.g., the Code Red attack).

When considering the source of potential attacks, keep in mind that approximately 50 percent of all attacks originate from within the enterprise. According to the CSI/FBI Computer Crime and Security Survey, this is a continuing trend that has been reported over the last several years.⁷ The adaptation of the IT Security Risk Analysis model has resulted in a better understanding of the financial exposure associated with a given security risk. Through this process, Verizon is able to help customers understand the risks presented in this new "cyberworld." Verizon is an industry leader in the quantitative analysis of security risks, and Verizon's customers can depend on our world-class security team to provide secure solutions in a world that is not secure.

Endnotes

1. Bob, B., Ellen, M., & Dan, G. (2001). *Information security is information risk management*. Proceedings of the 2001 workshop on new security paradigms. Cloudcroft: ACM Press.
2. Microsoft Corporation. (2004, February 2). *Identifying and managing security risks—understanding the security risk management discipline*.
3. Boltz, J., Doring, E., & Gilmore, M. (1999, November). *Information security risk assessment practices of leading organizations*. General Accounting Office/Accounting and Information Management Division.
4. Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). *Risk management guide for information technology systems*. National Institute of Standards Technology.
5. Tipton, H., Krause, H., & Ozier, W. *Risk analysis and assessment*. Information Security Management Handbook (4th ed.). Newport Beach: Auerbach Publication.
6. Halper, A. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2), 74-83.
7. Gordon, L., Loeb, M., Lucyshn, W., & Richardson, R. (2004). *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

