Understanding Insecure IT: Practical Risk Assessment

Simon Liu, *US National Library of Medicine*
Rick Kuhn, *US National Institute of Standards and Technology*
Hart Rossman, *SAIC*

IT systems have long been at risk from vulnerable software, malicious actions, or inadvertent user errors, in addition to run-of-the-mill natural and human-made disasters. As we discussed in the last issue ("Surviving Insecure IT: Effective Patch Management," pp. 49–51), effective patch management is essential for shoring up security vulnerabilities, but we'll still never witness perfect patch management and risk-free IT systems. Risk assessment is therefore critical for identifying, analyzing, and prioritizing IT security risks.

Risk assessment involves gathering and evaluating risk information so that enterprise stakeholders can make mitigation decisions. Once we identify the risks, we can rank the probability of each one's occurrence and its impact on the organization. Some risks are more likely to occur than others, and different risks can affect an organization in different ways, so a practical assessment can help ensure that enterprises identify the most significant risks and determine the best actions for mitigating them.

Processes and Approaches

We can break risk assessment down into two basic tasks: analysis and evaluation. Analysis uses available threat, vulnerability, process, and asset information to identify threats and estimate the associated risk, and evaluation compares this estimate against a set of criteria to determine the risk's significance and impact. Risk assessment can be qualitative or quantitative and accomplished via automated or manual methods. It generally includes the following activities:

- *Identify at-risk assets.* Ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize helps determine which operations and assets are the most important.
- *Identify potential threats.* Some threats that could harm and thus adversely affect critical operations and assets include intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- *Estimate the possibility.* Knowledgeable individuals in the organization or hired as consultants can provide historical information and judgment about the likelihood of some threats materializing.
- *Determine the impact.* The potential losses or damage that could occur if a threat materializes should also include recovery costs.
- *Develop mitigation options.* Identifying cost-effective actions to mitigate or reduce the risk can include implementing new organizational policies and procedures as well as technical or physical controls.
- *Document the results and develop an action plan.* After conducting the analysis, a "lessons learned" summary along with a plan for the future can help put a lot of priorities into perspective.

Quantitative analysis assigns a value to each risk element such as asset value, frequency, severity of vulnerability, impact, and control cost. Risk equations determine the total and residual risks and typically provide loss expectancy as well. Specifically, a quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on the likelihood that a damaging event will occur, the costs of potential losses, and the costs of mitigating actions the organization could take. In this approach, risk = probability of loss × cost of loss; managers must balance the expense of reducing vulnerabilities

against the calculated risk. The quantitative approach often requires the use of some historical or subjective input, so it can be difficult to apply to IT security: we can expect new vulnerabilities with new applications or major upgrades of existing ones, but it's nearly impossible to anticipate the severity of flaws or the time it will take before their discovery. Because of these complications, a purely quantitative approach isn't always feasible due to the lack of reliable data (although it can be useful in comparing expected loss under various assumptions).

Managers must balance the expense of reducing vulnerabilities against the calculated risk.

Qualitative analysis blends limited quantitative data with experience and personal judgment; it doesn't require probability data and uses only estimated potential loss. This approach often uses scenarios to describe the threat and potential loss, so its results typically rank likelihood and impact on a relative scale. The qualitative approach is simpler and faster to complete than a quantitative assessment, but it doesn't generate specific quantifiable measurements. Ultimately, when reliable data on likelihood and costs aren't available, a qualitative approach can define risk in more subjective and general terms, such as high, medium, and low. However, this means that such assessments depend more on the expertise, experience, and judgment of those conducting the assessment.

Methods and Tools

Risk assessors can use various methods and tools to perform their analyses. Some of the most popular options include the following:

- The Computer Emergency Response Team Coordination Center (CERT/CC; www.cert.org) is a federally funded research center operated by Carnegie Mellon University. CERT's risk assessment product includes the Operationally Critical Threat, Asset, and Vulnerability Evaluation (Octave) suite of tools, techniques, and methods. Octave comes in three flavors: the original method, which forms the basis of the Octave body of knowledge; Octave-S for smaller organizations; and Octave-Allegro, a more streamlined approach.
- The Information Security Forum (ISF; www.securityforum.org/index.htm) is an international association of private companies and public-sector organizations. It has several complementary products and tools for risk assessment, including the Standard of Good Practice for Information Security, Fundamental Information Risk Management (Firm) and the Firm Scorecard, the Information Security Status Survey, Information Risk Analysis Methodologies (IRAM), the Simple to Apply Risk Analysis (Sara), and the Simplified Process for Risk Identification (Sprint).
- The US National Institute of Standards and Technology developed the Risk Management Framework for US government agencies; currently, many enterprises in the private sector also use it, and the US Committee on National Security Systems has adopted it for national security systems. It provides a risk-based approach to security control selection and specification and considers effectiveness, efficiency, and constraints due to applicable laws, policies, standards, or regulations (http://csrc.nist.gov/groups/SMA/fisma/framework.html).
- The Central Computer and Telecommunications Agency (CCTA) is a UK government agency providing computer and telecom support to government departments. The CCTA's risk assessment product includes the CCTA Risk Analysis and Management Method (CRAMM; www.cramm.com), which includes a comprehensive range of tools for asset dependency modeling, business impact assessment, threat and vulnerability identification, and required and justified control identification. The CRAMM method is mostly qualitative, but it can extend to quantitative evaluation.
- The International Organization for Standardization (ISO; www.iso.org) is a network of the national standards institutes of 159 countries. The International Electrotechnical Commission (IEC; www.iec.ch) prepares and publishes international standards for all electrical, electronic, and related technologies. The ISO/IEC published ISO/IEC 27001, the de facto information security standard that provides best practice recommendations for those who initiate, implement, or maintain information security management systems. The standard contains 12 main sections, and is a reference model and source of input for many risk assessment methods and tools.
- The Information Systems Audit and Control Association (ISACA; www.isaca.org) is an international organization for in-

formation governance, control, security, and audit professionals. It published the Control Objectives for Information and related Technology (Cobit), which provides a reference framework for management, users, and information system audit, control, and security practitioners. Cobit allows for assurance initiative planning and scoping in a standardized and repeatable way that enables assessment under a single framework.

Risk assessments in certain sectors are mandated in regulations such as the Health Insurance Portability and Accountability and the Sarbanes-Oxley acts. But regardless of sector, organizations must apply the appropriate approach to different aspects of risk analysis and classes. Methods such as Firm and Sprint are most useful in high-level analysis, such as risk profiling. But a detailed analysis to identify specific measures for reducing event impact and probability is best supported by methods such as Octave and CRAMM. For organizations creating their own customized assessment methods and tools, ISO/IEC 27002 and Cobit can help guide development.

Practical and Useful?

On paper, risk assessments seem like a no-brainer that every organization should undertake, but they have their fair share of complaints, typically about their ability to be both practical and useful:

- *Lack of demonstrated business value and benefit.* Some people feel assessments are too subjective to provide anything more than conceptual information.
- *Impractical actions to address risk.* Assessments don't always address risks at a sufficiently granular level and seldom deliver pragmatic, implementable advice to business owners.
- *Tedious and time-consuming.* Assessments require extra work beyond normal duties and operational activities.
- *Lack of skilled personnel.* Assessments are complex and require special skills to perform the job properly.

Other practicality issues such as the lack of reliable data could derail risk assessment efforts. Reliable information about a security attack's likelihood and the costs of damage, loss, or disruption caused by a security event are either limited or impractical for ranking potential risks. Additional issues such as the difficulty of measuring intangibles or indirect costs can also challenge risk assessment efforts. Some costs, such as a loss of customer confidence, sensitive information disclosure, or a drop in employee productivity are inherently difficult to quantify. This missing data often precludes precise determinations about the most significant risks and meaningful comparisons between cost-effective countermeasures.

In spite of these problems, it's still important for organizations to identify and deploy practical methods that effectively realize the benefits of risk assessment while avoiding costly attempts to develop conceptual artifacts that are of questionable usefulness. It's also critical that organizations focus their assessments on specific objectives to increase the probability that they will develop an actionable plan and realize its ultimate business value.

Because risks and threats change over time, it's important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of their mitigation mechanisms. Note, however, that risk assessments on their own are insufficient as risk management mechanisms: they must be incorporated into a broader program that includes periodic planning, continuous communication and collaboration with the business's stakeholders, ongoing measurement and reporting of risk treatment, and useful documentation of risk management activities.

Disclaimer

We identify certain software products in this document, but such identification doesn't imply recommendation by the US National Institute for Standards and Technology or other agencies of the US government, nor does it imply that the products identified are necessarily the best available for the purpose.

Simon Liu *is the director of information systems at the US National Library of Medicine. His research interests include IT architecture, cybersecurity, software engineering, and database and data mining. Liu has two doctoral degrees in computer science and higher education administration from George Washington University. Contact him at simon_liu@nlm.nih.gov.*

Rick Kuhn *is a computer scientist at the US National Institute of Standards and Technology. His research interests include information security, software assurance, and empirical studies of software failure. Kuhn has an MS in computer science from the University of Maryland, College Park, and an MBA from William & Mary. Contact him at kuhn@nist.gov*

Hart Rossman *is a vice president and CTO of SAIC. He also serves as a faculty member with the Institute for Applied Network Security. Rossman has a CISSP, a BA in communication from the University of Maryland, College Park, and an MBA from the University of Maryland, Robert H. Smith School of Business. Contact him at hart.m.rossman@saic.com.*