Communicating Information Security Risk Simply and Effectively, Part 1

In organizations, the topic of enterprise risk management presents a twofold problem: the calculation of the level of risk and effective communication to top management. An accurate risk assessment loses all its effectiveness if it is not properly understood by managerial executives with decision-making power. For effective communication, it is necessary to accurately represent the situation, connecting the business processes well known to top managers with their most significant threats. Knowing how to describe information security risk to top management effectively is essential to aid decision-making and ensure an organization is secure. Once the risk is communicated, mitigation proposals can be further examined, detailed and discussed, as discussed in "Communicating Information Security Risk Simply and Effectively, Part 2."[1]

Selection of Risk Factors

When speaking with top management, it is common to simplify concepts and make the context understandable to those who may lack specific technical knowledge. This is necessary to keep communication channels open, even at the risk of omitting important information or failing to emphasize the significance of other information. Here, the questions are "What information is important and for whom?" These questions must be considered to improve communication and achieve enterprise objectives.

The purpose of meeting with top management should never be to display one's own skills or to express one's own advocacy for new technology; the purpose should be to bring attention to specific issues that can impact enterprise objectives and require a careful risk-benefit assessment. A change in one's approach to communication can facilitate an understanding of the relevant topic. Instead of presenting a detailed, technological, specialized view, consider a simpler, more general presentation that highlights the links to and consequences for business objectives.

> "AN ACCURATE RISK ASSESSMENT LOSES ALL ITS EFFECTIVENESS IF IT IS NOT PROPERLY UNDERSTOOD BY MANAGERIAL EXECUTIVES WITH DECISION-MAKING POWER."

Presentations are often guided by how the speaker sees the issue under discussion. They are generally written by experts on the subject and include many technical details about the design aspects and the work undertaken. However, typically these details are already in the project documents, operating instructions or activity reports. If the details overshadow the overall vision, it may seem like a duplication of effort, with only a change in style.

Instead, the emphasis should be on the benefits of adopting a particular technology or type of work and the risk involved in doing so. A good high-level

Luigi Sbriz, CISM, CRISC, CDPSE, ISO/IEC 27001 LA, ITIL v4, UNI 11697:2017 DPO
Has been the risk-monitoring manager at a multinational automotive company for more than seven years. Previously, he was responsible for information and communications operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia) and was the worldwide information security officer for more than seven years. He developed an original methodology for internal risk monitoring, merging an operational risk analysis with a subsequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and an integrated system involving risk monitoring, maturity modeling and internal auditing. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn (*https://it.linkedin.com/in/luigisbriz*) or at *http://sbriz.tel*.

presentation does not immediately provide the details of the solution (and it may not do so later, if it is not required); it compares, through a gap analysis, the pros and cons for the enterprise itself. How this is done is less important than the result. Therefore, it is best to start from the context and the potential threats to arrive at the expected consequences, giving little attention to the path taken (the black-box concept).

Risk Data Sources

The starting point, the place to draw the information to be developed in the presentation, is the risk register.[2] It contains all scenarios, analyses and assessments and all decisions already made on how to achieve enterprise objectives and deal with risk. Although the risk register is an ideal source of information, it is too detailed to present to top management in full. Therefore, a summary can be presented in a bubble charts[3] that shows the risk level for all enterprise processes, assessed through a capacity maturity model (CMM).[4]

> "AT THE FIRST LEVEL OF A PRESENTATION, CRITICALITY SHOULD BE IDENTIFIED, BUT THERE SHOULD NOT BE AN ATTEMPT TO MAKE PEOPLE UNDERSTAND HOW RISK WILL BE HANDLED."

The maturity model is the intermediate step between the risk register and the summary chart, and it serves a dual purpose. The maturity model conveniently aggregates risk and introduces a solid bond between risk and control, whether such processes are already implemented or only planned. It also introduces vulnerability assessment. Vulnerability is a metric that measures the weakness of a control and the possible consequences.

The summary bubble chart should represent a broader scenario than one originating from a risk assessment based solely on the impact and probability values. The risk register and the CMM create a high-value bond, with additional information associated with the level of vulnerability and the ability to react (status of the risk treatment plan). However, even if it is rich in information, it is still a high-level summary to prioritize the risk severity for the enterprise as a whole; it does not describe the solution. The risk summary chart makes it possible to analyze the general risk context, preventing a clear understanding of the reasons for the choices made or the planned risk treatments. Attention is focused on assessing the most relevant issues (risk events) that must be addressed in relation to business objectives (global perspective), rather than on finding a practical solution to be adopted (operational context).

To clarify the importance of having the necessary information available to analyze a phenomenon, consider an everyday risk: losing one's house keys. Given the objective (always being able to find the keys) and the same quality of protection (the keys are available when needed), suppose there are three options related to the purchase of a keychain:

1. One equipped with Global Positioning System (GPS) technology
2. One with a photo frame
3. One with a light-emitting diode (LED) flashlight

In terms of the risk register, the three solutions are equivalent because they all meet the objective. The homeowner may perceive a greater benefit from one of the options, but only if they are aware of all three options.

Nuances and details cannot be added to synthesis without compromising the purpose of aggregation and the ability to understand the risk results highlighted. It is reasonable to expect the risk register to clearly identify the most significant risk factors, broken down by at least process and entity. To access the operational details of risk management for all critical risk factors, a different approach is needed, with additional information focusing on the aspects of interest. At the first level of a presentation, criticality should be identified, but there should not be an attempt to make people understand how risk will be handled. Presentations should always follow a top-down approach, from an overall perspective of the scenario to a detailed explanation of implementation choices.

Risk assessment is generally a bottom-up process. First, the risk manager participates in drafting a risk report, using all their knowledge and expertise to manage the risk effectively. Then the risk manager must be able to summarize the solutions and their critical issues using nonspecialist language to present the criteria associated with each choice. The aim is to involve top management in decision-making by providing concrete elements that allow them to make informed decisions about the consequences for the enterprise.

Risk Scenarios by Process

The risk register uses a bubble chart to represent the entire map of enterprise risk factors, and process managers use it to select the factors that pose the greatest risk to their own processes and, presumably, would require the most onerous actions and, therefore, the involvement of top management in the decision-making process. To ensure that top management understands the measures required to contain these threats, the qualitative levels of risk, impact, probability and maturity and the synthetic remedy plan must be transformed into a scenario that includes causes, actions and consequences.

Once the relevant risk factors have been selected, the severity of the threats must be highlighted relative to the intensity of the consequences for the enterprise in a context that is more focused on the operational process than can be deduced from the bubble chart of the risk register. The operating context is a representation of the entire process that schematically highlights the operational scenario from a business perspective, including interfaces with other processes, the personnel involved, the business assets involved and all the activities in progress.

To proceed effectively, it is necessary to choose a reference environment to contextualize all considerations. Here, the enterprise information security process is used to describe how to present data at a high level and communicate an effective risk narrative in terms of the operational context. Information security is a highly technological process with a significant influence on most business processes, on the assets used and on the resources employed, both human and otherwise. In terms of complexity and completeness, information security is a good reference environment for creating an effective presentation.

Highlighting the Severity of Threats and Consequences

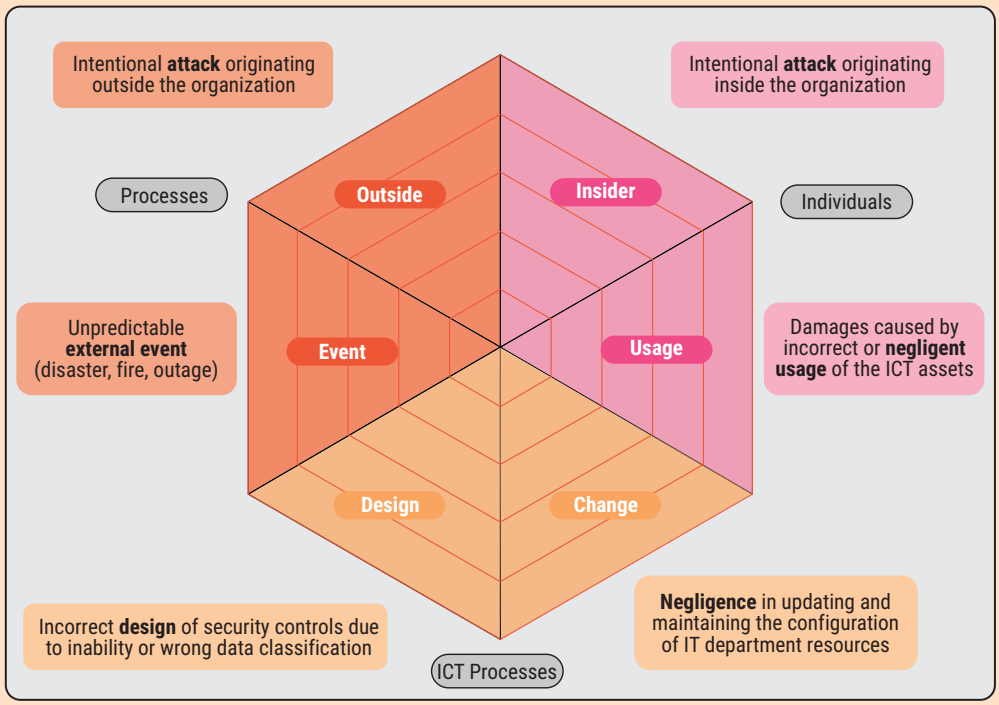
On a practical level, in the IT system adopted for risk management, for each process managed, risk owners can use a template (**figure 1**) to select the risk factors to bring to the attention of top management. The template, automatically fed by the risk register on threats for that process, is used to insert high-level notes to better focus attention on critical issues.

Threats managed by information security are classified according to the nature of the primary cause of the related risk from a business perspective rather than a technological one. Six significant threat zones have been identified based on an organizational and operational perspective. Each zone represents certain categories of potential causes of risk and severity levels of related consequences (in the absence of risk management) for the enterprise. In **figure 1**, three different colors represent three large areas—individuals, non-ICT processes, and ICT processes—identified as being homogeneous with respect to the type of threat source, the environment in which enforcement

Enjoying this article?

- Read *Optimizing Risk Response. www.isaca.org/optimizing-risk-response*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 1—Template for Information Security Risk and Threat Zones



activities are applied and the type of recipient of the potential impact.

Individuals

In this scope, the main players are the individuals. In this case, they are considered to be the direct or indirect causes of the measured risk level. The threat zones included in this scope are:

- **Insider (internal)**—An intentional attack carried out from within the enterprise. Mitigating this type of threat requires technical means if it takes the form of a targeted use of IT tools, legal means if it involves the fraudulent use of resources, organizational means if it exploits procedural gaps and training means if it requires the collaboration of the personnel involved. It is the most insidious type of threat because it can undermine trust among the staff and render all other measures null and void.
- **Usage**—Damage caused by incorrect or negligent use of assigned ICT assets. This threat is addressed by periodic training aimed at the user population and systematic and specific checks (e.g., using the policy of least privilege, choosing an option from a list instead of writing it down, regularly checking authorizations and need for use, evaluating penalties in the event of repeated violations, and forming and verifying the level of learning).

Non-ICT Processes

In this scope, the consequences of an external risk event primarily affect non-ICT business processes and are significant for business objectives. The threat zones included in this scope are:

- **Outside (external)**—An intentional attack originating outside the enterprise as a target, an unaware helper or a side effect. The consequences can affect all processes, owners or users of the resources involved in the attack. Addressing the threat requires an effective preventive control activity such as vulnerability assessments or penetration tests. An audit of the impacted processes guarantees the correctness of these assessments. The consequences may

extend beyond the monetary costs of potential physical damage, such as damage to the enterprise's reputation. In the case of a data breach involving personal data, there may be legal repercussions; in the case of loss of technology data, the entire business may be at risk.

- **Event**—An unpredictable external event not attributable to a specific attack, such as an extreme weather event, fire, pandemic or power outage. The consequences are mainly related to business continuity, but IT resources can also be compromised, both directly by the incident and indirectly due to a chain reaction. The solution requires a realistic business continuity management system (BCMS) for the entire enterprise,[5] with a focus on mitigating the impact on IT systems based on the risk analysis.

ICT Process

In this scope, both the source of the risk and the recipient of the consequences are internal to the ICT process. Causes are related to the methods of executing IT activities performed internally. The threat zones included in this scope are:

- **Design**—Incorrect design of security controls due to insufficient requirements, unreliability of assessments, incompleteness of procedures or inadequate data classification. In general, these types of threats affect the IT service, even if the event originates external to it. For example, if there is a power failure, the continuity system in the server room may fail to start due to previously undetected defects. The consequences can be serious if they impact critical business processes, customers or suppliers, or the corporate image. IT services are involved in all business processes, making it important to correct design problems that can compromise the corporate mission itself. The solution is application of the control methodologies most suitable for the specific type of business.
- **Change**—Negligence in the configuration or maintenance of systems or, in general, in any change to hardware systems, software applications, network configurations or internal ICT processes. The consequences generally involve the potential vulnerabilities introduced in the assets affected by the change. Management of such threats requires strict compliance with information security standards and best practices, adequate training for all operators, and the implementation of effective controls, both automatic and manual.

> "QUALITATIVE REPRESENTATION CREATES A MENTAL CORRELATION BETWEEN THREATS AND CONSEQUENCES."

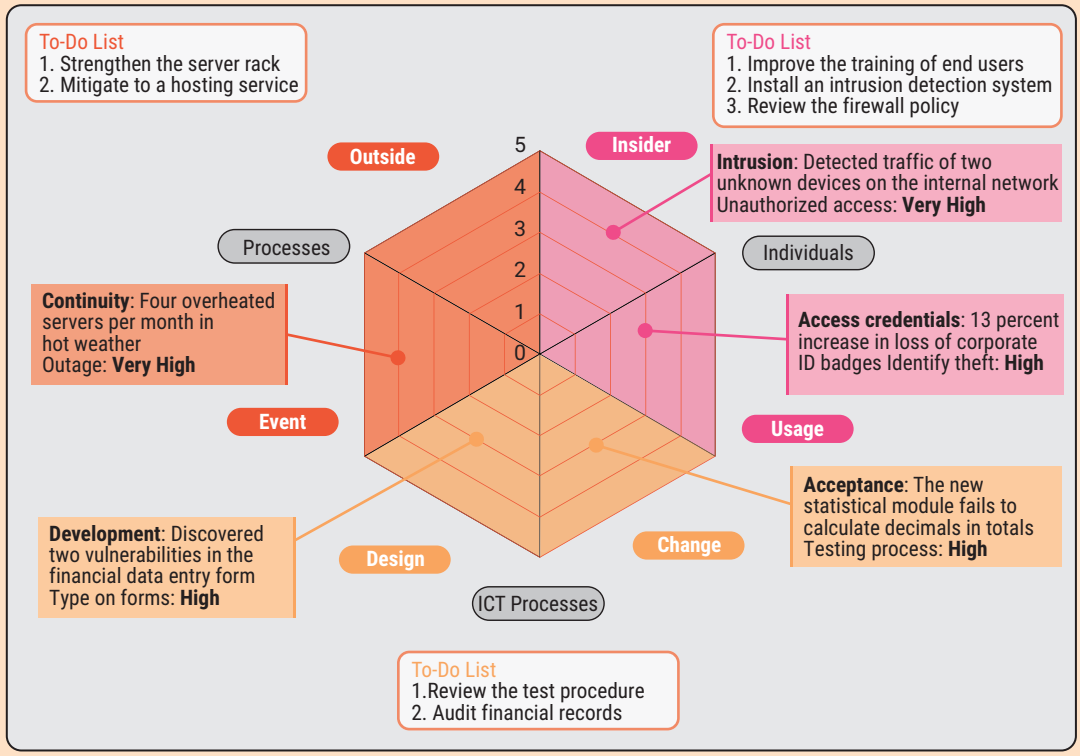
Any IT security risk event can be attributed to one of the six threat zones. Although these threat zones do not reflect the specialized information security risk issues, they have the advantage of allowing a more organizational vision oriented toward the consequences for other processes, human risk factors and the ability to perform the tasks of the process under analysis. The addition of predefined explanations and the use of colors and labels to distinguish the zones can help nontechnical observers understand the operational scenario of the process and the consequences for the enterprise.

Providing Details for Decision-Making

In the next phase, the goal is to assist management and relevant stakeholders in decision-making.[6] When critical processes and serious risk factors have already been identified, it is time to provide a level of detail that is more operational but still understandable to people who are not process specialists.

The objective of the abstract representation of risk is to create an overall view, linking the areas of business operation to the types of consequences for the enterprise as a whole for each selected risk. This results in the loss of some detail in the remedy plan, but this can be made up for in the new level of organizational depth. Now the focus is the level of synthesis among risk factors, application of rules and organizational scope.

Figure 2—Example of Relevant Threats Detected



An example of this particular representation of risk is shown in **figure 2**. The illustration is simple, without numbers (apart from the level of risk, 0–5), and it favors a reflection on the cause-and-effect relationship between the threat (either observed or potential) and the expectation of which objectives will be compromised. Qualitative representation creates a mental correlation between threats and consequences. It does not provide the path to the solution, but facilitates an understanding of the real severity of the threat. If further investigation is necessary, the protection measures proposed to contain the risk should be detailed in another prospectus.

Descriptions of the threats and the level of risk are extracted from the risk register. In **figure 2**, labels summarize the threat, and points indicating risk level are positioned on the grid. Each label describes the event that introduces the risk factor and, briefly, the consequences. The schematic narration is a simple way to help people understand the weight of the threat.

The color of the threat zone tells the observer the functional environment where the threat materializes. The functional environment is implicitly referred to in the label and is described in a general way in the notes, but it is clearly identifiable by those who are familiar with the enterprise. Consequently, it identifies the processes involved, the need for staff training or other interventions, the type of IT assets affected, the need for an organizational review, or the opportunity to improve communication. Text boxes (to-do lists) show the actions envisaged for each area. Some actions may affect several zones, but it is appropriate to include them only once in the most relevant zone.

Other information can be added to the visual representation, but this might decrease its overall clarity, so it is important to consider whether doing so is worthwhile. Different shades of the same color can also be used in the hexagon to highlight different levels of risk. The use of a hexagon is not

essential; a circle or another shape will work, too. It is also important to not dominate the text with flashy graphics.

Conclusion

This view of threats, more focused on organizational aspects than specialized processes, facilitates a high-level understanding of interactions with other business processes and helps to focus on the consequences for the organization rather than on technical details. Subsequent investigations are also necessary to fully understand the phenomena from the point of view of the organization rather than from the technical one, as discussed in "Communicating Information Security Risk Simply and Effectively, Part 2."

Endnotes

1 ISACA®, "Communicating Information Security Risk Simple and Effectively, Part 2," *ISACA® Journal*, vol 6, 2021, *https://www.isaca.org/archives*
2 ISACA, *CRISC Review Manual, 6th Edition*, USA, 2015, *https://www.isaca.org/resources*
3 Sbriz, L.; "Enterprise Risk Monitoring Methodology, Part 4," *ISACA Journal*, vol. 3, 2020, *https://www.isaca.org/archives*
4 CMMI Institute, *https://cmmiinstitute.com/*
5 International Organization for Standardization (ISO), *ISO 22301 Security and Resilience—Business Continuity Management Systems—Requirements,* Switzerland, 2019, *https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en*
6 *Op cit* ISACA, 2015