Why Was There No Warning?

Risk Management

Risk management is an old discipline. As such, some tend to underestimate its importance until something bad happens or a crisis is triggered. And COVID-19 brings up risk management again as a trending topic.

The classic risk management life cycle consists of risk identification, risk assessment, risk response and mitigation, and risk monitoring and reporting. The key challenges facing risk management practitioners today are found in the first two stages: risk identification and risk assessment.

In the past, risk maps tended to be more stable and easier to track. Perhaps, after a thorough and costly risk assessment, an enterprise could afford to track only the risk that had been identified and assume that no action in mitigation meant no changes in risk—and the other way around. There was a much simpler relationship between the implementation of controls and effective risk mitigation. It was a much more stable environment than today's environment. In other words, there were fewer dependencies and more straightforward results after controls were implemented.

Even in the past, taking this simplicity for granted involved certain dangers. However, doing so today is much riskier, due to three factors: complexity, noise and change.

Complexity

Current IT environments have become increasingly complex. All forms of cloud adoption platforms, be they Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS), coexist with traditional in-house IT solutions and with shadow IT. There are hidden dependencies between one system and another and hidden integrations ("seamless" using commercial language). The situation becomes more complicated when an enterprise is looking to be more agile or when time-to-market considerations are critical. Then, system complexity hinders the deeper understanding required to properly identify and assess risk. A thorough risk assessment can, unfortunately, be perceived as an obstacle to push digital products to market or to the organization.

Imagine a business initiative based on a system provided by vendor X as a SaaS model. The system provided by vendor X is actually hosted by a key cloud provider (Y). In this hypothetical situation, the identity of potential business users may not be clear. In addition, the enterprise may have not analyzed the background of vendor X, which happens to be a niche vendor. So, even if concerns were identified, there would be few to no alternatives in the market. Business stakeholders might be questioning the necessity of assessing security factors, worried about taking too much

Ramón Serres, CISM, CRISC, CGEIT, CISSP, CCSK
Is an industrial engineer and chief information security officer at Almirall (Pharmaceuticals). His areas of expertise include information security, IT governance and risk management. Serres has held various positions including business partner, IT manager for strategic projects, IT factory manager, e-business consultant and management consultant. His work has been published in the *ISACA® Journal*, and he has contributed to other publications and has been a speaker at events related to governance, risk and compliance, and cybersecurity.

> "NOISE IS DANGEROUS BECAUSE IT CREATES CONFUSION AND MAKES IT HARD TO KNOW WHICH INFORMATION IS RELEVANT, WHICH INFORMATION IS CREDIBLE AND WHICH DESERVES AN ORGANIZATION'S ATTENTION."

time and jeopardizing the business calendar. These are all hypothetical situations that actually happen in many enterprises, and they end up impeding the proper risk identification and assessment exercise. An explicit top-down endorsement of risk management is crucial to avoid attitudes that implicitly support "turning a blind eye" rather than taking full responsibility for risk identification and assessment.

Noise

The amount of environmental information reaching an organization through various channels and at all levels can trigger certain stress-inducing questions. Vendors make their pitches not only to the chief information security officer (CISO) or the information security department, but also to the chief information officer (CIO) or even top management. With so many technical and regulatory considerations and new trends cropping up (e.g., artificial intelligence [AI], 5G, the EU General Data Protection Regulation [GDPR], even COVID-19), senior management wonders: How does all this affect the enterprise? How relevant is GDPR? How will 5G affect the enterprise? Are all these so-called threat intelligence information services relevant? Is the enterprise really exposed to all the risk factors mentioned by external reports?

Noise is dangerous because it creates confusion and makes it hard to know which information is relevant, which information is credible and which deserves an organization's attention. The more noise there is, the easier it is to miss the point. In practical terms, this means it is easier to overlook a risk because it was not identified or because management failed to fully understand the risk assessment and the likelihood of a risk occurring or, more important, its business impact.

Change

Today, stability is lacking in the environment, in business models and in the IT infrastructure. The pace of change is accelerating. Trends such as DevOps also push that change. And, inevitably, the risk map is continually evolving. Therefore, as opposed to what would be done in the past, it would be unwise today to rely on a risk identification and assessment carried out three years ago. Every aspect of risk management must be constantly revisited and reconsidered. To be precise, this reconsideration is not only about re-evaluating the likelihood and impact of risk factors that have already been identified; rather, it is about identifying new risk factors that were not spotted the last time. Given the current context and circumstances, it is very likely that something new will appear on the risk map every time it is reconsidered.

This constant change is stressing the risk management life cycle and, unless senior management is fully aware of the need for ongoing reassessment, the frequency of risk reporting might be inadequate and the identification of new risk factors might be delayed.

Changes in the environment—both the IT environment and the broader business environment—can trigger changes in the risk factors to which an enterprise is subject. Examples of this (the list is not exhaustive) include:

- Changes in the IT environment include:
  - Publication of services that were not initially linked to the Internet
  - Federation of services
  - Activation or deactivation of protection services (e.g., multifactor authentication, endpoint detection and response [EDR])
  - Setup of new services in the cloud
- Changes in the business environment include:
  - Implementation of new business models
  - Digital transformation that affects business processes
  - Business partnerships that expose sensitive or highly confidential information to new risk

- Extension of the supply value chain integrating it with third parties
- Operation in new geographic areas
- New regulations

While reflecting on how changes in the business and IT environments can impact an organization's risk map, it is important to consider not only known risk factors, but also new ones. It is important to remember that risk maps are more like moving pictures than ever before.

Understanding Risk

Revisiting top management's understanding of the risk map is a healthy practice; in fact, it is a mandatory practice for those enterprises striving to stay alive. This is very much related to the noise factor. Given the volume of input, emails and information, top management may be unable to determine what is relevant and what is not. Risk managers like nothing better than to be asked to revisit risk and explain risk to ensure a full understanding at the top level. Quality conversations with senior managers can lead to a better understanding of risk and to a healthy questioning of the likelihood of certain risk factors and their business impacts.

A deep understanding of risk cannot be taken for granted. For example, certain risk scenarios may have been associated only with integrity and availability, but it suddenly becomes clear that confidentiality (the confidentiality, integrity and availability [CIA] triad) is also affected. Or perhaps when considering cybersecurity risk factors on manufacturing lines, the focus was on the availability of production lines, and the potential impact on integrity was overlooked. For example, control parameters in the manufacturing lines could be illegitimately modified, which should trigger a radical reconsideration of the risk map, depending on what the enterprise is producing and what kind of machinery is used in the manufacturing plants.

In certain cases, discussions with IT may be too centered around the availability of IT services, overlooking risk factors related to confidentiality. Information leakage is possible when information is stored in systems that are more exposed or linked to other systems that might be less protected (e.g., missing recent security patches).

Regulations are another factor that must be understood. Quite often, beyond the headlines announcing new regulations, there is no clear understanding of their impact on an organization. For example, the initial reaction to GDPR and its effect on enterprises has changed in the past two years. Time and experience have allowed IT practitioners to better contextualize GDPR's impact on organizations.

Active discussions about business impact are even more crucial than those about the likelihood of risk. By moving away from strictly academic approaches and adopting more pragmatic approaches, business impact can attract more attention. Business impact discussions at the senior management level and even at the board level are relevant to define risk tolerance and risk appetite.

> "QUALITY CONVERSATIONS WITH SENIOR MANAGERS CAN LEAD TO A BETTER UNDERSTANDING OF RISK AND TO A HEALTHY QUESTIONING OF THE LIKELIHOOD OF CERTAIN RISK FACTORS AND THEIR BUSINESS IMPACTS."

Conclusions and Recommendations

The constantly changing environments in which nearly all enterprises dwell today should trigger a clear intention to delve deeply into the "known unknowns." Likewise, there should be an attempt to minimize the nearly inevitable "unknown unknowns." As basic as this may sound, it takes time to identify the stakeholders, hold in-depth discussions, ask the right questions, and combine

top-down and bottom-up approaches to identifying and describing risk scenarios.

There are several recommendations to make that job easier:

1. Every risk update should focus on identifying new risk factors that have not been identified in the last risk update, not just monitoring the evolution of risk that had already been identified.
2. Assuming that the previous business impact assessment or probability estimate is still valid just because no mitigation actions have occurred is dangerous and probably not valid. In today's complex and changing environment, constant revisiting and rethinking are required to produce credible risk assessments.
3. Proper risk identification and assessment should be explicitly endorsed by senior management so that the organization understands risk management as a critical function.

By achieving a better and deeper understanding of potential risk scenarios, it is possible to avoid the question, "Why was there no warning?"