● Article

Rethinking Information Security Leadership

Dario Rossa,
Associate Partner, Spike Reply

Sergio Plasencia Alcazar,
Information Security Consultant,
Spike Reply

The increasing adoption of the latest innovations and disruptive technologies motivated by customer demands coupled with the desire for mobility and the use of cloud-based services are presenting companies with new information security challenges. Cyber security threats are on the rise because of these demands and this in turn increases the overall risk exposure for business.

While some companies are making strong investments in acquiring top-of-the-line security products to improve their information security architectures, others are allocating many resources to being compliant with the many and varied regulations, standards and policies. It seems the number of security incidents continues to grow.

What is wrong in this picture? Perhaps the most important piece of the puzzle is missing: A holistic approach that merges all these measures into a comprehensive and effective corporate information security programme. A holistic approach requires a privileged vision of the overall security strategy. This role is played by the Chief Information Security Officer or CISO. But how does this role fit into the overall enterprise governance model?

There is still a controversy about to whom the CISO should report. Traditionally, the CISO has reported to the CIO, which, however, has some downsides. On the one hand, not all CIOs are security-oriented whilst on the other hand, even if they are concerned about security, they will have to divide their budgets among other more traditional IT resources like applications, corporate software and hardware. This conflict over resources often impedes senior executives from taking the appropriate actions to prevent information security breaches. Moving information security outside the traditional IT organization can bring many benefits in terms of overall risk awareness, as well as correct and appropriate risk mitigation.

The impact of a materialised cyber security threat could affect the entire company, harm the organisation's reputation or cause a series of serious financial risks like the cost of recovery, customer claims or large penalties. For these reasons, the CISO should be part of the corporate risk management committee and a member of the board, directly reporting to the CEO. Regardless whether the CISO reports to the CIO, the CFO, the COO, the CRO or to the CEO, the key factor is that the role of the CISO should not be buried within or devalued by the company's organisational structure; it must have a direct communication path to the corporate leadership so it can provide senior executives with the correct and appropriate visibility into the company's security position.

More important than the CISO's reporting lines are the skills the CISO possesses. The CISO today needs not only the traditionally required technical skills and a good understanding of risk management; he also needs an understanding of the business. A CISO should be able to drive security to the different business units and processes; he also should be able to report in an appropriate and meaningful way to his audience, which will often be senior management rather than technologists.

The CISO's job today is mostly about assessment and prioritisation, i.e., being able to define the right scope and addressing the highest corporate risks within the available budget and time constraints to lower the risk levels to a threshold of risk appetite that has been accepted by top management. Understanding business risks and having the ability to implement risk mitigation in an effective way are required. These skills require strong relationship building, the ability to speak at all levels of the organisation and establish and demonstrate value. Companies are looking for multi-disciplinary profiles and highly adaptable individuals who are able to perform a dynamic range of duties. That balance of executive profile with both a broad technical foundation and leadership is extremely rare.

The CISO role is evolving as companies are beginning to appreciate the value of adopting a risk-based security approach. In terms of information security, a risk-based approach means raising IT security risk awareness to the right corporate levels and embedding security into business processes, since information security risks impact the whole organisation.

This approach will enrich traditional information risk management, which is often not integrated into the overall enterprise risk management process and limited to conducting risk analysis and risk-assessments on an ad-hoc basis.

In summary, this holistic approach will lead to:

- Adding and setting up proper communication channels with the leadership teams.
- Allowing the leadership team to assess the overall risk exposure and make sound decisions in terms of cost vs. risk reduction.
- Defining action plans downwards throughout the organisation with a goal to reduce risk in a cost-efficient and timely manner.
- Adding risk-monitoring dashboards to review and track information risks existing within the organisation.
- Embedding security in the project life cycle of an asset.

Companies need to go one step beyond the tick-the-box approach to information security for compliance reasons, which will not necessarily create a more secure environment.

Successful companies understand the benefits of a proper information security management system and the importance of the CISO as a key leadership role for implementing a holistic and risk-based approach to information security. ●