Protecting Information—Practical Strategies for CIOs and CISOs

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

Devassy Jose Tharakan, CISA, ISO 27001 LA, ITIL, PMP
Has more than eight years of experience in IT infrastructure security. He works with a leading financial entity in India as information security manager. In this capacity, he is responsible for enterprise security architecture and projects to counter cybersecurity attacks and he heads the security audit practice. In his prior engagement with Elenco Emirates Group as group IT manager, he was active in various infrastructure security knowledge forums in United Arab Emirates. His passion is to help enterprises adopt the right security strategy for better risk management and increased efficiency. He has helped many banking, insurance, retail and defense enterprises redesign their security infrastructure and adopt information security strategies.

Information is a vital business asset, but it is not always recognized as such. Information leaks have crippled many organizations in the past, sometimes to the point that repair is impossible. The failure to visualize the effects of loss of critical information can lead to major consequences. Organizations that do not position their information security group (ISG) strategically within the organization's structure often fail to receive the desired benefits. Stakeholders complain that their ISG is always a cost center, i.e., its function and resultant budget allocation are always high compared to other departments. Many employees feel the ISG is effective only in a reactive mode—responding to (but not necessarily anticipating) security incidents. Quantifying return on investment and ensuring the exact benefits from information security projects are relatively difficult.

Information security is usually a top priority for the chief information officer (CIO). CIOs should ensure a top-down approach and culture to working toward information security within the organization. A practical way of initiating information security is for the CIO to work with the chief information security officer (CISO) to define a governance framework and then entrust the operational responsibility entirely to the CISO. In many organizations, CIOs lose technical focus due to the exponentially fast-changing technology landscape. The challenge they face is to approach the security landscape technically, convince the board of this approach, move the ISG from a cost center to a profit center and invest proactively. The ideal way to accomplish this is for the CIO to introduce a revenue model projecting the possible losses that may result from not making these changes, e.g., impacts of a security breach supplemented with a cost-benefit analysis.

IT security governance should not be confused with IT security management. IT security management is concerned with making decisions to mitigate risk, while governance determines who is authorized to make decisions. Information security governance refers to the leadership, organizational structure, roles and responsibilities, and various processes established for information security. While management recommends security strategies, governance ensures that security strategies are aligned with business objectives and consistent with regulations.

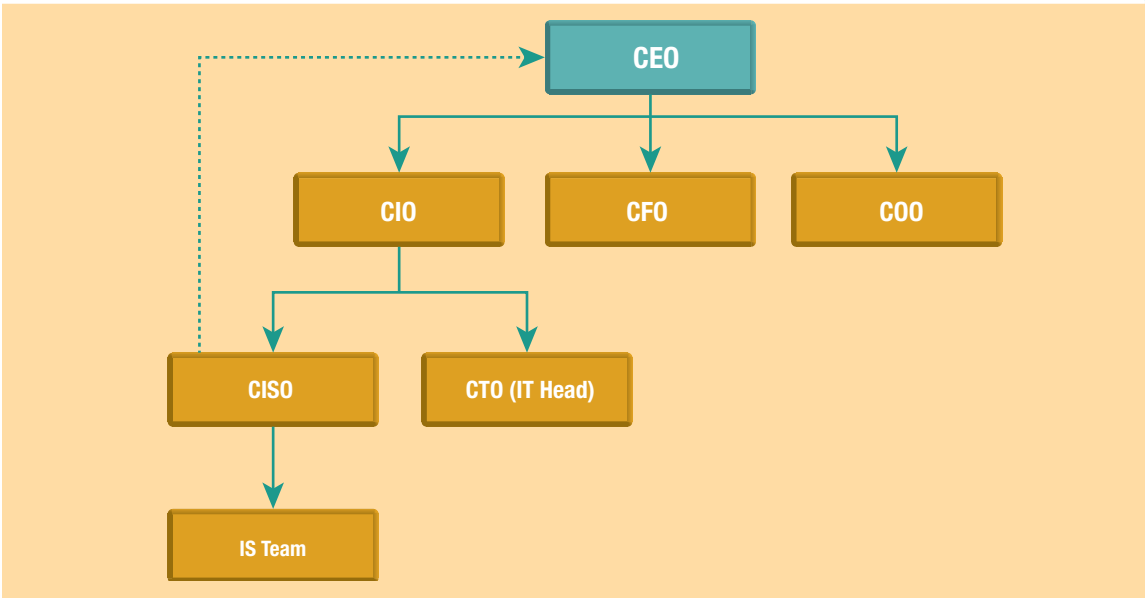
Accurately Positioning the CISO and Delegating Tasks

Information security should be a priority at the board level, so the next priority of the CIO is the tactical positioning of the CISO (**figure 1**). Certain organizations mandate the CISO to report directly to the CIO (meaning the CIO has authority over the CISO) and, in a dotted-line way, to the chief executive officer (CEO) meaning the CEO has influence, but not authority. Such organizations care a lot about information security. This reporting structure enables the CISO to handle escalations effectively and ensure support even from top-level stakeholders.

By developing and utilizing a sound security governance framework, the CISO can ensure that information security strategies are well aligned with business objectives and applicable laws and regulations. While the CISO standardizes and fine-tunes the individual information security requirements of each business group, the CIO should be the master integrator initially. Once operations are mature, the CIO can effectively delegate the responsibility of integration to CISO. The CIO and CISO should balance internal security, compliance needs and budget considerations.

The CISO should analyze, in depth, the value addition from information security projects and streamlined operations. The security managers,

Figure 1—Scope of Auditable IS/IT Risk Management Activities



selected by the CISO, should work with internal business groups in selecting the right tools that are effective and scalable in the given context.

The CISO

In the information security governance program, the roles and the responsibilities of the CISO should be well defined. One of the main responsibilities entrusted to the CISO is to draft a long-term information security strategy and obtain approvals from the board. This should be consistent with security plans for the individual systems. The CISO should be a strong mentor and should always encourage team members to adopt a consulting posture to address the security requirements of business groups and conceptualize the external threat landscape. The CISO should collect feedback based on the defined metrics and report to the board on the effectiveness of the information security program.

Prior to protecting all of the available information, initial attempts should be focused on identifying where critical information resides within the organization and who owns it. Data classification based on information criticality should be the foundation of any information security strategy. Once critical information is identified, success depends upon the controls used to protect it.

The Role of the Information Security Team

The information security team, which operates under the leadership of the CISO, should always be at the disposal of the business to consult and guide. Rather than spending all of its time developing security policies and implementing them, the information security team should work together on strategies to mitigate operational risk. Upper management should ensure that the information security team gets the right amount of visibility and respect from all of the core business functions. This can be done by framing information security as a core value and priority of the organization.

The priority of the information security team is to identify the areas of low and high risk in the organization. Risk frameworks should align closely with enterprise risk management (ERM) portfolios, if available. Such alignment helps avoid the ambiguity that can arise when there is conflict among individual risk management strategies for various information security and business continuity projects.

Mitigating Operational Risk

Adequate segregation of duties (SoD) and control responsibilities should be established in all of the functional areas of an organization. It is not always required to have professionals who are very technical or experienced perform basic tasks. For example, user access can be provisioned by a trained member of the security operations center (SOC) team. It is recommended to cross-train the operations team members, which can help in organizing and improving an enterprise's internal business continuity plan.

> **"The information security team... should always be at the disposal of the business to consult and guide."**

Many medium-sized enterprises use a hybrid model of outsourcing their security operations by maintaining a small team in-house primarily for budget control. Outsourcing security operations is a good choice for medium-sized organizations, as it helps them reduce the hassles of maintaining an always-functioning environment. The outsourced team may have considerable specialized knowledge on security operations acquired from its work with multiple clients—knowledge that is not possessed by the in-house department.

Of course, outsourcing is not without risk. There is always a chance vital information may leak about an enterprise's network, security architecture or vulnerabilities in the architecture. But this concern can be addressed through instruments such as nondisclosure agreements (NDAs).

For larger organizations, especially for those in the government or financial domains, it is always better to have an in-house team for primary security operations, as the degree of data confidentiality involved is relatively high. The incident response time of in-house teams always seems to be better than their geographically separated outsourced counterparts. In countries where weak legal systems exist, stringent criteria should be used to evaluate support contracts from outsourcing partners or security vendors. The terms, conditions and responsibilities mentioned in the contract should be completely unambiguous and workable by both parties. Any legal disputes arising during the valid contract period can increase the risk posture of the organization that outsources key security functions.

Effective strategies should be deployed in such cases to maintain the integrity of information security between the in-house team and the vendor. The technical capabilities of the vendor should be evaluated before the engagement. This can include a review of financial statements, past performance of the outsourcing partner and brand reputation. Some vendors will highlight extravagant team profiles during the initial discussions and fail to deploy them when the project is awarded. It is recommended to have an exit strategy and backup plan if any of the critical security vendors or partners fails to meet the set expectations, which would abruptly raise risk levels.

Conclusion

As experienced when working with a defense-sector manufacturer in United Arab Emirates, the importance and ease of having a well-structured information security system became apparent. The foundational pillars of information security were laid out by the government, and adopting them by an enterprise was extremely easy.

But in developing countries, such as India, many companies struggle to maintain a fully functional information security ecosystem. The expectations and responsibilities entrusted to CIOs and CISOs are quite high. In such cases, the CISO can take control by acting as the master integrator of information security, as that role is best suited to ensure that information security goals are well aligned with enterprise goals. This should, in turn, create a strong security ecosystem. Combined with an in-depth knowledge of the underlying architecture, the CISO can equip the information security team to better respond to information security concerns and cyberrisk.

Enjoying this article?

- **Learn more about, discuss and collaborate on information security management in the Knowledge Center.** *www.isaca.org/topic-information-security-management*