HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com or
publication@isaca.org

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Ganapathi Subramaniam heads the information security function at Flipkart *(www.flipkart.com)*, India's leading e-commerce marketplace. An accomplished professional with 24 years of industry experience, Subramaniam's passion and profession has always been information security. Until recently, he was employed at Microsoft Corporation India as its chief security officer, performing the role of a security evangelist within its sales and marketing support group. He has previously worked at Accenture and big four firms such as Ernst & Young and PricewaterhouseCoopers. As a conference speaker and columnist, he has addressed numerous gatherings of chief information officers and chief information security officers worldwide.

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 choose the Comments tab to share your thoughts.

Go directly to the article:

Q I run a newly established information security function in a European organization and work in an enterprise that is partially alien to controls. While there is fullest support from the top/senior leadership within the enterprise in terms of need for controls and their implementation, it does not seep into all levels below, and pockets are unfamiliar with security controls implementation. While such pockets may appear insignificant in terms of size, their support would make a material change.

How should I go about establishing the security function and building a culture that is supportive to controls implementation?

A Good question. This scenario is not alien and may sound familiar to a number of readers around the world, each having tackled it in his/her own way. I have also seen this question discussed at a number of conferences over the years.

The formula is simple: influencing without authority. There are many books on this topic, and my favorite one is by Robert Cialdini. As always, the following is an indicative list and not an exhaustive one:

> "The formula is simple: influencing without authority."

- Establish a security council consisting of key executives/ senior management from your organization whose roles can be defined as follows:
  - Approve the roles, responsibilities and accountabilities on information security and business continuity.
  - Approve the security road map aimed to reducing risk and helping operate in a risk-aware environment; the level of protection provided must be commensurate with the risk exposure.
  - Approve all information security policies and standards.
  - Approve all critical security exceptions or waivers to policies and standards.
  - Maintain risk and compliance oversight of the entire information security and business continuity program.
  - Provide sign-off on the open security risk.
  - Receive all security assessment reports/reviews.
  - Receive security metrics reports on security to ensure a holistic view.
  - Ensure security and continuity management move progressively and demonstrably toward achieving a mature and sustainable process.
  - Provide compliance oversight for the entire organization, function-specific and project-specific BCP development, and the testing process.
  - Monitor the implementation of tests as per the plan and schedule.
  - Review and approve the continuity strategy accepting residual risk.
  - Review reports on actual invocation of the plan and lessons learnt during crisis management.
- Categorize key individuals into multiple buckets—decision makers, influencers, sneezers (please refer to the book *Purple Cow*),[1] blockers/ aliens, friends/allies—and for each type have specific plans to win their support and trust. It may not be possible to achieve it in all cases. However, an influencing strategy suiting the types of individuals will help achieve our objectives.
- Ensure good negotiation. Know clearly that you may not be able to achieve your objectives on day one. Identify areas where you are willing to yield, as well as the nonnegotiable ones. For example, software license compliance may be a nonnegotiable item. Create a list of nonnegotiable controls and nice-to-have controls.
- Identify a list of allies within the organization who may be willing to help spread the message. Security must not be seen as the responsibility of only the security team.

- Tackle the blockers separately. Winning their trust and support is imperative to the success of the security team. Collaboration is a must. Talk the language of risk. If you cannot take everyone together with you, it may be difficult to roll out all the controls. Explain the impact to the business in the event of nonimplementation of security controls.
- Consider implementing detective or monitoring controls, if getting preventive controls implemented appears to be a challenge. For example, it may not be possible to implement Universal Serial Bus (USB) disablement for usage with removable media. Another option is to have a monitoring system that will alert you in the event of any attempt of data leakage/spillage.
- Remember that what worked at one organization may not work at another. Thus, try to put forward a road map aligned with your current organization's business agenda.
- Begin with policies, followed by infrastructure standards.
- Complete gap assessment using a standard controls framework such as COBIT® or ISO 27001:2013.
- Use all external drivers—industry regulators, external auditors and insurers—to drive your agenda.
- Roll out compliance and monitoring programs that include areas such as vendor security controls assessment.
- Create an incident management framework and implement it as a priority.
- Combine patch management with vulnerability assessments to contribute to the implementation of an appropriate controls framework.
- Have a clear metrics program and publish numbers. Numbers can provide the magic.
- Develop and roll out an awareness program.
- To repeat, speak the language of risk and business impact always. A number of controls can be seen as a theoretical need.

Q&A

ENDNOTES

[1] Godin, Seth; *Purple Cow: Transform Your Business by Being Remarkable*, Penguin Group, USA, 2003