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 have 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 How do I ensure that my organization has controls to protect itself from cyberrisk? In other words, what are the key controls that my company must implement to protect itself from cyberrisk?

A There are excellent security frameworks available as public documents that can be used as cybersecurity baseline controls.
Here is my list of essential controls:

1. **Patch management**—It is essential to have a structured patch management process. It does not mean that all patches have to be applied, but the enterprise has to make a conscious decision on which to apply and which not to apply. Patch management should be done as a priority for critical applications. While many enterprises apply patches for their IT infrastructure on a priority basis, it is common knowledge that the same rigor is not applied to patch management for software applications.
2. **Administrative privilege control**—It is key to remove administrative privileges from all and grant them only to a select few as determined by job need. Some individuals see it as a status symbol to hold admin privileges. Local admin rights must be removed for a significant majority of users.
3. **Dynamic analysis**—Conducting dynamic analysis, which uses behavior-based detection capabilities instead of the conventional approach of relying on the use of signatures, helps enterprises to detect malware that is yet to be identified. Such dynamic analysis can be undertaken at the enterprise's main gateway, the end point or the cloud, depending on the specific, relevant scenario. Customized sandboxes will help perform structured dynamic analysis.
4. **Host-based intrusion protection/detection system (IPS/IDS)**—Host-based IPS/IDS's detection strength is based on behavior instead of conventional signatures.
5. **Segmenting**—Segmenting the network based on business criticality is yet another essential control. Active Directory and other authentication servers should be able to be administered only from a selected number of intermediary servers called "jump hosts." Jump hosts must be well secured, and jump host access must be limited to a predefined list of users and network devices/equipment. Ideally, jump hosts will have no Internet access.
6. **Multifactor authentication**—Though a number of users view it as painful, it is essential to implement multifactor authentication in the interest of the enterprise.
7. **Internet access**—Direct Internet access from all end points/desktops/laptops must be denied and must instead be processed through a proper proxy.
8. **Passphrase policy**—For service accounts and privileged accounts, it is essential to implement a passphrase policy instead of a password policy; this is yet another area of common resistance.
9. **Web site access**—Access to web sites must be via their domain names and not by IP addresses.
10. **Removable storage media**—Usage of removable storage media must be appropriately controlled—though any restrictions on these are viewed by users as a loss of rights. Any enterprise keen to protect its sensitive information from leakage must restrict access and grant it based on a business need.
11. **User education**—It is not necessarily for all business users, but about educating the developers to write secure code and infrastructure experts to manage it in a secure manner. While users from the business appreciate the risk to the business, it is these experts from the IT world who require more convincing.

12. **External email exchange management**—When emails are exchanged with entities external to the enterprise, it is essential to adopt and implement protocols such as transport layer security (TLS).
13. **Strong asset management**—In terms of having an inventory of authorized devices, equipment and software are essential. Asset management is another area that does not get accorded its due priority.
14. **Web application testing**—Whether the web applications are developed in-house or by a third-party, it is essential to test them for vulnerabilities. They must also be tested via simulated attack scenarios.
15. **The staging environment**—Security testing such as a vulnerability assessment or a penetration test must be done in a replica of the production environment; otherwise, the gap between the environments becomes the weakest link in the chain.
16. **Wireless networks management**—Access must be granted on a need basis with adequate restrictions, and sundries must not be allowed to connect in an unrestricted manner. Ideally, network admission controls mechanisms must be in place.

This is a very indicative list and must not be deemed as exhaustive. Please choose a security framework relevant and apt to your enterprise and use it. These days, cyberrisk insurers also provide guidance documents that they consider prerequisites for any enterprise to buy cyberrisk insurance policies.

In my opinion, it is essential to identify relevant controls and implement them in the most appropriate manner rather than implementing a huge list of controls that are irrelevant and inappropriate. And, of course, the best controls rely on competent professionals to make them work effectively. Sadly, it is a globally accepted fact that there is a huge shortage of cybersecurity professionals. However, ISACA offers on cybersecurity *(www.isaca.org/cyber)*.