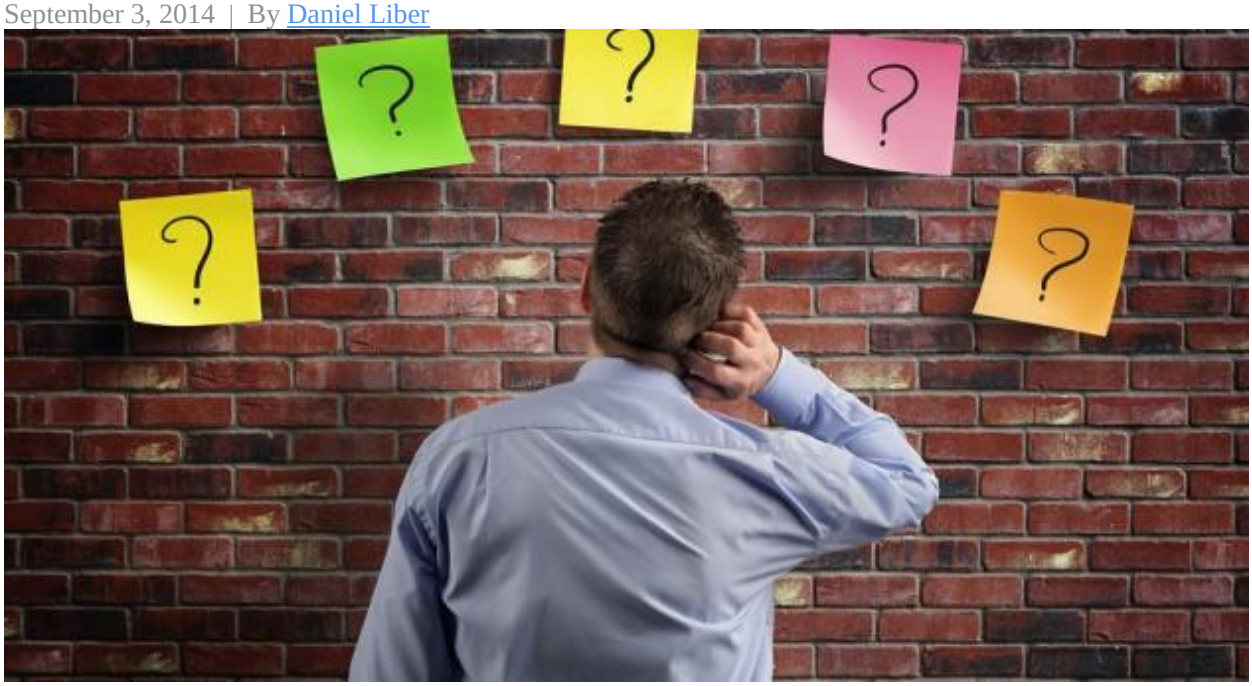
Safety & Security
Web Article

https://securityintelligence.com/dos-and-donts-security-management-in-a-growing-company/

Do’s and Don’ts: Security Management in a Growing Company

September 3, 2014 | By Daniel Liber



Security management can be a tedious job. Whether you are the chief information officer (CIO), chief technology officer (CTO) or even the chief executive officer (CEO), it can be hard to deal with possible risks and apply appropriate controls. For companies that maintain their relative size in terms of revenue, number of employees and target markets, this task may be somewhat easier. However, growing companies tend to forget that increasing any parameter means security management is shifting as well. Don’t stress out if your company hasn’t appointed a direct supervisor for the security field and you’re unsure what exactly is needed. For an easy jump start, the

following are the foundations and basic do's and don'ts that will help you understand the scope of this role.

Do: Supply Resources for Security Purposes

The most common mistake when considering — or reconsidering — the security management's agenda is providing the means to handle the targets that were chosen by the directives of security (or perhaps by the senior management itself). Like any other department in an organization, it's hard to do magic when you are running on insufficient funds. This is at the top of the list since growing businesses tend to focus on products and services development, sales and unbalanced finance distribution.

From a security manager point of view, it isn't easy to persuade a chief financial officer (CFO) or vice president of finance to increase your resources. However, it is sometimes only possible to fight fire with fire, and the best argument is that poor investments in security management will likely result in expenses that supersede the original budget.

Don't: Neglect Your Network Security

Short time frames for product releases, hectic development cycles and trying to please many customers — does this sound familiar? If so, there's a good chance that you might be trading off your company's network security to meet those demands. Perhaps a lack of developers or information technology staff are making you believe security threats are low-risk. Actually, these roles are vital for keeping your company's assets safe. You may have ninjas or rock stars for programming tasks, but companies also need a superhero for managing network security. Between domain separation, resource authentication and authorization and event audition, the responsibility is great. Treat these roles with great respect.

Do: Train, Train, Train

So now that you're all set with a neat budget and a security team, the next step toward proper security management is training. Not only is this objective important, but it is also ongoing. Like your company, the world of security is ever-growing and ever-changing, so your employees must undergo periodic training and certification. Due to the unique nature of growing companies, training sessions should be held more often than they would be at a more static enterprise since new employees will be quickly introduced to the company. It is also useful to use short yet powerful tools instead of long sessions. Occasionally forwarding an interesting webinar or composing a memo about a recent attack is a nonintrusive way to remind employees about security.

Don't: Kill All Security Issues at Once

It's easy to be misled when it comes to growing companies and security breaches. Even though there may be fewer issues to tackle, some are still difficult to solve and combat by implementing a proper solution. A common framework for risk management is still required, regardless of the number of security issues. There are many tools to help you plan the right security risk management program for your company. When they are utilized correctly, everyone should have a clear idea of what needs to be addressed immediately and what can be treated later on.

Do: Discuss Security Gates With Product Managers

When it comes to stable enterprises, the security policy and management is headed by the chief information security officer (CISO) and CIO, who supervise the entire department or team. The policy is usually self-dictated after a long history of balancing the needs of a business versus security. On the other hand, when it comes down to growing companies, there is a good chance the security team is small enough to sit in one room. It is also likely that the company's business units (product managers, business analysts, etc.) will be nearby.

Companies that wish to promote their products or services as fast as possible sometimes neglect to include security management throughout the required specifications. This “coziness” could be an advantage if you can walk to the next room over and talk through any gaps regarding features or requirements the business units are trying to promote.

Don’t: Avoid Security Feedback From Your Customers

When it comes to new products, such as a first stable version or a beta version, feedback is an ultimate must-have. Beyond quality assurance and the release, most enhancements come from the “battlefield” of customers’ installations and malfunctions. Some of these customers also test the products for security issues and provide feedback from testing results. Due to the nature of a growing company, the security-related feedback is sometimes pushed aside for feedback on functionality. It is not recommended to ignore any kind of feedback; however, some customers would prefer you address the security feedback first. This is usually asked by companies that come from security-oriented industries or in cases when the product relates to security. You do not want to find yourself on a security-indifferent vendors list.

Do: Know the Industry’s Way of Security Management

Perhaps you know everything about the market of your product, from dominant players down to the tiniest feature in a competing product. Obviously, you must own that knowledge to promote your company and product. But what about the security topics in your industry? Many companies are sometimes unaware of discussions held at an industry level that revolve around security. Unfortunately, these companies tend to get acquainted with those discussions only after they are breached or attacked. It doesn’t matter whether your company offers a service based on a public cloud or has a flagship product developed by numerous teams. Best practices, security guides and emerging controls are out there, and it’s up to you to catch up.

Don’t: Think You Are Incident-Proof

Another security that is somewhat forgotten is incident handling. Proper security management specifies actions and protocols in case of data loss, breach detection and critical vulnerability detection (in a product). In most growing companies, there is a minor to nonexistent incident response plan as most security efforts are narrowed down to active security rather than passive security. Planning ahead impacts not only security but reputation as well. Nobody can prepare for every vulnerability or breach out there — and that’s not the purpose of such a plan. The incident response planning should exhibit coverage for most threats that are relevant to your company or product. The key ingredient for that is mapping out threats, attack vectors and vulnerabilities in your business.

Traditional security management is considered to be mature and stable. New methodologies of software and business development forced companies (not just their products) to be scalable — a challenge withsecurity implications that must be addressed.

Tags: attacks | Chief Information Officer (CIO) | Chief Information Security Officer (CISO) | Chief Technology Officer (CTO) | Cybersecurity | growing companies | IT Security | Network Security | Risk Management | Security Intelligence | Security Management | Security Training