LENIC CONSULTING AND TECHNOLOGY SERVICES LIMITED

/'sə:vis/... we define service!

(Formerly CCJL Services Group Limited)

The Target-Aligned Information Security Framework

When technology fails...

We can almost guarantee that your company has made a significant investment in security mechanisms to protect your information technology infrastructure. But we are just as positive that, in spite of the extensive use of cutting-edge technologies, security holes still exist that can expose your company to the loss, exposure or corruption of its information assets, potentially resulting in millions of dollars in recovery cost, not to mention public embarrassment.

One of the reasons that seemingly first-class security measures often fail to do the job is that they are developed as isolated solutions to very specific types of threats and, therefore, are no match for well-structured, multi-faceted attacks. Also, because more and more of our information assets tend to be in electronic format, it is extremely tempting to rely only on technological measures to protect them. For example, intrusion prevention systems such as firewalls may eliminate external attacks on your web server but will not protect you if an employee decides to post sensitive information to a public online community.

ICT Security vs iSecurity

While ICT security focuses more on protecting a company's information systems and infrastructure, information security or *iSecurity* focuses on protecting the information assets themselves. It approaches the problem by first asking the question, "Why would someone want this information and how could it be used in a harmful manner?" It then continues on to look at the combination of events that must take place for someone to gain access to the information or modify its content. When we focus on the *information asset* itself rather than just the infrastructure that makes it available, a much wider concept of security emerges that includes everything from the electronic database that holds it to the number of people that handle it before and after it's stored away. By concentrating on the ultimate target rather than simply its environment, it is possible to develop a much more holistic security profile for the organization, one that can stand up to a wider variety of attacks.

Getting the bird's eye view

The establishment of an Information Security Framework ensures that the Bank's security policies and procedures are not developed in a vacuum but, instead, are a response to a comprehensive understanding of the nature of its information assets, the threats against them, the likelihood of realizing those threats and, finally, the consequences of ignoring those threats. A comprehensive iSecurity Framework also facilitates improved user compliance because there is a definitive reason for each procedure that is imposed upon them. This knowledge of the "why" also helps senior executives accept the need for certain levels of investment in information security.

Reactive vs Proactive Security

Companies can choose to respond to security threats in one of two ways. Either they adopt a *proactive* strategy and try to anticipate/protect against as many scenarios as possible or they take the *reactive* route and institute a variety of fail-safe mechanisms in an effort to recover quickly from an event when it does occur. Each approach has its advantages. Supporters of the reactive approach maintain that it is expensive and foolhardy to attempt to "wrap the organization in cotton wool" in the hope of preventing some as-yet-undefined attack. They argue that since security threats change every day, it is better to spend precious company dollars developing response mechanisms that ensure that the company is back to normal operations within the shortest possible timeframe.

On the other hand, advocates of the proactive approach focus instead on the unpredictability of the total cost of recovering from an incident and the impact the attack may have on future income. Their reasoning is that a hundred thousand dollars of prevention is worth millions of dollars in overtime, public relations and legal costs and lost revenue. In reality, the best approach to information security is a combination of both approaches by making sure that the investment in proactive security measures is placed where it provides the most benefit. An iSecurity Framework provides the necessary context for all security investment by developing a comprehensive threat profile, determining the likelihood of the occurrence of each event and then creating security profiles that mitigate against that risk.

iSecurity & Defense-in-Depth

The three most critical attributes of any information asset are its:

- ✓ *Availability* – How easily and how quickly can we access it?
- ✓ *Integrity* – Can we trust the content?

- ✓ *Confidentiality* – Is it only accessible by those authorized to do so?

All an entity needs do in order to launch a successful attack is to compromise one of the components of the human and technical infrastructure that protects these three attributes. These components include but may not be limited to perimeter monitoring systems, authentication systems and procedures, as well as the protection of the media on which the information resides or through which it is communicated.

Defense-in-depth refers to the use of a variety of multi-level and multi-lateral security mechanisms that address each of these components so that each asset has a complete security profile. Since it adopts a birds-eye view of the company's security profile, an iSecurity framework ensures that vulnerabilities in one area are supported by strengths in another, thereby ensuring that the whole is greater than the sum of the parts.

Even more benefits…

Another way that an information security framework reduces your company's risk is in its application of the theory of multiple "gates" to reduce the probability of a successful attack. In other words, the more locks an attacker has to pick, the more likely it is that the attack will be unsuccessful, either due to the increased likelihood of detection during an attempt or because the increased time and effort required acts as a deterrent. An iSecurity Framework also extends this multi-faceted approach beyond the realm of preventive mechanisms and into the area of response scenarios. So, in the event that an attack is successful, there is more flexibility in how the breach is detected, how the relevant personnel are alerted, how the source of the breach is identified and how the security "hole" is closed to future attacks.

What's inside the framework?

An iSecurity framework covers all aspects of an organization's security policies, beginning with who has the responsibility for governing the framework itself and ending with how the policies are monitored for compliance and readiness. It also includes strategies for dissemination, training and change management. The security policies themselves are quite extensive, addressing issues such as access privileges, identification and authentication, change authorization, non-repudiation, fail-safe mechanisms as well as monitoring, alert and response strategies. Because of its comprehensive approach, the framework will also include the company's policies on Business Continuity Planning, since this falls under the heading of *platform security*, one of the main components of defense-in-depth.

How do we get it done?

The iSecurity Framework is created using LeNic Consulting And Technology Services Limited's (LeNic's) proprietary Target-Aligned Security Framework (TASF) methodology, which was developed using years of research and refined through carefully monitored industry trials. Since the framework itself is a powerful tool that, in the wrong hands, can be used to launch a successful attack against the company, the majority of its development takes place internally and only certain sections should be publicly disseminated. In addition, since the framework affects all operations and procedures, it is extremely important that the framework is developed using a cross-functional team consisting of both management and line staff from among the various departments, with input from LeNic's iSecurity consultant only where necessary. In this way, key personnel feel as if they truly own the result and are more likely to be an asset when the time comes for dissemination and compliance.

The framework is developed in five (5) phases. Each phase begins with an orientation seminar in which new concepts are introduced, outputs are clearly defined and specific tasks are assigned to the various participants. Each new phase builds on the results of the phase that precedes it, so that the framework is documented as the project is executed rather than waiting until the conclusion of the final phase, by which time critical bits of information may have been forgotten. It is strongly recommended that the entire process take no longer than 120 days so that the results are still relevant within the prevailing environment. The process is designed such that the client will develop its own documentation templates for each phase, further ensuring that confidential information is not disseminated to external entities unless absolutely necessary.

What will it cost me?

The cost of the exercise is dependent on the extent of LeNic's involvement in the process. The project plan is designed so that our participation is limited to conducting the orientation seminars, reviewing the output of each phase for completeness and providing our clients with the information necessary for them to make informed decisions as to which security mechanisms will be best suited to their environment. In this way, we have managed to keep costs at a reasonable level. Due to a lack of in-house technical expertise, some of our clients may request that we assume additional responsibilities, which would naturally increase the overall project cost. However, regardless of any organizational or financial constraints that may exist, our primary focus is to protect you, our clients, so we will always find a creative way to get the job done so that you are completely satisfied with the final result. After everything is said and done, your security and the security of your information come first.

P.O. Box 5852 • Kingston 6
Tel: (876) 754-8986 / (876) 632-9326/7 • Fax: (876) 908-2249