Agility NETWORKS

e-Newsletter

September 2016

Don't confuse Regulatory Compliance with Data & Network Security! Part II

Protect what's most important!

In our July edition, we touched on the difference between being in compliance versus being secured (and how often businesses and executive teams misconstrue regulatory compliance for security). In this month's edition, we will finish our two part series by helping you understand proper expectations and a sound strategy in order to protect what is most important to your business.

Just a refresher from July:
"Regulatory compliance" can be defined as properly answering the questions and fulfilling the conditions of a given published set of requirements. A business must adhere to conditions from an external source (usually a governmental agency). Plain and simple, compliance audits are designed to capture the state of a given organization's operations at a given moment in time. It is black & white.
On the other hand, being "secure" must be seen as being fluid and ever changing --as the daily operations of your business change -- but inextricably entwined with what is critical for the continued successful functioning of your business. For each asset you possess, you must establish the appropriate level of scrutiny and exercise that scrutiny on a full-time and constant basis. You can put devices in place to serve as warning when the asset you are trying to protect may be in jeopardy of being compromised, but you must also anticipate that these measures could be circumvented, leaving you uninformed of the threat to your asset(s). Security always exists in varying shades of grey.

So...while you may invest anywhere from tens to hundreds of thousands of dollars to avoid a fine for being non-compliant/failing a regulatory audit, that entire investment may be pointless shortly thereafter if your security is penetrated and assets are stolen. More than half of businesses that suffer a significant data breach go out of business within six months. All your investments in regulatory compliance won't reverse that.

So it becomes crucial to include "being secure" in your decision making process during your business planning. In most security planning processes you begin by auditing and valuating your data and other business assets. Part of the reason for this is to assure that you don't spend more securing an asset than that asset is really worth. There are also some assets that you cannot put a value on, because losing them or having them compromised would put an end to the business. Ask yourself the following questions:

* Which of your company assets, if compromised or stolen, would cause your company to have to cease functioning?
* Which of your company assets, if compromised or stolen, would damage your company's brand and your differentiation from the competition?

If you start your process by identifying and securing these assets, many of the other assets become significantly easier to secure to the appropriate level required. You also achieve the peace of mind that comes from knowing

you've done everything possible to protect the business itself. And if some of this improves your ability to achieve regulatory compliance, then that's a bonus. Just remember, before you can think about complying with regulations you must be certain that your business can and will continue to function and your brand will retain and increase its value.

Also keep a close lookout for the point of diminishing return. Your security investments can range from a few thousand to hundreds of thousands or millions. There comes a point where the next increment in additional security may be small but the additional cost considerably more. Especially at points like these, it is important to gauge the need for security against the potential cost. What you have already accomplished may be sufficient, while the increment may be far more expensive than the asset is actually worth.

In the context of company data assets it is most important to put highest value assets first. This requires evaluation of each asset on several key criteria:

Confidentiality - What would be the loss if that data asset were exposed to others and was no longer proprietary to your company? For example, how much would Kentucky Fried Chicken suffer if their secret recipe was disclosed? Their product would be commoditized instantly, eliminating that key element that makes KFC special. Their business would, at the very least, radically change if not eventually end.
Valuation – How much, in pure monetary terms, would it cost your company if you lost a particular data asset? One good reason to do this is that many companies spend far more than a particular asset is worth protecting that asset. This often happens when particular assets fall within the scope of an upcoming regulatory audit and thus become artificially more highly valued, perhaps simply by default. It may often be better to save your money and take the risk.
Criticality – First and foremost you must clearly recognize what data losses would stop your business from functioning altogether. Neither compliance nor security matter much anymore when you're not there anymore. Exercise great care here. Many companies do not consider or appreciate the criticality of certain data entities, processes, and other assets that could cost them the company if compromised.
Availability – Often data assets are exposed because there is a perception that they need to be readily available and often to too wide a circle of potential users. More scrutiny is needed to determine just how available a given data asset needs to be. Often the cost of securing certain data assets can be reduced simply by restricting access thereby reducing the need for access security measures.
Integrity – There are two basic components to data integrity. The first is that the data is trustworthy. In a secure environment data is only modified appropriately by appropriately authorized people. The second component is to evaluate how important it is that, in the event the data is corrupted, that it be restored to a trustworthy state with minimal loss. Further, how important is it that the corrupting party be identified. As an example, say a nurse becomes unhappy with the hospital that employs her. Using her access she modifies a patient's allergy information. Subsequently the hospital administers a medication that this patient is allergic to. Obviously the hospital is exposed to litigation if the patient has a bad allergic reaction or worse. Clearly the first component of integrity has been betrayed, the second component is high as is the third.

So, it's far beyond simply having data compromised or corrupted. Simple exposure could possibly result in the end of your business. No business is going to worry about paying fines for lack of regulatory compliance when it's out of business.

To conclude, if you don't feel secure with your current security investments, go back to basics. Assess your assets, developing a strong understanding of which are truly critical to the ongoing conduct of your business in the way you wish to conduct it. Then identify those steps which must be taken to satisfy your concerns.

One of the challenges business owners face is that regulatory compliance and security are often “lumped together” in the budgeting and administrative process, when they really should be treated separately and addressed individually. This can actually be a positive when actions are taken and investments are made to assure regulatory compliance incidentally improve security, but owners need to remain cognizant of the primary distinction between regulatory compliance and security; that one assures satisfaction of a requirement and that the other assures the ongoing conduct of the business.

We hope you found this two-part piece to be interesting, educational and somewhat useful as it relates to your business!

Sincerely,
Your Agility Team
