Agility NETWORKS

e-Newsletter

June 2016

Great news! You passed your regulatory compliance audit!!! The bad news...you got hacked anyway.

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

The usual story goes something like this; Your team just passed its regulatory compliance audit with flying colors the first time out. The government can cease their threats about that $50,000 fine. The CEO is thrilled and the CFO is talking raises! Just then your colleague bursts into your office. "We've just lost $10,000,000 from one of our client accounts." "But how?" you ask, "We are fully compliant!!!" Well, you later find out that some hacker compromised the firewall and got into your clients credit card accounts. So the $10,000,000 lost is just the tip of the iceberg. The hackers also pulled hundreds of other customer records with all of their information. Your troubles have just begun... You did pass your compliance audit! You checked off every box – for compliance, but not security.

This is a story that is playing itself out at all types of businesses time and time again these days. The lesson here is, just because all the lights are lit on your firewall, it does not mean that your network (or the data contained within it) is secure. Unlike regulatory compliance, being "secure" is not a fixed, defined state at a given moment in time. Regulatory compliance requires specific answers to specific questions. If all questions are answered properly then you are considered "in" compliance as opposed to "out" of compliance, a simple binary decision. Yes or no, true or false, black or white. However, security is always in shades of grey.

Always keep in mind that relative security is the best we can ever hope to achieve because as long as there's a key... any lock can be compromised by anyone who can duplicate or approximate that key. Can we help you make it incredibly difficult? Absolutely! But we cannot make it impossible. Here are the relative definitions of each:

Compliance – Adherence to requirements from an external source (industry specific or government) -- could just be suggestions or guidelines but often carry specific penalties or other consequences. Once achieved, as signified in the passing of an official audit, compliance can usually lead to complacency.

Security – A protection program based on the custom abilities of the business and what matters most to the business and what allows it to continue functioning at the level of success and/or profitability its accustomed to. The return on security investments often comes in terms of reduced risk.

The fact is that regulatory legislation was never written specifically to address the issue of network or data security. Guideline documentation for legislation such as HIPAA barely even mentions security at all. Yet many executive teams --often times guided by their own misperceptions --continue to believe that achieving one automatically assures the other. This is not the case. Regulatory legislation will always, by nature, lag behind innovation in the real world that we face every day. The market innovates, then the government regulates. So no set of regulations

can ever assure that your network and your data are secure from the current threats, not that they are even designed to do so. They are not.

Regulatory Compliance Audits are designed to capture the state of a given organization's operations at a given moment in time. Once the company has prepared for a regulatory audit and the audit is performed, that's it until the next cycle. Mission accomplished! Job done. On the other hand, security requires a constant interaction between the management of a business and its assets. Constant scrutiny not only of the assets themselves but also of the measures put in place to protect them is an absolute requirement for an optimally secure environment.

This is not an interpretation or a matter of opinion. The fact is that regulatory measures just don't provide or assure full security. They were never designed to do so. Use PCI (Payment Card Industry) Security as an example. In a typical business PCI might account for 20% of their data management caseload. If you are fully compliant with the PCI standard your credit card transactions may be more secure. But what about the remaining 80% of your data? And while it's clear that 20% compliance can't equal 100% secure, it doesn't necessarily even mean that you are 20% secure. The two may overlap but they have no real relationship to each other.

On that note, stay tuned for our September edition and Part II of this series where we will share how to properly set your own expectations, develop the right strategy and plan accordingly so that you can secure and protect what is most important to your business.
