



Compliance ≠ Security:

- The good news is that you passed your regulatory compliance audit
- The bad news is that you got hacked anyway
- Set your expectations and your strategy to protect what's most important

June 2009

*Your CEO is thrilled
and your CFO is
talking raise. Your
significant other can't
wait for you to get
home to celebrate.*

*Just then your
assistant bursts into
your office.*

You're so smug.

Your terrific team just passed their regulatory compliance audit with flying colors the first time out. The government can keep their threats about that \$50,000 fine. Now you can sit back and bask in the glory. Your CEO is thrilled and your CFO is talking raise. Your significant other can't wait for you to get home to celebrate.

Just then your assistant bursts into your office. "We've just lost \$5,000,000 from one of the accounts." "How?" you exclaim, "we're fully compliant!!!" You later find out that a hacker compromised your firewall and got into your credit card accounts. So the \$5,000,000 lost is just the tip of the iceberg. The hackers also pulled thousands of customer records with all of their credit information. Your troubles have just begun.

But you did pass your compliance audit.

While this tale is fictitious, it's a story that is playing itself out at companies time after time. Just because you've achieved full regulatory compliance does not mean that your data and your network are secure.





Regulatory Compliance Does Not Mean You're Secure

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 executives, whether guided by their IT management or their own misperceptions, continue to believe that achieving one automatically assures the other. This is not the case.

We must treat our business' key life indicators first as well.

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.

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 of an optimally secure environment.



This is not an interpretation or a matter of opinion. The fact is that compliance just doesn't have the basic ability to provide or assure all security. It was 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're 20% secure. The two may overlap but they have no real relationship to each other.



Compliance is not the End of the Spend – So where do I put my investments?

*...before you can
think about
complying with
regulations you
must be certain
that your business
can and will
continue to
function...*

The answer depends upon what's most important to you; playing by the rules, or keeping your business running. The decision making process is similar to coming upon an auto accident and commencing to set the broken leg one of the drivers suffered, only to notice afterward that the driver is no longer breathing and his eyes are fixed and dilated. This is why first responders are taught to check for breathing and bleeding before anything else. We must treat our business' key life indicators first as well.

Companies invest heavily in regulatory compliance because they're supposed to, but the fact remains that most companies in business today are not fully compliant with the regulatory requirements related to their business. So while you may invest anywhere from tens to hundreds of thousands to avoid a fine, 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 the investments in regulatory compliance won't reverse that.

So it becomes crucial to include this decision making process in 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 our company assets, if compromised or stolen, would cause our company to have to cease functioning?**
- **Which of our company assets, if compromised or stolen, would damage our company's brand and our 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 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 does come a point where the next increment in additional security may be small but the additional cost considerably more. Especially at points like these is it important to gauge the need for security against the potential cost. What you've already accomplished may be sufficient, while the increment may be far more expensive than the asset is actually worth.

Protect What's Most Important

Popular self-help author Stephen R. Covey urges readers to distinguish between what is merely urgent and what is important when he says we should "put first things first."

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:

Criticality

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.

Valuation

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.



Confidentiality

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 the Coca-Cola Company suffer if the secret formula for Coke Classic were disclosed? Their product would be commoditized instantly, eliminating that key element that makes Coke special. Their business would, at the very least, radically change if not eventually end.

Availability

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

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 possibly dies. 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 can result in the end of your business. No business is going to worry about paying fines for lack of regulatory compliance when they're out of business.





*Would your
business stop if
you couldn't send
or receive email for
any period of
time?*



How Do I Get Started with this Evaluation?

First embrace the idea that OBJECTIVITY is your best friend. The thought here is similar to giving a potential client or employer your references. Of course you're going to give them references that you know will be positive about you. Similarly, if you assign a "security team" to do "penetration testing" on your network, you're going to have them attempt to hack servers that you assume to be most secure. It's human nature.

But remember that your objective here is to protect and secure your brand, your business, your life's blood. You want to end up assured that your most valuable assets are as well protected as possible, not just that you can get past an audit. So start by engaging an experienced professional auditor to conduct a comprehensive Information Criticality Assessment. This will focus on what's most critical to the ongoing operation of your business.

In doing this it is also important to take your own interests out of the equation. If the auditor asks you what's most important, you may be tempted to say, as an example, "E-Mail" because you spend most of your day on email. But would your business stop if you couldn't send or receive email for any period of time? Would you not be able to substitute phone calls during that outage? But what about your point-of-sale system? If it was compromised could you or could you not switch back to manual ticket writing processes until it was restored? An objective, third-party auditor will find those elements that, if compromised, would compromise your brand and thus your business.

Security Professionals call this Open Scope Testing. You don't tell them where to look or what to look for. They survey everything and find the paths of least resistance to compromise those things that are most critical to your business. Whether it's physical access, electronic, social, or access through inherent malfunctions in your systems, an objective third-party auditor can quickly focus on what your business needs to do to become "secure" as YOU define secure. Only then will you find not only the peace-of-mind you need, but you will likely also find that you have more than sufficient budget remaining to focus on simple regulatory compliance issues.



What's the difference between regulatory compliance and security?

Just because all the red lights are lit on your firewall doesn't mean that your network or the data contained within it are 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. Security is always in shades of grey. 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. We can make it incredibly difficult, but we cannot make it impossible. Relative definitions of each would be:

Compliance

Compliance - adherence to requirements from an external source - 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 leads to complacency.

Security

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 profitability they are accustomed to. The return on security investments often comes in terms of reduced risk.

So "secure" must be seen as being as fluid and changing as the daily operation of your business changes, but inextricably entwined with what is critical for the continued successful functioning of your business. For each asset we possess, we must establish the appropriate level of scrutiny and exercise that scrutiny on a full-time basis. We can put devices in place to warn us when the asset they are protecting may be in the process of being compromised, but we must also anticipate that these measures can be overcome leaving us uninformed of the threat to our asset.



Just as each company is different, its brand is different, its differentiators are what make it different, and its risks and assets are different, each company needs to secure its risks and assets differently.

Also, regulators seek to make everything regular; that is, they seek to achieve uniformity and consistency of method among members of a given community so that everyone does certain things in exactly the same way to assure that nobody has an advantage and nobody takes advantage of anyone else. Security simply cannot come in a one-size-fits-all package. Just as each company is different, its brand is different, its differentiators are what make it different, and its risks and assets are different, each company needs to secure its risks and assets differently. And since each day brings new potential threats each company must secure its assets differently today than it did yesterday, and differently again tomorrow.

While “regulatory compliance” can easily be defined as properly answering the questions and fulfilling the requirements of a given published set of requirements, security must be defined as having the sense that all of your assets are protected from compromise or theft to a level appropriate to the value of each asset. Regulatory Compliance is black & white, while security always exists in varying shades of grey.

The potential backlash of this is also important to observe. When investments in regulatory compliance are mistaken for investments in security organizations run the risk that those responsible when security is breached will use regulation or those responsible for compliance with it as their scapegoat, explaining that all the investments went there leaving them incapable of properly securing the assets, or even faulting the inadequacies of the regulatory legislation for their failure.

Ultimately, since achieving security can equal perpetuating the business, the responsibility for security rests with the business in its entirety.

Getting Back to Basics

The simple fact is that regulatory legislation will always, by nature, lag behind innovation in the real world that you 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.



*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.*

When world markets turn weak, and investors don't feel secure in their current investments, they go back to basics like gold and other precious metals. Apply the same wisdom here. 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 managers 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 taken and investments made to assure regulatory compliance incidentally improve security, but managers need to remain cognizant of the primary distinction between regulatory compliance and security; that one assures satisfaction of a requirement and the other assures the ongoing conduct of the business.





Always remember to protect what matters most, and that regulatory compliance is not necessarily going to always be your foremost concern.

Decisions regarding security are business decisions more than they are technical decisions

Recommendations

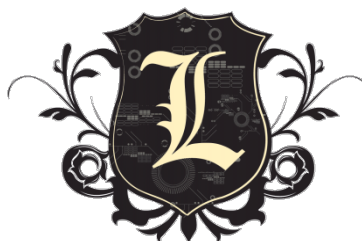
- Always remember to protect what matters most, and that regulatory compliance is not necessarily going to always be your foremost concern. Bypass “technical advisors” who do not address the business issues with you first. What matters most may not always be data or even technical in nature. True security experts focus on business value when assessing where to focus first. When they go to determine how vulnerable you are they attack your business’ vulnerabilities, not just your technology.
- Both your degree of regulatory compliance and the security of your valuable business data assets are issues that must be addressed by professionals, just like your accounting, legal issues, or medical concerns. Both are very much health issues, regarding the health of your business. Select a professional services provider who understands the distinction between compliance and security who can make sure that you are properly and adequately addressing both.
- “Secure” goes well beyond your data network and your data. Decisions regarding security are business decisions more than they are technical decisions. You must maintain security at every level, from your physical premises to your personnel selections to everything that comprises your business, maintaining a global view of security for your business.
- Immediately accept that objectivity is something you and your personnel are incapable of when it comes to assessing, evaluating, testing, or otherwise challenging your own security measures. You want to engage experienced professionals who can and very likely will breach your best security efforts. Only by exposing these weaknesses can they be properly addressed, and, make no mistake, they are there.
- Industry experts agree that adopting and constantly maintaining a best-practices approach to information security is one of the best ways to facilitate regulatory compliance.



Remember that everything you spend on compliance and security is wasted if you don't end up secure

Your greatest enemy is complacency. You must maintain constant vigilance at all times.

- Keep a keen eye out for “Security Budget Bloat”. One of the litmus tests one should apply when gauging the value of investments in regulatory compliance is to ask what security improvements will also be brought about by the investment.
- Be aware that many requests for investment in regulatory compliance are actually being made to improve security with the foreknowledge that the likelihood of approval for the expenditure is greater if compliance is the given reason. Permit this.
- Write to the agencies that regulate your industry. Encourage them to show more awareness of the importance and need for improved security. If any of their requirements reduce your security let them know that so they can fix it.
- Regulations tend to lag behind innovation. Government agencies write regulations at a given moment in time. Then the technology industry innovates. Then government responds to that innovation with more regulations. Try to foresee and get ahead of this curve to increase your preparedness and reduce your overall expenditure.
- Your greatest enemy to security that is commensurate with the value of the assets is not the hacker out there looking to attack. Your greatest enemy is complacency. You must maintain constant vigilance at all times.
- Remember that everything you spend on compliance and security is wasted if you don't end up secure. Prioritize information security measures first, then regulatory compliance issues.





Security, at the end of the day, is a feeling, one might call it a “gut” feeling that you know you’ve done everything you can do to protect that which is most valuable to you.

A Few Closing Thoughts

Especially at a time of such economic upheaval it would be hard to find anyone who would believe for a moment that doing what your government tells you to do is the best and most important thing to do? This is not to suggest or promote anarchy, but rather to make the statement that we are each ultimately responsible for ourselves, and the “right to bear arms” extends to strategic business weaponry used to protect ourselves by securing our assets to our own satisfaction. As any good business strategist will tell you, the goal must always be to “protect and grow.” You cannot grow if you do not protect.

Regulatory Compliance is, by design, a set of empiricals designed to achieve parity or consistency amongst a community of similar entities. There is no emotion involved. There is no passion. It’s simply a metric which must be satisfied.

Security, at the end of the day, is a feeling, one might call it a “gut” feeling that you know you’ve done everything you can do to protect that which is most valuable to you. You are deeply personally involved. Your passion for it must run high. Certainly while you may do your utmost to comply with regulatory legislation, it will not be at the cost of compromising that which keeps your business running and healthy.

About LARES

Lares is a vendor-independent security consulting firm that helps companies secure electronic, physical, intellectual and financial assets through a unique blend of assessment, testing, and coaching. We are committed to identifying the key assets of your unique business and creating a customized strategy to protect you in today's volatile business environment and beyond. Certified Information Systems Security Professional (CISSP)

The Lares team is comprised of extensively trained and highly experienced information security professionals who are dedicated to providing a comprehensive approach to organizational information security. Our approach allows our clients to make informed decisions about their information security programs and effectively "protect what matters most".

To learn more about Lares and how we can benefit your company's security please call us at (720)217-3087 or visit us at <http://www.lares.com>.