Realtime publishers

Data Protection and Compliance in Complex Environments

The CSO Executive Series

Primary Concerns of Regulatory Compliance and Data Classification

sponsored by

CREDANT®

We Protect What Matters

Kevin Beaver

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Primary Concerns of Regulatory Compliance and Data Classification

Information systems complexity creates the ultimate irony when it comes to managing business risks. For the longest time, we've strived to achieve a certain level of computer system functionality. For instance, people want to be able to access backend databases through a pretty graphical user interface (GUI) over their mobile devices—and they want it now! With necessity being the mother of invention, IT vendors, architects, and managers have responded by providing such access. Unfortunately, the law of unintended consequences has created a situation whereby information systems have become so complex that data protection is seemingly impossible. Add regulatory compliance into the mix and you—as an information security executive—have an ostensibly treacherous road ahead.

Drivers and Motivators of Data Protection

Ideally, businesses would do what it takes to protect data simply because it's the right thing to do. However, many executives somehow missed that memo or skipped over that class in business school. More appropriately, the selfless concern for others is not necessarily the mode of operation for most businesses. So what happens when businesses don't regulate themselves? Government agencies and industry regulatory bodies step in and make them do it. Enter compliance as we know it today.

Privacy and security regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Payment Card Industry Data Security Standard (PCI DSS), and the state breach notification laws in the US, as well as international regulations such as the UK Data Protection Act, the German Federal Data Protection Act, and the Australian Privacy Act, to name just a few have become the driving force behind data protection in business today. The mantra is "We're compliant with this and that regulation, so we're good to go." It's not that simple, however. Compliance in and of itself is not a good strategy. For data protection to be effective long term, we have to look at it from a risk management point of view.

The Compliance Crutch

Simply securing data because a third party says you have to does not fix the underlying problem. However, it does make people happy—at least for the short term—which explains why compliance is the ultimate "destination" for many businesses today. The problem is that you simply don't know just how far it will get you and just how long it will last.

Taking things a step further, you have to consider the value data protection measures bring to the business. The numerous fiduciary responsibilities that go along with running a business—data protection included—make logical sense. Then there's reality. When you look at the primary function of any given business, it's to create and maintain customers. This means selling goods or services for a reasonable price that allows the business to create a satisfying experience and keep people coming back. In order to do this, the business needs to keep costs down. Be it marketing costs, manufacturing costs, operations costs, or IT and security costs, money that's not "wasted" goes directly to the bottom line. Alas, many people see data protection as one of those things that takes money away and doesn't give anything in return. Certain people who believe this are exactly right. Not because of their insight but because of how they're going about their data protection initiatives.

As with anything else in business, there's a right way and a wrong way to ensure the protection of sensitive business data. Data protection in today's complex environments requires a reasonable mindset, solid processes, and a good set of tools to make things happen. When this approach is taken by everyone involved, the business value of data protection will shine through.

Working with Other Stakeholders

As an executive in charge of security and compliance, there are three roles—be it a single person or a team of people—you'll likely interface with on a periodic and consistent basis: audit, compliance, and legal. It's easy to view these people as your enemies who simply exist to point out all your shortcomings. However, if you approach this from the perspective of how you can all work together and how they can help you accomplish your goals, you'll find it a much easier path to travel. The reality is that before you can be successful in any business endeavor you need to have the right people on your side. Might as well start with the people with whom you're interacting with the most.

Working with audit (be it internal or external) may prove to be the most challenging of the three. I've personally found most auditors to be extremely helpful and easy to deal with. However, there's a certain stigma associated with the audit function, and that perspective can create an environment of "us versus them." If not handled properly, this situation can evolve into a culture that continually works against the very things you need to accomplish. Rather than focusing on the negative, be up front with them regarding your needs and find ways to not only meet halfway but also to improve the visibility of data protection and compliance overall.

Working with compliance tends to be more of a strategic partnership. The person in charge of compliance is responsible for keeping up with a myriad of state, federal, and international privacy and security regulations, and you're in charge of making it all happen, so there's going to be a lot of collaboration. From their perspective, it's mostly about adhering to this, that, and the other regulation. For you, it's about protecting data by analyzing all the threats and vulnerabilities present in the business. Given these differing approaches, it's important to work closely with one another. However you advance toward the end result, your relationship with compliance is one you'll want to focus on nurturing and building because neither of you can go it alone.

Finally, working with legal counsel (be it internal or external) is most certainly something you don't want to take for granted. This is true for two reasons: 1) this person can provide insight on business risk you may not have thought about before and 2) this person can help you get things done. In the past, it seemed the majority of lawyers I worked with were not very tech-savvy and thus couldn't contribute much in the way of information security. However, this is changing and has a profound effect on compliance and data protection. Given that such lawyers have the ear of executive management, having them on your side could prove to be the most valuable relationship of all.

How to Get the Buy-In You Need

Being a decision maker doesn't mean it's going to be easy to accomplish everything that needs to be done. You still need to be able to get people to buy into what you're proposing. The most important thing you can do to get subordinates, peers, and executive leadership on your side is to build trust. This means doing what you say you're going to do and being open to other people's opinions. People will only buy into your ideas when they're convinced that you're a person of integrity and on their side. Furthermore, trust is as much competence as it is character, so it's important to maintain your technical edge and make smart choices in your job.

You can also get people on your side by staying involved with other areas of the business outside of security and compliance. In fact, analyzing the job functions and responsibilities of others can highlight areas of risk that you might not have known about otherwise. Also, it's critical to continually share the value and positive results from your efforts with your peers and executive management. There's nothing worse than great ideas and accomplishments that no one knows about.

Finally, you have to be prepared to answer "why" when it comes to your compliance and data protection expenditures. This is especially important when it comes to people who can actually do something about it. To be successful with this, it's important to understand that people are motivated by two things: the desire to gain something and the fear of losing something. You have to put what you're proposing in terms of the people you're selling it to. What is it that motivates them? What turns them off? Tweaking your approach and presenting your ideas in this fashion can help you seal the deal—and accomplish your own goals—more than anything else long term.

When working with these stakeholders, it's important to remember that you're all in the same boat working towards a common goal of ensuring regulatory compliance and minimizing business risks. If you approach these relationships with this mindset and seek out how you can help each other and learn from one another, chances are you'll end up building your credibility and improving your relationships with many other people who can also help you succeed.

Building Blocks of Data Privacy, Protection and Compliance

Developing a solid program for minimizing business risks and ensuring ongoing compliance depends on several key factors. First you have to have a clear mission and set of goals which outline what you're trying to accomplish. Everyone's approach is going to be a little different, but by and large, your key vision will likely involve implementing the proper information systems controls in order to keep threats from exploiting vulnerabilities that lead to business risk. You'll then have specific goals stating what you want, when you want it done by, and what has to be done to make it happen.

First and foremost, you have to understand what's at risk. You can't secure what you don't acknowledge. Knowing where things stand at any given point in time is where you ultimately want to be. This involves two fundamental building blocks of managing information risks: visibility and control. You have to have insight into your environment and the proper controls in place before you can provide an honest assessment of information risks. Doing so requires balancing documentation along with solid business processes and reasonable technical controls. From data classification standards to security policies to contingency plans, everything is dependent on how well you've poured the foundation.

Another critical element is for you to understand the needs of your customers (internal and external) and being able to balance security with productivity and usability. A surefire way to pigeonhole yourself and the overall information security function within the business is to put a set of rules in place that get in the way of doing business.

When it comes to compliance, if you approach these things in the appropriate manner, compliance will emerge as a byproduct of it all. Rather than letting compliance drive your data protection needs, it can be the other way around, which will ultimately prove to be a smarter way of going about it.

In order to successfully manage your information risks, you need to know not only what you're doing but also that what you're doing is appropriate. You can't just go by the book. Data protection and compliance are not black and white, on or off. A fundamental requirement of managing this properly is having the ability to understand the technical side of the equation. Sure, security and compliance are mostly business-oriented issues, but understanding the nuts and bolts of how it all works is invaluable. Even if you're not a techie, it's never too late to learn software and networking essentials. Such skills will undoubtedly help you make better data protection and compliance decisions moving forward.

Planning Your Controls Framework

Information security and audit standards and frameworks are popular for a reason: other people have already done half of the work you're responsible for doing. However, you can't just jump in head first throwing some standards in place and calling it complete. Picking the proper controls framework can be tricky. You want to be able to manage risks in the best way for your business. But you also need to please your auditors and have business partner and customer needs to satisfy as well. Further complicating the matter, your IT and security staff may not be familiar with managing things this way, so it can take some adjustment.

From Control Objectives for Information and related Technology (COBIT) to Information Technology Infrastructure Library (ITIL) to International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 and 27002, you can go—and are often pulled—in many directions. Many larger organizations have adopted COBIT and ITIL, while many midsize and smaller businesses often choose the ISO/IEC route. There's no one best framework. In the end, the right option is often to combine aspects of the various control frameworks into a hybrid system that best suits your business. The most important thing is to understand that there's no wrong choice.

> **When Best Practices May Not Be the Best**
>
> Be careful falling into the "best practices" trap. There's a baseline of what common businesses need to successfully manage information risks, but beyond that every situation is different. Simply relying on what other people think is the best way to manage such risks does not—and will not—translate directly into what's best for your business. This underscores the importance of understanding what's truly at stake along with what level of compliance you need to reach and then balancing both with your business culture, politics, and unique needs.

The laws and regulations your business is obligated to comply with makes adopting a controls framework even more important. But what extent do you need to plan things out in order to meet some of these obligations and objectives? Do you really need to have a unique set of controls in place for HIPAA/HITECH, yet another for PCI DSS, and so on? Absolutely not. If you take a close look at the various privacy and security regulations, they all have one thing in common: they're essentially the same! Sure, the wording and approaches are somewhat different and they each have their unique caveats, but by and large, each and every government and industry regulation wants to ensure that a management system is in place for maintaining the confidentiality, integrity, and availability of sensitive information.

By managing information risks at the highest level possible, you can accommodate all your business' regulatory requirements in one fell swoop. The only way to do this is to have a solid security controls framework in place. The next article will go beyond the "why" and "who" and explore "how" to implement these essentials to ensure that you manage data protection and compliance in the most effective and cost-efficient ways possible.