Realtime publishers

Implementation Strategies for Fulfilling and Maintaining IT Compliance

Kevin Beaver

sponsored by

QUEST SOFTWARE®

Copyright Statement

Chapter 2: The Costs of Compliance and Why It Doesn't Have to Be So Expensive

One of the greatest impediments to compliance is the perceived cost of doing things the right way. Business leaders struggle enough trying to justify the most basic of IT expenditures. Now some government bureaucrat or industry regulator is requiring that they spend even more money to become compliant with their rules. The question becomes: Where's the payoff? How are all of these compliance controls really going to serve the business long-term? These are legitimate concerns indeed.

> **Remember**
>
> The short-term goal is to be compliant and close the compliance gaps. The long-term goal is to minimize business risks.

Overhauling your IT systems isn't cheap—or free—but it certainly doesn't have to break the bank in the name of compliance. That is, if you approach the issue with the right mindset.

Realities of What It Will Cost to Become Compliant

Don't let the supposed high price tag of compliance scare you off. You've got some work to do before coming to any conclusions. First, it's imperative to understand exactly where things stand in your environment. That is, what are your compliance gaps and information risks? Odds are things are not as bad as it may seem. The best way to go about understanding what compliance gaps and information risks are present in your environment is to perform a security assessment. To be specific, an information risk assessment that looks at all the big areas of IT in your business.

Many people make the mistake of putting security controls in place and documenting their policies and procedures without first understanding what threats, vulnerabilities, and overall business risks they're up against. Furthermore, many people address the compliance "basics" like firewalls, antivirus, and data backups without first understanding what's actually required of them.

> **Tip**
>
> Regardless of what anyone may be advising you, don't purchase a single technology, document a single policy, or implement a single business process in the name of compliance until you figure out what you're up against.

An in-depth information risk assessment looks at all aspects of IT in and around the business including operational and administrative processes, technical systems, physical environment, and people. Figure 2.1 shows the core elements of an information risk assessment.

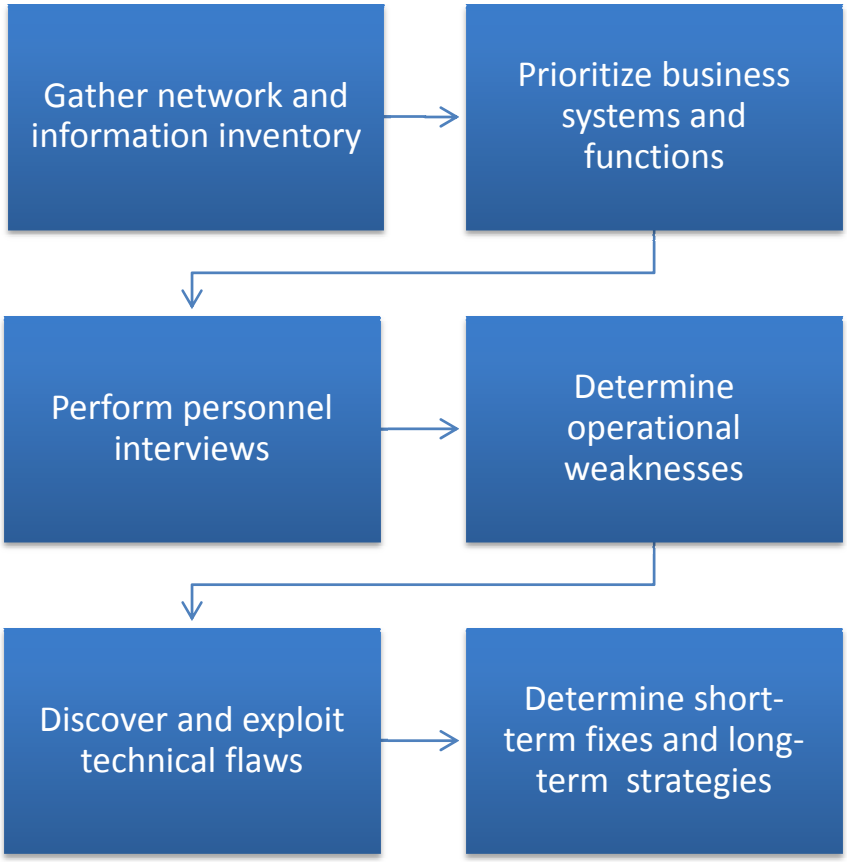

Figure 2.1: Essential elements of an information risk assessment.

Many people go about performing information risk assessments in different ways, but the overall goal is to determine where things currently stand and how the issues can be improved over time to minimize business risks. Ultimately, you'll want to come up with a plan that addresses your business' immediate needs as well as longer-term requirements.

Looking at the bigger picture, the compliance tie-ins with information risk assessments are clear. In fact, a common information risk assessment deliverable is a compliance gap matrix that outlines areas for improvement as they relate to the various regulations your business faces.

Remember

There's a reason regulators require a risk assessment in many of the information security and privacy regulations such as HIPAA, GLBA, and PCI DSS. If you don't take a risk-based approach, there's no reasonable way to understand where you need to direct your attention and resources.

Once you perform an in-depth information risk assessment, you'll know where you need to focus your time and money. First and foremost, you'll want to address the urgent issues on your most important systems, such as the ones highlighted in red in Table 2.1.

	High Likelihood	Medium Likelihood	Low Likelihood
High Impact	• Credit card data stored on unencrypted laptops • SQL injection present on healthcare portal exposing ePHI • No periodic and consistent security tests being performed	• No data backups being performed on critical database servers • Travelers sending unencrypted emails over unsecured Wi-Fi • No formal user awareness and training program	• Outdated and untested disaster recovery plan • Weak OS passwords on development workstations
Medium Impact	• No security incident response plan • No formal security oversight committee exists	• Lack of endpoint controls on IT computers that house security policy documents • User identity and access management process leaving unused accounts enabled	• Exploitable missing patches on an internal Web server housing HR data • Missing security policies
Low Impact	• Visitors browsing the Internet using their personal laptops on the corporate network	• Outdated anti-malware software on standalone training computers	• Poorly-configured software exposing marketing Web site data

Table 2.1: Results of a qualitative analysis can help determine information risk.

These results are a very simplified view of the outcomes of an information risk assessment. Your methodology, findings, and priorities will differ. However, the IT-related weaknesses and risks that matter will surface if you dedicate the time to look at things with a critical eye.

Once you've resolved the most immediate needs (high-priority and high likelihood of occurrence), you can move on to the medium-priority issues and so on until everything is in check, at least for the time being. After you've reached a reasonable level of security and compliance, you can then focus on expanding your reach across all parts of the enterprise. This includes other areas that may not fall within the scope of compliance regulations but need to be secured nonetheless.

Remember

Focus on the basics when starting out. Look for and deal with what's urgent and important and then grow your compliance and security programs out from there.

Every situation is different but generally speaking there's really only a small set of technologies needed to achieve and maintain compliance. You don't necessarily need the latest whiz-bang technologies, you don't have to go to the cloud for solutions, and you don't have to follow the masses who are buying into all the marketing hype. This goes back to your information risk assessment. Where are your gaps? Where are you bleeding? What technologies and business processes are going to be needed to do the right things long term?

You may be surprised by what can be accomplished in terms of compliance and minimizing business risks by simply using what you already have at your disposal:

- Network security controls such as:
  - Firewalls with intrusion prevention and layer 7 protection capabilities
  - Router access control lists (ACLs)
  - Ethernet VLANs
  - Wireless network controls such as WPA-PSK and RADIUS
- Operating system controls such as:
  - Microsoft Active Directory (AD) for user management
  - Windows Group Policy Objects (GPOs) for policy enforcement
  - Data backup software
  - Patch management software such as Windows Update and Windows Server Update Services (WSUS)
- Application and database controls (including homegrown solutions) such as:
  - Secure application development platforms such as C# and Java
  - Proper input validation
  - Stored procedures
  - System activity monitoring, logging, and reporting
- Mobile device controls such as:
  - Password protection and intruder lockout
  - Storage encryption
  - Remote wiping
  - Data synchronization

Free built-in controls such as these can serve many people well. However, you might find for various reasons that you need more robust enterprise controls offered only by third-party vendors. Either way, by focusing on your essential needs, you can knock out a lot of compliance requirements without having to spend a lot of money.

After you determine your overall information risks, you'll likely find that they can be categorized (see Figure 2.2).

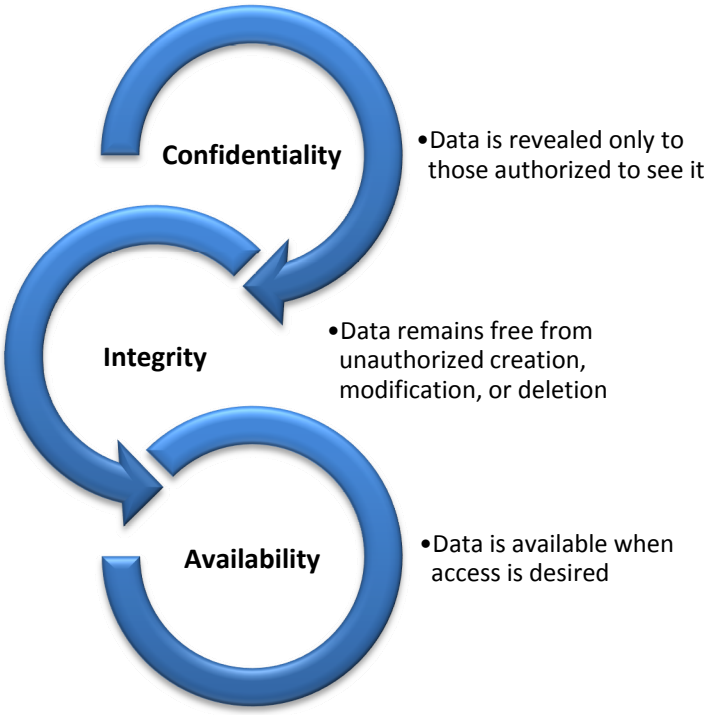

Figure 2.2: The three components of information security and compliance.

Since the beginning of IT as we know it—dating back several decades—confidentiality, integrity, and availability have been the cornerstones of information risk management. Many of the regulations reference these cornerstones in their requirements because the reality is you're not going to be able to reach any semblance of compliance without addressing all three areas through technology, business processes, and people.

As you move forward with your compliance initiatives, it's important to think long-term and build out your environment to also ensure your network, applications, and data aren't being attacked. If you look at the higher-level issues associated with network attacks and data breaches, you've got to make sure that all of your technologies are working in concert to ensure that things are in check in all the right places. This includes factors such as:

- What technologies are in place to assist with user provisioning (adding new accounts), re-provisioning (changing users roles and privileges), and de-provisioning (removing user accounts)? Are your business processes and documentation aligned with your technical needs?
- How does your network traffic enter and leave the network? A great way for malware infections (that is, advanced persistent threats), employee Internet abuse, and vulnerability exploits to occur is to not fully understand what your protocols, top-talkers, and so on look like—and should look like—on the network at any given time.
- Are you being alerted to the proper security events? Are your operating systems (OSs), databases, and applications configured properly to record and track suspicious activity?
- Can you honestly say that you know which information is stored where on the network? Given the complexities involved, it's easy to overlook unstructured information spread across the enterprise especially on workstations and mobile devices where it's often assumed to not even exist in the first place.
- What endpoint controls do you have in place for malware protection and patch management? Have you hardened your systems from attack based on widely-accepted standards from NIST, The Center for Internet Security, and even the vendors themselves, such as what Microsoft provides in its free Security Guides?
- How are you keeping up with your mobile devices? Are you doing enough? Laptops, netbooks, tablets, and smartphones are very likely creating the largest compliance gaps and information risks in your business today.

Being able to answer these questions with confidence is a maturation process. It requires making sure your technologies are supporting what you're doing and what the business needs long-term and that they're not just in place to please an auditor or fill a compliance check box.

Be it lack of time, information systems complexity, or whatever, the need for continual control and visibility are placing a bigger and bigger burden on us each year to the point where it's tough to keep up. This is where automation comes in. Automation is arguably the most important element of a solid compliance program. You're going to have to rely upon automation wherever possible—it is a requirement of long-term compliance (see Figure 2.3).

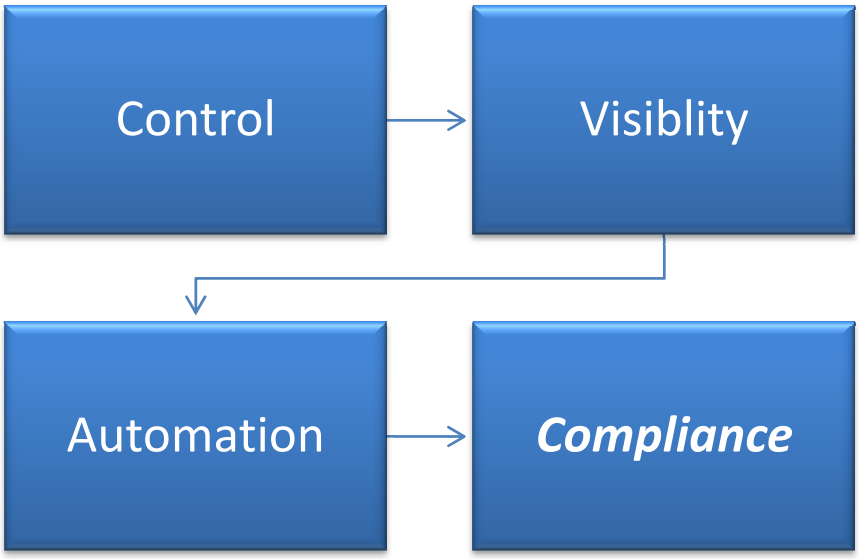

Figure 2.3: The essential flow that supports the compliance process.

Money properly invested in automating compliance can be money very well spent. The initial capital expenditures may be a bit much, but once you realize the benefits—the economies of scale—related to doing it right the first time, you can save a tremendous amount of money long-term.

> **Tip**
> You cannot just put security controls in place and assume they'll magically meet your compliance needs. You have to do them well. Not addressing your compliance gaps and security risks properly and in the right order can create a false sense of security, which can actually worsen your information security posture and compliance status.

Looking further into compliance and security, there's a deep-seated need for ongoing management and administration. The visibility and control required for compliance isn't going to happen automatically—even with automation. Any new technologies you install or business processes you put in place are going to require additional staff resources to ensure everything's in check. Looking beyond your investment in technologies and so on, your professional resources will likely be your largest ongoing expenditure. Be it in-house employees or via external consultants, the various tasks that IT professionals need to perform consistently and periodically for ongoing compliance are highlighted in Figure 2.4.

Figure 2.4: Common requirements for IT staff working toward overall compliance.

Depending on the size of your organization, the complexities of your environment, and the unique compliance needs of your business, you might have one person dedicated to each of these areas or you might have one person—perhaps even an outside consultant—who handles it all. Every situation is different. The important thing is to ensure that all the right areas of IT compliance are getting the attention they deserve.

Remember

Use the resource you've already invested in. Be it people or technology, you likely have at your disposal a set of knowledge and tools that can help you tremendously with compliance oversight.

Long-Term Ramifications of Not Implementing Certain Controls

I believe that most people in IT and business management want to do the right things when it comes to compliance and security. There are some, however, who seem to *get it* more than others. These are the people that go beyond the minimum set of compliance requirements and security "best practices" because they see the bigger picture. The commonality among those who go above and beyond what's needed to get by is the ability to think long-term. Successful business people have an uncanny ability to know about the long-term consequences of the choices they're making today. Such behavior can have an impactful effect on compliance and information risk management as the business moves forward.

Remember

IT and business leaders' ability to see down the road 1, 5, and 10 years, thinking about the long-term ramifications of their decisions—or lack of decisions—is one of the most important aspects affecting any given organization's compliance outcomes.

In order to predict the outcomes of your current decisions regarding compliance, it is beneficial to step back and ask yourself the following questions:

- If our IT compliance program was perfect in every way, how would it be different from the way things are right now?
- What would we have more of?
- What would we have less of?
- What should we do or not do knowing what we know now?

The ugly reality is that there are so many dangerous assumptions being made regarding compliance and information risk management. All too often, I see situations where people believe that having a firewall, passwords, and antivirus software are enough. That approach is dated and no longer valid. Even at the enterprise level, there are executives I've come across that believe this is all that's needed to have a secure and compliant network environment.

Warning

Firewalls, passwords, and antivirus controls are just the beginning. Do whatever you can to educated management—and users—on the fact that compliance and security aren't that simple.

Rather than relying on point solutions that address individual security threats, you have to have a holistic program that supports your security and compliance initiatives (see Figure 2.5).

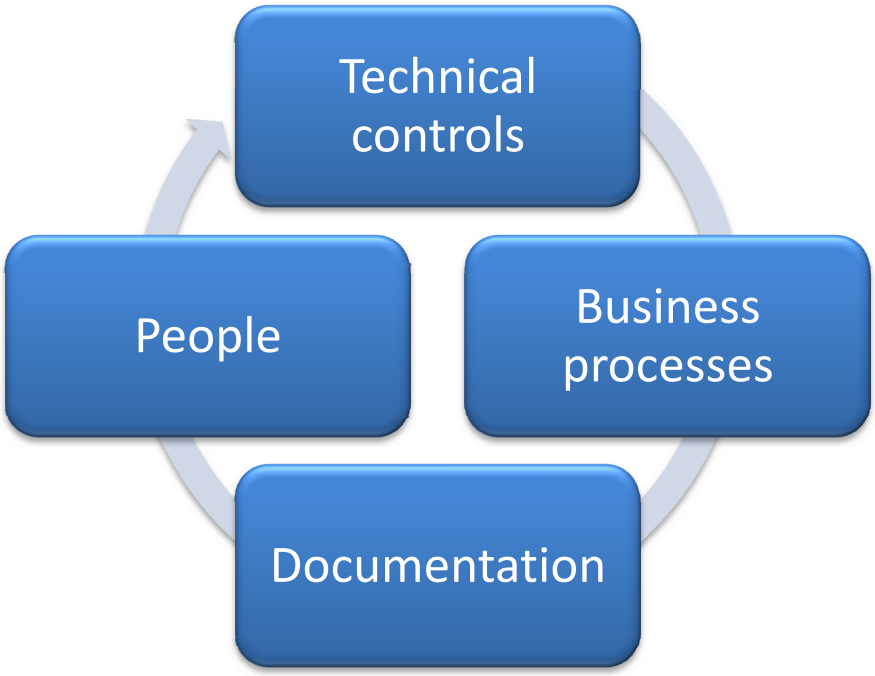

Figure 2.5: Essential elements of a holistic program supporting compliance and security.

Technology solutions managed in a siloed fashion look good on paper—perhaps even in reality at first glance. However, security controls that don't work well with others or provide real insight for event correlation aren't good for long-term compliance.

Compliance—like information security—is dynamic, constantly changing. It's got a life of its own. Things can change on a whim at any given point in time, including:

- Laws and regulations
- Threats and vulnerabilities you're trying to defend against
- Business circumstances (growth, mergers/acquisitions, downsizing, and so on)
- Technologies that your business and employees rely on to make things happen

Keeping up with all these nuances in and around compliance can be a near full-time job for the many people involved.

The Long-Term Costs of Non-Compliance Can Be Hefty

A recent study* of 46 multinational organizations by the Ponemon Institute found that the long-term costs of noncompliance are much greater than the costs of compliance. Specifically, the study found the cost of non-compliance, which varied greatly by industry, was on average 2.65 times the cost of compliance. The research also showed that the smaller the gap between compliance and non-compliance costs resulted in a lower occurrence of data breaches over a given 12-month period. Furthermore, organizations that do not perform compliance audits (28% of those surveyed!) experience the highest compliance costs. No surprise there.

The reality is that the long-term costs of ignoring compliance requirements can be much greater than the costs of implementing a solid baseline of controls. Some lessons to be learned from this study include:

1) Ignoring the realities of IT compliance is costly.
2) It pays to perform ongoing assessments/audits to see where things stand with compliance.
3) No business, regardless of size or industry, is immune from the costs—and consequences—of non-compliance.

**The True Cost of Compliance*, Ponemon Institute January 2011
http://www.tripwire.com/ponemon-cost-of-compliance/pressKit/True_Cost_of_Compliance_Report.pdf

The numbers say it all. The initial costs of getting compliance right the first time are much lower than continually fighting it—or evading it—altogether.

In my work performing security assessments, I've seen over the years how much simpler compliance and security can be when you just do it. This is especially true for small and medium businesses (SMBs), but the same concept can apply to the largest of enterprises, non-profits, and government agencies.

Odds are that your network, applications, and business are as basic and as simple now as they'll ever be. There's going to be continual growth with new parts of the business, new computer systems, new and evolving applications, and so on. It's the universal law of business progress: everything that you're managing and supporting right now is going to grow in complexity. Therefore, it's imperative that you get a handle on compliance now before it becomes more difficult in the not-too-distant future.

Remember

Focus on compliance now while your business and IT environments are (relatively) simple.

When the proper documentation and technical controls are put in place and everyone is working with a security mindset early on, things can be so much simpler. The odds are your business is going to grow as things move forward; it's going to be a lot simpler and cheaper to put the right technical controls, documentation, and business processes in place now as opposed to waiting until some point in the future to try to integrate it or, worse, layer it on top of an unstable foundation.

Other Cost Considerations You Might Not Have Thought Of

I can't tell you how often I see businesses addressing each regulation as a standalone issue. For example, a business may put resources toward HIPAA compliance. Once that's in place, the focus is on the HITECH Act, then PCI DSS, state breach notification laws, and so on. Like the reliance on siloed technical controls, trying to meet the individual requirements of each and every compliance regulation will, at best, be a continual uphill struggle.

Another common situation is when an IT director, compliance officer, internal auditor, network administrator, and so on are each focusing on all the different requirements of the various regulations that they're up against. This can create numerous burdens and costs for the business, such as those Figure 2.6 shows.

Figure 2.6: Duplicated efforts and investments can make compliance more complicated and expensive than it needs to be.

Many of these issues will only serve to make your environment more complex. When you reach such a point, usability and convenience suffers, which can lead to just the opposite of the desired effect you're aiming for. Rather than wasting so much time, effort, and money, you can combine your efforts into a broader approach to address information risks like I covered in Chapter 1 and earlier in this chapter. Doing so allows you to kill one, two, or even three or more birds with one stone so to speak by utilizing the economies of scale in the overlapping areas of compliance such as:

- Access control
- Authentication
- Audit logging and monitoring
- Encryption
- Patching and maintenance
- Physical security
- Policies and procedures
- Incident and contingency plans

The list can go on and on, but you get the point.

> **Remember**
>
> A great way to increase the cost of compliance is to address each and every regulation in a serial and standalone fashion.

Having said all of this, I don't want to trivialize the realities of each of the regulations you're up against. You *will* have to address each and every unique compliance requirement to ensure you're meeting your obligations. But if you approach this task properly, you'll still save yourself and others a tremendous amount of time. It all starts with a compliance matrix spreadsheet you can put together (or find online) that lists your specific requirements and shows the areas of overlap. You can build things out from there.

Another area that can contribute to compliance costs is the education of your compliance managers. Many compliance managers I've worked with have the regulations themselves down pat and have a good relationship with their organization's internal audit team. These are great first steps, but many compliance managers are often disconnected from other key players in the organization like information security managers and network administrators. This lack of communication often creates a false sense of compliance—especially when there's not a leader at the top facilitating and overseeing everything.

Look at your current situation and see how your compliance is plugged into IT. You'll likely find some disconnect. One of the best ways to resolve this issue is to ensure that a security or IT governance committee is in place to get everyone on the same page. Getting management on board with compliance and security is also essential. If true management support is not there, it'll be impossible to achieve any semblance of compliance.

Another commonly-overlooked issue is training and education—not on the part of users but rather the very people working to ensure the business is compliant in the first place. Make certain whoever is responsible for day-to-day compliance is getting the training he or she needs. There are numerous compliance, audit, and security seminars and conferences around the country each year that provide excellent resources for staying current. Finally, solutions to your compliance struggles may already be at your disposal. Look at your own social network. See how you can share ideas with colleagues within your own organization, peers in similar industries, and other trusted third-parties. You could even hire a college student as an intern to research and investigate how compliance is working in your organization and provide a fresh perspective. The most important thing to remember is that some of the very best ideas can come from people you never would've thought about.

Costly Oversights

Many people have found out the hard way that you cannot secure what you don't acknowledge. You have to know what's where and how it's currently at risk at any given point in time. Without the proper visibility, control, and automation, security is just not going to happen. In fact, the very worst could arise and you suddenly have a data breach on your hands.

> **Remember**
>
> You cannot change what you tolerate when it comes to IT compliance and security.

As soon as it's assumed that all the critical issues have been uncovered is the prime time for something to go awry. All it would take for this to occur is user accounts that aren't deactivated and subsequently abused, weak passwords on a wireless network or Web application that expose sensitive records, or lost or stolen laptops that expose, well, pretty much everything.

> **Common Compliance Oversights**
>
> Although the compliance regulations apply to organizations across the board, every situation is different. Not only does every business have unique requirements, management has their own risk tolerance. Regardless of these factors, I see a predictable set of compliance gaps in practically every information security assessment I perform. The following list highlights the top issues I see:
>
> - No security committee or a dysfunctional attempt at a security committee that often has too many people or the wrong people
> - No security incident response plan that outlines the organization's response to hack attacks, data breaches, malware outbreaks, and so on
> - Outdated, overlapping, and inconsistent security policies that no one is responsible for maintaining
> - Numerous missing patches, typically on servers and database systems

- Web site/application flaws such as SQL injection and weak login mechanisms
- Mobile devices running without disk/storage encryption
- Little understanding of what information is where across server and workstation shares, portable storage media, and smartphones
- Minimal user awareness of what's required and expected
- Lack of training for IT staff—training that helps them not only understand the threats and vulnerabilities but also keep up with the latest trends
- No consistent information security testing program that looks at external hosts, Web applications, the entire internal network, as well as mobile devices

Take the time to review these areas of your business. You'll likely find there's room from improvement.

The widespread existence of common compliance gaps is related, in large part, to the "assuming all's well in IT" mindset. You cannot have technical solutions and checklist audits and assume that all is well. Today's reality with our information system complexities, audit and governance requirements, and the compliance insight that's required, you have to dig in much deeper to truly see if everything is working together for the greater good as it should be. This is especially important once you fix the low-hanging fruit and get the security and compliance basics down pat. The more "secure" your environment, the harder it's going to be to uncover the issues that are still creating risks. The important thing is to know that they're there.

Tip

So you've performed a compliance audit or security assessment and assumed to have plugged all the holes? It's now time to dig in deeper. Using internal resources or, ideally, an unbiased external resource with a fresh set of eyes, look at your network with a more critical eye and perhaps a fresh set of tools. In addition, ask your employees tough questions, and you'll likely find many more areas that need to be addressed. I've heard it said many times that such an exercise can be a very eye-opening experience.

Technology to the Rescue

When you step back and think about all of these issues, the latest and greatest compliance and security technologies are being marketed for a reason. The vendors are out there innovating and developing new products, new services, and new approaches to the problems you're currently facing. Be it cloud computing, mobile computing, network security, or user management, the vendors are getting paid to innovate. They have an incentive to make their products better and our lives easier. Take advantage of this!

Remember

Marketing hype is cheap. Don't just jump on the bandwagon based on what someone is saying you need. Instead look at other areas of the market such as what analysts are saying, what consultants and authors are recommending—even what your colleagues in different businesses and industries are doing. Go beyond what one particular vendor or systems integrator is telling you and get an overall perspective.

Compliance Case Study

CupNa Manufacturing is a large company specializing in the production of automotive parts. The business has its own health plan and therefore is considered a covered entity under the HIPAA security and privacy rules. CupNa Manufacturing also performs a sizeable amount of credit card transactions each year and falls under the umbrella of the PCI DSS rules.

For the past several years, various teams inside the organization were responsible for their own areas of compliance. The legal and HR team that oversaw the health plan had their own means of addressing the HIPAA requirements. A high-level yet expensive annual HIPAA audit was performed and everything appeared to be in check. An Acceptable Usage policy that employees had to sign was the extent of the security controls around electronic protected health information (ePHI).

On the financial side, the IT team and security manager had crippling controls over the systems associated with credit card data. In fact, the controls were starting to spread out across the enterprise creating serious usability issues especially on the factory floor.

There was a great imbalance in how compliance was being handled by each of the parties—to the point of serious gaps and risks in one area and too much security in the other. Once the dysfunctional overlap became obvious, CupNa's CFO, Marty, got involved. It was determined that more than $150,000 a year was being spent unnecessarily on duplicated efforts related to compliance and security. Not having any prior experience with IT compliance, Marty suddenly had buy-in when he saw how much money was being wasted by the company's compliance inefficiencies and how much there was to lose if a breach occurred.

Marty had the clout within the organization to help establish a formal security committee and to help strike a balance between HIPAA and PCI DSS compliance given their equal importance. Although the scope of the two regulations is different, there are numerous similarities and overlapping systems within CupNa to warrant addressing both at the same time. To this day, Marty stays on top of the ongoing compliance and security assessments that the business hires an outside party to perform on a bi-annual basis.

If there's anything to be learned about compliance costs, it's

- Use what you've got,
- Spend your additional time and money wisely and, perhaps most importantly,
- Just use some good old-fashioned common sense.

Coming Up in the Next Chapter

Moving past the cost considerations, it's time to talk more in-depth about simplifying and automating in order to minimize risks and enhance compliance. In order to keep security and compliance from being continual thorns in your side and to ensure things are kept in check, you're going to have to focus on these areas moving forward. In Chapter 3, I go in-depth on how the complexity of your information systems environment largely determines how things are going to turn out and what you can do about it.