The Ties That Bind

The regulatory and IT threat landscape has made both security and compliance strategy a vital part of business operations. How can the two departments work together to achieve business goals?
The Keys to Developing—and Maintaining—the Proper Security and Compliance Balance

It’s no secret that the number of both industry-specific regulations and data-related threats has increased dramatically in recent years. The trend has forced businesses to increase focus on information management processes—especially as they relate to maintaining security and compliance. The mistake many companies make is thinking that security and compliance are one and the same. In reality, top-notch security does not necessarily mean the business is compliant with regulations, and compliance processes do not automatically equal information protection.

How can organizations develop the right security and compliance balance? The biggest factor will be communication between the two departments and their business leaders to determine where resources can be combined. In this SearchCompliance handbook, we examine strategies for fostering a security-and-compliance relationship that will ultimately benefit the business as a whole.

In our first article, expert Ed Moyle explains why, despite their sometimes adversarial relationship, security and compliance departments can benefit from aligning their strategic goals. In our second article, author Christine Parizo examines why a compliant organization is not necessarily a secure one, and vice versa. In our third article, I look at how an organization-wide risk assessment is an important attribute when identifying where best to consolidate security and compliance efforts.

As the regulatory and security landscape grows more challenging, we hope you find this handbook helpful to your organization’s efforts to create a proper balance between compliance and data protection.

Ben Cole
Editor, SearchCompliance
Three Strategies to Align Compliance and Security

Maintaining compliance is a difficult job, both in scope and in practical application. There is a vast array of regulations with which organizations need to comply, and the number is constantly increasing. Determining which ones apply to a particular company depends on organization-specific factors such as vertical industry, geography, type of business services performed and data collection activities, to name just a few.

In application, it’s also difficult because the personnel closest to the specific technology involved in meeting key regulatory compliance requirements are often outside the compliance team’s direct management responsibility, while the output of their activities is very much within it.

As an example of this last point, consider a regulation like the Health Insurance Portability and Accountability Act (HIPAA). HIPAA includes very specific standards and implementation specifications that govern what compliant organizations must have in place in terms of security controls, including data encryption, technical monitoring and user-account requirements.

For the majority of the covered entities, compliance teams are chartered with ensuring that these specifications are addressed. Many of these same teams, however, do not have direct oversight over the implementation, operation or monitoring of the technologies that they address. Instead, these technologies may be under the purview of information security teams, under the auspices of broader IT, outsourced to service providers or run by other departments.

This situation has the potential to lead to an adversarial relationship between the compliance and security departments. Compliance teams sometimes feel that their concerns go unheeded, for example, when a requirement
remains unaddressed despite investment in other areas. By contrast, technical or security personnel may look at compliance activities as siphoning budget from investments that reduce technical risk. This can be a challenging situation, but there are strategies to help overcome these hurdles or even ensure that they don’t arise in the first place.

1. BUDGETARY ALIGNMENT
Many times, budgetary and spending considerations are a key element of the friction between compliance and security teams. Despite the prevalence of this contention, very rarely is budgetary planning a joint activity that includes both stakeholders. Combining the two departments during budgetary planning can help, particularly when planning spans multiple years. Any plan that goes beyond the current budgetary cycle will obviously need to be somewhat malleable, but the exercise of putting it together is in itself useful.

Benefits of setting a multiyear strategic plan that addresses budget and spending include allowing prioritization decisions, even fractious ones, to be negotiated well ahead of time. It also allows soft costs like staffing considerations and controls operationalization to be accounted for. The point is that agreeing on budget priorities jointly can ameliorate disagreements, nip subsequent resentment about specific investment decisions in the bud, and decrease the amount of adjudication required by management or governance teams when departments don’t see eye to eye.

2. STRATEGIC ALIGNMENT
Implicit in the above strategy is an alignment—or at least a tentative agreement—between the goals for both the compliance-focused part of the organization and its security teams. As a part of that effort, another useful approach is to explicitly conduct strategic planning that addresses both compliance and security goals. Specifically, setting a mission for both teams that acknowledges and, where practical, even includes the core objectives of the other can help reduce workload and increase efficiencies on both sides. When these goals are aligned, opportunities for collaboration can emerge that
wouldn’t be seen otherwise.

For example, including measurable risk reduction as a goal for both departments helps simultaneously address compliance and security requirements. Many regulatory requirements require a risk-based approach anyway, but a joint effort to figure out how to measure, weigh/prioritize and report on that risk can obviate some sources of contention.

**3. CONTROL ALIGNMENT**

Lastly, there are sometimes disagreements about the order in which controls should be prioritized in terms of time and budget. But when examined closely, very often the specific controls required under governing regulatory requirements also provide security value. In addition to alignment on budgets and overall goals, it’s also helpful to approach specific controls as a joint activity between security and compliance. Specifically, the two departments should discuss what controls are needed and where.

The goal is to create an inventory of controls that are already in place and those that are desired for the future. Understanding what you have in place now allows you to analyze and document current controls that have overlapping security and compliance benefits. It should also identify areas where there are controls you desire but do not have currently in place.

Knowing what you’d like to have but don’t allows you to find overlapping areas where both security and compliance goals would be forwarded with one investment. This helps you build a stronger business case and, if combined with budgeting exercises, might even open up creative ways to fund it. —Ed Moyle
Walking the Compliance-Security Tightrope

**Nothing illustrates the** difference between compliance and security better than the recent holiday retail fiascos, when millions of credit card numbers were stolen from large retailers, including Target, who were assumed to be compliant with industry standards and regulations.

After the stories broke regarding the breached retailers, it became clear that compliance gaps are almost guaranteed to lead to security problems. According to experts, compliance and security aren’t mutually exclusive, and both need to be attended to regularly.

One of the mistakes that organizations tend to make is applying a set of compliance standards and assuming that will be enough to also remain secure, said Hans Guilbeaux, director of information security and compliance for Farmington Hills, Mich.-based consultancy assure360.

“Unfortunately, a lot of companies think compliance is one-size-fits-all or that, conversely, they can go to a third-party vendor and buy compliance in a box,” Guilbeaux said. “What I frequently hear ... is that compliance is one checkmark away from being hacked.”

It’s important to remember that malfeasants know what they’re doing and where the vulnerabilities are. Regulators aren’t necessarily security experts, either—even those examiners that visit organizations to ensure compliance, according to Matt Wilhelm, CEO of Cleveland, Ohio-based IT consultancy enCompass Group LLC.

“Oftentimes, they’re not IT folks at all,” he said, and these examiners are often just looking at the checklist: patch management, regular firewall logs and other items on the compliance list that don’t necessarily equal security. “They themselves can’t keep the hackers out,” Wilhelm added.

But compliance—full compliance—remains
critical, and not just to protect customer information. “In our business, we’re constantly saying, ‘How do you put a dollar value on that?’ ... One data breach could destroy brand value and brand equity,” he said.

For example, even though Target offered a 10 percent across-the-board discount after its recent data breach, it still had a less-lucrative holiday season because people stayed away, Wilhelm added.

EMBRACE COMMON SECURITY, COMPLIANCE GOALS
When you boil it down, security and compliance end up being two sides of the same coin, according to Mike Chapple, senior director for IT service delivery at the University of Notre Dame in Indiana. “Compliance is going to be what you need to satisfy obligations to external parties (like) regulators,” he said. Security, on the other hand, is making sure that the application controls are in place and that the organization is taking sufficient steps to protect information, he added.

Using compliance as a starting point isn’t a bad thing, according to Chapple. “When you’re looking at the different regulations out there, for the most part, the things (regulators) are requiring organizations to do are things they should be doing as good security practice anyway,” he said.

The first step for organizations that want to strike a balance between compliance and security is to conduct a risk assessment, Chapple said. While these are typically required on an annual basis for compliance purposes, it’s important for organizations to approach risk assessments as more than an exercise and as an essential, thorough piece of security to determine vulnerabilities, he said.

“It’s important to have compliance plans, and that goes back to not creating a program that just studies for the test every year... but instead having a documented plan that looks at what are each of the requirements facing the organization and what is our response? How are we implementing those?” Chapple said.

For example, compliance with payment card industry standards requires submission of quarterly vulnerability scans to the
organization’s bank. Those scans would go into the compliance plan and be assigned to a team member, who would then submit the results and save the records of the scans in a designated place.

Communication between IT and legal is critical to making security and compliance work. Many organizations do this by forming compliance bodies within the organization.

“Whenever you want to review your compliance status, you should be able to look at those plans and see that there is a control in place to meet each one of the requirements of a particular regulation and that somebody has validated compliance with it recently,” Chapple said.

Finally, communication between IT and legal is critical to making security and compliance work, according to Chapple. Many organizations do this by forming compliance bodies within the organization, such as committees made up of representatives from different departments. These committees may either cover just IT or all of the organization’s compliance obligations. Often, those committees consider broader risk categories for the organization as well, he said.

Ultimately, organizations should choose to use compliance guidelines as the foundation for a security program. The business can then communicate these guidelines across the organization to ensure all departments have the opportunity raise concerns. The organizations that take this approach to balancing compliance and security are better poised to stay on the right side of regulators and avoid breaches.

—Christine Parizo
Break Down Barriers With Risk Assessments

Although they have many of the same goals, an organization’s compliance and security departments usually do not work together enough to meet common objectives.

Breaking down the barriers between compliance and security teams, however, can reduce redundant processes, combine resources and even improve organization-wide risk management. But while there is much common ground between the security and compliance departments, the trick is finding where that common ground is.

A good place to start is to embrace common security and compliance goals that eliminate company-specific risks, then develop business processes based on these goals.

“I think it’s increasingly down to the business to take a risk-based approach to say, ‘Is being compliant going to be efficient for us, or do we need to do things over and above that?’” said Steve Durbin, global vice president of the Information Security Forum.

More often than not, Durbin said, it is more beneficial to start with security. A company could be following all of its compliance stipulations to a “T” and still have many security vulnerabilities.

“I’m on the side of the fence that security comes first—if you have good security, then you will mostly be checking the right boxes from the compliance standpoint,” Durbin said. “Compliance will only take you so far these days because we are operating in a fast-moving, dynamic environment where we are always connected—you have to do more than just be compliant.”

Although security takes a more holistic approach to protect and manage business information, the compliance and security balance depends largely on the organization’s unique needs and vulnerabilities. In highly regulated fields such as finance, for example, compliance...
may be a slightly higher priority, or one that is at least equal to security.

To properly balance security and compliance, stakeholders from the two departments should help identify redundant processes and where resources can be consolidated.

“It’s about sitting down with all of the stakeholders—the compliance department and the security guys—and working things out from the outset so you don’t have those overlaps,” Durbin said.

THE RISK-BASED APPROACH TO SECURITY AND COMPLIANCE

As both IT threats and industry regulations have proliferated in recent years, security and compliance have become high-profile—and very costly—business endeavors. As a result, it benefits organizations to determine where resources can be consolidated to enable both.

If smartly implemented, policies such as identity and access controls can provide big benefits to both compliance and security. For example, an essential part of most companies’ information security efforts are controls delineating what employees have access to specific records. Similar controls are also required under many compliance regulations, so businesses benefit when they can identify both compliance and security vulnerabilities that would benefit from the access-related policies.

This strategy is similar to the risk-based approach to security, compliance and other business operations that has become popular in recent years. If organizations first identify the unique existing and emerging risks the business faces, they can then gather stakeholders to determine common responses to these threats.

Like security and compliance efforts, risk management works best when strategy is communicated between several departments. Sometimes, one source of risk threatens multiple business processes, especially if these risks are related to compliance regulations, said Renee Murphy, a senior analyst at Cambridge, Mass.-based Forrester Research Inc.

This makes data classification vital to both security and compliance processes. Information governance efforts such as retention and deletion schedules can help an organization identify what information absolutely must be
kept to remain compliant, and what trivial data can be completely deleted so it is no longer a security threat.

“If you are not doing data classification when your data is growing by leaps and bounds, how will you get your head around risk management as it pertains to that data asset?” Murphy said. “If you have a rapidly growing data environment that is growing by terabytes per quarter and you are not actively determining what data’s important and what’s not, you can’t apply risk principles to it.”

Clearly outlining the company’s risk profile and assessment is essential to identifying specific compliance and security vulnerabilities. From there, communication between the key stakeholders will be important for the marriage of security and compliance processes to be successful, Durbin said.

It’s also important for business strategy leaders to remember that 100% security is virtually impossible in the digital age, Durbin said, and to try to take a more philosophical approach to security and compliance consolidation.

“What you are trying to do is minimize opportunities for things to go wrong, trying to have the correct processes in place so, when things do go wrong, you can recover effectively, so you can manage fallout associated with that,” Durbin said. —Ben Cole
**ED MOYLE** is director of emerging business and technology at ISACA. Moyle previously worked as a senior security strategist at Savvis and a senior manager with CTG. Prior to that, Moyle served as a vice president and information security officer at Merrill Lynch Investment Managers.

**CHRISTINE PARIZO** is a freelance writer specializing in business and technology. She focuses on feature articles for a variety of technology and business-focused publications, as well as case studies and white papers for business-to-business technology companies. Christine has a background in litigation technology and compliance and was an assistant news editor for searchCRM prior to launching her freelance career.

**BEN COLE** is site editor for SearchCompliance. Prior to joining TechTarget, Ben was the online editor for HealthLeaders Media, based in Marblehead, Mass. He began his journalism career as a reporter with the Massachusetts daily newspapers The Gardner News and the Sentinel and Enterprise.