THE ART AND SCIENCE OF COMPLIANCE

FORESITE

www.foresite.com | 1 (800)-940-4699

INTRODUCTION

Today, regulatory and legislative compliance obligations seem endless and ever-changing. Corporations are faced with enormous challenges in attempting to manage complex IT security programs, meet numerous compliance objectives, and deliver evidence on different schedules to multiple parties.

Whether your objective is to secure your enterprise, achieve compliance, or both, success may be elusive or even seem impossible at current staffing levels or within budgetary constraints.

Moreover, the speed and frequency with which security breaches are occurring require expertise and nimbleness beyond that of most companies' IT departments.

The solution lies in fusing experience, expertise, technology, processes, and vision into a laser-like approach. This is an approach that monitors, reports, and protects your most valuable assets — one that is on point, all the time.

THE PROBLEM

In most modern corporations, CIOs and their staffs face the challenge of providing evidence of compliance to internal auditors, regulators, business partners, and even customers — each of whom want this information in different formats on differing schedules.

Seeking direction, they look to IT vendors and software resellers that recommend a mind-numbing array of products and services — all promising dramatic results, efficiency improvements, cost reductions, return on investment, and more. These are promises and claims that someone within the organization will spend countless hours analyzing, discussing, and testing, before eventually recommending which strategic technology purchase might solve the problem.

Assuming that foundational technologies are already in place, the recommended list commonly includes a GRC (Governance, Risk, and Compliance) framework, a systems management solution, a vulnerability management suite, a SIEM (Security Information and Event Management) application, or an enterprise workflow platform — or even some esoteric combinations.

Imagine — an endless buffet of vendors and solutions to choose from in almost every area of technology and security management, all designed to help you achieve compliance.

But here's the reality: Many Fortune 500 corporations have invested millions of dollars in security technologies and enterprise IT solutions and employed armies of IT personnel and highly skilled security professionals, only to consistently fall short in their quest for compliance.

Worse, many of these corporations have subsequently been found to be non-compliant with their regulatory or legislative obligations. For that, they have faced fines, financial penalties, or even a revocation of merchant status with their financial institutions.

And worse yet, some of these companies have suffered data breaches that made national news, reducing customer confidence and losing market share — even going out of business.

MORE PROBLEMS

- Strained IT budgets and finite resources require security teams to support a continuously growing list of responsibilities.

- Contention for attention is universal. How can security analysts effectively maintain focus on guarding an enterprise and responding quickly to attacks when also performing normal security functions? Organizations all prescribe different roles and responsibilities for analysts, but these are some common activities that compete with guarding and protecting an enterprise:

    - Alarm monitoring and incident response
    - Log review and management
    - Vulnerability management
    - Patch management
    - Identity and access administration and management
    - Anti-Virus/Anti-X administration and management
    - First line user support
    - Firewall or other access control change request management
    - Reporting and metrics

- Shortage of qualified cybersecurity professionals is a global problem despite the growing number of colleges offering bachelor and graduate degrees, or at least coursework, in cybersecurity. In March 2013, Computerworld reported that the demand has grown three and a half times faster than the demand for other professionals in IT-related jobs. This means fierce competition for the precious few qualified candidates.

- Compliance requirements are a moving target. Because of their dynamic nature, organizations are forced to rely on a virtual army of attorneys and subject matter experts to comprehensively review, interpret, and apply the rules and regulations to which an organization must conform.

The General Solution

Most organizations are already painfully aware of the challenges just described. Before discussing a specific approach to compliance, it's important to recognize some fundamental truths and basic strategies.

Fundamental Truths

1. **Compliance does not equal security**. An organization can be 100 percent compliant with PCI, SOX, GLBA, or any other standard and still not have a secure environment. As more than 100 years of U.S. legal proceedings demonstrate, simply having an established framework of controls to work within cannot prevent creative individuals from inventing new forms of malicious behavior. Much like how society often generates new laws and regulations to solve loopholes, software companies generate patches and updates to solve vulnerabilities.

2. **Compliance is subjective**. Regardless of in-house expertise, organizations must respect the authority of auditors, QSA, or vendors in interpreting regulations and in judging how successfully specific controls have been implemented. Yet, these individuals come from diverse backgrounds, and have varied degrees of experience and different levels of technical expertise — all of which influence how they interpret both the compliance requirements themselves and the level to which they have been achieved through technology or process.

   This is specifically why the art of compliance (as opposed to the science) is so dynamic and often frustrating for technologists: It is not black and white. It takes a combination of political savvy, negotiation, technical expertise, regulatory and legislative knowledge, flexibility, and effective communication to define and agree upon common goals.

3. **Security has not changed since the dawn of man**. The art and science of protection — whether it be people, property, food and resources, technology, or data — boils down to some very simple and universal concepts. Whether compared with physical security standards or battle-tested kinetic warfare defense concepts, the only real difference is that technology has only increased the speed and scale at which we are able to conduct operations to protect the things that matter.

Basic Strategies

Most organizations have already made some investment in common IT security technologies and have developed processes to support them. These include firewalls, IDS/IPS, content filtering, and anti-virus tools, as well as the list of activities listed in the bulleted items under the "Contention for attention" paragraph on page 4 of this document.

The Specific Solution

Investments in general security technology and resources are critical first steps in achieving compliance. But what makes all the difference in consistency, quality, and success is whether organizations apply a strategic focus on activities that actually matter.

Start with the end in mind. This is the most important component in achieving compliance success. Organizations need to work closely with auditors and customers to understand the precise scope of their compliance objectives and to define specific and realistic deliverables.

- All too often, IT and IT security staff will have a contentious relationship with auditors. This is absolutely the worst scenario for developing compliance efforts, often resulting in unrealistic deliverables and timeframes requiring impossible levels of effort. It is essential to take the time to fully understand what the auditor is tasked with delivering to the business, agency, or customer and then offer ideas and examples that can help them be successful. This approach allows the organization to guide the conversation and ultimately control the discovery and scope of the discussion.

- Once the audit is in progress, the focus must shift to the actual deliverables. These deliverables are the template for an ongoing process that will become easier and less painful once institutionalized. By the time of the next audit, a current and updated package of all the deliverables from the previous meeting that have already met objectives should be ready for auditor review. Gaps due to changes in requirements or environment should be minor.

Nothing is perfect. It's important not to become mired in semantic analyses of requirements. And equally important to prevent philosophical debates between security experts and auditors.

Enter conversations with the understanding and acceptance that meeting compliance objectives will still leave security gaps — because compliance does not equal security. If this is so sacrosanct that the security purists on the team just can't let it go, don't invite them to the meeting with the auditor as it will negatively impact (and may completely derail) planning efforts, as well as destroy any possibility of a positive outcome.

Asset inventory. A full and complete understanding of what data exists, how sensitive it is, and where it is located eliminates the possibility that the entire organization will be considered in scope for compliance.

The asset inventory must include all systems and applications, what data they contain, and where they are located. Without a proper asset inventory and a process to maintain it, compliance will be prohibitively expensive. Moreover, it is more likely than not to exceed the capacity of resources to ever successfully achieve compliance. While this may seem like a minor detail, it is not. It is a critical priority to build and maintain an accurate inventory.

Blocking and tackling. The level of effort required to provide evidence of compliance will be less of a burden by having comprehensive process documentation for existing processes, such as patch management, configuration management, access control and user management, vulnerability management, log review, and others mentioned above. These processes must be documented and up to date at all times. They are also essential items in an initial planning meeting, and provide good discussion material.

The Foresite Solution

Here's where we get personal. Your organization isn't just any organization. Where do you stand on the compliance and security spectrum? When you look at the reports of data breaches in the daily news and realize that the victims were using the same technologies you have deployed to protect your enterprise, do you ask yourself what is wrong with the whole industry, or what is wrong the way you do things in your organization? And what can be done?

Good questions. Here are some straight answers:

The IT industry has indeed lost its collective focus on the basics. We have become dependent upon vendors, outsourcing, and automation. We have streamlined our business processes to rely upon technology far beyond our capacity to support them manually when that technology fails to perform. We run faster and faster every day, expecting more and more from a dwindling pool of qualified resources.

It falls on you. The breadth of your staff's responsibility has been creeping in scope, in most cases without you even realizing it — much like the proverbial frog in a pot who is cooked before he knows it.

When it comes to meeting your compliance or security objectives, you must start by giving constant attention — with a laser-like focus — to basic activities. Some processes, like monitoring your enterprise for malicious activity, reviewing user activity, reporting on exceptions, and responding to incidents, must be in place and documented to provide solid evidence of due diligence to achieve compliance.

Investing in technology (despite the price tag) is the easy part of the solution. Managing the technology infrastructure 24x7 is the real challenge.

The fact is: You can't do it alone.

You need Foresite to enable your success. When it comes to compliance, we can do the manual labor and heavy lifting. Our security experts meet with you and your auditors to fully understand in detail what your compliance objectives are and help you come to an agreement on the deliverables that will enable your mutual success.

That important planning meeting with your auditors or customers that we discussed earlier is where it starts and where Foresite can ensure you set off on the right path — because we have the credentials, the resources, the expertise, the vigilance, the vision, the insight, and the foresight this effort takes.

And then, we keep at it, around the clock and every day of the year. We protect your enterprise and perform your organizational due diligence for your auditors and your customers whenever and however you need it.

Think About This

If you've already made a substantial investment in security technology and compliance solutions, yet you're still falling short of your objectives, the problem may not be merely software or staff.

It's more likely symbiosis.

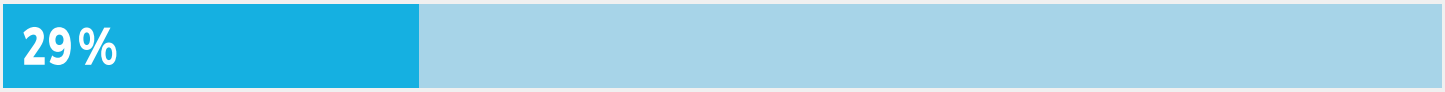
It's about how they work together according to a vision, with commitment, and within a proven process—one that anticipates, analyzes, detects, and manages your situation 24/7.

Compliance is far more than science. It's an art.

Alarming 2013 Statistics

Source: 2013 Verizon Data Breach Investigation Report

of breaches were spotted by an external party



of breaches were social engineering

of network intrusions were exploited weak or stolen credentials

of these cases were the result of a compromise that took hours — or in some cases only minutes — to occur

of the breaches reported took months (62%), and even years (4%), to discover . . . a 10% increase over 2012

Conclusions Drawn

- Attacks are inevitable
- Companies should devote more time and effort to:
    - Detection and remediation
    - Preventing attacks from becoming breaches
    - Preventing breaches from becoming financial and reputational disasters

Thoughtful Questions

- Why do technology investments in firewalls, IDS, system monitoring/management, or SIEM fail to protect?
- What do you do when technology cannot solve for the human element?
- Are current technologies deficient?
- Is the problem getting worse?

Compliance doesn't necessarily result in good security — but good security supports and improves compliance.

Four Steps to Improving Security

Source: Ernst & Young

1. Link information security strategies to business strategy and to overall desired business results.

2. To better define needs, start with a blank sheet when considering new technologies or architecture. Break down barriers and remove biases that may hamper fundamental change.

3. Execute transformation by creating an environment for successful and sustainable change to the way information security gets delivered.

4. Delve into the opportunities and the risks of new technologies. Prepare for use of social media, big data, cloud, and mobile, because they're here to stay.

Effective Information Security Transformation does not require complex technology solutions. Instead, it requires leadership as well as the commitment, capacity, and courage to act — not a year or two from now, but today.

About the author

Clay Wilson, Foresite Vice President of Global SOC Operations, is an expert in the field of network security and managed services. Clay draws on more than 20 years of engineering and operations management experience in data-sensitive industries, including financial and telecom. His credentials include CISSP, CISM, CISA, CRISC, PCIP.