APTARE®

White Paper

What is the True Cost of Regulatory Compliance?

It's not just fines and other penalties of non-compliance. Manually managing spreadsheets, writing scripts, compiling reports, and babysitting auditors can sap time, resources and budget.

Managing complex and dynamic compliance requirements can run enterprises more than $3 million annually. Automatically collecting compliance information in a single reporting platform in real time can dramatically streamline auditing and compliance reporting processes.

The most common case study for showing the importance of maintaining regulatory compliance is almost universally attributed to a 2006 settlement by Morgan Stanley with the Securities and Exchange Commission to pay a $15 million civil fine. Allegedly, the company repeatedly failed to provide tens of thousands of emails as part of an investigation that was spearheaded by the SEC over several years. The incident was widely reported in the press, and compliance officers to this day continue to cite the cost of the fine as a wakeup call to their organization's leadership that compliance efforts need to be a priority.

However, the $15 million is only the most publicized impact of compliance. For every Morgan Stanley there are thousands of organizations that are spending millions of dollars on merely maintaining compliance—representing hundreds of millions of dollars that is taken out of the global economy each year that could be better spent on research and development, opening new markets, or creating efficiencies in the supply chain. In some cases, regulatory compliance has turned into an end in of itself rather than a means to improving information security.

Organizations can reduce the financial impact of maintaining compliance by creating visibility into the storage environment and processes; automating the data collection and analysis stages; and streamlining reporting.

This white paper explores:

- The labor involved with maintaining, reporting, and proving compliance
- The cost of that labor to the organization
- Using storage reporting solutions to alleviate the true cost of regulatory compliance

Compliance is Costing Organizations More and More

It's no secret that regulatory compliance is a tricky animal. Compliance officers have to be continuously vigilant all year for that two week period when auditors pay a visit. The consequences of being unprepared can be extremely dire (just ask the folks at Morgan Stanley), potentially resulting in millions of dollars in fines on top of the millions already being spent on an unsuccessful compliance strategy.

The Ponemon Institute surveyed 46 large organizations in a variety of industries in 2011 and found that the average cost of maintaining compliance was $3.5 million per year and that the cost of being non-compliant was $9.4 million per year. That $6 million in savings makes it certain that organizations will continue to lay out the budget to sustain vigilance.

But the fact remains: maintaining compliance is expensive. According to a Thompson Reuters report, compliance officers at large enterprises are finding life increasingly challenging as regulations continue to evolve and expand. They're spending more than one day per week (up to one-quarter of their time) on compliance administration, including tracking and analyzing regulatory developments and amending their organization's policies and procedures to meet those changing requirements. Fortunately or unfortunately, depending on your perspective, administrative time has remained stagnant around one day per week despite this increase in complexity. Are compliance officers getting more efficient or are some things falling through the cracks?

What Compliance Entails

Regulatory compliance requires creating, amending, and applying policies; manual administration and scripting; detailed analysis; complex reporting; and providing proof of varying compliance status.

Policy creation and management. Compliance officers are required to work with the business staff to ensure business priorities are being met. However, sometimes these priorities are in direct conflict with regulatory requirements—as what was likely the case with Morgan Stanley. While there was a regulatory need to archive email communication for seven years, aggressive storage policies that overwrote backup tapes to reclaim that storage were likely set up to delay media buys and save budget. Morgan Stanley likely could have avoided the investigation and the fines by identifying the overlap. However, manually managing these policies and cross-checking them isn't a reliable or efficient way of ensuring all requirements are being met. It takes time, resources, and staffing that can be better spent on other priorities.

Collaboration and integration. Despite the widespread adoption of virtualization and cloud technology, most business systems continue to be managed in a silo, each with its own administrators, management tools, polices, and lexicon. What this means for compliance is that the compliance officer is required to collect information from each environment, collate the information, translate it into a cohesive, common language, and create readable reports that can be shared with management staff and other stakeholders.

All this, of course, takes time. The Thompson Reuters report shows that security professionals in the federal space spend more than 50 percent of their time going down a list of regulatory requirements and checking off each item one at a time. That time can be better spent on bolstering defenses, learning about new threats, or improving incident detection.

Analyzing the information. Compliance officers also have to cull databases to identify events that have to be addressed and work to resolve the issue. Not only do steps have to be taken to prevent the event from occurring in the future, the process needs to be recorded and reported on for future audits.

Compliance Reporting. Once recorded and compiled, compliance reports need to be shared with business managers and other stake holders who need to understand the organization's compliance status. Above all, time needs to be spent collecting and translating the data into actionable business information. Ultimately, the management team is responsible for compliance, and they need easy-to-read, actionable reports. It takes time to create and disseminate that information—again, taking administrators and compliance officers away from their core duties.

Proving Compliance. Proving compliance can be just as labor intensive. One day a guy in a suit with a badge shows up and starts asking questions. You put him in a cubicle in the corner of the office and keep your eye on him. You answer questions. You provide data. You run reports. You're basically babysitting the auditor as he pores through your records looking for anything that isn't up to code. And it isn't getting any better. According to Thompson Reuters, 65 percent of compliance officers expect to spend more time liaising and communicating with outside auditors in 2013 than in the previous year.

Using a Central Storage Reporting Solution for Regulatory Compliance

It's gotten to the point that regulatory compliance has become so complex, so costly, and so time-intensive that it has become an end unto itself rather than a way to improve information security. This, of course, is dangerous thinking. Protecting and securing business data should be the ultimate goal of any compliance strategy. Efforts should be made to reduce the financial impact of regulatory compliance, and resources need to be rededicated to bolstering defenses, learning about new threats, or improving incident detection. Lessons learned from compliance should be leveraged to achieve the ultimate goal of protecting business information from any threat.

Streamlining the regulatory compliance relies on visibility into the storage environment and processes; automation throughout the data collection and analysis stages; and simplified reporting. The best way to achieve this is by deploying a single, consolidated storage reporting solution that can centralize data protection and security information in a single platform, giving compliance officers the information and visibility they need to meet any regulatory compliance challenge.

Visibility:

Knowing what is out on your network is the most important requirement of maintaining a reliable yet efficient compliance strategy. How can you protect data that is stored on infrastructure that you don't even know you have? Regular audits can provide accurate inventory information, but the process of collecting information, collating it in a central location, and keeping it updated is a complex, time-intensive process.

Data Protection Regulations You Should Know:

Sarbanes-Oxley: Passed in the wake of the financial accounting scandals in the early 2000s, SOX requires that data be stored so it's easily recoverable for an audit. Organizations must have written and enforceable retention policies, a searchable index of all stored data, viewable and readily retrievable data, and offsite storage of data.

Dodd-Frank Wall Street Reform and Consumer Protection Act: A reaction to Wall Street excesses that led to the Great Recession, Dodd-Frank ensures that the appropriate controls and procedures are in place to safeguard business data. This includes mandated data protection, disaster recovery, and archiving strategies. The law also requires that backup resources are tested for timely recoveries.

Health Insurance Portability and Accountability Act: HIPAA safeguards patients' personally identifiable information by regulating how long data is retained and how out-dated patient data is deleted and media is destroyed.

HITECH: Seen as an extension of HIPAA, HITECH requires health organizations to disclose any data breaches that put more than 500 patients' personally identifiable information at risk of exposure. Announcements must be made to the Department of Health and Human Services, the media, and the affected patients.

Others: Basel II, Basel III, ISAE3402 (formerly SAS70), Data Protection Act of 1998 (UK), EU Data Protection Directive, Safe Harbor (EU)

Organizations need a storage reporting solution that can automatically audit the entire environment—regardless of platform, business use, or physical location. The widespread adoption of virtualization and cloud computing have made infrastructure more spread out and heterogeneous than ever, so it's important that you're able to track data as it flows across multiple environments. Your solution should give compliance officers a view across virtual systems, cloud services, physical storage, and tape from one dashboard and provide real-time insight into allocated storage, utilized storage, free capacity, backup status, and event logs among other metrics.

Automation:

Manual processes are an efficiency killer. According to the Ponemon Institute survey, compliance officers reported that administrator overhead accounts for 60 percent of their compliance costs. That's time that can be better spent on more strategic projects that actually protect the organization.

Using a single solution to collect this data can help organizations put a process behind the regulatory compliance reporting process, centralizing the data in a single, secure location where it can be analyzed, archived, and reported on. Automation is not just a time saver; it can standardize data collection techniques, ensuring that compliance information is accurate and complete.

Simplified Reporting:

The complexity and potential for human error with manual spreadsheets and most home-grown compliance reports make them hopelessly inaccurate and incomplete—and that's putting it nicely. Many times even the people who put the reports together have a hard time analyzing the information and pulling out actionable data. Line managers and the leadership team? Forget about it. The reports might as well be written in ancient Aramaic.

Simplified reporting can be used to disseminate regulatory compliance information to the people who need it up and down the chain of command. Different reports—from an executive summary for the c-level suite to a detailed account of each backup for the auditing team—can be compiled and distributed at the push of a button. Even outside auditors can benefit. Instead of babysitting a regulator by providing information at his beck and call, compliance officers can simply give him a login to the storage reporting solution where he can access whatever information he needs (with authentications of course!). Not only will this save the organization time, the regulator will appreciate not having to dig around the pertinent information. It'll all be there for him when and where he needs it. Getting auditors on your good side can lead to a more enjoyable regulatory audit experience—something we can all appreciate.

Conclusion

With compliance efforts costing enterprises $3.5 million per year on average (and much more for healthcare and financial organizations), there is a real need to reduce administration associated with regulatory compliance. Fortunately, a central storage reporting solution that provides complete and real-time insight into storage, backup, and data protection environments can alleviate overhead, reducing the cost of regulatory compliance while strengthening compliance efforts.

Visit APTARE.com today to learn more about how to reduce your regulatory compliance overhead.

1359 Dell Avenue · Campbell, California 95008 · Tel +1 408.871.9848 · Fax +1 408.871.9858 · sales@aptare.com · www.aptare.com