Complying With the Inevitable

"For technology executives to become business executives, they must understand compliance"

Sue Bushell 02 July, 2008 16:55:50

Part 2 of CXO Priorities | COMPLIANCE

Most organizations face a "relatively high" risk of suffering a data loss that would expose them to extremely embarrassing publicity, according to the latest assessments by the IT Policy Compliance Group. And things can get very bad indeed, with the worst laggards on compliance routinely suffering 17 or more disruptions annually from IT security events.

How well each individual organization mitigates that risk depends on how it complies not only with its own policies but also with a host of regulatory and industry governance requirements on the handling and custody of sensitive data.

But while compliance may be a priority and most CIOs may be well aware of their responsibilities in this area, the picture on how well they manage compliance remains depressingly uninspiring. The Compliance Group's July 2007 Benchmark Research Report found that while most organizations are exposed to financial risk from data loss and theft, nine out of 10 are still failing to leverage compliance and IT governance procedures that could help mitigate financial risk from lost or stolen data.

> The CIO has a burden of duty to understand the broader ramifications of compliance and the consequences of non-compliance

The Compliance Group's research shows that the two out of every 10 organizations that are lagging have the most to gain from strong compliance efforts, the seven out of 10 deemed "normative organizations" can reduce substantial financial risk by improving their compliance efforts, while the one in 10 organizations categorized as "leading" are well positioned and suffer the fewest business disruptions. In fact compliance leaders suffer no more than two disruptions annually from IT security events, compared to the 17 or more disruptions suffered by compliance laggards. They also, unsurprisingly, suffer the least data loss and theft.

Financial losses will inevitably occur with data loss and theft, with the only question being when and by how much, according to the report. Compliance laggards are likely to make the front page of the paper for a data loss or theft once every three years or sooner, compared to once every 42 years or longer for compliance laggards.

The research found best practices for improved results include:

- Implementing more of the appropriate IT controls
- Reducing control objectives, making it easier to communicate, measure, and report
- Establishing higher standards for performance objectives
- Encouraging a culture of operational excellence in IT

- Monitoring, measuring, and reporting controls against objectives at least once every two weeks
- Allocating more funds to control automation

"The benchmarks show that firms excelling at compliance are those with the fewest data losses and thefts. The benchmarks also show that to avoid, mitigate, or delay the financial consequences of publicly reported data loss and theft, it is essential to drive operational excellence in IT by monitoring and measuring controls against objectives consistently, at least once every two weeks," the report says.
Benchmark results from the report suggest for most organizations, effectively reducing and sustaining compliance results mean overcoming 70 per cent of deficient controls that are IT security specific. For most organizations, defining, controlling, and governing these IT-related deficiencies means better managing the mix of labour and automation in IT to reduce and sustain results.

"The benchmarks show that organizations spending more on IT security have fewer deficiencies. Moreover, the findings show that organizations spending less on contractors and services and more on equipment and software to implement automated IT-based continuous assessment are faring better," the report says.

The benchmarks show that improving IT compliance depends on three critical factors:

The frequency with which IT compliance is audited and measured; how much time is allocated to IT compliance by the organization, and pending and spending allocation on IT security. Of these, the most important factor is the frequency of monitoring and measurement.

The CIO is ultimately responsible for the adherence to, and auditable demonstration of compliance procedures within the organization, says Pierre Ketteridge, a consultant with UK-based IP Performance. That means he or she has a burden of duty to understand the broader ramifications of compliance and the consequences of non-compliance, be it to SO17799, SOX, HIPAA or any other legislatory or regulatory body requiring compliance. He or she should have full confidence in the CSA, chief information security officer (CISO), or whoever fulfils that role within the organization.

"In larger enterprises, the compliance process is a continuous process, with divisions and departments being audited throughout the year, and the circle of conformance, validation and audit turning constantly," Ketteridge says. "In that environment, a team of internal audit consultants will be working with and briefing staff and management in an ongoing process.

"In smaller organizations the burden of collating information, validating and self-auditing may well be outsourced to external consultants on an ad hoc basis, which can lead to management and staff not fully understanding or 'buying into' the process. Resistance to meeting with the consultants, providing timely data and the like can all destabilize the 'self-auditing' stages of the compliance lifecycle."

When compliance efforts appear in danger of being destabilized, Ketteridge recommends adoption of self-evaluation and auditing tools to allow secure, subscription-based self-evaluation against Industry and regulatory/legislatory standards prior to undergoing official audit. That way, he says, managers can provide the required data in a self-managed, scheduled manner, with the onus and responsibility being clearly devolved to them, while validation is carried out offsite by qualified consultants.

Managing this process may fall to the CSA/CISO, Ketteridge says, but it is the CIO who ultimately holds responsibility for the compliance outcome, so that executive should have tight hold of the reins and understand the underpinning principles of the entire compliance validation/conformance/audit process.

But dedicated compliance efforts alone are not enough. The CIO also needs to champion the business need for

compliance, says Andrew Baker, vice president, IT operations at New York-based subscription fulfillment and database marketing company ARGI. He or she must continually articulate how compliance will advance various business objectives, ranging from staying out of jail to being more appealing to clients and customers who also value compliance, to not having to pay for the PR damage of being caught in a non-compliant state.

"The need to champion and evangelize when it pertains to security and compliance is very important, because there are many pressures to cut corners in these areas all the time as few see security as a business enabler," Baker says. "Hiring the right people and allowing them to do the job for which they have been hired is also a very important thing for the CIO to do."

At the end of the day, Baker maintains, security and compliance have to be built in to everything that is done by the organization at all levels, and not just bolted on after-the-fact. If security is only paid lip service by senior management, then the organization will pay no attention to it either, and a culture of corner cutting will be the norm.

Do Your Homework

It is also vital for CIOs to do their homework and plan well, says New York-based CIO and consultant Susan Hess, making sure they hire the right subject matter experts, including a strong security architect. And they must avoid micro management at all costs.

However, ultimately, Hess says, they need to bear in mind that it is they who will sign off on the compliance documentation as the responsible party.

"You as the CIO are the one in charge of managing the company's risk from the IT loss," Hess says. "Post Enron all C levels must create and build the best culture of compliance possible. Do your homework, use your resources, and listen to what peers in your industry are doing on all levels, SMB to enterprise, to create a culture of compliance.

"Then have a fresh look at it *again*. Ask questions. Plan well. Execute. "If possible have an outside audit. Then sign off and take a sigh of relief."

Click here for Part 3 of CXO Priorities | RISK

More about Enron, CSA, Micro Management