

ON THE RECORD

Strategies for
IT Business LeadersSeptember 2005
Number 57

Symantec Corp. CIO Mark Egan, author of "The Executive Guide to Information Security" (Addison-Wesley, 2004), shares his views on information integrity, and the evolving compliance and security landscapes.

Q: Who, beyond a CIO, should be involved in a company's information integrity strategy?

Egan: Because of regulations and today's threat environment, information integrity is typically overseen by a company's IT and security organizations with a fair amount of overview and oversight from a company's board of directors. Your board should evaluate your information integrity status and conduct a risk assessment once per quarter.



Q: How can CIOs balance the needs for information availability and security?

Egan: You have to keep in mind that you can never achieve total security. It's not possible because you'd never get anything done. With too many security barriers in place, you'd hit constraints in terms of the economics on availability. So, the first step is to look at your business and your priorities. Sort your applications into three categories: Mission critical, critical and standard. On Wall Street the mission-critical system would be the trading system. Here at Symantec it's our ERP system. Those types of systems need availability and security

solutions that recover everything in seconds. By contrast, a critical-type system is something you can live without for a few hours, and a standard system is likely a departmental productivity application that doesn't harm revenue if it's down for a more extensive period. Based on these classes, you can prioritize your security and availability needs.

Q: What common mistakes do CIOs make when pursuing information integrity?

Egan: Businesses often react to a newspaper article or a single incident. Instead, take a holistic approach and review your information integrity strategy every quarter. Over time, some systems will move from critical to mission critical. Look at your Web site, for instance. It likely started as a critical system for online brochures and marketing. But now it's a full-blown e-commerce system. With quarterly reviews you can track the evolution of your systems and prioritize your availability and security needs.

Q: How have compliance regulations affected information integrity activities?

Egan: The impact has been huge. You're seeing heightened awareness and support at the executive and board levels for information integrity activities. It's quite common these days to have a risk assessment group that reports to the board.

Q: How can organizations ensure information integrity during a merger or acquisition?

Egan: Let's first look at an acquisition involving a small company that's bootstrapped on technology. They likely haven't made IT investments for compliance. You've got to anticipate that they have very little in place when it comes to ensuring information integrity. So you have to bring them up to your level of compliance. You have to bring them up to a higher level and there's a lot of scrutiny. In a merger-of-equals scenario, you have to harmonize different approaches to compliance. Even if the two merging companies are in similar industries, you have to take a holistic view to your programs and systematically merge them and reevaluate your program on an ongoing basis.

Q: Describe your working relationship with Symantec Chief Information Security Officer Tim Mather. Who reports to whom?

Egan: Tim reports to me and has two broad responsibilities. First, Tim sets the strategy, policy and architecture for information security. One of his peers, who runs Global Infrastructure, does the day-to-day work and implements Tim's vision. Then Tim runs a comprehensive review of that work to make sure we're executing appropriately.

witnessed any Symantec downtime, the vendor's own credibility would have been at risk.

"It was a case where Symantec had to prove that it ate its own cooking," says Edward Golod, CEO of Revenue Accelerators, an executive consulting firm in New York. "If there were any security or data integrity issues during the merger process, Symantec would have lost face in the market place. By all accounts, the merger of IT systems went off without a hitch."

What's the secret to Symantec's own information integrity success? Egan credits his close working relationship with Symantec's key stakeholders. "You're seeing heightened awareness and support at the executive and board levels for information integrity activities," says Egan.

At the same time, Egan recommends that companies form a cross-functional governance team that includes HR, finance, legal, IT and other internal leaders who can define and implement corporate policies for information integrity. "All of your key departments need a seat at the table," says Anand, the Sarbanes-Oxley expert.

Unfortunately, some governance teams are out of touch with day-to-day business operations. They may be spending too much time reading the latest news headlines about executive convictions related to Sarbanes-Oxley, and too little time assessing their own business's performance. Here, Egan notes, it's critical for organizations to establish clear information integrity benchmarks and goals for future improvement. With