nerej
CELEBRATING 55 YEARS

Licata Risk cautions CFOs to take charge of IT security

September 12, 2013 - Financial Digest

Risk management usually falls in the domain of the CFO. However IT security often stays within the IT silo. This approach will not work long term; the CFO needs to take charge.

The CFO has to own IT security because:

1. IT security involves protection of assets, liability exposures and regulatory compliance. This is more than a technical IT matter;
2. It involves computer systems outside of the company, over which IT has no control;
3. It involves managing the flows of liabilities in contracts;
4. Cyber Risk insurance must be negotiated; and
5. Someone above the IT dept. has to be concerned about the insider threat from the IT unit itself (the folks with the most access - often complete and absolute access).

The CFO and his or her risk manager have to tie all these pieces together into a coherent risk management program. The CFO should think of the IT department (or the CIO if there is one) as consultants on one very important component of the RM program.

The CFO is in charge of producing credible financial statements. One thing that makes financials credible is protection of the assets and the revenue so prominently displayed, and minimization of new liabilities (from IT related lawsuits, for example) that could alter the financial picture. This involves protection from all kinds of losses; one of them is IT security failure. Additionally there is the need for compliance with regulations involving IT - from privacy laws to Sarbanes Oxley. This multitude of regulations mandates legal, administrative and physical security measures in addition to the pure IT controls. The CFO/risk manager must orchestrate it all.

When computer systems outside the company are involved, the IT department will not have the ability to control security. Computer systems other than the company's own will be used for things like electronic banking for bill paying, whether the systems of the banks or of other third parties. In these cases, the CFO/risk manager, along with counsel, will negotiate contract terms having to do with security and liability for breach. One key question will be who is assuming liability, and to what extent (not just the usual "gross negligence and willful misconduct") for breach of the payment "system."

Furthermore there is insurance to negotiate. The company's crime insurance must always include the Computer Fraud and Funds Transfer Fraud coverage grants. The language of the policy must be broad enough to encompass the payment system as a whole, not just the common limitation to "owned computer systems." This is risk management, not IT security.

Every company now uses the cloud to one extent or another. Cyber Risk insurance must be broad enough in scope to cover cloud activities and related potential data loss and interruption of income. There is no such thing as standard insurance terms - especially in Cyber - so it is a negotiation. Same with the contract with the cloud services provider: it must cover much more than the SLA

(service level agreement) which is usually the extent of the IT unit's involvement. (SLAs give promises of service and have stated liquidated damages amounting to return of fees, free service, etc.). SLAs are a smoke screen covering over the important contractual issues of indemnification and limitation of liability - or preferably lack thereof.

The CFO must take charge of data backup. The CFO must drill down into the backup system for the following reasons:

* The best IT can do is have what they think are state of the art backup systems. If they fail, not IT's fault - they legitimately did what they could. Preparation for failure resides above IT.
* Is there sufficient redundancy? If the core data is corrupted, what prevents the backup from being corrupted?
* Is there insurance to cover human error or system failure? Does the insurance loss valuation include restoration from original source documents, a very expensive proposition?

Finally there is the insider threat. Any employee can go bad, but the IT staff have the access to go along with it. At the top of the IT dept reside the keys to the kingdom itself. The doomsday scenario is destruction of all the data and simultaneous destruction of the backup as well. This could be the end of the company. Perhaps slightly less destructive would be theft and resale of the company's trade secrets.

The solutions to this problem obviously do not rest with IT. The CFO's risk management team must devise a plan which involves:

* Segregation and very limited access to the firm's intellectual property;
* Testing of data backup and extra copies of the backup kept in custody of other than IT itself;
* Audit of the performance, and monitoring of the activities, of the IT department by an outside IT consulting firm.

Separate from the insider threat is the provision of outside security consulting as a resource to IT who by nature are generalists, not security specialists.

The CFO owns risk management. Risk management owns IT security. IT is a resource for the risk manager. Implement this model and your company - and you - will be more secure.

Frank Licata is president of Licata Risk Advisors, Boston, MA.