IT Security Audit: Are You Doing Enough?

By: Abhishek Raval | Feb 09, 2010

Records. Numbers. Audit. Analysis. Pattern. Proactivity. Efficiency. This is generally how the cycle works with anything we try to document and analyse. Basically, an audit process lets us know where we stand. So where does audit figure in the IT domain? Ever tried analysing your IT security? Knowing how safe the IT set-up is through an audit? Biztech2.com gives you a lowdown on this trend that the CIO cannot afford to ignore.

"There are a number of security incidents that used to happen earlier. We started recording them year-on-year (YoY) in the Risk Register and remediating them consecutively. I have seen a reduction in those incidents over time. From each year to the next, the cost of security has also gone down." These words are from a man, who comes from an industry that has suffered some humiliating security breach incidents in the past in India. Suresh Iyer is the Chief Security Officer (CSO) for APAC with Aditya Birla Minacs. He admits that the company has been able to tremendously improve its data back-up testing process after it adopted a rigorous, calendar-based approach to security audit.

IT security audit: Where do companies falter?

IT security audit has been quite often considered as a one time process within organisations. They normally go for it just before the financial year closure. "IT security audit is not only done for the preparation of the financial year closure though it is branded in one sort of space to say that it is right to have the assurance as part of the financial closure process," says Iyer.

Non-alignment with business is another major issue with IT security audits. "The business is not adequately involved in the audit process," says Sunder Krishnan, Past President of Mumbai Chapter, ISACA and CRO, Reliance Life Insurance. He goes on to say that information security behaviour/ practices are not considered a part of the KPIs of business executives. Krishnan feels it is the responsibility of the CSO to make the management understand the importance of security. "He should be well versed with the business language to get the buy-in for security projects," says Iyer.

For example, when asking for a patch management server, the CSO should not start with 'I need a patch management server that will cost $ 25,000'. Instead, it should be communicated to the management that if the patches are in a stable condition in the organisation, it can bring about a decrease of downtime and foster revenues worth $ 350,000. With this message, it automatically makes sense for them to consider the process of risk mitigation more closely.

Vaguely drafted employee agreements is another point where enterprises falter during IT Security audits. The IT employee's offer letter is often very basic in nature. It doesn't contain important provisions of confidentiality, data protection etc. That's a mistake because in case of an eventuality of the same employee stealing the company data, the company will be at a loss as the initial documents are not foolproof to protect the company's interests. Moreover, the company will be unable to save itself from third-party litigation.

Audit best practices

There are various best practices to ensure a smooth IT security audit process. For companies that have a large employee base, who exchange data among themselves, there should be adequate documentation that regulates that the same data is not shared with outsiders, feels Huzefa Tavawalla, Associate at Nishith Desai Associates.

Security threat is both internal and external. Internal regulations can curb unsafe employee practices while contracts need to be watertight when dealing with vendors and third parties to protect the organisation's interests. In case of employees, offer letters should have appropriate clauses to ensure that the employer's interests are safe. Secondly, in case of e-commerce, proper clauses and physical policies should be in place for online transaction integrity.

"At a higher level, the best practice is to map audit programs to ITIL and COBIT standards," says Krishnan. Information security professionals should be asked to certify with security certifications like CRISC that focus on how to address IT risks. Going back to plainly drafted IT employee agreements, Vivek Kathpalia, Partner at Nishith Desai Associates suggests that it is advisable to get the templates of the agreement prepared by the company lawyers. They should also keep on updating the agreement according to the regulatory and legal changes effected during the respective period. This proactive approach has to be shown by the in-house team at the company level.

According to Iyer, having an Acceptance Register of the potential risks is very important. "The gaps that aren't supposed to be around, once these are identified, there are two options to close them. One is remediation of the problem and the other is to go back to the management and get the acceptance of the problem. So at any point in time, one should have an acceptance register and a closure register so that it becomes a smooth overall process," explains Iyer. For example, at Aditya Birla Minacs, e-mail encryption was limited. This was found out in the middle of the year. Adequate budget was not available at that point in time to enhance the encryption standards. It was accepted as a risk and in the subsequent year the required budget was allocated and proper encryption was made available. The entry was first made in the acceptance register and followed up with due action consecutively.

The regulatory angle

Finally, the regulatory changes in the country can affect the IT security audit process and can have huge implications for the company in case of a fraud.

"We expect some strict cyber laws to come into force this year so that fraud prevention and detection becomes a lot easier," says Iyer. Mobile commerce and e-commerce transactions will considerably drive these fraud detection practices. e-Filing of police and fraud complaints will be implemented.

There are some special concerns around sections 52, 64, 69(D), 70 and 70(B) in the IT Amendment Act 2008. Aditya Birla Minacs has given whitepaper inputs to NASSCOM in response to how to deal with certain cyber crimes. "We have specified the changes with respect to encryption. We have given detailed scenarios of data thefts, data transit, monitoring of gateways in real time etc," says Iyer.

Conclusion

IT security audit can give CIOs a view of the existing risks and how to go about tackling them. It is definitely not an area to be neglected and certainly not one that the CIO can afford to have loopholes in.