Incident & Breach Response , Professional Certifications & Continuous Training , Security Awareness Programs & Computer-based Training

Breach Management: Security Governance is Critical

IDRBT's Ramasastri on How to Manage and Fight Future Breaches

Geetha Nandikotkur (AsiaSecEditor) • March 23, 2016 15 Minutes

00:00 00:00

Dr A S Ramasastri, Director, IDRBT

Indian enterprises find it increasingly difficult to manage data breaches, given their rising complexity. And assembling pieces of the complex puzzle is a humongous task, says Dr. A. S. **Ramasastri**, director, Institute for Development and Research in Banking Technology.

To create a perfect cybersecurity ecosystem to fight future breaches, it is vital to assemble all the pieces of the puzzle including governance, skills, policy, systems, technology and solutions in the right proportion.

"Most importantly, evolving a security governance structure with the right ownership within enterprises - which can provide assurance to the organization on handling data breaches - is the need of the hour; this is completely missing," he says.

"While enterprises are making investments and deploying controls to protect organizations' data and information, there is no effort being made to sensitize the organization, policy makers and business heads about information security and risk management, which plays a major role in fighting future breaches," he says.

"I would think the concept of ownership attached to risk management within enterprises is missing across enterprises. Most often, we find security being discussed in silos," asserts **Ramasastri**.

To this effect, he says, every sector should have a cybersecurity chief who can form subcommittees to create an information sharing mechanism to share best security practices. This would be one way of giving assurance to organizations.

Another important component is building skills, which is a national mission, he argues. "Just like having different academies for defence, police and others, we need to have a cybersecurity academy across the states to build specialised skills which enterprises can look out for," says **Ramasastri**.

In conversation with Information Security Media Group during the Data Breach Summit Asia 2016, in Bengaluru recently, **Ramasastri**, a keynote speaker, reiterates the need for practitioners to hire the right talent and find ways to retain them, besides focusing on the art of integrating all aspects of security into a single interface. This is possible with a good security governance mechanism, he says. **Ramasastri** shares insights on:

- Establishing information sharing mechanism;
- Mechanism to recruit the right talent;
- Importance of data breach disclosure norms.

Prior to joining the Institute, Dr. **Ramasastri** was the Chief General Manager-in-charge of Department of Information Technology at the Reserve Bank of India. At RBI, he spearheaded many important projects including the Implementation of the Next Generation RTGS, adoption of international standards like XBRL and ISO 20022, conceptualizing and guiding of banks on Automated Data, and preparation of IT Vision of RBI for 2011-17. He is a member of the Institute's Governing Council, Member of Faculty of the RBI Staff College.