Ramping Up Data Security in Co-operative Banks

By Rishikesh Kamath
Vice President,
Products & Services

In August, 2018, the Cosmos Co-operative Bank (also known as Cosmos Bank), was robbed of INR 94 crores by hackers using malware that cloned debit card details of thousands of bank customers. They used a multi-pronged strategy to hack into the banks debit card payment system (specifically the servers that control the ATM switch). In a little under two and a half hours, money was withdrawn from ATMs across 28 countries using cloned debit card details. By the time it was detected, nearly 15,000 fraudulent transactions (Visa and RuPay cards) had already been made.

What is really alarming is that Cosmos Bank is not a new entrant, or a minor player, in the banking sector. In fact, it is one of India's oldest and largest cooperative banks. According to Wikipedia, Cosmos Bank is also among the first co-operative banks to implement a full-fledged core banking system across all of its 140 branches. The fact that one of the most technologically advanced co-operative banks in India was prone to a vulnerability of this scale, raises many questions around the overall data security preparedness of the co-operative banking sector in India.

WHY HAVE CO-OPERATIVE BANKS BEEN SLOW TO ADOPT?

Technology investments in the Indian banking sector have been heavily skewed towards large commercial banks (both in the public and private sector). Co-operative banks, by virtue of their limited financial resources, localized operations, few products and small client bases, have traditionally not aligned to changing technology trends. We have rarely heard of cooperative banks, small finance banks or regional rural banks take an ‘early adopter’ position on with regard to new technologies such as cloud, distributed computing, mobile banking, big data and analytics. In fact, while commercial banks have made the most of technology innovation, recent reports show that, out of the 1,500+ urban cooperative banks in India, more than one-third still don’t have an enterprise-class core banking system.

WHAT IS DRIVING TECHNOLOGY ADOPTION TODAY?

At the same time, we are seeing a number of significant trends that are driving technology adoption in the cooperative banking sector today:

- Competition by private banks who have increased their penetration to semi-urban and rural areas and are eating into their customer base with more competitive products
- Customers are quickly moving to digital banking, driven by the largescale adoption of mobile phones and strong, nationwide internet penetration. Banks which depend on traditional, branch-based banking processes will not be cost-competitive in the long run
- Speed and availability are becoming competitive differentiators in the banking industry today. Customers are expecting anytime / anywhere service, centralized operations and competitive pricing.
- Regulatory demands, such as implementation of Basel III, will require co-operative banks to adhere to stringent capital adequacy norms. This means that banks will need to leverage technology to improve their NPA position and manage risk better.
- RBI has recently announced a financial incentive of INR 9.4 lakh (per bank) for computerization of urban cooperative banks (INR 4 lakh for implementation and INR 5.4 lakh for maintenance over three years)
- Structural changes including the recent push by RBI to allow some urban co-operative banks (UCBs) to convert to small finance banks (SFBs). This move is intended to enable well-structured UCBs to grow and increase their range of offerings

HOW WILL THE DATA SECURITY SETUP NEED TO EVOLVE?

With the adoption of digital technology, co-operative banks would open themselves up to a huge number of data privacy and security risks. Limited investments in data governance, privacy and security have resulted in many of these organizations (especially the larger co-operative banks with nationwide presence) being vulnerable to incidents of data loss, ransomware, malicious hacking attacks, service denials and identity theft. As the technology ecosystem for these organizations starts to grow and evolve, their data security architecture will need to account for a number of important factors:

- **'Best-in-Class' is a Strategic Imperative**
  Hackers are highly motivated (for financial or criminal reasons) and are constantly working on ways to identify and tap new vulnerabilities in applications and infrastructure. Security tools and protocols, without compromise, need constant upgradation and remain 'best-in-class' to be effective. This will put significant pressure on technology teams to implement, maintain and upgrade security infrastructure.

- **B. Data Outside Systems Need to be Managed Effectively**
  For many co-operative banks who have not built sufficient process maturity and still rely on manual processes, a large proportion of data assets are actually stored in physical form (paper). Automation, therefore, becomes an important step when creating a governable data security environment.

- **C. Data Governance Policies Need to Be Tested Well**
  Regulatory oversight for co-operative banks have traditionally been as stringent as they have been for commercial banks. This, however, is changing very quickly. In the new, digitally enabled and consumer-driven world, co-operative banks will have to ensure that their data governance policies are water-tight and completely adhere to a wide spectrum of regulatory norms.

- **D. Security Infrastructure Must be Scalable**
  As the co-operative banking sector starts adopting best practices (in terms of customer services, products and technology) from commercial banks, they will need to incorporate a large number of data sources and channels. For example, internet banking apps, bancassurance products, payment gateways, mobile wallets, new deposit products, social media, retail tie-ups, demographic information, etc. Security infrastructure therefore needs to be scalable enough to handle the growing volume, speed and complexity of data that these banks would need to handle.

SECURITY MANAGEMENT IS A CONTINUOUSLY EVOLVING PROCESS

As the co-operative banking sector starts to ramp up its security infrastructure to meet new business challenges, it will find that this is a continuously evolving process that will require continuous upgradation of skills. While the industry takes initial steps to build a robust security architecture, it becomes imperative to partner with companies that are experienced in implementing, managing and continuously upgrading security infrastructure (at both technology and policy level). In India, infrastructure leaders like Netmagic have been offering comprehensive Managed Security Services for nearly a decade, which help large enterprises as well as smaller, growing organizations leverage SaaS based capabilities on a pay-per-use basis.