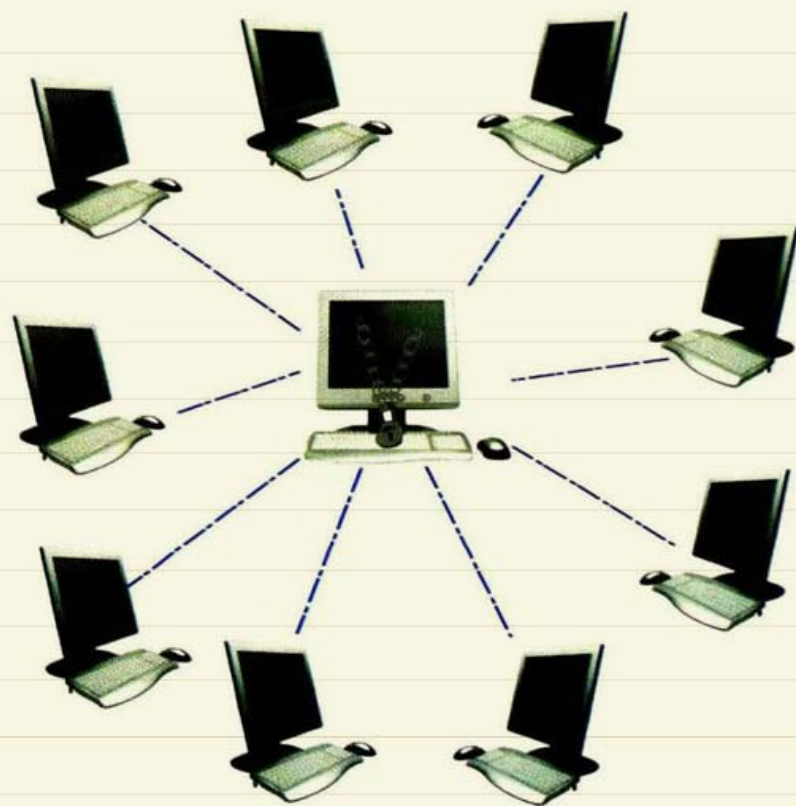


Safety Compromised

IT has moved from back office to total branch automation. Is overall risk mitigation possible?



Over the last decade or so, the Indian banking and financial sector has seen several transformations. The operating environment of banks has changed significantly in terms of liberalization of regulations, increasing competition from both domestic and foreign players and need to re-vamp the business, which came with the legacies of the protected era. Simultaneously, implementation of in-

clearing operations; the adoption of IT moved to the front desk in the form of total branch automation. Further, while competition gets tougher, there is now a constant pressure on IT departments to achieve more within tighter budgets. However, while the adoption of technology has brought several benefits to the financial institutions, various threats in terms of malicious software, unscrupulous insider and external fraudsters, natu-

■ **Business threat related to i-Banking:** To remain competitive in the industry, where all banks are putting efforts to ensure easy access and transaction process for their end customers, the associated security threats and challenges mount higher. Transmitting data across the Internet link, through secured and unsecured channel is always a challenge. With increased convenience of online banking, the threat of unscrupulous elements getting into the networks and perpetrating frauds looms large. In this context, the security governance, security policy and its implementation and the well-tested and reliable business continuity measures assume importance. As any system cannot be perfect, its audit and expeditious action on the findings become crucial to continuous enhancement of security systems in the face of ever-growing sophistication of potential attackers. The bank has to ensure and safeguard not only its information database but also customer's critical investments from malicious intender on the Internet. The requirement of encryption solution, digital certificate, secured connectivity for mobile users and customers, secured hosting environment have become extremely critical for all BFSI organizations.

■ **Managing and correlating threats across the enterprise network to contain risks:** Event correlation is the key to properly identify the true threats an organization is facing. Threat correlation ensures that risk management teams are always focused on the top most priority, simultaneously reducing potential risk and corporate liabilities. A good correlation solution has the power and scalability to collect, normalize, consolidate and correlate events from the largest organizations, enriching data

formation technology began in earnest in the sector. Starting from back office automation, which was aimed largely at processing of voluminous data and automation of cheque

ral and man-made disasters are real. Let's take a look at some of the top information security challenges faced by the banking and financial segment.

with extensible threat taxonomies, knowledge-base links and both user-defined and automated responses to threats. Recent security regulations for the BFSI segment have escalated

the demand for threat correlation.

■ **Near real-time mitigation of phishing:** A recent report by Cyveillance stated that number of phishing attacks grew by 50% in the first two months of 2007 from 800 to 1200. Further, another report by University of Indiana School of Informatics showed that an average of 8 to 14% of respondents to a phishing email go ahead and click on it. To safeguard themselves from potential risk, financial institutions need to get this number down.

■ **User provisioning and identity management:** User provisioning and identity management systems allow financial institutions to know who is accessing what and provide a suitable user experience by restricting or controlling access accordingly. In light of the increased cases of hacking and unauthorized access, enterprises are adopting automated policy enforcement that helps maintain optimum security levels while managing large number of users. Integrating digital IDs with provisioning systems can further help to lower total cost of ownership and maintain consistent security policy across users, applications and environments.

■ **Managing privacy and confidentiality of user data:** Customer related and transaction data forms the backbone of banking services; more so in the current scenario where banking is becoming virtual and transactions are becoming electronic. To fight the increasing competition, it is becoming critical for banks to maintain the privacy and confidentiality of user data.

banes-Oxley, HIPAA and BASEL-II. According to an IDC Survey, the worldwide information management for compliance market will cross the \$20 bn mark in 2009 growing at a compound annual growth rate of 22% through the 2005-2009 forecast period.

With the help of Security Service providers, financial enterprises can adopt inexpensive and unified approach to compliance management which also reduces the cost, time, effort and complexity involved in adhering to multiple regulations.

■ **Increased risk from internal network:** Most of the networks of BFSI organizations in India are increasing their geographical spread in order to meet business directives. This is exposing them to loss of administra-

branches in an effort to reach maximum market penetration, banks are now facing new challenges in ensuring maximum security from the various end points. Business demands nowadays, interaction from a dynamic environment beyond the bank's internal network, which imposes various threats. End point security solutions help banks to ensure compliance to implementation of certain pre-defined security controls on all the end point accesses. Further, preventing data loss, desktop firewall, desktop HIDS, Network Access Controls (NAC), patch management solution, anti virus solutions help banks in ensuring the compliance have a secured and wider network.

Managed Security Services has emerged as an important discipline to

An Eye on the Phish

Some recommended strategies to mitigate phishing risks

■ **Deploy transactional authentication software** Transaction authentication software applies numerous other factors that include the computer hardware, IP address, geo-location, time of day, user history, display settings, browser plug-ins to examine and approve each transaction. If the software finds any discrepancies then it escalates to management or begins to ask questions.

■ **Deploy software which quickly shuts down phishing sites** Enterprises should use service providers that screens the Internet 24 hours a day looking for phishing sites that may target you. In some cases they can prevent an attack from taking place while in others they can quickly respond and block the website.

■ **Educate the consumers** A concerted education campaign is needed by the financial institutions. It must describe the threats and appropriate counter measures over and over to the consumer such that they absorb and adopt.

■ **Deploy stronger authentication selectively** Stronger authentication should only be used for higher risk individuals in higher risk situations. This will help to mitigate the risk of common keyboard logger attacks but won't stop in the middle attacks. Consider usage of things like confirming cell phone calls, digital signatures and SMS messages to help mitigate your enterprise risk. One time passwords are also useful but are more expensive to manage.

Data Leakage prevention solutions and encryption solutions for mobile assets are being increasingly adopted by BFSI organizations to keep this data confidential and inaccessible from improper hands

■ **Regulatory compliance:** Globally, there are a staggering 16,000 regulations that businesses need to comply with, including significant legislation such as IT Act, SEBI Clause 49, Sar-

tive controls over internal users. Financial organizations are countering these threats by working with various zero-day prevention technologies like signature less behavior based protection solution and network access solutions for granting access to the network, only for valid, authenticated and known users.

■ **Need for end point security:** Due to the faster spread of the BFSI

address the above challenges, through integration of people, process and technology. Each of these three components should be managed considering the capabilities and limitations of others. When the components are considered as a whole, they should provide for adequate overall risk mitigation.

—**Prosenjeet Banerjee**

The author is associate vice president, global security services, HCL Technologies
maildqindia@cybermedia.co.in