

Bank Leumi deploys new technology for compliance with Basel 2 equivalent regulation

Following a large-scale embezzlement that eventually collapsed one of the country's small banks, Israel's Supervisor of Banks enacted Regulation 357 based in part on the Basel 2 Accord and somewhat similar to the US Sarbanes-Oxley Act. In effect from July 1st, 2004, the new regulation requires banks to, among other things, maintain a full audit trail based on computerized recordings (logs) of access, transactions and queries performed in their information systems. The logs should include the identity of the person accessing the systems, the place, time and particulars of the transaction, such as the account number accessed and the type of access (i.e. read, update, delete). The records management systems should also warn designated parties within the organization of unauthorized external activities as well as exceptional activities of the

various types of users, as defined by the bank management.

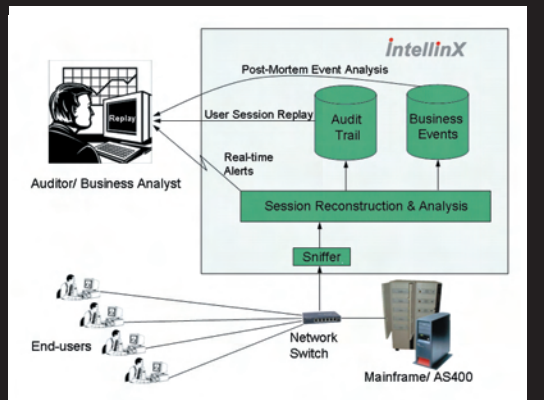
Founded in 1902, Bank Leumi is Israel's leading international financial group with about 250 branches in 19 countries, over 1.7 million customers, and assets under management in excess of \$100 billion. In the beginning of 2004, when the Bank of Israel published the new regulation, Mr. Sasson Mordechay, Senior Vice President and Head of Operations Division at Bank Leumi, assigned a highly experienced group of managers to a task force that would coordinate the compliance project throughout the bank. One of the main challenges the team identified was creating a full audit trail of the bank's mission critical legacy applications running on the central IBM mainframe. Unlike network devices and infrastructure systems, there are typically no tools for analyzing user activities at the application level, especially when the

applications are developed or customized in-house. In the case of Bank Leumi, most of its applications had no embedded logging facility, so creating a log of all actions performed by all end-users required modifications to many programs in dozens of applications. The team estimated that it would require about 100 programmer-months to accomplish this task. Furthermore, additional programming resources would be needed in order to keep the logging facility up-to-date during the natural course of maintenance throughout the lifetime of these applications.

In order to meet the compliance deadline and to save resources, the Bank Leumi task force looked for an off-the-shelf software solution with logging and alerting capabilities that support the new regulation without requiring changes to the legacy applications. The only solution the



Mr. Sasson Mordechay, Senior Vice President and Head of Operations Division, Bank Leumi



team found was IntellinX, a new patent-pending technology from Sabratec Ltd., a leading provider of legacy integration solutions. IntellinX records all interaction (displayed screens and user keystrokes) between all end-users and legacy applications in real-time. It features zero-footprint non-invasive sniffing of network transmissions from which the original screens and user keystrokes are reconstructed. The content of the recorded screens is analyzed in real-time, automatically recognizing screen titles, field captions and values, and user keystrokes. The data is analyzed using pre-defined rules that identify suspicious user acts or behavior patterns, triggering instant alerts to designated personnel. These alerts allow an auditor to immediately zoom-in on specific suspects and replay all their actions. The recorded sessions are stored by the system, allowing for new rules to be applied after-the-fact.

Mr. Mordechay approved the team's recommendation to evaluate IntellinX during a short Proof-of-Concept. The product, installed in the bank's test environment in a few hours, immediately started recording user activity in that environment. As IntellinX runs on a separate server and there is no need to install any software or hardware on the host system or the clients, there was no performance impact on the host, clients or network, and no risk to normal IT operations. The Proof-of-Concept provided the full audit trail required by the Bank of Israel regulation. Since this audit trail consists of very sensitive data, various security aspects were evaluated. Sabratec adhered to the bank's strict security requirements, including encryption and digital signature of the recorded data so it can, if needed, be admissible in court.

As the results of the Proof-of-Concept were very positive, Bank Leumi decided to move quickly,

purchasing the product and deploying it in its production environment. Compliance was achieved by July 1st, 2004, with 24X7 recording of all mainframe end-users. Initially, the product was used out-of-the-box, allowing replay of specific user sessions and queries such as "Which users accessed which specific customer's account within a specific time range?". Subsequently, the internal auditing unit will define business rules to track suspicious user behavior, triggering instant alerts. Defining new business rules is an ongoing process as the new rules can be applied to the data previously recorded in order to identify any irregularities that have already occurred.

For obvious reasons, Bank Leumi cannot disclose the exact rules it utilizes for fraud detection. Nevertheless, the following are examples of rules commonly applied in banking scenarios:

Example 1 - While bank tellers normally access customer account details by entering the account number, rarely is the search done by customer name. IntellinX can detect in real-time a teller who frequently or continuously searches for account details by customer name at a rate of 3 times higher than the average rate.
 Example 2 - Accounts belonging to celebrities or bank managers are typically handled in the same way as the accounts of regular customers (non-celebrities), rather than assigned to specific clerk. When a specific user continuously or excessively accesses these special accounts, IntellinX can

send an instant email alert to the designated auditor, advising of suspicious activity or malicious intent to exploit confidential customer information.

Example 3 - Bank clerks are authorized to add beneficiaries to or change customer addresses in customer accounts. In the case where a user frequently performs these actions or if the new address or beneficiary is the same for different customers, IntellinX can send immediate SMS to the designated auditor. In addition, since the system stores all changes made by the user in a separate auditing database, an auditor can later verify if these were previously approved by the customer or are part of a fraud.

While the above-mentioned rules can detect fraudulent attempts, the fact that all user actions are recorded may further deter users from committing fraud.

After running the IntellinX recording for several months and creating a full audit trail of some 10,000 end-users, Bank Leumi has reported that there is no impact on the performance of its host, clients or network and that the recorded data, because of its extremely condensed format, occupies less than one standard PC disk. Mr. Mordechay further states, "We are very pleased with IntellinX as a non-invasive solution for compliance and fraud detection. We are very satisfied with the support we receive from Sabratec and are expanding the use of IntellinX as the main logging solution for various types of client/server applications."

CEO

IntellinX is marketed in the US by Sabratec Technologies (located in New York City), for compliance with regulations that require full audit trail such as HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley and others. In Europe IntellinX is marketed through Sabratec's local partners. For more information on IntellinX please contact Sabratec Technologies at +1-212-513-0977 or refer to www.sabratec.com.