

Why it is critical to protect the DATA and why protecting a USER is not good enough...

bioLock is the only SAP certified technology that can protect data and tasks within the SAP system independent from the SAP User profile with biometrics and help to increase the bottom line:

- All companies want to increase their bottom line and they focus on increasing the revenue or decreasing cost. In the recent years a very important 3rd factor has been added to the list: **NOT LOSING MONEY!**
- Fact is that the so-called White Collar Crime (Internal Fraud) is the fastest growing crime in North America. In 2008, the **first single incident averaged \$175,000 in damages**. Every 4th incident was over \$1Million and 9 cases exceeded \$1Billion (Source: Certified Fraud Examiners). The average fraud damages were 7% of the revenue.
- It takes an a few years to detect an internal fraud scheme and it is normally only detected and stopped by internal whistle blowers. Conviction and punishment, as well as sending the right message to the employees, is mostly very difficult. Many successful **fraud cases are never even detected** since the thief is smart enough to stop before being detected, but the damages are already done. Chances are that you have fraud cases that you don't know about.
- In the case of UBS Paine Webber a time bomb was planted to disable 1000's of computers. The business loss was never estimated, but exceeded millions of dollars. It cost \$3.1 Million dollars to bring the computers back up and running. Everybody knew who was responsible but his lawyer established quickly that **40 people had a password** for the logon that was used to cause the damages. The lawyer used, what is called the SODDI defense (Some Other Dude Did It). Sine it is so hard to convict internal thieves, there is no deterring warning message to other employees.
- **Everybody has access to everybody's password** and an intruder will ALWAYS use a different logon with extended authorizations to commit a crime. In fact, all Segregation of Duties efforts (making sure that John can't purchase a new laptop for himself and then go in the finance system and pay for it) are based on the assumption that John can only log on as John and use his own authorizations. Customers will agree that this is a misconception and in the security world we know that John would log on as his supervisor anyway to purchase the laptop and then use a profile from the finance department to pay for it. See the password link below to learn, how easy intruders can get a password to any SAP user profile with extended authorizations. Password sharing is common practice and 82% of all passwords are written down (SAP Info). The solution is to uniquely identify the Actual User behind the User Profile.
- bioLock is the only technology that can offer you **5 additional levels of security**, completely independent from the SAP User profile. bioLock adds a "biometric door lock" (Learn more about this simple concept: [PDF](#)) and the customer defines, where they choose to add this biometric door lock (HR Data, Finance Data, Wire Transfer, Purchase Order Transaction etc. – physically every mouse click in the SAP system). Now they define in the bioLock application which person will have access to that protected task with their biometric template. So far the business has no control over which person has access to that outgoing wire transfer or which person can maintain that extremely critical credit card information. All administrators with SAP all and external consultants as well as certain managers might have access. Without using biometrics, it is IMPSSIBLE to control and stop, who can access which critical data.
- With bioLock, this task becomes very simple: Protect the selected critical task with our biometric door lock. Select a global check for that function to require any user to provide a biometric template. Now add a VIP list and define invited users for this function. Once you have added Joe and John to this VIP list they will be the only two people that could get access to the function and even better, a log file will prove – uniquely identified with biometrics – which person did that \$1Million wire transfer to the Grand Cayman Islands. **Next to the security aspect bioLock also offers for the first time clear accountability**. You don't need to protect every user in the organization with biometrics, just the ones that need to have access to the task that you wish to protect. Generally, only a few 100 users have to have access to critical functions (power users) and therefore, would be protected with the bioLock.
- As a result companies only need to implement bioLock for a few 100 selected users, NOT for all their named SAP Users. The installation and setup of the system will take about a week and there is no training required for the end user. Biometric devices are available, as mice, keyboards or external USB readers, like the Eikon from UPEK or the P5000 from Zvetco. Devices like the SecuGen Hamster are even FBI approved and FIPS 201 compliant. ~25% of all laptops being sold to corporations have a build in fingerprint sensor that is already compatible with bioLock. A typical bioLock installation will cost \$150,000 - \$500,000 – **a minimum investment compared to the actual damages**.

More info about bioLock at www.bioLock.us

More info about "true" fraud mitigation at www.fraudmitigation.com

More info about the danger of outdated passwords at www.showpasswordsthefinger.com

Or call / Email us for any questions: 813-283-0070, 1-877-bioLock or info@realtimeorthamerica.com