

## 7 Reasons to consider biometrics

1. Prevent Jail Time for your Corporate Executives
2. Stop Identity Theft, Financial Damages and Espionage
3. Avoid Expensive Lawsuits, Bad Press and Perception Damage
4. Enhance and Complete your Sarbanes-Oxley Compliance Efforts
5. Comply with Other Mandatory Regulations such as Data Protection Act
6. Save \$100,000 per Year on Administrative Cost – ROI in less than 3 years
7. Protect your IT System, Recover Monies and Send a Clear Message to Employees

Value Proposition

### 1. Prevent Jail Time for your Corporate Executives

Under the Sarbanes-Oxley Act, anyone who certifies any statement in the Section 906 certification knowing that the periodic report accompanying Section 906 does not comply with all the requirements will be fined up to \$1,000,000, imprisoned not more than 10 years, or both. Anyone who willfully certifies any statement in the Section 906 certification knowing that the accompanying report does not comply with all the requirements will be fined not more than \$5,000,000, imprisoned not more than 20 years, or both. Additionally, a violation is also a violation of the Exchange Act! (Source: What is Sarbanes-Oxley 2004). The charges against former Enron CEO, Ken Lay, carry a maximum penalty of 45 years in prison for the corporate trial and 120 years in the personal trial. Corporate Executives blindly hope that only authorized users have access to the financial data that could send them to jail. With 20 ways to get the password to anybody's user profile at any point of time, disgruntled employees could change or delete any financial data and frame executives (See 4 – Enhance SOX Efforts)

### 2. Stop Identity Theft, Financial Damages and Espionage

Your SAP System holds a large amount of valuable information: Finance, HR, Research, Production, Marketing and many other data that are vital to your company's success. Any unauthorized changes or even theft of these data could lead to major financial damages. Identity Theft is the largest growing crime in North America and most of your employees can get access to all of your employees and even worse, all of your clients confidential information. Other common thefts include issuing stock options, paying fake bills or salaries for employees that don't exist, as well as wire transfers to foreign bank accounts. Selling the data to the competition is even more lucrative! Up to 80% of the value of U.S. companies is tied up in what can be characterized as "intangible" assets-information such as: product designs, chemical or drug compounds, manufacturing processes, go to market strategies and customer lists. The first single incident will cost your company an average of \$159,000. Every fourth incident will exceed \$1Mio and more. A recent case a DuPont hit the news with the subject line: **\$400 million corporate espionage incident at DuPont**. bioLock will expand the scope and justification for biometrics from simple password replacement to fraud mitigation ([www.fraudmitigation.com](http://www.fraudmitigation.com)) Prevent unauthorized user access to "intangible" assets-information and uniquely identify and log activities from authorized users to prevent fraud and insure conviction!

### 3 Avoid Expensive Lawsuits, Bad Press and Perception Damage

The access to the SAP System is controlled with outdated and insecure passwords that offer no protection and no identity management whatsoever. Recent breaches at the Department of Veterans Affairs, AIG, UBS PaineWebber and many more have shown that these breaches resulted in widespread negative press and in the case of VA even in a \$26.5 Billion lawsuit! Other laws, like The California Security Breach Information Act, require companies to inform all their customers about any potential breach. bioLock will help to prevent these financial lawsuits, the embarrassing and costly measures to inform clients about breaches and the resulting negative press.

#### **4. Enhance and Complete your Sarbanes-Oxley Compliance Efforts**

Sarbanes-Oxley was established in 2002, with the goal to prevent “another Enron or WorldCom” and make investors confident again in investing in American Corporations. CEO’s and CFO’s are now required to certify that their companies’ annual and quarterly reports are accurate and not misleading, and that they have met their responsibility for evaluating internal controls. Companies spend millions of dollars every year on SOX compliance with a strong focus on Segregation of Duties. All this money is spent with the wrong assumption that only “Joe Smith” can log on as “Joe Smith”. With over 20 ways to get a password for any SAP user profile at any point of time, the company has NO CONTROL about who is logging onto the system using which SAP user profile. Any disgruntled employee could log onto the CFO’s user profile to change critical data for the financial statements. Every administrator could do the devastating changes with his/hers official authorizations! As a result the company could pay major fines and executives could be charged with jail time (See 1. – Prevent Jail Time). bioLock will prevent the severe penalties and potential jail time for executives.

#### **5. Comply with Other Mandatory Regulations such as Data Protection Act**

Other mandatory regulations such as, HIPAA, The California Security Breach Information Act (SB-1386), The Data Protection Act and many more require companies to protect certain data within their IT environment. HIPAA is the United States Health Insurance Portability and Accountability Act of 1996. HIPAA seeks to establish standardized mechanisms for electronic data interchange, security, and confidentiality of all healthcare-related data. Any company that is dealing with HR information in it’s SAP System must comply with HIPAA! Brevard County Government (NASA) won the InfoWorld 100 Award using bioLock to comply with HIPAA. SAP TV made a movie about the success story. The California Security Breach Information Act (SB-1386) is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised or the company has any indication that it could have been compromised. This law is not restricted to California corporations but applies to any company that has California Customers in their database. The recently signed Data Protection Act of 2006, sets national criteria for data protection and breach disclosures. bioLock will tremendously reduce the potential risk, help to comply with multiple regulations and prevent companies from negative public exposure.

#### **6. Save \$100,000 per Year on Administrative Cost – ROI in less than 3 years**

Users call the Password Hotline at least 4 times a year with password problems or to get a password reset (Help Desk Best Practice Survey 2000). Internal costs for the calls are calculated at \$40 - \$100+ (Gartner). The savings for a proposed 300 seat bioLock installation – to protect the most critical parts of your system - would be: 4 calls/year x 300 Users x \$40/per call = \$48,000/Year or \$144,000 in 3 years. Wasted end user time is calculated with 20 minutes a call (\$60/hour = \$1/min) resulting in \$24,000/year or \$72,000 in 3 years. Lost Productivity of at least 30 minutes a call will cost your company at least another \$36,000/Year or \$108,000 in 3 years. The total financial damages for a period of 3 years will be \$324,000 – far more than a bioLock package with comparable seats! bioLock will not only prevent you from major damages, but also offer an ROI in less than 3 years and will save \$100,000/year afterwards! See our “Warehouse Case Study” to learn about “Fast User Switching”.

#### **7. Protect your IT System, Recover Monies and Send a Clear Message to Employees**

It’s human nature to trust your fellow employees - the people at the coffee pot, on your company softball team, down the hall. That’s why it’s so natural for IT managers to focus their network defenses on outside rather than inside threats. What hit UBS PaineWebber shows just how dangerous that one-sided thinking can be. A disgruntled employee took down about 2,000 servers, leaving 8,000 brokers across the country unable to work. IT teams spend sleepless nights on conference calls with IBM and scrambled to reset servers, trying to undo damage that still, four years later, hasn’t been completely repaired. Repairing the damages – not even considering the lost business – cost the company over \$3.1 Million. 3 years later, the defense of the accused has established that over 40 people had access to that user profile with a known password, which was used to cause the damage and they are using the SODI defense (Some Other Dude did It). In other words, the prosecutors won’t be able to prove that it was their client and they will get away with the excuse that he was “framed” by a co-worker. bioLock will uniquely identify the person so a conviction and a potential recovery of damages is possible. In addition, it will send a clear – deterring – signal to other employees. Many damages are done by so called “clueless” employees, who allegedly did not know what they were doing. bioLock will make sure that they watch what they are doing now!