

05.04.2004 / Brevard County implements bioLock to protect HR data:

Space Coast Pioneers with Biometric Security

Government regulations are requiring more and more security for data. Florida's Brevard County has become a pioneer user of a revolutionary fingerprint security system that was developed specially for SAP customers.

No-one will be particularly surprised that a new analysis shows that the number one concern CIOs had coming into this year is security. The analysis was released by IT research company Standish Group and is the result of year-long research. Interestingly the research revealed that – on the downside – CIOs were having difficulty getting budgets to buy the products they thought necessary to strengthen their capability to protect data and infrastructure. On the upside though, respondents said it was easier to find funds for security than all other problem areas such as "upgrades and modernization" or "staff burnout".

Although the Standish research doesn't break down that detail, one area that companies and government entities have to fund is compliance. New laws to protect data are forcing companies to make the necessary investment. Take for instance the Health Insurance Portability and Accountability Act (HIPAA). US employers must know by now that employee medical information is almost sacrosanct under the new law. Breaches of confidentiality can result in large fines and other penalties, followed, of course by negative publicity and the inevitable lawsuits.

How to comply with HIPAA?

The advent of HIPAA is having an impact all across the United States so it is no surprise that the question of "how to comply" ended up within the information systems department at Brevard County, which occupies 72 miles along Florida's glorious Atlantic coast. Brevard is probably better known as the Space Coast, its title in Florida tourist books, as it is home to NASA, the Astronaut Hall of Fame and the Kennedy Space Center.

Brevard became a SAP customer in 1999 and has roughly 100 end users using several modules such as accounts payable, general ledger and human resources. As do all SAP customers, Brevard established, for security reasons, profiles so the user gets only limited access to certain transactions. Users got a combination of those profiles depending on their roles as end users or within certain departments.

While the password and sign-on technology worked somewhat adequately even though it was 6-8 digit passwords that were needed and had to be changed on a regular basis, Brevard's systems administrator, Rick Meshberger, and his colleagues saw problems with it when it came to the looming compliance with HIPAA. Meshberger cited the number one concern was to stop giving non-HR people the opportunity to change medical data about themselves and others which would completely negate compliance with HIPAA.

"HR department employees have authorizations were they can go in and look at everything about that end user. We were worried though if they were to leave their screen unattended; then anybody could go in and make any changes they wanted to, if they could," he said. The Brevard information systems team was equally concerned that end-users – including those within HR – were not careful about their passwords. "Some people had a tendency to write down their password in a place where it was easy to find or they would use very simple easy to break passwords," said Meshberger.

Access control via fingerprint

He and his colleagues had to come up with a way to ensure that when the HR people went into the

system to look at the medical data, Brevard was "sure that they are who they said they are." Enter a company called realtime North America, which is marketing bioLock, a product which it calls the first and only SAP-certified access-control-via-fingerprint solution developed specifically for SAP software and which has been released for SAP **R/3 4.x** and **mySAP Business Suite**.

The product was developed by the US company's German parent, realtime AG, which was founded by former SAP employees back in 1986. Realtime is an SAP solution house and has a client base of more than 200 "Fortune Global 500" companies, including Bayer, DaimlerChrysler, Siemens, Toyota, Esso, Procter & Gamble and Nestle.

BioLock looked like the ideal product for Brevard and Meshberger realized the county did not have many options except forcing the user to make sure they locked their screens or logged off of SAP if they were going to leave their desks. "That was going to be hard to enforce," he said.

Locking certain screens within SAP transactions

Before he signed off on realtime, Meshberger wanted the company to make some small changes to bioLock. "The way we wanted to use the solution they had not done before. So they had to do a little bit of engineering to do it for me. I didn't want them just to lock down the whole transaction, I wanted to be able to go in a lock down certain screens within that transaction."

Brevard wanted the transaction to be available to users who just wanted to access the non-secure data such as an individual's "working hours, pay status and what not." Said Meshberger: "I was already locking down PA20 and PA30 in a way that I could say 'these end users could only access these certain infotypes' but I wanted to lock it down a bit more in HR because they had more critical infotypes that I wanted to protect when they left their cubicles."

In fairly short order Brevard became a pioneer user of bioLock in the US. The software is easy to install; it doesn't affect the SAP software at all and it is easy to use. "So when the users typed in the Infotype 167 it would force them to put their finger on the keyboard fingerprint sensor before it would let them in. It's as easy as that," said Meshberger.

By choosing realtime's bioLock technology, Brevard can also implement a single sign-on capability to multiple systems, not just SAP. The single sign-on is as simple as clicking on the system the user wants and then entering his fingerprint.

Part of SAP's Homeland Security scenarios

The people at Brevard were not the only ones to recognize that the county had come up with an innovative solution. The US newsmagazine, InfoWorld, chose the county to be one of its recipients of the "Infoworld 100 2003" awards, which celebrate enterprise IT projects that have made the best use of technology to meet business goals. Entries were judged on a number of criteria including innovation and project complexity as well as integration issues and how project leaders worked with users and other business units.

SAP too has realized the value of realtime's bioLock. The company incorporated information about and a demo of bioLock as part of a large Homeland Security demonstration that SAP's public sector department organized.

Barbara Gaspard, who is SAP America's director of the US Demo Solutions team, said: "While we were building the Homeland Security demo we identified biometrics as a very viable solution component. Consequently we got in touch with realtime and then implemented their biometrics solution into our SAP Demo System and then incorporated it in our live Homeland Security demo. "The whole demo centers around Emergency Management and Preparedness. We realized that the realtime solution has got a lot of value and we were able to incorporate bioLock into one of our Homeland Security scenarios" she said.

Gaspard said her colleagues, which are the technical brains behind SAP demonstrations, were impressed by the bioLock product. "The realtime solution was very easy to implement. It went in like a breeze and there is a very easy-to-use customization menu that they provide within the SAP R/3 system. Then the last piece is to enable the biometric device whether it's a keyboard or a mouse," she added.

SAP's Homeland Security demo is still being shown. In addition some of the company's solution engineers are equipped with Cherry-manufactured biometric mice to enable them to go through the bioLock demo in other SAP R/3 demonstrations. Said Barbara Gaspard: "It goes beyond what was originally developed for Homeland Security. It is very easy to use this demo in other opportunities for functions we want to show as protected. It is easy to protect transactions because they built a nice customization dialog which means no-one has to go in and do programming. It was specifically written to talk to SAP's system and that's why it was so easy to get it to work."

The days of passwords are numbered

Not surprisingly realtime North America's COO, Thomas Neudenberger, is delighted with the rising profile of biolock. He is certain that the days of the password are numbered and that biometrics' use will be widespread in a couple of years. "Sachar Paulus, the chief security officer at SAP is on record as saying the first step to internal security is to be able to track information use. The only way to make this possible is biometric identity management because you need to uniquely identify the user. Passwords are highly insecure, extremely inconvenient and expensive to administer. Our mission is to close this generally-accepted security gap with modern, innovative technology," he said.

Pete Gunn, the Director of Safety and Security at the Florida Space Authority and the person who introduced bioLock to Brevard could not agree more: "I hope that the successful installation at Brevard will inspire more Government and private organizations across the nation to protect their vulnerable IT systems with innovative biometric technology."

John Sterlicchi
