

Unisys predicts Customer Convenience to Drive Next Wave of Security Innovation in 2009

Easier processes and more intelligent collation of information

SYDNEY, 20 January 2009 In 2009, demand for more convenient consumer experiences in services provided by both government and business will drive innovations in security designed to provide faster and easier processes, predicts information services company, Unisys.

Unisys believes that at the same time, ensuring privacy of customer information will remain a critical factor for public acceptance of any process that involves personal information. Organisations will need to continue to balance the mix of security, privacy and convenience in the services they offer.

According to Mike Webber, Manager Enterprise Security for Unisys Asia Pacific, In today's climate, consumer confidence is the new currency, and convenience is now a major factor in that confidence. People accept the need for, and in fact want, protection offered through effective security processes. But now they also demand a better experience - faster, easier and less cumbersome. But more convenient processes must still ensure privacy - loss of personal information can irreparably damage a customer's trust.

Whether it be faster processing of travellers at airports, more confidently verifying an internet or phone banking customer's identity, or providing access to your services in more customer friendly ways, we believe the focus in 2009 will be on putting the consumer first.

Government and businesses alike are looking for solutions that provide consumers with the greatest level of protection, while facilitating more convenient experiences and maintaining customer trust, said Mr Webber.

Unisys predicts the following security evolutions in 2009:

1. On the Move technology will evolve to quickly verify the identity of individuals at checkpoints or from a distance

Intelligent security systems that collate and interpret information from multiple sources

Australia will continue to be a world leader in biometric security innovation

Organisations will continue to shift from securing systems to securing information

1. On the Move technology to verify identity quickly at checkpoints and from a distance

In 2009, Unisys predicts the roll-out of identity verification solutions that capture iris and/or facial images from a distance to speed up security checkpoints, and to enhance the customer experience, where large numbers of people move through a bottleneck such as immigration control.

Traditionally, iris or facial biometric solutions require the person being scanned to stand still in a specific spot at a specific height, which is a slow process when a large number of people are involved - and one which often involves several cameras being placed on top of each other to cater for different people's heights. Unisys is working with governments and organisations to pilot a biometric approach, called Iris On the Move to take iris images at a greater distance and wider field of view, by finding the face of a person as they move at a normal walking pace. The image is matched against a database of registered images such as people with access to enter a secure area to let them in.

Iris On the Move improves the time it takes to verify an individual against a list of pre-enrolled people. At an airport it can speed up the security process by as much as four times, meaning that up to 30 people per minute can potentially pass through a security checkpoint depending on the level of interactive checks done, said Mr Webber.

According to the latest Unisys Security Index(1) 66 per cent of Australians would be happy to give banks, government or other trusted organisations their iris pattern in order to enhance security and protect against identity theft.

Our research (1) indicates that Australians strongly support new technologies that provide greater security, and by late 2009 we can expect to see Iris on the Move technology trialled in Australia, said Mr Webber.

2. Intelligent security systems that collate and interpret information from multiple sources

Unisys predicts the development of more intelligent security solutions that combine information from multiple sources in order to proactively make informed decisions about security and the potential need for action or streamline management of an individual's access rights.

To date companies have been slow to combine the security data they have at hand and analyse it in order to make timely and informed security decisions. However, technological advancements will make it possible to combine disparate pools of information. For example, higher resolution CCTV cameras, coupled with intelligent video software linked to facial recognition systems, will allow facial images captured in the footage to be compared against image databases such as a list of people of interest. Security personnel would be able to combine the activity they see in the CCTV footage with knowledge of who is involved to determine if action needs to be taken, said Mr Webber.

Another example is in the workplace where we are seeing more sophisticated identity and access management systems which allow organisations to manage user access to company resources and customer information that go beyond basic user ID and password access. They help ensure that only the people who are supposed to be accessing certain types of information, areas or equipment can do so.

Imagine if an employee's list of up-to-date accreditation, such as a licence to operate certain machinery, was linked to their ability to access and turn on that machinery. If their licence had expired, they would not be able to turn it on ensuring that neither they nor their employer were put at risk.

According to industry analyst IDC, organisations in Australia and New Zealand spent US\$89.4 million on IAM systems in 2007. IDC expects the market to reach US\$189.3 million by 2012.

3. Australia will continue to be a world leader in biometric security innovation

As an island nation, assuring border security is a fundamental aim for any Australian international airport. This must be balanced with the need to process travellers through airport controls. Larger aircraft, like the new double-decker A-380 Airbus, bring huge groups of passengers into an airport at a time and have heightened the issue of passenger facilitation.

We believe Australian airports will seek innovative solutions to speed up passenger movement through airport controls while also boosting aviation security. Airports have traditionally focused on securing infrastructure and baggage. Now they focus on people, Mr Webber said.

For example, the new Brisbane International Airport terminal has not only expanded capacity to cater for the Airbus A-380. It also features Smart Gate biometric-based kiosks where pre-enrolled passengers travelling from Auckland, New Zealand can use an Australian ePassport to process themselves speeding up check-in. Australia's use of biometric data across borders in this way is a world first. We can expect other countries to follow this progressive approach for improving traveller facilitation.

4. Organisations will shift from securing systems to securing information

Until recently organisations and their auditors considered strong network and system security was adequate protection for company and consumer information. However, this approach does not take into account the human factor.

High capacity miniature storage devices such as USB sticks are now commonly available and are capable of storing entire databases, customers' personal details, or sensitive commercial data. As a result, many organisations have had the security of their data compromised both intentionally and accidentally in spite of strong system security.

Organisations now need to secure information regardless of where it resides or what file format it is in. Unisys expects to see further development and adaptation of existing technologies that will ensure sensitive data is identified and is strongly protected from the first time it is written to a file. Only individuals who can properly authenticate themselves as being entitled to access that information will be able to open the file or see its contents, regardless of where that file resides, Mr Webber explained.

However, a holistic approach to data security needs to take into account the human factor. Many data security compromises are accidental. Organisations need to define, implement and enforce stronger business procedures around taking data outside the organisation. If you simply don't enable data to be saved on CDs and sent in the mail, you take away the risk of losing it in the mail.

We predict that in 2009 consumers will continue to demand that organisations provide secure systems necessitating a holistic approach to secure all touch points addressing technology, people and business processes. But consumer acceptance and take-up of these processes will be driven by improving the end-user experience making it faster and more convenient.

We believe the move towards faster facilitation for identification processes will improve consumer acceptance and satisfaction with the security processes that they deal with day to day, said Webber.

(1) The Unisys Security Index: Australia conducted September 2008 (www.unisyssecurityindex.com.au). The Unisys Security Index was developed as regular measure of community attitudes towards a range of financial, personal, internet and national aspects of security. It is Australias only regular snapshot of public perceptions towards security.

(2) ANZ Identity Management Market Set for Strong Growth and Fierce Competition, According to IDC, ComputerWorld, 10 July 2008

ENDS

Unisys on Security

Organisations and governments today confront potential security threats that didnt exist a decade ago. A nation's sense of security is an important indicator of political, economic and consumer forces and their interdependence. Security threats are global and their effects impact individuals on a daily basis. Unisys approach to security goes beyond bits and bytes recognising that the most effective solutions are going to be those formed through collaboration across interests.

For more information on Unisys security offerings visit: www.unisys.com.au/services/security/index.htm

About Unisys Asia Pacific

Unisys helps clients with solutions for more secure business operations by aligning technology with business strategy. Drawing on a history of industry innovation and expertise, Unisys provides specialised services, delivered by trusted consultants. In Asia Pacific, Unisys delivers services and solutions through subsidiaries in Australia, New Zealand, China, Hong Kong, India, Korea, Malaysia, The Philippines, Singapore, Taiwan and Thailand and through distributors or resellers in other countries in the region. For more information, visit www.unisys.com.

About Unisys

Unisys is a worldwide information technology services and solutions company. We provide consulting, systems integration, outsourcing and infrastructure services, combined with powerful enterprise server technology. We specialise in helping clients use information to create efficient, secure business operations that allow them to achieve their business goals. Our consultants and industry experts work with clients to understand their business challenges and create greater visibility into critical linkages throughout their operations. For more information, visit www.unisys.com.

####

Unisys is a registered trademark of Unisys Corporation. All other brands and products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

This release is intended only to provide a summary of its subject matter. It does not purport to be comprehensive or to render advice of any kind. No reader should act on the basis of any matter contained in this publication without first obtaining advice for its specific circumstances.