Review

Latin lessons
Why Brazil is leading the Latin American digital revolution

- Fighting fraud with smart banking cards
- Information overload – meeting the challenge of secure data storage
- Who has access to your personal data?
- How digital technology is transforming the developing world
Welcome

The Review gives us a great opportunity to look at digital security at work in the real world, making a difference for millions of people.

It’s more than business, it’s a societal trend. The world is going digital, becoming safer, faster and more convenient in just about everything we do: from communication to payment, from transport to eGovernment and much more. All around the world, and especially in emerging countries, the growing digital economy is an enabler of jobs, health and wealth. The impact we can have on the well-being of people in these countries only adds to our motivation.

The example of the project in Kenya where people pay for water using a cellphone (quoted in the feature that starts on page 16) illustrates how the most advanced technology can have tangible value for people in ways and places none of us could have foreseen just 10 years ago.

In this edition, you’ll also find articles about Brazil, which has become one of the most advanced laboratories for new digital services; and about EMV payment cards, which are clearly on the way to being adopted globally.

But since fraud isn’t going to stop any time soon, Gemalto’s focus remains on making this digital world safe, enjoyable, simple and trustworthy, so that no one hesitates any longer to embrace its benefits. We are proud that one out of every two adults on the planet already carries a Gemalto-made smart secure device. The next decade is going to be amazing!

Philippe Cambriel
Executive Vice President,
Secure Transactions Business Unit, Gemalto
Companies are increasingly willing to pay for more energy-efficient computers

Steve Gold
Digital digest

The growth of mobile networking

Mobile social networking is continuing to grow in popularity, with market leader Facebook announcing in September 2009 that 20% of its users worldwide – 65 million people – are now accessing the site on mobile devices.

This trend is being accelerated by the spread of smartphones – sales of which rose in Western Europe by 25% in the second quarter of 2009 – and by moves by mobile carriers to make it easier and more convenient for consumers to use their phones as the hub of their social experience.

For example, Vodafone 360, launched in October, is a web-based service that offers users instant access to all their contacts across numerous social networking and instant messaging sites, as well as music downloads, maps and an application store. Significantly, the service is accessible on multiple cellphone handsets, PCs and Macs, and is constantly, wirelessly synchronised between the user’s chosen devices, so that wherever they are, they can stay in touch with their friends.


Digital Europe

Europe’s digital sector is making strong progress, according to the European Commission’s ‘Digital Competitiveness’ report, published in August: 56% of Europeans now regularly use the Internet, 80% of them via a high-speed connection (compared with only a third in 2004), making Europe the world leader in broadband Internet. It is also the world’s first truly mobile continent, with more cellphone subscribers than citizens (a take-up rate of 119%).

Commenting on the report, Viviane Reding, EU Commissioner for Information Society and Media, said: “Europe’s digital economy has tremendous potential to generate huge revenues across all sectors... We should seize the opportunity of a new generation of Europeans who will soon be calling the shots in the marketplace. These young people are intensive Internet users and are also highly demanding consumers. To release the economic potential of these ‘digital natives’, we must make access to digital content an easy and fair game.”

Source: http://ec.europa.eu
Watch this!

The world’s first 3G watchphone will be available before the end of the year in Japan and Europe. The LG GD910, which looks like the sort of gadget James Bond might be kitted out with, is worn as a watch and boasts features including a 3.63cm touchscreen, a camera, an MP3 player, a diary and a dictaphone, as well as voice and video calling and text messaging.

Source: www.lge.com

How to make emails disappear

Researchers at the University of Washington in Seattle, USA, have created the world’s first self-destructing emails. Roxana Geambasu and Professor Hank Levy have developed a free program called Vanish that puts an expiry date on digital messages. Eight hours after being sent, Vanish emails become unreadable – even to the person who wrote them.

As Levy explains, the problem is that personal emails, perhaps containing bank or credit card details, can linger online for years. “You can’t ensure an email is really deleted because you don’t control it,” he says. “Your email company might store it on back-up tape. A judge could issue a subpoena to get old emails, or a hacker could steal them. They could be revealed by a system error, or you could simply have your laptop stolen.”

Vanish makes all this impossible. Like other encryption programs, it scrambles the text of an email, but then splits the digital key to decode the message into 10 pieces. These fragments are hidden on 1.5 million randomly selected computers – part of a network of machines spread across more than 200 countries.

This makes it almost impossible for hackers to locate the key fragments, and also gives Vanish messages their limited lifespan: as users log off from this network and their computers refresh their memories, the number of key fragments online decreases. After eight hours, on average, enough fragments will have been erased for the message to be unreadable – to the writer, the recipient or anyone else.

Source: www.h-online.com

14.6%

The information and communications technology (ICT) sector in Egypt grew by 14.6% in the financial year ending June 2009, reflecting the fact that the North African country is one of the world’s fastest-growing markets for outsourcing. Egypt has been aggressive over the past decade in pushing through major ICT projects in an effort to attract companies looking to establish major global service delivery centers.

Source: www.itnewsafrica.com

US$30 billion

A new report predicts that mobile payments made using Near Field Communication (NFC) technology will exceed US$30 billion within three years. This growth is likely to be driven by revenues from smart posters and mobile coupons. However, the first NFC-enabled cellphones won’t be available until late 2009, so vendors are developing interim solutions, such as stickers, in order to get NFC to market faster on existing phones.

Source: www.nfcnews.com

47%

A survey on security awareness by PC Tools found that 47% of men use the same password for every website they visit, compared with 26% of women. What’s more, nearly two thirds of men polled said they would open a link or attachment from a friend without first checking where it came from, compared with 48% of women.

Source: www.theregister.co.uk
Phishing is going out of fashion

Phishing emails, one of the scourges of the online world in recent years, have almost disappeared. According to IBM’s most recent ‘Trends and Risk Report’, the number of phishing emails (messages designed to trick users into revealing sensitive information) as a proportion of total spam fell in the first six months of 2009 to 0.1%. In the same period last year, the figure stood at 0.8%.

The German Bundeskriminalamt has come to a similar conclusion, reporting that only 10% of online banking fraud can now be traced back to fake banking websites. One reason for this is the almost universal introduction of indexed Transaction Authentication Numbers, which can’t be used by criminals to carry out fraudulent transactions.

Instead, criminals are increasingly using trojans (malicious programs that give hackers remote access to a computer) to obtain login and other online banking data directly from PCs. The trojans often penetrate systems via security vulnerabilities in browsers, but the report also shows that there are now more vulnerabilities in programs for processing PDF files than in programs for MS Office files.

Source: www.iso.org

Who knows where you are?

If you have a smartphone and you’ve downloaded applications (‘apps’ for short) from the Internet, it’s possible that your movements are being tracked. New software sends the details of phone owners’ GPS locations to market research companies, allowing them to build up a picture of people’s movements that they can use to target advertising.

The software, which is embedded in many popular apps, including Facebook and Twitter, can transmit personal details such as age and gender, and it can also see how long people spend using an app and where they are when they use it.

It’s always been possible to track standard cellphones – they act as radio transmitters, so a network provider can pinpoint where they’re operating from – but the person being monitored has to give their explicit permission and will receive SMS messages giving them the chance to opt out.

In contrast, in the case of many apps, the terms and conditions outlining who will receive the information are buried in the small print. Privacy campaigners who are concerned about the implications of GPS tracking say that few people who download the apps will notice this wording.

Source: http://technology.timesonline.co.uk
Wherever you do business, chances are we do too.

HSBC Payments and Cash Management have a worldwide network of local specialists. So whether your requirements be global or local, in Russia or in France, we have the resources and expertise to meet them.

By investigating your payments, collections and liquidity management needs, we can provide tailored advice on a global scale, maximising the benefits to you and your business. To learn more about cash management solutions that work anywhere, visit www.hsbcnet.com/hsbc/solutions

GLOBAL BANKING AND MARKETS

HSBC
The world's local bank
PERSONAL PROBLEMS
These days, everyone knows that protecting their personal data is vital, don’t they? Well, maybe not — a number of recent surveys suggest that many people still aren’t doing enough to safeguard their digital footprint.

The rise of eCommerce, online banking and social networks all pose a serious threat to personal data security. In a world where information is a valuable commodity to cybercriminals, a lack of public awareness about how to protect yourself when accessing online services is an ongoing concern for security professionals.

“The digital age has ushered in a whole new set of security challenges,” explains Jim Norton, Senior Policy Adviser, eBusiness and eGovernment at the Institute of Directors in the UK. “The old crimes around fraud have been given new twists as terrorist and criminal groups exploit weaknesses in the storage and management of identity information. It is necessary to put in place robust safeguards at the technology level, but also to complement these through training in good practice.”

This is especially pertinent in the world of business. Most firms now have a data security policy and employ basic safeguards such as firewalls and password-protected access to servers and email accounts. However, that still leaves the problem of employees’ behavior.

“Having a security policy doesn’t magically improve security awareness among staff,” confirms Chris Potter, a partner at professional services specialist PricewaterhouseCoopers, which runs a biennial Information Security Breaches Survey. “A ‘click mentality’ has grown up: users do what expedites their activity rather than what they know they ought to. It’s like the road speed limit – everyone knows they ought to keep to it, but only a few actually do.”

Enforcing digital security policies is difficult. A study of white-collar workers in the US carried out by ISACA (the Information Systems Audit and Control Association) in late 2007 found that 35% of employees had violated their company’s IT policies at least once, while 15% had used peer-to-peer filesharing at their place of work — opening the door to security breaches and placing sensitive business and personal information at risk.

“Considering that companies rely on their IT infrastructure to store and transmit sensitive company, employee and customer data, risky activities, including the ones this survey reveals, are a significant concern for all businesses,” says John Pironti, an IT security expert who represents ISACA.

The human factor

The rise of identity theft around the globe is worrying, especially when an identity can be stolen with relatively few pieces of personal information. If a criminal obtains a person’s credit or bank card number, they only need a few more details — such as their address, date and place of birth, and telephone number — to open fake accounts in that person’s name.

The rise of online social networks and the Web 2.0 paradigm as a whole have caused the most concern about personal data security. The desire to develop relationships and make connections using platforms such as Facebook and MySpace can be compellng. However, security professionals consistently see lax attitudes to the sharing of personal information on these platforms.

In 2007, security specialist Sophos took a random selection of Facebook users and found that 40% would happily reveal personal information to other users, such as their email address, phone numbers and date of birth — all basic items that can be used to clone an identity. Graham Cluley, Senior Technology Consultant at Sophos, says: “While accepting friend requests is unlikely to result directly in theft, it is an enabler, giving cybercriminals many of the building blocks they need to spoof identities, gain access to online user accounts, or even infiltrate their employers’ computer networks.”

More worrying was the fact that Sophos also discovered that Facebook users were circumventing the site’s security systems. “Facebook’s privacy features go far beyond those of many social networking sites,” says >
“Personal data has become a commodity to which we all have to attach a value”

Cluley. “This is about the human factor – people undoing that good work through sheer carelessness.”

The millennial generation
One might assume that the younger generation is least likely to make basic errors such as those described above. As the offspring of the baby boomers, young people aged between 13 and 24 have been dubbed ‘the millennial generation’. The first generation to grow up in a world dominated by technology, they take today’s media and communications for granted.

However, even the young are often careless with their personal data when using computers and mobile devices, according to Young People and Emerging Digital Services, an extensive survey carried out in summer 2008 on behalf of the European Union (EU) that looked at attitudes to electronic identity among 15- to 25-year-olds in France, Germany, Spain and the UK.

The survey found that young people are aware of basic security measures: 50% of respondents stated that they always update their anti-virus protection, 59% scan data with a security program and 55% delete cookies from their computers. However, more than 85% of those questioned regularly provide their name, age and nationality to services on the Internet, and 65% give their full postal address. This is often because they want to access online services that require them to reveal more personal information: 70% said they will disclose this information in order to benefit from a better service.

Moreover, young people tend to be skeptical about the levels of privacy that are possible online. Whereas 52% of the general population agreed with the statement that personal information on the Internet is kept private, only 27% of young people believed that this was the case. To remedy this, they tend to want practical tools to help with their personal security, rather than just awareness-raising initiatives.

Public relations
There’s certainly no shortage of such campaigns. In the US, for example, there’s the website OnGuard Online, along with the information on the Federal Trade Commission’s Fighting Back Against Identity Theft website, while the Safer Use of Services on the Internet (SUSI) project has run in Europe. Meanwhile, Gemalto has launched JustAskGemalto.com (see panel, opposite) to answer people’s questions about keeping their personal information safe while using technology.

Nevertheless, older people in particular may still need educating about the consequences of flawed personal security measures. In the UK, the Digital Britain report (published in June 2009) gives the example of a woman in her eighties who uses technology to keep in touch with family and friends — using her year of birth as her email password.

Of course, this is likely to become less of an issue as the millennial generation grows up. In the meantime, it’s up to governments, security professionals and financial services companies to reinforce the message that every individual must think about how much personal information they reveal about themselves, even when they use what appear to be the most innocuous digital networks.

It’s also important for older people to become more aware of how, and how much of, their personal data is revealed, stored, manipulated and communicated online. Ultimately, when we use digital services, personal data has become a commodity to which we all have to attach a value.
JustAskGemalto.com was launched in January 2009 in the US and France to help end-users understand more about online and digital security. More than 800,000 people visited the site in its first two months, and visitor trends paint a fascinating picture of the real questions, perceptions and concerns people have about the digital world. By early July, the site had had more than 1 million unique visitors.

### United States

The Communications section of the site was by far the most commonly visited by consumers in the US (see graphic, below left). The SIM card was the focus of numerous queries and still appears to be an unknown device to many users. However, there were fewer questions about mobile payment and mobile banking.

Personal Data was the second most visited category, with the most popular question being ‘How private are my emails?’ There were also a lot of visits to a group of questions about phishing and other email scams; consumers clearly recognize phishing as a serious menace, but remain unclear about how to guard against it.

Questions about Traveling focused on ePassports, which are a source of some confusion: the most frequently asked question was ‘Do I have an ePassport?’ Although people do tend to understand why this technology has been adopted, media-fueled controversy about piracy and hacking continues to prompt concerns about issues such as malicious access to personal data in official documents.

In the Working section, visitors expressed concern about malware and spyware, issues that have been widely publicized. Users are also worried that the lack of identification on open WiFi networks may equate to a lack of security.

In the Surfing category, the questions asked about online banking suggest that it is widely understood, but there is still concern about security levels and methods.

### France

French consumers are as concerned about Communications as their US counterparts (see graphic). In fact, people rarely listen in on calls or hack cellphones, but these issues attract attention because they have been widely covered by the French media.

Under the heading of Personal Data, French consumers have many questions about the security of online passwords. They clearly know why they exist, but haven’t yet mastered them, as questions such as ‘How do I choose a secure password?’ indicate.

Data confidentiality is a major concern, and one that relates equally to biometric passports, the Carte Vitale (the French health card) and online banking. It seems the French view technological innovations with suspicion, asking questions such as ‘What kind of information is stored on my biometric passport?’ But they have just as many questions on how to apply for an ePassport and the documents they need to provide.

Like the Americans, the French are concerned about WiFi network security, but they have fewer concerns about email. Finally, under Surfing, questions about the risk of computer viruses received the greatest number of hits, reflecting the media attention devoted to this issue.

Indeed, the results from both countries suggest that media coverage of issues around digital security has the greatest influence on consumers’ perceptions and fears. While this is no bad thing if it prompts consumers to find out the facts, it is a concern that their knowledge of digital security is largely based on what is usually negative coverage.

---

**Questions and answers**

JustAskGemalto.com was launched in January 2009 in the US and France to help end-users understand more about online and digital security. More than 800,000 people visited the site in its first two months, and visitor trends paint a fascinating picture of the real questions, perceptions and concerns people have about the digital world. By early July, the site had had more than 1 million unique visitors.

Conversely, the lack of interest in articles about social networking may indicate that users have a falsely high level of confidence in the safety of their personal data on such sites.

Finally, under Buying, questions such as ‘What is the safest way to pay online?’ proved popular.

### FAQs

The three questions most frequently asked by American visitors to JustAskGemalto.com in the first two months after the site’s launch were:

- ‘LOST MY PHONE! WHAT ABOUT MY CONTACTS?’
- ‘CAN SOMEONE LISTEN TO CALLS I MAKE FROM MY CELLPHONE?’
- ‘WHAT CAN I DO IF MY CELLPHONE IS STOLEN?’

French consumers have similar concerns. The top three questions asked on the French site were:

- ‘LOST MY PHONE! WHAT ABOUT MY CONTACTS?’
- ‘CAN SOMEONE LISTEN TO CALLS I MAKE FROM MY CELLPHONE?’
- ‘CAN MY SIM CARD BE HACKED AND USED REMOTELY?’
The 2008 Beijing Olympics became as much a showcase for China’s technological advances as for its athletes — and the 2016 Games will offer a similar opportunity for Brazil. While cutting-edge technology may be more traditionally associated with Tokyo’s glittering skyscrapers and frenetic pace than with Rio de Janeiro’s sandy beaches and laid-back lifestyle, Brazil already leads Latin America in technological take-up.

Gerson Rolim, executive director of camera-e.net, is one enthusiastic proponent of technology in Brazil. Founded in 2001 as the Brazilian chamber of eCommerce, camera-e.net’s objective is to foster the use of Internet technology as a strategic tool for the country’s economic development. And with good reason: eCommerce is big business for the country. A massive 44% of all Internet commerce in Latin America originates in Brazil, according to Rolim. Mexico comes in a distant second, with 15%.

Brazilians are such enthusiastic online shoppers that there is even a huge annual web ‘blowout’ sale devoted to Internet-only shopping, in which dozens of retailers offer deep discounts to customers who pay by MasterCard.

A trusted digital identity
This thriving eCommerce marketplace is underpinned by the security provided by digital signature technology, which protects both shoppers and retailers. The infrastructure of digitally encrypted signatures is well developed in Brazil — in fact, only China has more digital certificates. But the task at hand for Latin America is expanding the online marketplace beyond the borders of tech-savvy nations such as Brazil and into neighboring countries with less developed digital infrastructures, such as Argentina and Uruguay.

Mercosul — the regional trade agreement between Brazil, Argentina, Paraguay and Uruguay — is currently addressing this issue of a common digital marketplace.

“In Brazil, we are very developed in this field, but that’s less the case in Argentina, Paraguay and Uruguay,” says Mauricio Coelho, director of public key infrastructure (PKI) for Instituto
“Only China has more digital certificates than Brazil”

Nacional de Tecnologia da Informação (ITI).
“In order to do commerce with them, we need to help them develop their technology to the same level that Brazil has already.
“Today in Paraguay, they have almost nothing — they just have a law that requires digital certificates to make electronic signatures. They don’t have a PKI yet, so it’s impossible to do new forms of business with them.”

Beyond commerce
But there is more to business than the buying and selling of goods. The existence of an infrastructure of everyday transactions and public services can strongly influence an international company to invest on foreign soil. Online retail transactions are just one of the ways in which digital certificates are being used in Brazil.

The biggest innovation is the planned introduction of new national ID cards embedded with an electronic chip that contains unique identifiers and personal information. The government is currently creating the legal framework that will enable states to issue the new cards, referred to as RIC (Registro de Identidade Civil). Once this process has been completed, pilot schemes will follow.

The move is an attempt to overhaul the cumbersome paper document system that took to count votes in the 2002 Brazilian general election using electronic voting systems

12

The percentage by which traffic accidents fell in Mexico after eDriver licenses were introduced

40%
Currently exists in Brazil. A single smart ID card will eventually replace five separate paper documents that correspond to an individual’s national ID, social security number, driver’s license, voter registration and taxpayer ID – as well as containing a full set of fingerprints, a photograph and facial recognition technology.

Every smart card will be read using an encrypted PKI. This means that the system will not only be simpler and more convenient in future, but it will also make identity theft much harder, and forgeries will be extremely difficult indeed.

The true cost of identity fraud
Identity fraud has been a big problem in Brazil – in part because the current documents are not centralized.

“Right now, I could have an identification number in each of the 27 estados [states] – each one has its own database and they are not connected,” explains Coelho. “With RIC, that’s not the case.”

Stopping identity fraud can have an enormous financial impact. The Brazilian government currently wastes an estimated 15 billion reais (US$8.5 billion) every year on social services that were acquired by false application.

Eliminating things like false driver’s licenses would also have a financial trickle-down effect. The switch to eDriver licenses in a number of states in Mexico, for example, has reduced traffic accidents by 40%. When you consider that road accidents have cost Brazil 28 billion reais (US$16 billion) in 2009, a 40% reduction would mean that more than 10 billion reais (US$5.7 billion) could be used for something more productive.

But even without a national ID card, Brazil is using digital signatures and biometric data in novel ways to enhance the efficiency of government services. For example, many courts in the Brazilian judicial system operate entirely with electronically signed documents. No longer do judges and attorneys have to go to the courthouse to file legal papers in person; they do everything electronically.

Mauricio Coelho says that the courts that have adopted this system operate much more efficiently. In fact, the experiment has been so successful that the entire Brazilian judicial system is expected to adopt this electronic document system in the next three to five years.

“In the justice system, we have data showing that a process that once took 800 days now only takes 40 days,” he says. “In financial terms, we have seen cost reductions of something like 60%. It’s really amazing.”

In fact, any legal document can be signed digitally if it uses PKI technology. Government contractors also use digital certificates to make bids on jobs and send their invoices.

The digital vote
But perhaps the biggest success is the widespread usage of the new electronic voting systems. In the past, a Brazilian citizen could only vote in an election in his or her home
“Brazil was the first country to have fully electronic elections”

city, because voter registrations were only maintained locally. This rendered voting difficult for business travelers, made electoral fraud easy and meant that it took a long time to determine the results of elections.

Brazil introduced the first electronic voting machines in 1996 and was the first country to have fully electronic elections. Today, its electronic voting system has gained widespread acceptance, partly because of the fact that it speeds up the vote count tremendously. In the 1989 presidential election between Fernando Collor de Mello and Luiz Inácio Lula da Silva, the vote count required nine days. In the 2002 general election, the count took less than 12 hours – and some smaller towns were able to hear the results just minutes after the polls closed.

In the most recent elections, several cities tested new voting machines that verify voter registration via a fingerprint scanner. Voters simply swiped their fingerprints to prove their identity and then made their selections by pushing a button next to the name and photograph of the candidate of their choice.

The goal now is for other Latin American countries to not only follow in Brazil’s footsteps, but also come up with their own novel uses for the technology, finding new ways to improve on the efficiency and security of every aspect of digital life. Because the better things work, the more time there is to enjoy the other thing Brazilians do best: relaxing with an ice-cold coconut on the beach.

Hot on Brazil’s heels...

While Brazil is the leader in Latin America’s digital arena, other countries are also making strides. In Mexico, the government has introduced the groundbreaking Seguro Popular project, which aims to provide social security benefits to underprivileged citizens.

As part of the initiative, Seguro Popular introduced an eHealthcare smart card based solution in 2006. The smart card functions as both a means of identification and an ‘e-purse’ in which subsidies for treatment and prescriptions can be stored. Because the smart card can only be accessed by healthcare professionals using a special card reader, it records and stores patient information securely, thereby reducing both fraud and administrative costs.

Digital technology has also been applied to healthcare in Puerto Rico. There, the government has introduced the Tarjeta Inteligente de Salud (Health Smart Card), which integrates a microprocessor. It is the largest deployment of healthcare smart cards in Central America to date and has been hailed as an exemplar of how they can benefit healthcare providers, insurers and patients alike.

A more entertaining application was introduced in Argentina. Personal, one of the country’s three cellular carriers, now offers Microsoft’s Instant Messenger (IM) service. This allows Personal subscribers to use Windows Live to chat with friends on a cellphone-to-cellphone and cellphone-to-PC basis. This program is now available in many other Latin American countries as well.

Because the IM facility is on the SIM card, the adaptation of the popular Microsoft product has all the same features as on a PC. These include viewing connected contacts, changing the user’s availability status and keeping several chat sessions open simultaneously. What’s more, subscribers can access IM from any mobile device, making for 100 per cent service availability.
There is a direct parallel between the introduction of information and communications technology (ICT) and economic growth in the developing world. For example, the World Bank’s most up-to-date research shows that for every 10% rise in the number of high-speed Internet connections, there is a concomitant 1.3% increase in per capita gross domestic product (GDP). This is because such technology gives often low-income people access to information and business opportunities that were previously unavailable to them.

Developing the broader IT and IT-enabled services (ITES) sector (which includes a range of services that are commonly outsourced, such as call centers, medical transcription and data processing) also holds out obvious prospects, given that less than 15% of the potential market is currently being exploited. According to management consultants McKinsey, IT services represented a US$325 billion potential revenue opportunity in 2007, while ITES represented US$150 billion. Encouragingly, market research firm Gartner also predicted that the global ITES segment will grow from US$170 billion in 2008 to US$240 billion in 2012.

This situation is particularly significant for developing countries, where the service sector in a more generic sense already accounts for 35% of employment and 50% of GDP. Therefore, by extension, the development of IT and ITES is likely to contribute directly to job creation, not least by boosting cross-border trade in an increasingly globalized world. Even more positively, experiences in both India and the Philippines show that each new job created in the IT and ITES space results in the creation of between two and four other positions elsewhere.

But these aren’t the only considerations. The creation of ICT infrastructure can also bring about a fundamental transformation of developing world economies, since it generally leads to the formation of new business models for the delivery of public services.

Mobile and wireless telephony is particularly valuable in this context. Of the 4 billion mobile devices in use globally, about 3 billion are now used by citizens in the developing world. The mobile platform is emerging as the most powerful and efficient way for people in developing countries to access services such as banking, education and healthcare — services from which many were previously excluded.

As a result, the mobile platform is extending the economic opportunities of the rural poor and is considered key to reducing poverty. In Kenya, for example, telecoms company Safaricom introduced a minute-sharing service for its pre-paid cellphone users. The aim was to provide people in rural areas, who found it difficult to purchase pre-paid phone cards, with a means of accessing the service. However, many Kenyans also started using it as a currency replacement — paying for taxi fares using their cellphone credits, for instance.

Another example of the transformative power of mobile payments also comes from Kenya. Some water companies there are now installing modern wells for free to provide rural communities with access to clean drinking water. An integrated cellphone payment system is introduced at the same time and customers are charged on a pay-as-you-go basis when they take the water.

The transformation begins

Inspired by examples like this, the World Bank is actively encouraging the increased rollout of broadband connectivity worldwide. The organization is also accelerating the number
of projects aimed at transforming service provision to low-income populations using ICT. To this end, it recently introduced the Government Transformation Initiative (GTI).

GTI came into being following a roundtable discussion between the World Bank’s President, Robert Zoellick, and the chief executives of 11 private sector companies, including Gemalto. Laurent Besançon, GTI coordinator at the World Bank, explains the rationale. “We wanted GTI to be a partnership between the World Bank and industry, and we designed it together,” he says. “We feel that much of the knowledge in this area is located in the private sector and so, rather than invent something ourselves, we felt it would be more productive to leverage the expertise that’s already out there.”

Instead of embarking on a wide range of efforts, the GTI team decided to focus on two key areas, eGovernment and ICT skills development, which they then subdivided into three main categories: eProcurement, eIdentity (eID) and cloud computing. The latter was felt to be important as a means of helping governments to reduce ICT costs by enabling public authorities to either share services or access third-party ones.

Because eProcurement makes the purchase of goods and services more automated and transparent, it is also considered valuable in terms of cutting public expenditure (by 20-30%, on average) and reducing opportunities for corruption. It can also open up the market to bids from small to medium-sized enterprises. For example, after investing US$1.6 million in an eProcurement system in 2004, Brazil’s central government generated savings of US$107 million in the first year alone, while its suppliers saved a further US$35 million.*

Meanwhile, eID is seen as a crucial means of facilitating eGovernment, which in itself is >

*2009 Information and Communications for Development Report, World Bank
viewed as critical to economic development. Electronically delivered public services are proven not only to reduce transaction costs and processing time, but also to boost government revenues.

One of the key issues for eGovernment is how to authenticate the identities of individuals. This is particularly important when delivering state benefits that involve a transfer of cash, in order to ensure that the money goes to the intended recipients. Being able to trace cash transfer flows makes it easier to prevent fraud. According to Besançon, this can “suddenly make governments more self-sufficient, as funds are not being leaked. Instead, they reach the intended recipients and flow into the economy when they’re spent. It also means that scarce resources can be allocated to other sectors that need them”.

A fundamental prerequisite for authenticating citizens’ identities, however, is establishing a registry of those citizens. Such data banks haven’t always been established in the past, particularly in war-torn countries. Here again, the World Bank believes that commercial companies have a role to play. “Some governments have found private-sector partners that were able to help them with this kind of thing,” says Besançon. For example, Gemalto helped Gabon to establish the identities of its citizens when it introduced a health card there.

**Raising the funds**

GTI intends to achieve its goals in two key ways. First, the World Bank’s Global ICT Department has established a Project Development Facility (PDF) based on donor investment. This will ‘jump start’ the creation of between 20 and 30 three-year demonstration projects, of which between five and ten are expected to relate to eID. A further five to ten initiatives are likely to
be divided between the other two categories already defined and, if they are successful, the remit of the remaining 10 to 15 will be expanded to cover new, yet to be decided areas of interest.

“Participants can use the PDF to help develop feasibility studies and adapt their legislative framework if need be,” explains Besançon. “It’s about helping them to prepare for government transformation in a way that can hopefully be replicated on a large scale.” The feasibility studies will then be used to assess the viability of individual proposals. Implementation will subsequently be financed by sources arranged by participating countries. These sources are likely to include development finance institutions and the private sector.

The progress of the feasibility studies will be reviewed at annual Government Transformation Forum meetings, which are designed to showcase best practice.

Pilot schemes
The initial pilots being discussed include an eProcurement scheme in East Africa, an eID initiative in central Asia to create a business model for the use of eID on mobile telephony platforms, and a cloud computing pilot for business licensing or tourism applications.

“It’s about test-driving the Facility,” says Besançon. “We’re using workshops and knowledge exchanges to see the constituency of the countries, but it’s up to them to decide what they want to do in each area.”

One example of an existing eID project that combines the delivery of social services with identity and payment is the pioneering eHealthcare program in Algeria. Its aim is to streamline healthcare administration, claims and reimbursements through the use of smart technologies, including microprocessor cards and associated software and services. The cards need to be highly secure, because they contain sensitive data that can show authorized people what healthcare has been provided to the cardholder, by whom and at what cost.

Alongside their security features, they also need to be easy to use, so that they can provide rapid access to the data by different people including beneficiaries, doctors, pharmacists and social security agencies. By mid-2010, some 7 million cards will have been distributed to Algerian citizens.

Sharing knowledge
The second key element of GTI will be put in place in the near future. This will comprise two peer networks supported by the World Bank’s Global ICT Department and the World Bank Institute.

The first, which is scheduled for launch at the Forum, consists of influencers from some 20 countries who will act as local champions, encouraging high-level governmental support for proposals. The second, which is being piloted for the eProcurement track, comprises about 30 practitioners. As heads of procurement for departments such as health, they are involved at the implementation level.

The idea behind the creation of the peer networks is to enable participants to exchange knowledge and ideas around business models and best practice, particularly in relation to governance. Besançon explains: “It’s really about looking at how we can support governments in leveraging ICT to transform the delivery of services, and how we can help them to access expertise. We want to help accelerate their thinking, as well as their ability to embark on such projects.”

A progress review is scheduled to take place in 2010, but the success of GTI will also be measured in various ways within 10 to 18 months of projects being initiated.

“We’ll evaluate things like the speed of rollout, the level of savings achieved and the numbers of people gaining easy but secure access to services,” says Besançon. “Another important measure of success will be how replicable the business models are, because we’d like this initiative to have a domino effect and lead to more government leaders embarking on similar projects.

“Projects involving ICT are high risk and high reward, but the point of GTI is enabling people to access expertise, best practice and business models to help them minimize those risks,” he concludes. “It’s not about developing countries reinventing the wheel on their own – it’s about tapping into the right expertise to help them solve problems.”

“The creation of ICT infrastructure can transform developing world economies”

Society _ ICT and developing countries

Images: Panos, Corbis

www.gemalto.com
Taking a toll
Every driver knows that sinking feeling as a toll plaza appears on the horizon — usually preceded by a long line of cars waiting their turn to pay. Fortunately, toll operators are constantly looking for ways to streamline their operations, not least because the cost of manual toll collection eats into their profits. One solution is to use EMV contactless payment cards (see page 28); the driver simply swipes their card across a reader, the payment is automatically deducted from their account and they can drive on with minimum disruption.

The technology
Gemalto’s MPCOS EMV microprocessor card has many applications in areas such as eID, healthcare and financial services. Multiple applications are often combined in a single card, such as the Asyacard DIT offered by Bank Asya in Turkey. As well as being a credit card, a contactless payment card and a loyalty card, it can be used to pay at all road tolls in Turkey.
This graphic, by software artist Jer Thorp, was created by tagging every article in the New York Times from 1981 to September 2009 that contained the phrase ‘computer security’, then analyzing the topics and organizations mentioned in those articles and finding the connections between them. Each individual line represents a single connection. The graphic illustrates the fact that security has been a concern ever since computers came into general use in large organizations.
From customer profiles to logs of website traffic, businesses now generate a flood of information on an hourly basis. Market intelligence firm IDC recently reported that nearly 300 exabytes (that’s 300 billion gigabytes) of information is created globally each year. So it’s not surprising that businesses are quickly realizing that their data silos need adequate protection against loss.

Indeed, the loss of data in a business is akin to suffering a major fire or flood damage. According to a University of Texas study, 94% of companies that suffer a catastrophic data loss don’t survive it: 43% fail to reopen and 51% close within two years. Add to that the statistic that 6% of all PCs will suffer a data loss in any given year (according to IT research specialists Gartner) and it’s clear that data backup and storage is essential. As a result, continuity strategies—which all businesses must have in place to protect themselves against the unexpected—are quickly becoming a key component.

So the challenge that enterprises now face is how to develop their markets, with their burgeoning information requirements, and balance this with server-level and endpoint data security, all with convenient user-level access.

Data overload
The data management technologies that enterprises currently employ usually center on local data silos that use server-based technology for backup and retrieval. Networked access is now common across the enterprise space. However, aging technologies such as tape, NAS and RAID arrays are increasingly buckling under the demands that businesses are placing on these technologies.

As a result, one of the most dramatic developments in data storage and management has been the move to cloud-based storage. Enterprises are realizing that they can both extend their usage of the Internet as a SaaS (Software as a Service) platform and employ it as virtual data infrastructure.

For enterprises looking to streamline their data management needs, and simultaneously reduce costs, the services offered by cloud computing seem to be the perfect solution. With their vast data storage facilities, large organizations such as Amazon can use their technology to offer services to the wider business community. And with the news that Google has developed its own operating system, Chrome—which has the Internet as its native environment—businesses and individuals alike can expect more diverse services to take care of their data storage and retrieval needs.

However, cloud computing isn’t a complete and flawless solution to data management issues: the administration of large volumes of data must always begin with the data owner. It’s also important to realize that cloud-based data management must have at its heart robust security measures that protect the information not only when it’s in storage, but also when it’s in transit.

Securing bits and bytes
Wherever data is stored, there’s also the question of using encryption to protect it, while still permitting access to authorized users. In this area, a software-only encryption system that interfaces with storage platforms is no longer robust enough. With more decentralized access to sensitive data a daily requirement, systems that base their encryption on two-factor authentication (2FA for short), or use hardware that is independent of the accessing platform, such as USB keys, are proving to be an efficient way for enterprises to rapidly improve their security.

End-to-end encryption is essential, according to Richard Walters, Product Director at Overtis Systems. “We’re now starting to...”
Smart solutions

The data management and encryption solutions that are suitable for you will depend partly on the size of your business:

SMEs (small to medium-sized enterprises)
- Desktop encryption
- Mobile data security
- Cloud-based backup

Large enterprises
- Two-factor authentication with encryption
- SAN (storage area network) encryption
- Mobile data security

see utilities that allow users to create encrypted vaults where data can be instantly encrypted, exported and shared securely," he says.

“ Vaults, and also the encryption of data ‘on the fly’ when it’s moved or copied to removable media, begin to address the issue of encryption of unstructured data.”

Walters’ advice is to look for well-respected standards of encryption such as the use of FIPS 140-2 certified crypto libraries. This is an IT security accreditation that is used by government departments or in regulated industries that need to collect, store, transfer, share or disseminate sensitive but unclassified information. Gemalto’s Protiva Smart Guardian, for example, is an FIPS 140-2 level 3 certified zero-footprint personal security device that is designed to protect portable data.

Walters adds that the use of strong encryption algorithms such as 256-bit AES (Advanced Encryption Standard) is also worth looking out for.

Data in transit

Many organizations will have a level of security built into their data policies, but then use little or no encryption when sending sensitive data over the Internet. The rise of online backup services has raised concerns about how the data that these companies are handling is actually archived and accessed. Even using encryption can still leave file names potentially visible to unauthorized users. More robust security when personal data in particular is handled by businesses is essential, along with an integrated approach to data storage and communication.

“The volume of data is doubling every 16–18 months in most businesses, fast outstripping existing storage capacities,” says Andy Hardy, UK Managing Director of Compellent Technologies.

“The knee-jerk reaction — simply throwing capacity at the problem — is an expensive and ultimately unmanageable solution. The most logical new approach is to deploy an automated, tiered storage platform that runs all your really important ‘active’ data on fast, expensive drives such as FC [fiber channel] or SSD [solid-state drive], while all your less-important ‘inactive’ data drifts down to cheap, larger capacity SATA [serial ATA] drives.”

The levels of encryption that are in use can vary. Triple DES (Data Encryption Standard), AES or Blowfish encryption using 256-bit keys are common in the most advanced data archiving services. Combine that with RAID backup, which ensures that mirrored copies of the data stored are constantly updated, and the raw information is secure. However, a major
issue that many businesses are wrestling with is how to archive their data, and yet still have easy access to the files and other media that they need on a day-to-day basis.

**Get smart**

Many businesses are now looking closely at the ways in which smart card technology (products such as Gemalto’s Smart Enterprise Guardian) might be able to deliver the levels of security they are looking for.

What is clear is that the volumes of data that have to be managed by businesses and individuals alike will increase rapidly over the next few years. However this information is stored, manipulated and accessed, robust security must be fundamental – and encryption can deliver that security.

Companies are realizing that traditional means of securing their data that use a hardware/software approach are no longer flexible enough for their needs. With enterprises now working in geographically divergent locations, and with employees increasingly working via mobile technology, smart card based encryption systems are proving themselves to be the perfect solution — not only for user identification, but also to protect sensitive data from unauthorized access.

**Consumer protection**

The average consumer now stores nearly three terabytes of data (according to research from storage solutions company Data Robotics), which means that information management is now an issue for the home as well as for businesses.

The data that consumers want to store and access can be on a wide range of devices, from PCs and cellphones to removable media, and now the Internet (via the growing cloud computing market). More and more consumers are becoming aware of the importance of securing that data – which is why encryption is starting to become common in the consumer market.

For instance, services such as CellCrypt and PhoneCrypt provide robust yet user-friendly encryption for cellphones, while models using the Symbian operating system have encryption systems such as Secusmart, which offers a MicroSD card based solution.

Meanwhile, the iPhone has spawned its own environment for security applications, with more than a dozen now available; these range from free apps such as Lockbox and 1Password to free personal encryption systems such as Secret Safe and Splash ID.

Users of desktop and notebook PCs also have a number of third-party encryption platforms to choose from. The current market leaders include SecureDoc and DESLock Plus, while even the ubiquitous Zip file can now be encrypted with Secure Zip.

Many consumers are also using removable media to store and transport data, and the USB flash drive has become hugely popular. Security is paramount, simply because these devices can so easily be lost or stolen, and devices that address this issue are now appearing on the market.

For example, Gemalto has launched the YuuWaa, which combines a USB flash drive with encryption systems to offer secure file storage and sharing.

“By bundling local and online storage, portability and security, YuuWaa provides an innovative and cost-effective way for people to keep and share their digital data safely,” says Juana-Catalina Rodriguez, YuuWaa Sales and Marketing Director at Gemalto.

Despite all these options, no universal encryption system yet exists, so a piecemeal approach to data protection will remain the norm for the foreseeable future.

With the amount of data that consumers are storing increasing with each passing year, however, fast and easy encryption systems that provide robust security, yet also give users convenient access to their information, will surely be developed. The interoperability of encryption systems across all data storage platforms is the holy grail of data management developers.
Bank of America is the leader in mobile consumer banking in the US, with 2 million customers who have signed up for its mobile banking services. The bank has now started to roll out mobile-based promotions and is developing remote deposit capture and person-to-person mobile payments.

According to a report from telecoms analysts BuddeComm, cellphone companies in Venezuela achieve an average revenue per user (ARPU) of US$26. This makes it the most profitable country in the Latin America and Caribbean region, where the average ARPU is US$16.

Cellphone penetration in the Latin America and Caribbean region is now estimated at 80% – well ahead of the world average of 58% – and has passed 100% in 15 Caribbean and three South American countries. In early 2009, there were 458 million cellphones in the region, compared with 106 million fixed-line phones.

The European Union has pledged to invest €18 million in research into LTE Advanced technology, which will underpin the next generation of mobile networks. The technology promises to offer ultra high-speed mobile internet connections – up to 100 times faster than the current 3G networks.
By the end of 2009 there will be an estimated 120 mobile money services operating in the developing world. One of the biggest is Kenya’s M-PESA, which had 6.2 million registered users by March this year — up from 2.1 million a year earlier.

Kuwaiti telecoms company Zain now operates in 24 countries in the Middle East and Africa. It has created a multinational network by scrapping roaming charges across its markets and is now rolling out its mobile money service, Zap, across this network.

Online trading is extremely popular in the Philippines, and this is driving take-up of mobile payment systems, with 7.2 million people now using them. The volume of daily transactions is steadily increasing, and a high proportion are person-to-person transactions where money is transferred from one cellphone to another — the typical payment method for buyers and sellers on online trading sites.

According to bank card network operator China UnionPay, there are now 19.2 million people using mobile payment services in China. In the first half of 2009, 62.69 million mobile payment transactions were conducted, for a total of RMB 17.04 billion (approximately US$2.5 billion); this represents a year-on-year increase of 42.4% and 63.7%, respectively.

Mobile payments are growing in popularity in Cambodia, where only 0.5 million people (out of a population of 14 million) have a bank account, but 3 million own a cellphone. Typically, blue-collar workers in towns and cities use the technology to send money to family members in rural areas.
As the end of 2009 approaches, there’s a good chance that the credit and debit cards in your wallet conform to the EMV standard. (The initials stand for Europay, MasterCard and Visa, the three companies that developed the standard.) According to the Smart Payment Association, its members had delivered more than 580 million smart payment cards by the end of 2008 – a 39% increase on the previous year. Most of Western Europe now uses EMV cards, as do major countries including Japan, Australia and Brazil, and plans are well under way for their deployment across the rest of Europe, Asia and Latin America.

EMV cards provide much higher levels of security than the old magnetic stripe cards, thanks to unique security keys in the microprocessor. Most EMV cards currently in circulation use SDA (Static Data Authentication), but DDA (Dynamic Data Authentication) cards are even more secure; these store an encryption key that generates a unique number for each transaction.

Versatile technology

Although EMV cards are all based on the same technology, banks around the world are deploying them in different ways and incorporating different features. Barclaycard led the way in September 2007 when it became the first organization to introduce contactless technology on credit cards with the launch of Barclaycard OnePulse in the UK – a three-in-one Oyster card (for use on public transportation in London), credit card and contactless payment card. Since then, banks and other enterprises have deployed EMV for loyalty cards, payment cards for public transportation and road tolls, and even for soccer season tickets (see panel, opposite).

The many commercial and cross-partnership opportunities that smart card technology can facilitate are certainly attractive, but the key factors that are helping to spur the wider adoption of EMV cards are the growth of eCommerce and the urgent need to combat ‘card not present’ fraud.

The results can be dramatic: according to Banque de France, the 2006 introduction of DDA cards in France reduced the annual losses attributed to card fraud from €17.5 million to €5.0 million. Better fraud protection has allowed banks and credit card issuers to push through a ‘liability shift’, whereby merchants, not card issuers, are now liable for any fraud that results from transactions on systems that are not EMV-compatible.

One consequence of the widespread rollout of smart banking cards is that, when they are introduced in one country, fraud tends to ‘migrate’ to neighboring nations that are still using magnetic stripe cards. As Jorge Belmar, Managing Director for Chile and Peru at ATM solutions provider NCR, put it recently: “If we [in Chile] don’t start using this technology soon, it is very likely that all fraud attempts
related to [magnetic stripe cards] will be in Chile, because it will be easier to attack.”

**Coming to America?**

One country stands out from the list of those yet to adopt EMV cards: the United States. According to Kevin Gillick, Executive Director at GlobalPlatform (the international specification body for smart card infrastructure), current fraud loss is viewed as a ‘cost of business’ in the US and is considered to be at an acceptable level.

This may change before too long, however, given the publicity being given to the practice of card skimming, where a criminal swipes a bank card through a device that copies the data from the magnetic stripe and then creates counterfeit cards using that data. The US Secret Service estimates that losses from ATM skimming total about US$1 billion a year, or US$350,000 a day.

The exploits of Alberto Gonzalez have added fuel to the fire. Before he was caught earlier this year, Gonzalez stole more than 135 million credit and debit card numbers by planting ‘sniffer’ software on the computers of major companies. He was only able to do this because the cards he was copying were magnetic stripe cards.

So will the US see the light soon? It’s hard to say for sure, but there is one promising sign. The EMV consortium, which expanded in 2004 with the addition of Japanese company JCB, welcomed another new member in February this year: American Express, traditionally one of the main champions of magnetic stripe cards.

---

**Barclaycard OnePulse (UK)**
- Credit card
- Contactless payment card
- Oyster card for travel on London’s public transportation network

**Petronas Maybankard Visa (Malaysia)**
- Credit card
- Contactless payment card
- Loyalty card for Petronas gas stations; users can earn treatPoints, convert their points into gas vouchers, and get on-chip e-coupons for instant redemption and discounts at selected merchants

**Asyacard DIT (Turkey)**
- Credit card
- Contactless payment card
- Integrated municipal toll and transit application; owners can use their cards to pay tolls on major roads and bridges across Turkey, including the two bridges over the Bosporus in Istanbul

**Manchester City FC MasterCard Seasoncard (UK)**
- Pre-paid season ticket for entry to Manchester City’s soccer stadium
- Contactless payment card
The Review meets futurologist Ian Pearson and asks him to make some predictions about the technology we'll be using in a few years' time.
The taxi driver can’t find the house. “It’s this satnav system,” he moans. “And this is what they call progress…”

We eventually arrive at the address in a tree-lined suburb in the south-east of England and I’m tempted to ask the driver in to meet Ian Pearson, a man who has a fascinating insight into progress.

“Well, he’s going to have to get used to it,” says Pearson, smiling at my tale of the meandering cabby, “because we’re in an era of ongoing change, and improving technology is driving it. People will look back in 100 years and see this period as similar to the Industrial Revolution. The rate of change is accelerating, and I can’t see it slowing down until 2050 or 60.”

Pearson relishes being alive at such a pivotal point in history, and the need to understand a swiftly evolving society means his skills as a futurologist are in demand. He works for Futurizon, a small futures institute, where he writes, lectures and consults globally on all aspects of the technology-driven future. But how did he get such an interesting job title?

“My background is in engineering and I worked as a network designer at British Telecom,” he says. “As my career progressed, I wrote a number of papers on the future, on subjects such as TV and computer games. These were well received, so I concentrated on strategic thinking and became a full-time futurologist in 1991.”

Missed opportunity

But his superiors didn’t take all of his ideas so seriously. “I saw the potential of SMS text messaging in 1991, but my managers said: ‘Why send a text when you’ve got a phone in your hand and can leave a voice message?’,” Pearson recalls ruefully. “A couple of years later, a student working at Nokia sent one almost by accident, and the rest is history.”

Pearson is not at all bitter about this experience and doesn’t see his ability to anticipate future developments as a way of making money. “I’m a fan of Tim Berners-Lee’s approach to developing tech,” he says. “He could have become stinking rich with the World Wide Web concept, but he decided it was better for the planet that he collaborated with others and shared his ideas.”

Talking of technology, how does Pearson think that mobile devices such as cellphones and laptops will develop?

“Using Moore’s Law [the idea that the number of transistors that can be placed on an integrated circuit doubles every two years] as a starting point, I think the cellphone is likely to disappear over the next 20 years and be replaced by an assortment of digital jewelry,” he says. “The phones of today will look like those huge, clumsy models from the early ’90s that we now scoff at.

“So, something looking like a brooch will in fact be a little power pin for a visual system that may take the form of glasses, or even a type of contact lens. Looking just five years ahead, you’re going to see people walking around with video visors the size of a pair of ordinary glasses. Companies are already working on a system that has tiny laser built into the lenses of glasses, with images being delivered straight on to the retina.”

And if you think that cellphone users ‘talking to themselves’ on Bluetooth headsets looks strange, you ain’t seen nothing yet. By 2020, Pearson believes people will be gesticulating wildly at their own personal 3D environment.

“I anticipate that people will use ‘active’ contact lenses that will provide different functions based upon a user’s gestures,” he explains. “These lenses will be connected to the web and will have the ability to overlay reality with an information-rich 3D world.”

He believes fashion and ego will also be an influence in the creation of new communication tools. “Today we have examples of people implanting chips into themselves so they can buy cocktails in a particular bar. People want the latest and coolest tech, and this drives the sector,” he says. “In the future, you will be able to get electronic information printed onto the skin, which will enable people to streamline their interfaces so they can buy things anywhere. You’ll be able to buy an ice cream on a nudist beach by waving your arm at the van.”

Stronger security

But while this vision of the future appears fun and productive, Pearson sounds a note of caution about security in this brave new world. “Small, incredibly sophisticated devices will need equally brilliant security measures to combat people who want to misuse them. Even today, with miniaturization in its infancy, there’s a move towards using hardware devices to break into tech systems, rather than software delivered via the web, because they’re harder to detect.

“The future will see people using devices such as communication brooches as ID and passports, which offers great convenience but raises many questions about the safety of the data,” he adds. “At that point, identity theft will include not only the stealing of information, but also the replication of physical characteristics. It’s a world that will pose many ethical problems. Nevertheless, while I can currently see more questions than solutions, I’m generally optimistic about our ability to create the answers.”

Unfortunately, my time is up. As Pearson walks me to the door, he mentions other predictions he is working on; topics include man’s expansion into space and the coming social unrest around the lifestyle disparity between the globe’s older and younger generations. Outside, the cab is waiting to take me away into an uncertain — but intriguing — future.
In brief

Safer mobile working

With the launch of Protiva Smart Guardian, a smart card-enabled personal security USB device, Gemalto has made it possible for businesses with a mobile workforce to protect the integrity and security of their data. Smart Guardian allows employees to securely access sensitive and confidential corporate information, as the encrypted data never leaves the device and any attempt to break in to Smart Guardian will cause the data to be deleted. To unlock the device, users simply insert their authorized portable token and enter a passphrase.

Award for a joint effort

Gemalto and Vodafone Group R&D have won an Identity Deployment of the Year Award for a collaborative proof-of-concept identity application that enables strong authentication of an OpenID across the Internet or a mobile network. OpenID allows individuals to use the same username and password at different websites, without the need to install any software. The concept application combines the ease of use of OpenID and the security of smart card based two-factor authentication.

North and South America

Securing the cloud

Users of one of the leading cloud computing services, Amazon Web Services (AWS), can now protect their accounts with a new Multi-Factor Authentication (MFA) feature from Gemalto. The Ezio Time Token is a small, lightweight, long-lasting device that produces a unique six-digit one-time password (OTP); the user simply presses a button on the device and the OTP is displayed. The MFA feature allows users to combine something they know (their email address and password) with something they have (the Ezio device) in order to ensure that only authorized people are accessing their AWS account.

A 4G partnership

Verizon Wireless has selected Gemalto to provide an over-the-air platform and Universal Integrated Circuit Card (UICC) for the industry’s first Long Term Evolution (LTE) mobile broadband network. The platform and circuit card will help Verizon to deliver a secure and reliable multimedia data connection, provide global roaming and remotely add new UICC card applications and services on its 4G LTE wireless broadband network.

Making music together

Universal Music Group and Gemalto have signed an agreement to jointly promote the Smart Video Card as a new channel for distributing music. Smart Video Card is a Gemalto innovation that embeds a DVD-compliant optical disc into the card body of a regular SIM card. The disc can be preloaded with 120MB of multimedia content that can be played in a standard DVD player or on digital devices such as PCs, mobile handsets and MP3 players.

Certified by MasterCard

MasterCard has certified Gemalto’s Trusted Services Manager technology, enabling Gemalto to support the launches of mobile contactless payment programs according to MasterCard’s security requirements. The certification will reassure banks that they can roll out payment services with the highest level of security and data confidentiality.
Asia and Oceania

Queensland’s drivers get safer licenses

The Australian state of Queensland has chosen Gemalto, together with plastic card manufacturer Placard, to provide its Sealys electronic driving licenses to the Department of Transport and Main Roads. More than 3 million drivers in Queensland currently hold laminated driver’s licenses on which personal data is printed. The new cards will significantly improve the security and privacy of this data by storing driver information electronically, making the license hard to copy and counterfeit.

Europe and Africa

Three’s company

Gemalto is currently the only company supplying all three mobile operators in China as they prepare to launch 3G services later this year. Gemalto is supplying its UICC and R-UIM cards to China Mobile, China Telecom and China Unicom.

A scalable solution for Nigeria

InterSwitch, a leading provider of secure electronic payment solutions in Nigeria, is deploying Gemalto’s complete Ezio strong authentication solution to secure its ePayment services. Gemalto has supplied its Ezio Strong Authentication Server, as well as delivering EMV card readers and unconnected tokens, all customized with InterSwitch’s logo. As a result, InterSwitch can now enable its banking customers to perform secure eTransactions using either their EMV card and reader or a token.

NFC payments on trial in Singapore

Gemalto provided personalization services for a trial of mobile payments in Singapore this summer. More than 750 merchants took part in the three-month pilot, launched in May, in which 300 Citi M1 Visa Platinum card members were able to buy items at Visa payWave merchants by waving their NFC-enabled phones in front of a contactless reader at the point of sale.

A German reader

Gemalto has launched Ezio Optical TAN, a unique optical authentication reader for online banking, specially designed for Germany. The reader is the size of a credit card and fits in a wallet. To carry out and sign online transactions, the user simply holds the device in front of their computer screen; optical sensors capture the data the user would normally enter from the reader’s keypad.

Optelio certified for use in Saudi Arabia

Gemalto’s Optelio banking card has been certified as meeting the requirements of the Saudi Arabian Monetary Agency. This, together with other existing certifications, enables Gemalto to complete its existing Multos offer for the Saudi Arabian banking market, and to support local financial institutions in their migration to EMV cards.

m-payments come to Uganda

MTN Uganda has chosen Gemalto as the technology partner for its mobile payment (m-payment) program. Gemalto has provided a comprehensive solution that includes the server for connecting the operator with its banking service provider and the SIM cards that store and execute the m-payment application. The program provides a secure, convenient and affordable means for MTN Uganda subscribers to carry out peer-to-peer fund transfers using their cellphone, whether or not they have a bank account. It also makes m-payment accessible to users who don’t have Internet access.

The number of cities with a population of more than a million that use Gemalto’s contactless transport cards. The latest addition is Brussels in Belgium, where the deployment of Gemalto’s Celego card will allow the city’s inhabitants to benefit from the speed and convenience of contactless technology when traveling on the subway, buses and trams.
HOW GREEN IS IT?
Steve Gold looks at some of the steps the IT industry is taking to reduce its carbon footprint

There are many ways in which developments in technology can help to cut carbon emissions. For example, now that the technology enabling remote working is widely available, employers are increasingly allowing staff to work from home, thus cutting down on commuting. The spread of electronic ticketing and m-payments will reduce the amount of paper used for printed tickets, and you could argue that SIM cards are intrinsically green, as they’re effectively small computers that don’t consume energy.

However, a cynic might point out that these energy savings pale into insignificance compared with the enormous amounts of energy the world’s computers and cellphones consume. To put it another way, it’s all very well for a small company to turn off its PCs outside office hours — but even if every business in the area does the same, the effect can be negated by a single non-energy-efficient data farm run by the local authority.

This message is starting to get through. According to the 2009 Green IT Report, a global study by Symantec, companies’ green IT budgets are rising and they’re increasingly willing to pay more for energy-efficient computer systems. The report noted that 97% of the firms surveyed were discussing a greener IT strategy and 45% had already implemented green IT initiatives.

It’s probably no coincidence that these figures come at a time when governments and other public bodies are focusing on reducing carbon emissions. New carbon trading regulations will come into force across the EU in 2010, while in the US, the International Code Council (ICC — the organization that develops the codes used to construct buildings) has launched its International Green Construction Code.

According to the ICC, commercial buildings consume 40% of a typical country’s energy and produce roughly the same level of carbon emissions. The aim of the initiative is to reduce the carbon footprint of commercial buildings through the use of energy-efficient technology, including computer systems, on both new and existing sites. The final draft of the Code — which the Obama administration is set to make mandatory for new buildings in the US — will be published in early 2010.

Meanwhile, the major IT vendors are showing the way forward with their own green projects. IBM has been working with the Swiss Federal Institute of Technology to develop a water-cooled, high-performance computer called the Aquasar, which recycles waste heat and helps to reduce energy consumption at data centers. About 10 liters of water is circulated around the computer three times every minute to leach the heat from the server’s blades and transfer it to the host building’s heating system. As a result, the Aquasar’s carbon footprint could be as much as 85% smaller than that of comparable air-cooled systems.

Microsoft is doing its bit with the release of the Environmental Sustainability Dashboard. The free-to-use software, which is available to Microsoft Dynamics AX customers, allows mid-sized businesses to capture auditable data on four of the core environmental performance indicators identified by the Global Reporting Initiative: direct and indirect energy consumption, greenhouse gas emissions resulting from energy consumption, and emissions resulting from activities such as transportation, commuting and business travel.

Companies that make cellphones and other portable devices are also busy looking for ways to improve energy efficiency. For instance, the new Nokia 7205 Intrigue cellphone has a display that only lights up when a call or text comes in. Meanwhile, manufacturers of smart cards and readers are increasingly seeking to introduce greener products and processes. These include the use of eco-friendly materials, as well as recycling and end-of-life initiatives.

Will these measures really make our IT greener? For me, the answer is a cautious ‘yes’, but it will have to be a team effort involving individuals and businesses. Legislation helps, but as former UK Home Secretary Douglas Hurd once said, without the support of the population, laws cannot be truly effective. The speed of progress towards truly green IT will depend partly on the demand from consumers for devices, and the companies that produce them, to be energy-efficient.

“SIM cards are intrinsically green; they’re small computers that don’t consume energy”
The Drive for Security.

Lexar Enterprise Solutions offer the best of both worlds—USB flash drives designed to be intuitive and manageable while meeting stringent security compliance standards. Government and business employees are empowered to be responsive and agile, while their data is protected from tampering and compromise. Critical data has never been more secure on a USB flash drive.

To learn more, go to www.lexar.com/enterprise
Tell us what you think

We hope you have enjoyed this issue of The Review. To help us make it even better, please take a few minutes to answer the questions below; then simply moisten the gummed area, fold and seal the page where indicated, and put it in the post (you don’t need a stamp).

1. Which technology/security business magazines do you read?

2. How do you rate the design of The Review?

   ❑ Very good  ❑ Good  ❑ OK  ❑ Poor  ❑ Very poor  ❑ Don’t know

3. How do you rate the quality of the written articles?

   ❑ Very good  ❑ Good  ❑ OK  ❑ Poor  ❑ Very poor  ❑ Don’t know

4. What do you intend to do with your copy of The Review?

   ❑ Retain it for future reference  ❑ Pass it on to a friend or colleague  ❑ Discard it/recycle it

5. What subjects would you like to see covered in future issues?

6. How did you obtain your copy of The Review?

   ❑ By mail  ❑ At an event  ❑ Given to me by a colleague  ❑ Other

Subscribe to The Review for free

The Review is published three times a year, bringing you news, views and insight about the global digital security industry. Subscriptions are free and we deliver the magazine directly to you. What’s more, the first 50 people to subscribe using this form will receive a YuuWaa – the new digital storage solution from Gemalto, with 10GB of total storage and a flash drive backup. Simply tick the box (right), fill in your details and return this form to the address overleaf.

Terms and conditions: the YuuWaa will be sent to the senders of the first 50 correctly completed forms received by Gemalto. No correspondence will be entered into. There is no cash alternative.

Full name

Company

Address

Email address

Yes, I would like to receive a free subscription to The Review. Please tick here

Yes, I would like to receive Gemalto’s e-Newsletter, a regular publication with our latest news, offers and resources. Please tick here
Gemalto Review Research
Wardour
Walmar House
296 Regent Street
London
Great Britain
W1E 3BR