Issue 1 2017

gemalto
security to be free

THE REVIEW

Smart insights for a digital world

KEEP CARING

As mobiles get more complex, operators must make customer service a top priority

Smart innovation

"Mobile is at the heart of innovation. Innovation is at the heart of mobile." This is a sentiment, so well articulated by the organizers of this year's Mobile World Congress, with which we wholeheartedly agree.

In this edition of *The Review*, we highlight the many areas in which mobile is integral to new developments in the sector. Most notably, in "Your body is now your password", we investigate the growing use of biometrics to enhance security and customer authentication in a world where people are increasingly using their smartphones to pay.

For this very reason, last December, we entered into agreements to acquire 3M's Identity Management Business. For government applications, biometrics are becoming an indispensable way to enable authentication methods that are both strong and user-friendly. However, we also anticipate strong demand from the commercial sector, where biometrics offer more convenient authentication for a host of digital services.

Biometrics will play a major role in governments' push towards eServices. In "Dematerializing documents in the digital era", we highlight how governments are using this ground-breaking technology to revolutionize citizens' lives, giving them easy and convenient access to official documents. In particular, we showcase an exciting new project in the US that allows drivers to carry their driving licenses on their mobile phones.

As our smartphones offer increasingly complex services, providers are going to need to pay even more attention to delivering outstanding customer experience management. In "Happy talk?", we consider what that should look like in this new era.

There is much more in this issue that highlights the role mobile is playing in innovation, from digital banking to cashless agriculture to the Internet of Things. We hope you'll recognize many of the big themes debated at Mobile World Congress reflected in the pages of this edition.

We hope you enjoy the read and, if you are visiting Mobile World Congress this year, we look forward to welcoming you to our stand.

Frédéric Vasnier
Executive Vice President
Mobile Services & IoT, Gemalto

gemalto.com @gemalto linkedin.com/company/gemalto

The Review is published by Gemalto Corporate Communications – www.gemalto.com

For further information on *The Review*, please email laurence.manouelides@gemalto.com

The Review is printed on Cocoon Silk 50 paper. Certified as an FSC mixed sources product, Cocoon Silk 50 is produced with 50% recycled fiber from both pre- and post-consumer sources, together with 50% FSC certified virgin fiber from well-managed forests.

Contributors

Nicholas Booth
Nicholas worked in IT support within the health, financial services and public sectors before becoming an IT journalist.

Adam Oxford
South Africa-based Adam has been a technology journalist for the past 15 years, writing for titles across the world.

Tim Green
Tim was a senior analyst at *Screen Digest* before launching B2B title *Mobile Entertainment* in 2005.

Kate Bevan
Kate is a journalist and broadcaster who lives and breathes technology. She writes for, among other titles, the *Financial Times*.

David Howell
David reports on technology and computing. He also works as a consultant to small businesses moving online.

Tamsin Oxford
A journalist and editor for nearly 20 years, Tamsin specializes in IT and has edited titles such as *PC World*.

Elliot Wilson
Elliot is a technology, business and finance writer, specializing in emerging markets. He has worked in the UK, China and India.

The Review is produced for Gemalto by Wardour, Drury House, 34–43 Russell Street, London WC2B 5HA, United Kingdom +44 (0)20 7010 0999 wardour.co.uk

COMMUNICATIONS MANAGER, GEMALTO *Laurence Manouelides*
EDITOR-IN-CHIEF *Eila Madden*
GROUP ART DIRECTOR *Steven Gibbon*
PRODUCTION *Jack Morgan*
PRODUCTION DIRECTOR *John Faulkner*
SENIOR ACCOUNT MANAGER *Matt Goodenday*
CLIENT SERVICES DIRECTOR *Emma Fisher*
CREATIVE DIRECTOR *Ben Barrett*
MANAGING DIRECTOR *Claire Oldfield*
CEO *Martin MacConnol*

'wardour'

Cover illustration: Jacquie Boyd/Getty

Read more online

For more on the latest trends in technology and digital security, visit *The Review*'s online partner, */review*, at **gemalto.com/review**

In this issue...

"If customers query the way a function works or ask for a new one, they should see these features on their handsets soon after sharing this input with their service providers"

IDESHINI NAIDOO, MTN SOUTH AFRICA

Read more on page 8

Europe's driverless car race takes to the roads

Japan's Nissan is set to be the first carmaker to test its driverless vehicles on Europe's roads after it invited leading figures from the UK automotive industry to try out an autonomous model of its LEAF electric car in London.

German rival BMW has also said it plans to put a fleet of 40 autonomous test vehicles on the road in Europe and the US but that won't happen until the second half of 2017, while Nissan's demos were planned for Q1 of this year.

Nissan said it wanted to give passengers, including government officials and technical and safety experts, the chance to experience and test its driverless technology in a live, diverse city environment.

Nissan's Propilot technology controls the accelerator, brakes and steering using data obtained through a mono camera. More sensitive than a color camera, the mono can see lane markings and other vehicles in 3D.

BMW's driverless technology is based on a collaboration with Intel and Mobileye, an Israeli technology firm that develops vision-based driver assistance systems.

News of Nissan's demos follows recent announcements from the company that a refreshed version of its Qashqai model and the new LEAF, both coming soon, will be equipped with driverless technology to enable single lane autonomous driving on motorways.

Sources: **newsroom.nissan-europe.com; wired.co.uk**

GETTY

SNAPSHOT

PRODUCTIVITY PUSH

Scenario modeling by the McKinsey Global Institute (MGI) has revealed that automation of individual business activities could boost global productivity by 0.8% to 1.4% a year. A new MGI report – *A future that works: Automation, employment, and productivity* – looks back at how significant technological innovations through the ages have pushed productivity rates up.

1850-1910: steam engine

The invention of the steam engine got industry moving by enabling factory owners to use steam-driven machinery and transport goods around the world at a much faster pace. Productivity rose by 0.3% a year.

1993-2007: early robotics

During this period of early robotics, productivity grew 0.4% annually.

1995-2005: IT

Advances in IT revolutionized the workplace, pushing productivity up by 0.6% a year.

2015-2065: automation

McKinsey predicts that the adoption of robotics, artificial intelligence and machine learning could give a much-needed annual productivity boost of between 0.8% and 1.4% to the global economy.

Source: **mckinsey.com**

Smartphones lose their edge

The smartphone industry is awash with rumors that we could be one step closer to a bezel-less phone after Apple was granted a patent for an organic LED screen full of holes.

Traditionally, engineers have had to build a mobile's hardware – such as the ear speaker and home button – into the opaque edge, or bezel, of the phone. That's because the technology needs openings to operate.

Apple's patent, awarded by the US Patent and Trademark Office, would allow various pieces of hardware to be mounted behind a display screen with perforations so small that they would be hidden to the naked eye. This would allow engineers to design a smartphone with a true edge-to-edge display screen.

Apart from being a thing of beauty, full-screen phones would help engineers to meet the growing demand for more compact mobiles by allowing them to move essential hardware behind the display screen.

Apple says its patented technology would also allow it to create a completely transparent phone, enabling a user to look through the handset and see digital images overlaid on real-world objects. This "heads-up display" technology would be Apple's first foray into augmented reality.

Source: **appleinsider.com**

GETTY

No more flat battery woes

Getting caught short with a flat phone battery could soon be a thing of the past.

SolidEnergy Systems, a Massachusetts Institute of Technology (MIT) startup, has developed an "anode-free" lithium metal battery that's twice as energy dense as lithium ion batteries. That means a similar-sized battery can last twice as long, or a battery that's half the size can give the same amount of charge.

Lithium metal batteries aren't new but, until now, they've struggled to gain commercial success because of a tendency to overheat. Qichao Hu, MIT graduate and now CEO of SolidEnergy Systems, solved that problem by adding a liquid electrolyte solution to the thin metal foil that replaced the battery's anode.

Without the liquid electrolyte solution, the metal foil only worked at 176 degrees Fahrenheit or higher, hence the tendency to overheat. Hu's solution allows the battery to work without any heat at all.

Hu's years of development mean his company is ready to bring a rechargeable lithium metal battery to market that's non-flammable and can operate at a wide range of temperatures. Better still, it can be manufactured using the same equipment needed to make traditional lithium ion batteries.

SolidEnergy Systems is trialing its super battery in drones but it hopes to see it widely used in smartphones and, eventually, in electric cars.

Source: **news.mit.edu**

> We see biometrics as an essential component of all customer touchpoints, from eCommerce to mobile wallet payments"

MICHAEL SASS, MASTERCARD

Read more on page 12

GETTY

New mobile app for East Africa's farmers

Payments firm MasterCard hopes to help bring growth and prosperity to thousands of small-scale farmers across East Africa with a new mobile app that digitizes the buying and selling process.

2KUZE, which means "Let's grow together" in Swahili, connects smallholder farmers, buyers, agents and banks together via a digital platform. Farmers can find buyers, sell and receive payment for their goods entirely by mobile phone. This is hugely convenient for farmers who often have to walk for hours to sell their produce at markets.

"Eighty per cent of farmers in Africa are classified as smallholder farmers having less than one to two acres of farming land, making it extremely difficult to drive growth and prosperity within this community," says Daniel Monehin, Division President for Sub-Saharan Africa and Head of Financial Inclusion for International Markets at MasterCard.

"We believe that by using mobile, a technology that is so ubiquitous among farmers in Africa, we can improve financial access, bring in operational efficiency and facilitate faster payments." Farmers get the added benefit of the security of mobile commerce and payments.

2KUZE came out of the MasterCard Lab for Financial Inclusion in Nairobi. It is currently being piloted by 2,000 farmers in Kenya's Nandi Hills through Cafédirect Producers Foundation, a not-for-profit organization that works with 300,000 smallholder farmers globally.

If successful, MasterCard says 2KUZE could pave the way to a cashless agricultural sector in East Africa.

Source: **newsroom.mastercard.com**

Wave goodbye to "password fatigue"

Cloud-based apps revolutionized the way we work, but now their proliferation is leading to lost or forgotten passwords, resulting in reduced productivity and "password fatigue". It's creating problems for IT departments too. According to research firm Gartner, lost or forgotten passwords account for 20% to 30% of help desk tickets.

The explosion in cloud-based apps also poses numerous security issues. Remote and easy access makes it difficult for IT to track who is accessing the apps, and when. If an employee leaves a company, how can IT ensure they can no longer access the multiple apps? Finally, users don't always understand why using two-factor authentication is the better option.

These security weaknesses can make organizations vulnerable to phishing, hacking, or sheer brute force attacks.

SAML authentication, or Security Assertion Markup Language, is one potential solution. The XML-based open standard for exchanging authentication and authorization data between parties is produced by the Organization for the Advancement of Structured Information Standards and has been around since 2002.

SAML allows users to log in to multiple cloud-based apps using just one username and password – a process known as "identity federation". Authentication is carried out by a trusted Identity Provider, which is alerted by the cloud-based app every time a user attempts to log in. SAML's open standard status means it works across all cloud-based apps.

If more organizations adopt the standard, they could see a fall in the security risks of using cloud-based apps and IT administrators would no longer need to manage and monitor multiple log-in credentials. When users leave, for example, just one set of credentials would need to be revoked. This centralized authentication, management and control would be a huge benefit.

SAML is a win for users too. A common user experience across all application log-in processes could mean finally waving goodbye to password fatigue.

Source: **oasis-open.org**

Explore *The Review*'s online partner, */review*, at **gemalto.com/review**

Building secure smart cities in India

India's government has been urged to keep security in mind as it embarks on an ambitious project to create 100 smart cities across the country, driven by the Internet of Things (IoT).

Ministers have pledged to create a US$15 billion IoT industry in India by 2020 and estimate that this will account for 5%–6% of the global IoT market. They hope the smart city network will help to boost economic growth and improve the lives of citizens.

The government's four-pronged strategy will see parts of selected cities retrofitted or entirely redeveloped with smart solutions. Other options include developing greenfield sites or applying smart solutions to city-wide infrastructure. Kochi, Surat and Chennai are among the cities selected for transformation.

Numerous sectors, including transport, health and energy, have been identified for development. Solutions include intelligent traffic management, telecare and smart energy. Ministers say solutions such as intelligent traffic management could reduce average commuting time and costs, improving productivity and quality of life for citizens.

Security experts have welcomed the ambitious plans but say increased volumes of data produced by a network of 100 smart cities will leave the nation prone to cyber attacks. They say ministers need to think about implementing end-to-end IoT security, which would protect the digital identities of individual devices, data in transit between devices, and data stored in the cloud. In addition, they need to implement access management systems so that different parties can only access the data that they need to.

Source: **smartcities.gov.in**

GETTY

Event calendar

Gemalto regularly participates in trade shows, seminars and events around the world. Here's a list of those taking place in the next few months.

Date	Event	Sector	Location
Mar 7-8	PayForum 2017	**Banking**	Paris, France
Mar 10-12	29th National Convention of SCOP	**Banking**	Philippines
Mar 14-16	Passenger Terminal Expo	**Government**	Amsterdam, The Netherlands
Mar 15-16	AAMVA Workshop & Law Institute	**Government**	Minneapolis, IN, USA
Mar 27-29	High Security Printing	**Government**	Baku, Azerbaijan
Apr 26-28	ID4Africa	**Government**	Windhoek, Namibia
May 1-2	Seamless	**Banking**	Dubai, UAE
May 1-3	Connect:ID	**Government**	Washington, D.C., USA
May 10	Payments & Innovation Forum	**Banking**	Santiago, Chile
May 16-18	IoT World	**IoT**	Santa Clara, CA, USA
May 21-24	AAMVA 2017 Region IV Conference	**Government**	Portland, OR, USA
May 28 - Jun 1	Mobile World Congress	**Mobile Services & IoT**	Shanghai, China
May 30 -Jun 3	Computex	**Mobile Services & IoT**	Taiwan
Jun 4-7	CCMTA	**Government**	Yellowknife, NT, Canada
Jun 7-8	Telematics Detroit 2017	**IoT**	Novi, MI, USA
Jun 12-14	27th ACI EUROPE General Assembly, Congress & Exhibition	**Government**	Paris, France
Jun 19-21	High Security Printing Latin America	**Government**	Guatemala City, Guatemala
Jun 19-22	AAMVA 2017 Region II Conference	**Government**	Chattanooga, TN, USA
Jun 26-28	Money 2020	**Banking**	Copenhagen, Denmark
Jun 27-28	SDW 2017	**Government**	London, England

AUTHOR NICHOLAS BOOTH
ILLUSTRATION JACQUIE BOYD

HAPPY TALK?

Ten years ago, mobiles were simply phones; now they offer a myriad of lifestyle options. Managing the complicated relationships with our handsets is a mounting challenge for service providers

A decade ago, when we used "mobiles" to simply talk to each other, the most popular handsets had boringly functional names like 6310. These days, the devices in your hand have exotic associations like Android, Galaxy or Apple, suggesting themes of infinite possibilities and organic growth. It is no longer a simple phone but a combined unit of computing, filming and broadcasting capacity with way more processing power than NASA used in 2014 to launch the Orion spacecraft – the first step of a mission to take astronauts to Mars.

Yesterday's mobile telcos are now communications service providers (CSMs). As relationships with these machines deepen, the job of monitoring and meeting subscribers' expectations – known as customer experience management (CXM) – has multiplied in complexity. Originally, CXM was related to the connection between two callers across an analog network. The modern digital network, with its galactic range of services and subscriber base, caters for much higher expectations.

GREAT EXPECTATIONS

Ownership of smartphones across the globe has gone from 100 million to 2 billion in 10 years, according to BI Intelligence. Users expect to host video conferences and get instant gratification on every blockbusting download of work or entertainment.

The new networks are much more granular, comprising many more autonomous units (cells) created with many more signaling devices. As a result, there is potential for more complex and intelligent management – which obviously involves more work.

Coupled with the massive growth in workload are much shorter deadlines. In the days of analog networks, management analysis was a sort of monthly post-mortem of historical data.

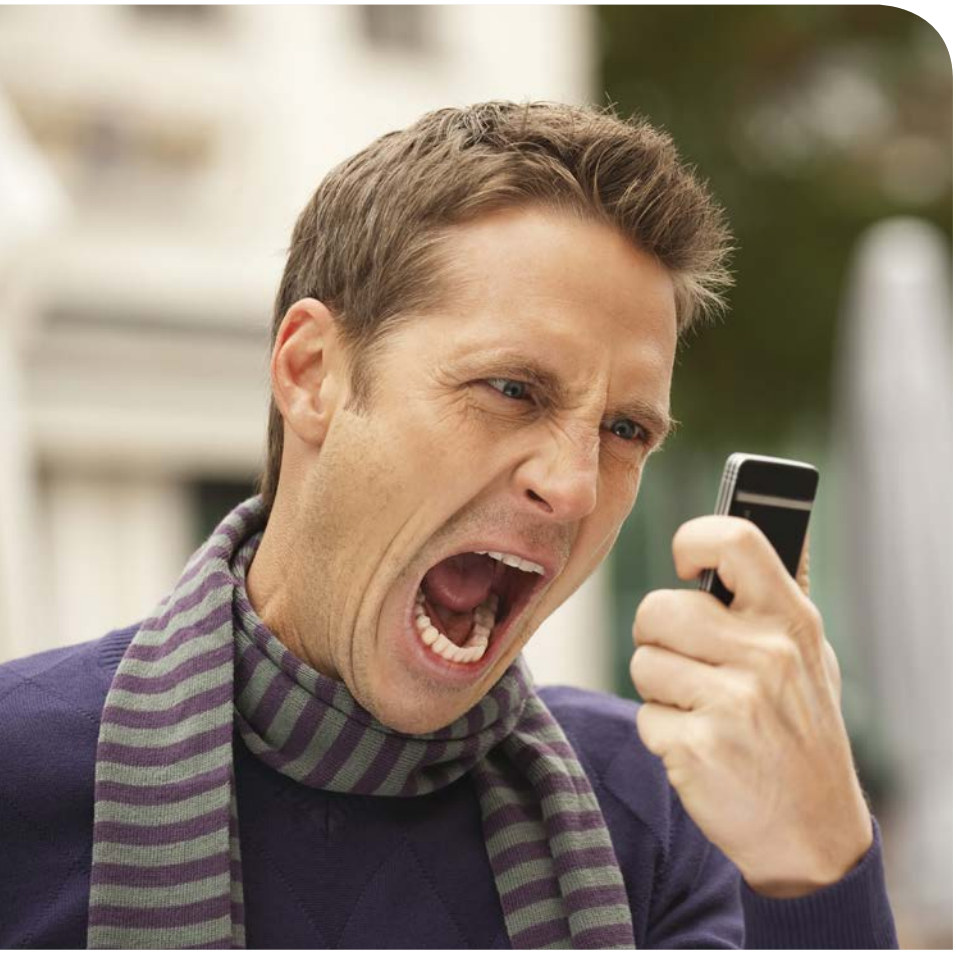
These days, intelligence must be instant. The most important and demanding demographic within the modern CSM subscriber base – the young – are glued to their screens and addicted to the feed of news and entertainment. Delays in accessing their primary means of communication, entertainment and information, through social media such as WhatsApp, Snapchat, Facebook, Instagram, YouTube and Google, can create instant withdrawal symptoms of rage and discontent.

GRAVE CONSEQUENCES

The consequences of bad network performance can be fatal. Modern consumers would defect to a rival network at the drop of a Snapchat session – if they weren't constrained by their contract. So the discipline of CXM has changed from being reactive to proactive.

The sale is different now too. Once, subscribers were retrospectively billed on the numbers of minutes they consumed. Now they buy data packages, which allude to bundles of services, which call for immediate management to protect both parties in the relationship. If a customer has paid for a certain amount of Gigabytes-worth of movie footage from Netflix, they mustn't be allowed to over-step that limit, or the mobile operator's running costs for servicing the client will exceed their revenue. On the other hand, if a customer cannot post on Instagram because, without realizing it, they burnt through their data bundle watching that viral


I want to be able to browse anytime, anywhere 😄



GETTY

A customer should be able to contact customer service multiple times in different ways, without having to start all over again

video on YouTube, they are likely to be dismayed. Timely reminders that they are about to exceed their limit are not just good manners but the type of sensitive handling needed to stop client defections.

REAL-TIME ANALYSIS

These timely interventions can only work if there's instant access to the right information and it can be acted on immediately. Human operators can take input on one level, such as customer feedback on Twitter, or instant messaging – but they can't keep pace with the speed of change needed to configure accounts to cater for thousands of subscribers.

The data floods in from apps, sensors, Radio-frequency Identification (RFID) tags, internet browsing and social media. The formats range from 140-character tweets to Gigabyte-sized videos. Wading through all that unstructured information and making instant, accurate judgments, not to mention timely interventions, is a huge challenge. Which is why Big Data analysts lament the four big "V signs" they encounter daily – variety, volume and velocity, all of which need to be met without sacrificing veracity.

This is why CSMs are in constant talks with IT partners to create systems that can automatically put all this information into context and act on it. This "real-time" analysis is a relatively new science, with the development of business rules and intelligent pattern recognition algorithms still at a relatively early stage.

RIPE FOR BETTER SERVICE

Mobile operators don't have a great track record in this area, says Rob Bamforth, Principal Analyst on Business Communications for Quocirca. "The technology is ripe for better customer service because everyone – technically inclined or not – wants to use [their mobiles] for just about everything," Bamforth adds.

The integration of all elements of response will be vital since each customer interaction uses some part of the finite resources, such as the network bandwidth and the computing power that drives the video services, which are jointly used by millions of subscribers. Those resources will be juggled with increasing fluidity and skill by software-defined networks (SDNs).

Cohesion among all the channels of communication with the clients will be another imperative. A customer should be able to contact customer service multiple times in different ways, without having to start all over again. So if they started the job of, say, changing their account details on the desktop computer at home, they should be able to pick up when they start trying to complete the task as they use their mobile while sitting on the train. There's nothing more frustrating than having to explain yourself all over again, whether it's to a series of people or a series of machines.

"If customers query the way a function works or ask for a new one, they should see these features on their handsets soon after sharing this input with their service providers," says Ideshini Naidoo, Chief Customer Experience Officer of MTN South Africa.

MASSIVE CHALLENGES

The number of variables presents a massive management and security challenge. A basic principle of engineering dictates that the more moving parts there are in a system, the more likely it is to go wrong.

Connected customers are constantly engaging with all kinds of services, from games to shopping, through multiple channels. The freedom of choice has changed customer expectations and behavior. As more consumers engage through multiple channels, security experts must lock down more exposures.

Find out about building trust in mobile apps at **bit.ly/2k4c4Ct**

> Social network trawling for complaints and issues is all very well, but it's far better to spot problems before they grow"

ROB BAMFORTH, PRINCIPAL ANALYST, BUSINESS COMMUNICATIONS, QUOCIRCA

The process of identity verification across multiple platforms and channels is a crucial battle. While CXM means that customers must be able to access their information on any of their devices without having to sign in every time, the heads of security and compliance will want to know that the safety of that information is not compromised. Locking it down as efficiently as possible, without complicating the process, can actually improve the customer experience.

On the other hand, user defections are likely to rise in proportion to the clumsiness of the sign-up and sign-on processes. A multi-factor authentication or Identity Federation can help users who struggle to remember multiple passwords.

Tomorrow's CXM needs to include these security features while still being seamless and friendly, says Bamforth. But above all, it needs to be much more proactive. "Social network trawling for complaints and issues is all very well, but it's far better to spot problems before they grow," says Bamforth.

THE NEW CXM FRONTIERS

There are two fronts on which CXM can be addressed: the underlying infrastructure and the interface with the customer. Belgium's Telenet is doing some impressive work on the first frontier, addressing concerns over Wi-Fi dissatisfaction. When some subscribers claimed their connections were inadequate, Telenet's in-depth root cause analysis unveiled several issues, many driven by circumstances in the customers' homes, such as the size of the house and the materials it was made from.

Telenet decided to make its answers to this problem into a marketing exercise to strengthen the customer's relationship with the company. Its solution was a free visit to customers with in-home issues during which the installation was checked and optimized where possible and effective solutions were suggested when necessary.

Meanwhile, UK operator O2 created a spin-off network, GiffGaff, which uses social media and rewards to galvanize users into supporting each other. GiffGaff is a "mobile virtual network" that uses the infrastructure of the parent company but has its users' data ring-fenced into a sub-category that is managed differently. The innovation behind GiffGaff is that it rewards users for helping each other by giving them extra minutes. This effectively turns its user base into a self-managing entity.

FUTURE DIRECTIONS

In the future, that support could be provided by artificial intelligence (AI), one branch of which is an AI-driven automated customer service called Chatbots. These virtual attendants learn from the answers given to frequently asked questions and can eventually second-guess the answers to the majority of questions that people pose. They are fed from a "knowledge base" that learns over time and can provide a consistent level of customer service.

The Korean telecoms market, where there are already 5G networks being test-marketed, is a good indicator of future directions. SK Telecom, ranked number one in the Korean Customer Satisfaction Index and National Customer Satisfaction Index for 19 consecutive years, bases all product and service offerings on intelligence from its CXM systems.

"[Our] competitiveness is a function of special price plans designed to meet customer usage patterns along with designated mobile devices," says an SK Telecom spokesperson. The CXM uses everything from a voice-activated AI service to COOKIZ, a kids-only life platform. Its newest initiative is to create a customer-oriented counseling service center for those aged over 70.

Another service provider in the UK, Fuss Free Phones, has also created a service aimed at making the customer experience easier for a specifically older demographic by making the interfaces more simple and screening calls. "By simplifying the customer experience, we can make our subscribers much more secure," says CEO Simon Rickman.

There's a twist nobody expected. The old dogs of telecoms are teaching the new CSMs to learn new tricks. ■

> Connected customers are constantly engaging with all kinds of services. The freedom of choice has changed customer expectations and behavior

WHAT USERS WANT FROM THEIR MOBILE OPERATORS

A new global survey from Gemalto offers insight into what smartphone customers will expect from their mobile operators in 2025. In the survey of nearly 2,000 mobile users from six countries, respondents were asked what type of customer care they expected. The following five scenarios came out on top:

34.0%
I expect to be able to speak to an artificial intelligence on demand to answer any connectivity queries I have.

33.3%
I expect my mobile network to provide me with a highly personalized service where my account manager knows what I'm looking for, when and how I like to be contacted, and what I can afford.

31.7%
I expect to be contacted primarily by SMS.

28.5%
I expect to be contacted primarily by email.

27.7%
I expect the service from my mobile network operator to resemble a digital personal assistant, like Siri or Cortana, through my mobile device. I'll be alerted to changes in data use, best options available to me, bill reminders, roaming information, and will receive advice.

To read *Mobile Customer Experience 2025: what will end users need and expect?* in full, visit **tinyurl.com/mobile-2025**

AUTHOR: DAVID HOWELL
IMAGE: GETTY

For more from Gemalto on biometrics for identification and authentication, visit **bit.ly/2k7yFP9**

As mobile payments rapidly expand, security and consumer authentication have never been so important. With new forms of biometric authentication now available, physiology is the future of security

YOUR BODY IS NOW YOUR pA55w0Rd

With the arrival of Touch ID on the iPhone, biometrics moved out of its specialist niche and into the mainstream. Biometric identification has been used for several years for building access, for instance, but the iPhone was the first major consumer product to offer the technology. Since then, Apple Pay has advanced mobile payments and cemented biometric authentication as a key form of security for the future. Indeed, according to research by Acuity Market Intelligence, all mobile devices will have embedded biometric sensors by 2020.

A continued increase in cybersecurity threats has meant more robust forms of authentication are needed – especially where ePayments are concerned – to protect personal security. What is clear is that the continued use of established alphanumeric passwords does not offer the level of protection now required.

The human body has many unique features that can be used as a form of identification. From fingerprints to the pattern of veins in the hand to a person's gait, or even their heart rate – the use of these unique features as a biological ID has been evolving for decades.

BIOMETRICS IN ACTION

Now, other companies, alongside Apple, are starting to roll it out to a wider group of customers. MasterCard recently launched its Identity Check Mobile that uses biometrics such as fingerprints or facial recognition to verify a cardholder's identity, simplifying online shopping. Last year, Alibaba demonstrated what it calls its VR Pay system, where users simply nod their heads to buy goods when inside a virtual reality environment.

The financial services sector is also embracing biometric authentication.

Japan's Ogaki Kyoritsu Bank plans to use palm readers in its branches to identify its customers. An update to Citi's banking now allows customers to use a range of biometrics, including facial recognition, to log on to their accounts. Facial recognition is also being used by Spain's BBVA bank, enabling new customers to open accounts. And by simply taking a selfie, Brazilians can now sign up for mobile and online banking with an initiative from Neon.

According to BCC Research, the global biometric technologies market will reach US$41.5 billion by 2020. Fingerprint technologies as a segment should rise from US$8.8 billion in 2015 to US$24.4 billion by 2020, with a compound annual growth rate (CAGR) of 22.8% through the forecast period. The face, iris, vein, and voice technologies segment of this market will increase from US$4.2 billion in 2015 to US$11.9 billion by 2020, a CAGR of 22.9% for the period.

"We think that using biometric technology is a good compromise between the user experience and a good level of security, which is needed," says Michael Sass, EMEA Lead, Identity Solutions at MasterCard. "Also, we see biometrics as an essential component of all customer touchpoints from eCommerce to

mobile wallet payments. And an interesting additional touchpoint is also call center authentication."

WIDENING USE

Using biometrics to authorize payments is just one use of the technology. Many governments are actively developing new programs of identification that will use biometrics as their foundation. In Tunisia, for instance, proposed legislation calls for all citizens to carry an ID card encoded with various forms of biometric data. In Australia, the first phase of its Face Verification Service is now up and running, enabling the Australian Federal Police to initially match photos of new citizenship applicants with images on file. And the Philippines' Bureau of Immigration plans to link facial recognition at Manila's Ninoy Aquino International Airport to Interpol's databases to combat crime and terrorism.

Opposition from human rights and privacy groups has been vocal. Biometrics clearly offer an authentication solution, but the level of personal information that citizens would need to encode isn't yet understood by many governments.

Could organisations that want to adopt biometric authentication also find themselves facing opposition from consumers? A recent survey of UK and US shoppers from Computop concluded: "Given that 56% of US and UK respondents say they think retailers already ask for too much personal information, the issues of identity theft control and privacy may outweigh any perceived benefits [for shoppers]." That said, most consumers welcome the convenience of not having to remember multiple passwords, and being able to skip lengthy arrivals queues at airports, thanks to the mass deployment of biometric ePassports.

A clear issue is education. Bianca Lopes, Vice President Business Development and Strategic Marketing at biometric software firm BioConnect, says: "Three years ago, Apple did us all a tremendous favor by adding Touch ID to their iPhones. While the comfort level has increased significantly, there is still a lot of work to be done to educate the population that the commercial use of biometrics is much different than that of law enforcement."

Despite caution about biometric authentication voiced by human rights and privacy groups, and some consumers, there are growing signs that people are becoming more comfortable with, and trusting of, the technology. In a recent Gemalto survey, more than 50% of respondents believed that fingerprint identification helped protect them when using mobile apps. A MasterCard survey found that 92% of respondents wanted biometrics to replace passwords for eBanking services, and almost 75% believed that biometric-protected payments reduce fraud.

One of the most compelling arguments in support of using biometric technologies is their ability to link a user to the devices they are using for payments. "Device Binding" links an authorized user to their phone, for instance, with the biometric authentication preventing the cloning of the cryptographic keys that are being used to identify the user. Gemalto implements this technology with its Ezio platform.

MULTIPLE FACTOR AUTHENTICATION

As the level of security and authentication inevitably increases, multiple factor biometrics are likely to be used. Where facial recognition can be difficult in low light, or voice recognition in noisy environments, it makes sense to have several biometric tests available. Also, matching the level of biometric identification to context will see, for instance, a lower level of biometric authentication when using call centers but much more stringent biometrics to make payments via mobile devices or to access banking services.

"The different interactions that different biometric modalities require means that each is appropriate for distinct uses," says James Moar, Senior Analyst at Juniper Research. "This means that multimodal biometric authentication will become more common, or used for different kinds of transaction within the same device – for example, fingerprint for device log-in because it's like pressing the home button, and passive facial recognition for in-app usage, so that no further button presses are necessary."

As the level of security and authentication inevitably increases, multiple factor biometrics are likely to be used

> There is still a lot of work to be done to educate the population that the commercial use of biometrics is much different than that of law enforcement"

BIANCA LOPES, VP BUSINESS DEVELOPMENT AND STRATEGIC MARKETING, BIOCONNECT

In addition, Rob Norris, Head of Enterprise and Cyber Security EMEIA at Fujitsu, says: "Some biometrics are more secure than others; however, this is often traded off by increased cost. This is not a case of 'one size fits all' since no one biometric is suitable across all domains or risk profiles. These risk profiles should be fully understood when selecting the type of biometric to use."

A BIOMETRIC FUTURE

The use of biometrics will expand. Consumer payment authentication is just the tip of a large biometric iceberg that will increasingly include biometric data for eGovernment service delivery and law enforcement.

MasterCard's Michael Sass concludes: "Digital identity is where this technology is evolving to. Many countries want to be able to identify their citizens digitally to deliver various services. This is becoming increasingly important. When you want to deliver services such as eGovernment, being able to accurately identify a citizen [through digital means] is necessary. I think over the next decade, biometrics will mature enough to allow reliable and accurate digital identification for many electronic services that governments will want to develop for their citizens."

Biometric technology has been accelerating for several years. The need for more robust identification and authentication platforms has expanded development. Banking and consumer payments are driving this sector now, but with more widespread acceptance of these technologies, iris and face scanning at airports will become commonplace. Biometric encoded personal documents will also become accepted, with eGovernment services only accessible with biometric identification.

With more esoteric forms of biometrics including ear scans, gait and even scent being tested by the US Department for Homeland Security, we all have a biometric future ahead of us. ■

A BIOMETRIC EUROPE

According to research by Visa, consumers across Europe are interested in how biometrics can help them make faster and more secure payments. Nearly three-quarters (73%) see two-factor authentication, where a biometric is used in conjunction with a payment device, as a secure way to confirm an account holder.

When looking at the range of different payment situations at home or on the high street, over two-thirds (68%) want to use biometrics as a method of payment authentication. Online retailers have the most opportunity for gain as nearly a third (31%) of people have abandoned a browser-based purchase because of the payment security process.

In addition, with over two-thirds (67%) of consumers recognizing the importance of security details to protect one's identity, new forms of authentication must reach a balance between speed and security.

Key findings

The research found that biometric authentication is almost equally valued in face-to-face payment situations where speed efficiencies are a priority as it is for online transactions. This is reflected in the findings:

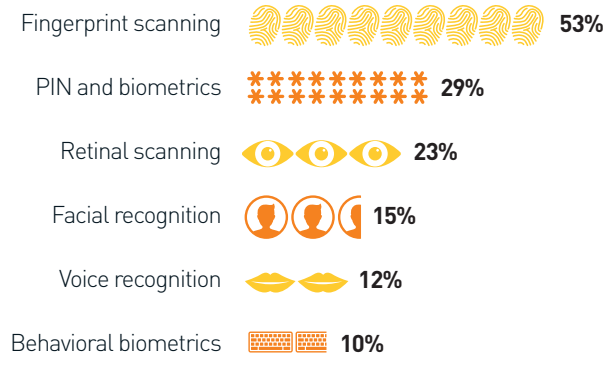
- 48% want to use biometric authentication for payments when on public transport
- 47% want to use biometric authentication when paying at a bar or restaurant
- 46% want to use it to purchase goods and services on the high street – e.g. groceries, coffee and at fast food outlets
- 40% want to use it when shopping online
- 39% want to use it when downloading content.

Factors for uptake

In the study of more than 14,000 European consumers, the research reveals that discretion and familiarity with biometric forms are important factors for uptake. With the advent of mobile payments, fingerprint recognition is deemed to be the most favorable form of biometric payment for its ease of use and security. When looking solely at the perceived security of biometric technologies, 81% of consumers see fingerprints as most secure, followed by iris scanning (76%).

"Biometric identification and verification has created a great deal of excitement in the payments space because it offers an opportunity to streamline and improve the customer experience," says Jonathan Vaux, Executive Director of Innovation Partnerships at Visa. "Our research shows that biometrics is increasingly recognized as a trusted form of authentication as people become more familiar with using these capabilities on their devices."

Consumer preference for using biometric authentication for payments in the future



AUTHOR TIM GREEN
ILLUSTRATION PAUL OAKLEY

The IoT is full of promise, but it will only work if users get connectivity and security, and providers get a return on their investment. In this three-part special report, we take a look at how the IoT industry can tackle these challenges

CONNECTING, SECURING AND MONETIZING THE IoT

Turning things on

To understand the journey of the Internet of Things from concept to the mainstream, it helps to start with Barbie. In 2016, Mattel debuted Hello Dreamhouse – a featured-packed connected home for the doll. Kids can tell the voice-activated home to do over 100 things. They can turn on the lights, order a pizza, open the doors. Yes, this is the smart home you might dream of. And Barbie already owns one.

Barbie is living the dream because of a revolution in connectivity that's making previously dumb objects smart and – more importantly – able to talk to each other.

Manufacturers have been embedding processors in everyday products for years. Washing machines, watches, microwaves – they all contain chips. Even Barbie has an embedded processor and rechargeable batteries in her legs. But the emergence of multiple connectivity options changes everything. Before, a washing machine could merely be pre-set. Now, it can tell the manufacturer it needs a new part. Previously, a doll could be played with. Now, it turns on the lights in the dollhouse.

THE INDUSTRIAL IOT

Connected Barbie and smart washing machines may grab all the headlines, but the so-called industrial IoT is a much bigger deal. Nearly all business sectors are looking into the IoT because of its potential to deliver efficiencies and improve revenues. Research firm IDC says 31.4% of organizations surveyed have launched IoT solutions, while 43% will do so in the next 12 months. It says the market will be worth US$1.29 trillion in 2020. Meanwhile, Ericsson predicts that there will be 29 billion connected devices by 2022, of which 18 billion will be related to IoT.

All sorts of industries are being transformed, including the world's oldest – agriculture. John Deere, historically a maker of farming equipment, has committed its future to the IoT. One of its innovations is a sensor that measures the pressure being exerted on each seed as it's planted. The sensors can communicate data via Wi-Fi to an iPad in the cab of the tractor, and the driver can make adjustments.

In retail, clothes chain Zara uses Radio-frequency Identification (RFID) technology to track stock in real time and make its "just in time" model even more efficient. Steffen Sorrell, Senior Analyst at Juniper Research, says: "Retailers have used RFID tags in the warehouse for years, but only now are they properly realizing the benefits. The next step will be linking them to beacons and dynamic signage in-store."

Barbie smart homes, connected tractors and tagged blouses point to an exciting future. But it's not here yet. This is why some jokers call the IoT the Internet of No Things.

NUMEROUS HURDLES

Clearly, there are numerous hurdles holding back the revolution. One significant barrier centers on the harsh environments of heavy industry. Historically, users

For more from Gemalto on the IoT, visit
tinyurl.com/Embedded-to-IoT

> The greatest competitor IoT companies face is what consumers are doing without the IoT. If [what firms offer] is difficult or complicated, forget it"
>
> **SVEN NEWMAN, PARTNER, DAYLIGHT**

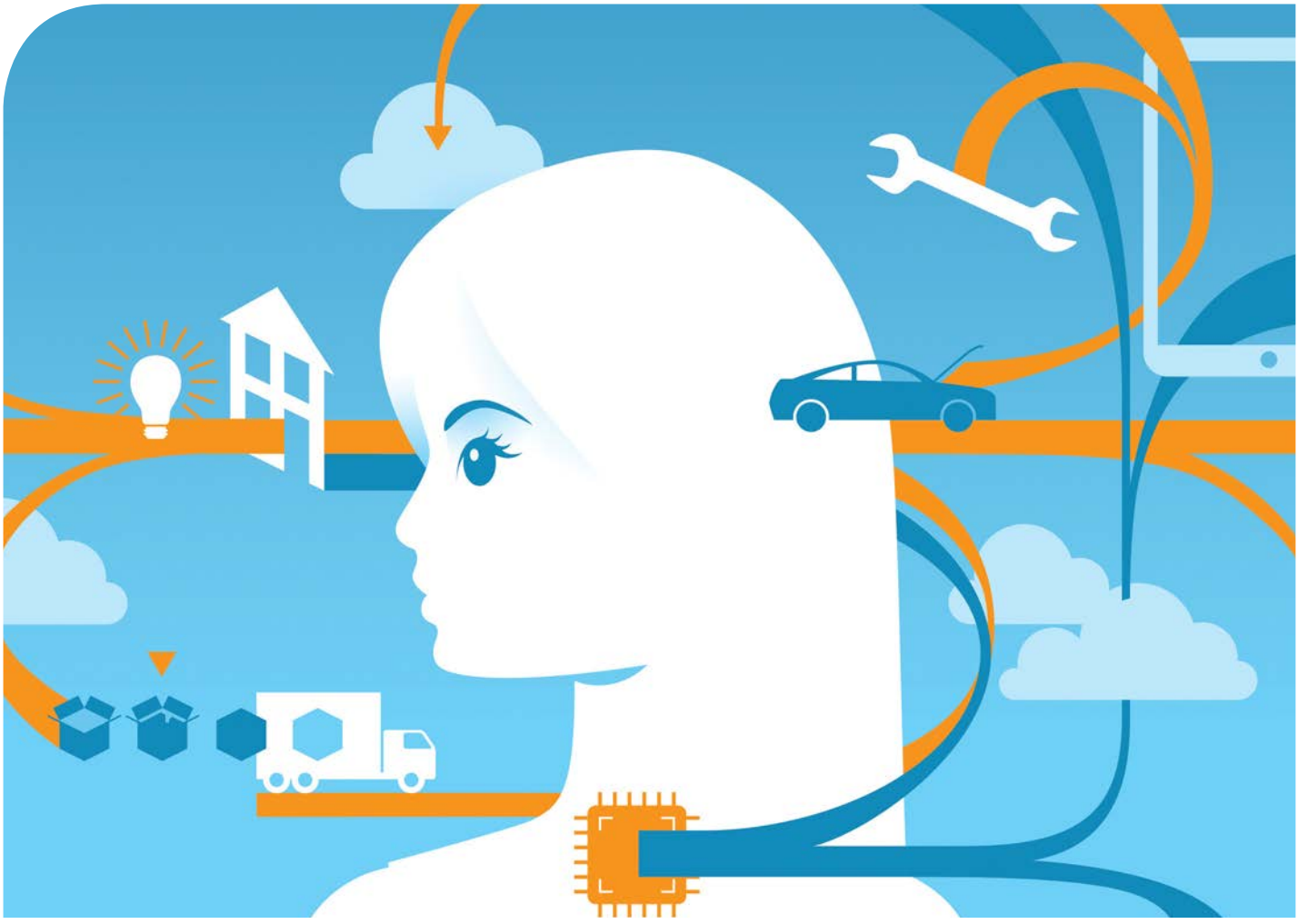
have connected consumer devices by placing a delicate plastic SIM into a slot. This approach cannot work in an underwater meter or on an oil well. To tackle this, connectivity specialists have developed a special ruggedized SIM for IoT use. It can withstand extremes of vibration, temperature, and humidity – and has a 10-year lifespan.

Another barrier is security. Consumers are understandably deterred by the ease with which hackers can take over smart devices or listen in to the data. Predictably, hackers have modified the Hello Barbie app to reveal passwords and other confidential information.

Design is also a choke point. There is no consistent user experience available to consumers when setting up and operating IoT objects, which are so disparate. Some have screens, some don't. Some are single purpose, some multi-functional.

It pays to keep things simple. Sven Newman, Partner at design agency Daylight, said on the Adobe blog: "The greatest competitor IoT companies face is what consumers are doing without the IoT. If consumers experience something intuitive, they will consider adding a new routine or product to their life. If it's difficult or complicated, forget it."

One of the most celebrated IoT devices to date, the Nest thermostat, shows the value of simplicity. It's just a round silver dial with an LCD display in the center. Users set it up just by turning the dial, and the display



> The [Amazon] Echo is interesting. People seem happy to talk to a machine in the home in a way that's not acceptable outside"
>
> **STEFFEN SORRELL, SENIOR ANALYST, JUNIPER RESEARCH**

turns red or blue to indicate whether it's heating or cooling. It sold over a million units.

But, to repeat, the challenge is replicating one delightful user experience across so many disparate device types. In fact, Nest's story illustrates the problem. The company had a vision to build a family of products and create its own ecosystem for the smart home. But that didn't happen. In 2016, Nest changed its management and strategy amid falling sales.

COMMUNICATION AND CONNECTIVITY

Today's IoT consumers – and manufacturers – are faced with an array of often incompatible options. Multiple connectivity types are available, from Wi-Fi to Bluetooth to 4G. Devices produced by different makers often don't easily communicate with each other.

Even IoT suppliers require clarity. Encouragingly, connectivity specialists have started to provide mobile operators and others with solutions to address this. They can offer dashboards that give equipment suppliers real-time visibility of network status.

On the consumer side, the explosion of confusing options is something that Apple, Amazon and Google are trying to solve. Apple's HomeKit, for example, gives device makers a platform through which to connect objects to apps. Meanwhile, Amazon Echo and Google Home do the same via one voice-activated tower.

Sorrell says: "The Echo is interesting. People seem happy to talk to a machine in the home in a way that's not acceptable outside. But its long-term future depends on its ability to monetize. Maybe Google has a better shot here, though there is a trust issue when it comes to Google and data."

Sorrell is referring here to Google's historic tussles with regulators over its approach to data collected from Gmail, Street View and so on. One can imagine how unsettled some Home users would be if a private chat "overheard" by Google Home about buying a new kettle, for example, led to AdWord banners for kettles.

> Today's IoT consumers – and manufacturers – are faced with an array of often incompatible connectivity options and devices

"All the devices that come with the Google Assistant are designed with privacy in mind," a Google spokesperson told *Computerworld*. "We only process speech after the hotword "OK Google" is detected. If the hotword is not heard, the audio snippet stays local on the device and is discarded."

Another question mark over the adoption of the IoT concerns connectivity. There are multiple options. For shorter distances there are Bluetooth, RFID and Near Field Communication (NFC). For long distance, there are 4G, Wi-Fi, Thread, ZigBee and Narrowband IoT (NB-IoT). The latter has been developed to minimize the power consumption and spectrum efficiency of devices. In some cases, battery life can be more than 10 years. NB-IoT can co-exist with 2G, 3G, and 4G networks, and is already live with Vodafone.

THE IMPACT OF 5G

The arrival of 5G will also make a difference. 5G is not just faster than Long-Term Evolution (LTE), it also offers 100 times better latency, up to 100 times more connected devices per unit area and a 90% reduction in energy usage. All of this hugely multiplies the number of devices that can connect simultaneously.

LTE and 5G are self-evidently very appealing to IoT device makers. They are always on and cover most of the world. But will manufacturers buy a SIM card and data plan for every device they ship? Clearly not. This is why the mobile industry has developed a new kind of embedded SIM (eSIM) that can be soldered in place.

It's especially useful for car makers. The eSIM can withstand vibration and heat, and can be remotely programmed to work with any selected operator. So cars built for export can connect to local networks when they arrive at their "home" destination. With an eSIM, drivers would just pay for usage instead of a traditional subscription model with fixed monthly fees. And there would be no need for the car maker to have multiple SIM agreements in every country. General Motors, Jaguar Land Rover, Renault Nissan, Scania and Volvo have already committed to the standard.

The development of the eSIM proves that collective action can introduce shared IoT standards that benefit everyone. Happily, the same movement is happening in software. For years, there were two rival consortia developing competing IoT protocols. In 2016, the Open Interconnect Consortium and the AllSeen Alliance put aside their differences to form the Open Connectivity Foundation (OCF). That has to be good news for OEMs.

How secure are connected devices?

In October 2016, a ragtag army of CCTV cameras, digital video recorders (DVRs) and printers teamed up to overwhelm the internet infrastructure company Dyn with traffic. Inevitably, Dyn went down. And so did its clients – including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

The cameras and DVRs didn't know they were taking part in the mission. Rather, they had been infected by malware to become the Mirai botnet – a robot network established by hackers to conduct DDoS (distributed denial of service) attacks.

Security experts call these bot networks zombies because they just sit there until directed to do something by miscreants. Traditionally, zombies ran on computers. Now, with the advent of the IoT, a huge new hole has opened up. Millions of new connected devices are available to hackers. Most are insecure. After all, who bothers to password-protect their CCTV cameras? Or their Barbie dolls?

NEGLIGIBLE SECURITY

For John Shier, Senior Security Expert at Sophos, it's all evidence that the first generation of domestic IoT devices has negligible security. "The main weakness is at the production stage," he says. "The devices are made with little security in mind. Most feature hardwired passwords that can't be changed, and code that can't be upgraded. Even if the firmware can be updated, it's beyond the capability of most users to do it."

Shier's colleague James Lyne, Global Head of Research, spent many months testing connected devices. He used a brute force password tool to access hundreds of CCTV cameras in less than an hour.

Lyne says: "These devices require no username or password and contain no cryptic keys. There hasn't been a security model like that in computing for over 10 years. Yet we have this model for devices people are using in their homes right now."

Unsurprisingly, perhaps, money is often to blame. Shier says: "These companies want to be first to market, and security protection just costs money and slows production down."

For companies specializing in digital security, the world of connected devices poses specific challenges – most of which don't apply to servers, PCs and mobiles. Companies with no history of product security often make IoT devices. Some devices don't have user interfaces. Others are fiddly and inaccessible.

EXISTING SOLUTIONS

Happily, solutions do exist. The first step is to assess priorities. For example, it's far more important to protect access to a smart lock than to protect its activity data. And there are many simple protections that involve minimal effort – such as taking a device off the internet. After all, if the only purpose of a camera is to relay footage to a nearby recorder, does it really need to beam data to the cloud?

But when a device does need to be connected, there are four key factors to consider:

- Authentication – only approved users can access the device.
- Confidentiality – the data is kept secret.
- Integrity – hackers can't change the information sent.
- Availability – the device can't be prevented from sending data.

Needless to say, it's not just devices that need to be secured. The cloud infrastructure they are connected to must also be protected so that device flaws don't disable the whole system. This much was clear from the Mirai botnet attack mentioned earlier.

Spending on IoT security will jump from US£348 million in 2016 to US$547 million in 2018, and will increase at a faster rate after 2020, says Gartner

Even though the flaw was in the devices, it was the network as a whole that suffered.

It's likely that enterprise users will tackle these issues first. After all, they have far more to lose than suburban users of smart sprinkler systems.

Analysts agree. Research firm Gartner says worldwide spending on IoT security will jump from US$348 million in 2016 to US$547 million in 2018, and will increase at a faster rate after 2020. Gartner argues spending should be even higher. It says 25% of attacks on enterprises will involve the IoT, although the IoT will account for less than 10% of IT security budgets.

Needless to say, major players in the industry are dedicated to tackling IoT security. Tech firms including BT, Intel and Vodafone launched the Internet of Things Security Foundation (IoTSF) in 2015.

And IoT security specialists have developed their own strategies to help IoT firms protect against attacks. Typically, they offer a three-pronged approach: encrypting data in the device, securing the data on the cloud, and managing device identities.

This last pillar is often overlooked, but it's vital. One of the great challenges of the IoT is correctly identifying the device sending the data. After all, most have no human "owner". And the issue is made more complex when devices change hands or are decommissioned.

CONTROLLING ACCESS

Gemalto's solution, for example, ensures that a company can remotely provision keys for every device and thereby maintain control over who has access to it. Haider Iqbal, Segment Marketing Manager for IoT, On-Demand Connectivity and OEM at Gemalto, says: "Having a strong identity management system is really important. It means a service provider can configure new keys and even the OEM that made the devices can't get into them. If the ownership has changed, no one else can exploit that."

Getting a return on investment

If the analysts' bullish projections for the IoT are proved correct, it will be because the IoT makes – or saves – money. So the question is: how?

Well, the first priority is to remunerate the companies that are building the IoT infrastructure. Multiple players are contributing IP, software and data to make this revolution happen; they must make money from their investments. They need solutions to protect against software tampering, reverse engineering and outright theft.

But assuming the IoT infrastructure is built, what are the incentives for manufacturers? For many, cost savings are one obvious pull.

Take Philips Healthcare. In 2014, the company began fitting its hugely expensive patient scanning machines with the ability to send simple text alerts to engineers. The messages would essentially say: "There's something wrong, come and fix me". It means Philips Healthcare can maintain working machines rather than fix broken ones. And it saves US$250,000 a year.

Now, the company is drilling further into the data to derive more efficiencies. John Romero, a National Support Specialist (MRI) at Philips Healthcare, says: "With all the extra data we have now on machine failures, we can build a more holistic view of what works. We can start thinking about replacing parts that we sense may be about to expire, for example, rather than waiting for an alert saying they are already failing."

COMPLEX MODELS

In the consumer space, the models are more complex. Someone – the consumer – has to pay, and there are many in the value chain that want their cut. These parties include the providers of:

- The smart module inside the device
- The device itself
- Connectivity
- System integration
- Applications.

This is, of course, very different from the industrial world of "dumb" devices, in which a single manufacturer has little or no relationship with a consumer after selling a product. In this simple set-up, a consumer pays once. Job done. But that doesn't necessarily work when a product delivers a service over months and years.

For more from Gemalto on software monetization, visit **gemalto.com/software-monetization**

> With all the extra data we now have on machine failures, we can build a more holistic view of what works"

JOHN ROMERO, NATIONAL SUPPORT SPECIALIST (MRI), PHILIPS HEALTHCARE

Thus, the IoT turns product companies into service providers. This is exciting. A recurring subscription can be a very attractive business model. But in reality it can be hard to change the consumer mindset. Fitbit is a case in point. The company sells around 20 million trackers a year, but it also offers Fitbit Premium. It costs US$50 per annum and offers richer data and a personalized fitness plan. Though Fitbit Premium was launched in 2010, it contributed less than 1% of revenue in 2015.

The IoT turns product companies into service providers. A recurring subscription can be a very attractive business model

However, for many companies, there's no option but to embrace this new reality. After 120 years of selling lightbulbs, Philips Lighting saw the potential of the IoT (and the simultaneous threat of long-life LED bulbs) and committed its future to "lighting as a service". It teamed up with Cisco to develop its offering. Shortly after, it agreed a deal with Amsterdam Airport Schiphol in which Schiphol only pays for the light it uses.

Frank van der Vloed, General Manager of Philips Lighting Benelux, explains: "I drink water, but I don't have a reservoir in my basement. Many people are used to pay-as-you-go models. Add to this energy savings from LED technology and the sustainability of the overall system and the proposition is compelling."

With its new strategy, Philips has clearly "seen the light" and made a significant bet on a service-based future. Who knows, maybe it can win the contract to illuminate Barbie's Dreamhouse. ■

AUTHOR KATE BEVAN
PHOTOGRAPHY DARE & HIER MEDIA

Having grown up in war-torn Rwanda, Nicaise Ishimwe, Quality Assurance Analyst at emovis, is determined to use her talents to build connections between people and use those connections to create lasting solutions

PROBLEM SOLVER

Nicaise Ishimwe has spent a fair chunk of her life on the move: now living in Ireland, she arrived there at the end of 2014 to work for emovis via a childhood in Rwanda and student days in Algeria and France.

That's a lot of ground covered, both literally and metaphorically, for someone who's only just into her 30s, but when speaking to Ishimwe, it becomes clear that she's someone who's determined to use her experiences to build connections between people, and use those connections to solve problems.

With those two aims, it's perhaps not surprising that Ishimwe is an engineer with deep experience and expertise in mobile telecommunications. She now works for a company creating and delivering tolls technology and solutions for highway providers around the world. "I was always someone who wanted to find solutions to problems," she says. "In school I loved mathematics and problem-solving."

That's a tough industry for a woman to be in, and, says Ishimwe, she is the only woman on the tech side of the company. So why pick a company so far from home, and one where she would be a lone female technologist?

"I joined because I have an interest in intelligent communications and in developing smart mobility solutions. It seemed like there was the possibility to apply my skills there and to make a difference."

And as if that were not challenging enough, Ishimwe, whose mother tongue is French, adds: "I wanted experience in an English-speaking country."

CHALLENGING CIRCUMSTANCES

Ishimwe's determination was forged in the most challenging of circumstances: she was a child when tensions in Rwanda erupted into genocide, with some 800,000 Tutsis killed in the space of just three months. "When it happened I was living with my mum and my father was away in rural areas; he was home only at weekends. My mum was looking after four kids and it was sometimes very hard – we were all very affected.

"It had a huge impact on me: I learned that we need to love each other, that we need to live in love and peace. It affects the way I interact with others: I try to understand their opinions and views and not to judge."

And so, in 2004, Ishimwe took up a scholarship offered by the government of Rwanda to study at the Université Mouloud Mammeri de Tizi-Ouzou in Algeria for her first degree in science and technology. From there she went to Lyons in France to study at the National Institute of Applied Sciences (INSA).

Despite moving so far away from Rwanda, home was nonetheless very much on Ishimwe's mind: "Growing up where I did, I saw things destroyed after the genocide – the infrastructure was gone. That made us realize that we needed to work hard for the development of our communities, and our parents and our government encouraged us to study hard to help others."

ENGINEERING EDUCATION

Ishimwe's studies increasingly led her to focus on three main areas: wireless and wired communications, computer networking and software development. This resulted in her completing not one but two degrees: one in networks engineering and a master's in electrical engineering.

As part of her studies, Ishimwe did three internships that set her on the path to her current job as a Quality Assurance Analyst at emovis. "When I did my first internship I developed an application for public transport information and that helped me grow an interest for the transport sector, so I

For more from Gemalto on women in tech, visit */review* at **bit.ly/2l14rtq**

Ishimwe’s studies increasingly led her to focus on three main areas: wireless and wired communications, computer networking and software development

was looking for opportunities to apply my skills in software and in mobile telecoms,” she explains.

It was that interest that kept her in France rather than returning home to Rwanda. Moving to work for Alstom Transport in Villeurbanne, Ishimwe turned her attention and her talents to systems to monitor trains for SNCF, the French rail operator. “I was working on a system to monitor indicators and metrics from different pieces of equipment via a central system – it meant we can monitor from a central point to make sure trains are moving nicely and ensure the safety of the train.”

She also worked on a cab radio system for on-board communications between the driver and passengers. Both of these projects leveraged her skills in mobile telecoms technology, and helped her develop them further, and so when the opportunity came up to move to Ireland, Ishimwe was ready to make the jump.

A BIG JOB

The job at emovis is a challenging one, with many facets to it: “I joined as an application specialist, making sure that the applications satisfy customers’ and the tech specifications,” she explains. “That means I’m the liaison between developers in Croatia and the operations team; I’m tech support, providing product knowledge to make sure the applications are well installed and maintained. I ensure the quality and that all change requests and corrections are tested and validated, and that the software delivery is all correct.

“It’s a big job and it can be hard and challenging. But with time you get to know the product and the issues that come, and you get to know how to deal with them.”

One of those issues – and a huge challenge facing the tech industry – is the constant threat of data breaches. She says digital security is a key area: “That’s

Working conditions are not flexible enough to accommodate the changing needs of women and families as people move through their careers

WHY TECH NEEDS WOMEN

When Melinda Gates was studying in the 1980s, she says around 37% of computer science and law graduates were women. Today, around 47% of law graduates are female. In computer science, that figure has fallen to 18%.

It's a problem that Gates, co-chair of the Bill and Melinda Gates Foundation and a computer science graduate, plans to tackle with a new initiative to get more women into tech-related fields and keep them there. Her solution is two-fold: plugging the leaks in the education pipeline when females are most likely to drop out of tech-related subjects, and encouraging companies to have family-friendly policies that make it easier for women to juggle work and home life.

That's essential if the tech sector is to improve its record on gender diversity. A 2015 study, by tech title *CNET*, of some of the leading tech companies in Silicon Valley revealed that while women made up 29.1% of the overall workforce, they accounted for 22.5% of leadership positions and just 15.6% of tech staff. That's against a landscape where women make up 51% of the US population and 59% of the US labor force.

The upshot of this imbalance? Businesses that are failing on diversity are taking a hit on their bottom line. A study by the US's National Center for Women and Information Technology found that businesses perform better financially, and in terms of productivity, when women occupy a significant proportion of top management positions. It also found that gender-diverse technology organizations and departments are more likely to stay on schedule, under budget and show improved employee performance.

the main element one should focus on. Customers need to feel they can rely on security – if there's a possibility of a breach of their data, they tend to back down."

She adds: "It's not rare that we hear a company has had a breach. That can have a huge impact, not only financially but also in terms of confidence. People question if they should continue to use your product. It's really something developers should focus on."

Being the only woman in a team could be difficult, but, says Ishimwe, that's not an issue at emovis. "I work hand in hand with others who are good managers and good co-workers. Fortunately I don't have many challenges: they are a supportive company; they have the culture of supporting each other and communicating with each other to understand the issues. It hasn't been hard at emovis at all."

However, that's not the case elsewhere in the technology sector, says Ishimwe. "In other companies I've observed women who were facing issues and difficulties getting themselves respected: it would be hard for them to get their decisions respected; they were challenged."

TACKLING INEQUALITY

Despite a growing awareness of and focus on the problems of sexism and discrimination in the tech industry, there's still a long way to go before the

For more from Gemalto on women in tech, visit **bit.ly/2kmejyK**

> Women need proper professional development so that they have the opportunity to reach higher positions"
>
> **NICAISE ISHIMWE, QA ANALYST, EMOVIS**

sector generally is as welcoming to women as emovis has been for Ishimwe.

She believes better visibility for the women already in the tech industry would be a big help. "One of the main challenges is that we don't have many role models as women," she says. "We are not well exposed or put forward as examples, and we need the examples of women who have excelled to be visible. We need those women to share their experiences and inspire others."

One key problem is that working conditions are not flexible enough to accommodate the changing needs, not just of women, but of families, as people move through their careers. "Women are trying to stay in the industry," says Ishimwe. "We need to make sure that women stay in those companies – one reason they leave is because they don't have the opportunities to progress and reach higher positions. Women aren't supported enough in companies."

So what can be done? Ishimwe has a quick, sure answer to that question: "Companies need to develop actions such as sponsorship, mentorship and training and you need to start at entry-level, where women are looking for jobs. Women need proper professional development so that they have the opportunity to reach higher positions."

And it's not just in companies that we must think about how to encourage women into the tech industry, adds Ishimwe: it should begin at a much younger age, in schools. "There needs to be information in schools about the industry that breaks the perception that it's male-dominated. We need to help girls understand that it's an area where women can excel."

TOUGH TRANSITIONS

Ishimwe sees herself as someone who has made a number of transitions, not all of which have been easy. Moving to Europe from Africa was a jolt, she says: "When I moved from Rwanda to Algeria it was a kind of transition – Algeria has a French influence, but moving to France really was a challenge. The pace of work and the way of teaching was completely different to what I was used to."

However, Ishimwe feels lucky to have had supportive people around her as she adjusted to life in Europe. "Something I did badly when I began was I thought that I could do things by myself. But you need to rely on other people who have had the experience. I had people who were very welcoming, and loving and supportive."

And now Ishimwe is passing on that support to others through her work with Women in Tech Africa, which not only supports African women in the sector but also looks to the future with its emphasis on providing role models for girls and young women.

Having joined the organization in 2015, Ishimwe is now the leader of the Irish chapter. "In the beginning I was just a member, but I realized that I needed also to help other women, so I reached out to the founder to see if I could get involved.

"Now I organize events in Ireland to provide opportunities for women from Africa to network, to know what others are doing and to reflect together on what we can do for our African communities. We learn from each other and we invite role models – women who have succeeded – to come and share their experiences in technology."

FUTURE AMBITIONS

Ishimwe plans to remain in Ireland for now, but going back to Rwanda is very much on her mind. The genocide, she says, "was something huge that touched people everywhere. For me it was hard to understand how people can hate each other to that level, and how governments and international organizations were not able to stop it.

"We grew up more energized from that. We learned that anything can happen, and the lesson is that we need to live in love and peace. Going back in the future is something in my mind."

She adds: "I would like to start a business; I'd like to do something in telecoms. But wherever I am, I hope I have the opportunity to make an impact, to contribute to what is happening." ■

> Ishimwe is passing on support to others through her work with Women in Tech Africa, which provides role models for girls and young women

NICAISE ISHIMWE: HIGH ACHIEVER

2006 Graduates from the Université Mouloud Mammeri de Tizi-Ouzou in Algeria with a BSc in Science and Technology

2010: Graduates from the INSA de Lyon in France with a double degree in telecommunications: networks engineering and electrical engineering

2011 Joins Alstom Transport in Villeurbanne, France as a consultant Verification and Validation Engineer, on behalf of AVISTO Telecom. Ishimwe undertakes verification and validation activities of on-board and board-to-ground train communication systems and a remote monitoring system for train fleets

2014 Moves to Ireland to join emovis technologies as a Quality Assurance Analyst, specializing in applications. She acts as a liaison between the software development and emovis Ireland operations teams, focusing on changes affecting the M50 toll system and the Irish electronic tag interoperability system

2017 Acquires an MBA from the University of Wales. For her thesis, Ishimwe focuses on workplace gender diversity and firm financial performance among Ireland-based tech companies

AUTHOR TAMSIN OXFORD

Smart mobile technology and ingenuity are transforming government and citizen interaction and identity

DEMATERIALIZING DOCUMENTS IN THE DIGITAL ERA

GETTY

Three words define the potential of government to succeed in the implementation of a digital strategy – trust, interoperability and mobility. According to a report developed by the Secure Identity Alliance and the Boston Consulting Group, governments can potentially save US$50 billion when implementing eServices by 2020, but only if frameworks are secure, trust is prevalent and policy is watertight. Added to this is the digital citizen, who expects government to deliver 24/7 services that cut back on admin, improve quality of life and are accessible on mobile.

DIGITAL VALUE

There are numerous eGovernment initiatives around the world that have shown the value of well-honed digital implementation. Neville Cannon, Research Director, Public Sector at Gartner, says: "[Estonia] came out of the Soviet Union with a citizenry that didn't have a lot of trust in government and had to work really hard at [rapidly] establishing a digital infrastructure [that was transparent]. They have done this incredibly well. It is very difficult to win the trust and faith of people as a government – the volumes of data mean the burden of proof is much higher."

In Spain and Finland, Mobile ID is being used to create a cross-border identification solution that is compliant with the European Union's eIDAS Regulation, which enables secure and seamless electronic interactions between business, citizens and public authorities. Mobile ID allows users to access eGoverment services from both countries using a universal digital identity. Turkey was the first country in the world to adopt a mobile signature solution. The network provider, Turkcell, gave subscribers the ability to access online services using an electronic signature that was both highly secure and legally binding. And

To find more about eGovernment in Estonia, visit Gemalto's */review* at **bit.ly/2jiLoth**

> The younger generation rarely carries a wallet and uses apps for most activities, so it makes sense to create a mobile solution"
>
> **STEVE PURDY, VP OF MARKETING, GEMALTO**

in Oman, a national electronic ID card was the first eGovernment system of its kind in the Middle East, providing users with the ability to authenticate their identities on any device.

In the United States, the trends and imperatives of the eServices era have driven the development of a digital driver's license pilot across four jurisdictions – Colorado, Idaho, Maryland and Washington DC. "The initiative takes the driver's license and puts it onto the mobile phone, improving the way people present and prove their identities to business and government organizations," says Steve Purdy, Vice President of Marketing for Gemalto. "The younger generation rarely carries a wallet and uses apps for most activities, so it makes sense to create a solution that's accessible on a mobile platform and ties back to this growing demographic."

TRUSTED ECOSYSTEM

Gemalto won a government grant from the US's National Institute of Standards and Technology (NIST) to develop this trusted ecosystem for Digital Driver's Licenses (DDLs) and ID cards on mobile devices. "NIST wanted a solution that went beyond just possibility," says Purdy. "It had to show the ability to go into production and become something everyone would use."

Currently still in the pilot stage, the project is focusing on four areas: enrollment, updates, attribute sharing and law enforcement. It has been broken down into two phases – the first establishes the DDL, which can be used on a mobile phone with complete security and privacy; the second looks at the potential of attribute sharing – the ability to use the DDLs to confirm identity and data in a variety of situations, from renting a car to buying a home.

"It's a really exciting technology and there are a lot of things you can do with it," says Purdy. "With this program, the DDLs can be used in neighboring jurisdictions, not just in their issuing state. Drivers have full control over their data and can use their DDLs to verify their identity when pulled over by law enforcement. They can potentially also use them to identify their age and identity at various establishments such as liquor stores."

Bonnie Fogdall, Operations Manager at the State of Idaho's Division of Motor Vehicles, adds: "The development of the digital driver's license is in its infant stages. There are many challenges. However, one of the key drivers is associated with ensuring safety and appropriate authentication for both the driver and those needing to view the license. Understanding and meeting the needs of both the license holder and the verification agency is the primary focus."

The digital citizen expects government to deliver 24/7 services that improve quality of life and are accessible on mobile

WINNING TRUST

"Unfortunately, if eGovernment isn't done well, it can waste money, duplicate effort and potentially lose the trust of the people it serves," says Cannon. "In the US, the Office of Personnel Management was breached and saw 21.5 million records hacked. That alone is cause for concern. The whole idea is that government should show it can hold onto things securely. The reality is that if a foreign government wants your data, they probably already have it."

If done well, however, eGovernment can deliver numerous advantages: costs can be cut as services are delivered more effectively; outcomes are improved across sectors; and education and health are more dynamically developed to introduce sustainable economic prosperity. Digital information and data gathered through eGovernment services can potentially give policymakers the right tools to improve service design, make more informed choices, speed up service delivery and drive development more effectively. Cannon predicts that the next few years will see government try to get more from their data to generate money and efficiency. New technology will change how governments operate and what citizens expect.

"eGovernment initiatives are the future of government and what is expected by the 'now' and 'future' generations that we serve," concludes Fogdall. ■

AUTHOR ADAM OXFORD
ILLUSTRATION RHUBARB RHUBARB

TAKING ON THE CYBER HACK

The cost of cybercrime is spiraling into inconceivable numbers as attacks get more sophisticated and easier to launch. Companies need to focus their attention on protecting their most precious assets

Putting a combined cost on the vast number of data breaches, data manipulation incidents and other cybercrime attacks that are increasingly common is impossible – but, being human, we try. IBM and the Ponemon Institute, which conducts research on privacy, data protection and information security policy, reckon that the average consolidated cost of a data breach for a large corporation is US$4 million. Research firm Cybersecurity Ventures says the overall cost of cybercrime was US$3 trillion in 2015 and will rise to US$6 trillion a year by 2021. Grant Thornton International, the professional services firm, is more conservative: it puts the direct cost to business at closer to US$300 billion a year.

Putting a combined cost on cybercrime attacks is impossible – but, being human, we try

Whichever number you choose, it's inconceivably big, because cybercrime is big. Gemalto's online Breach Level Index lists incidents in which almost six billion records have been lost since 2013, of which just 4% were encrypted and therefore useless to attackers. Dave Clemente, lead researcher in the cybersecurity team at Big Four accountancy firm Deloitte, says that some industries are better than others at evaluating damage and risk, but traditional cost–benefit analysis isn't always the best place to start.

ADDING IT UP

"It's quite a bit easier to quantify in financial services," Clemente says, "because everything is measured in some way. Any big bank can break down the level of payment card fraud in their country, and get a good view of how much is taking place and what needs to be spent to reduce that. It is harder in other sectors. In pharmaceuticals, there's a lot of data that is very sensitive – like trial results – but it's not valuable per se." Big data dumps of personal details regarding customers or staff – including email dumps or

membership records – carry reputational costs that are hard to measure.

"Whether it's malicious leaks or whistleblowing," says Clemente, "as more and more of our lives are digitized, it becomes easier to do." Last year saw personal data stolen and leaked from UC Berkeley, Snapchat, Wendy's restaurant chain, Cisco, AdultFriendFinder.com, the National Payment Corporation of India, Hotmail, Gmail and many more. Dropbox discovered that 68 million accounts had been breached four years ago and, in possibly the biggest theft of information to date, Yahoo! confessed that at least half a billion customer accounts may have been compromised in an attack dating back to 2014.

Significantly, in the case of Yahoo! it was believed that the attack was state-sponsored. Given the recent furore over accusations that a foreign state sanctioned not just the theft of email data but its use to influence the 2016 US presidential election, the political cost of cybercrime is rapidly becoming as significant as the financial.

INCREASED AWARENESS

Clemente says there is a positive angle to last year's headline breaches: customers are far more aware of data security than in the past, and the reputational damage caused to companies by breaches is no longer quite as high. Take Sony's problems over the last few years. A massive leak of the email database for Sony Pictures (which the FBI believes was facilitated by North Korean spies) severely compromised the company in 2014. And, in 2011, details from some 77 million accounts were stolen from its PlayStation Network. Yet PlayStation 4 has outsold its rival, the Xbox One, by a ratio of two to one, while Sony Pictures' revenue rose 7% in 2015.

Headline-grabbing data breaches mean that companies are now more realistic about security

Headline-grabbing data breaches also mean that companies are now more realistic about security. "Most companies acknowledge that if they haven't been breached, they probably will be," Clemente says, "or that they have been and just don't know. Companies have a different expectation even to three years ago."

This heightened awareness has been helped by the proliferation of laws that require US companies to report data breaches to authorities and those affected, as well as the European Union's (EU) General Data Protection Regulation (GDPR), which comes into force in 2018 and will require EU companies and those who store data there to report breaches. However, even if companies have heard of GDPR and are preparing for it – which is far from a

A NEW THREAT FROM THE IoT

There will be many things that 2016 is remembered for in the history books: Brexit, Donald Trump's US presidential election victory, Colombia's peace deal with the FARC guerillas. It may also go down as the year that the Internet of Things (IoT) became a weapon to be exploited by cybercriminals. In December, tech websites reported on the case of an Android-powered smart TV that was infected by ransomware.

The most worrying development, however, is arguably demonstrated by the Mirai botnet, which was used to attack IT security journalist Brian Krebs' website and Dyn DNS. The simple malware from which it takes its name searches the public internet for connected devices like domestic routers, CCTV cameras and digital video recorders and, if they're unsecured or locked down using only default username and password pairs, infects them with a memory resident program that can be used to launch an attack.

George Conrad leads the team at Google that has developed Project Shield, the anti-Distributed Denial of Service (DDoS) platform that was eventually used to stop the attack on Krebs. He works with hundreds of news organizations that find themselves being taken offline by DDoS attacks, often as a result of state-sponsored opposition to their work.

Kenya-based website *Africa Uncensored*, which is run by a team of investigative journalists, suffered a DDoS attack three times in its first week before it was taken under Shield's wing. "Our moonshot goal," says Conrad, "is to eradicate DDoS as a form of political censorship."

GETTY

given – Clemente says that these laws are only partially effective. "We're not even close to 100% reporting yet in the US, and it's unlikely to get there in the EU."

Elle Todd, who leads the media and technology team at law firm Olswang, agrees that the GDPR won't be a fix-all solution, at least not immediately. She says that although the legislation is coming into place and there's plenty of best practice advice available, most companies don't realize what it takes to deal with a data breach until they've been through one. That means that they may still be unprepared for the compliance issues of GDPR. "The GDPR advocates more sector-based initiatives and guidelines," she says, "but these haven't been produced yet, so it's hard for companies to understand what it all means."

The most common way for any criminal to access an organization's data illicitly is still via social engineering

GETTY

THE WEAKEST POINT

Despite increased awareness of security at the individual level, Clemente points out that the most common way for any criminal to access an organization's data illicitly is still via social engineering. "We're never going to get individuals to recognize every phishing email, and those emails are getting better too," he says.

Todd adds that the downside of more consumer awareness is that now there's a danger of "data fatigue". Since breaches are inevitable, a "why bother" attitude can sneak in despite efforts to keep the issue topical. Many banks now put unskippable warnings about recent phishing attacks on their homepage, which is good, but the risk is that they become part of the web's ignorable background noise, like end-user licensing agreements (EULAs) and cookie warnings.

While the jackpot for cybercriminals is still financial information like credit card details that can be used or sold on, "data manipulation" threats – in which information is changed, falsified or threatened – are on the rise and offer quick profits for crooks.

Deloitte's Clemente says that in 2013, when the Associated Press's Twitter account was breached by hacker group the Syrian Electronic Army, and a fake headline about an attack on the White House was published, stock markets dropped within seconds. While it's unlikely that attack was financially motivated, he points out: "Someone could have made serious money and I'm sure that won't have gone unnoticed."

The issue of data manipulation is likely to become a bigger problem than social engineering as more and more business processes automate and include data from devices connected to the Internet of Things. As well as phishing for Twitter credentials, today's data thieves are just as likely to be exploring ways to alter sensor data to their financial advantage. Jason Hart, Gemalto's Chief Technology Officer for Data Protection, gives the example of criminals who corrupt climate and agricultural data gathered by sensors in order to manipulate stock market prices. It could be months before such a breach is discovered, he says.

THE RISE OF RANSOMWARE

The threat that most agree is rising fastest, however, is that of "ransomware". Ransomware is a software infection that compromises a user's computer and threatens to delete or alter data unless money is paid. The extortionists typically target small companies which don't have the resources to fight an infection without risking their business, and demand amounts that are less than it would cost to send the experts in.

"Small companies are very unprepared," says Craig Rosewarne, MD of Wolfpack Information Risk. "Where it's moving is that the infection won't just be one or two machines, it'll be the whole network." With amounts demanded ranging from US$50 to US$1,000, Rosewarne says that many small companies will simply pay up.

Todd agrees that small companies are particularly vulnerable. "For a lot of smaller companies there's a real concern when they look at the high-profile breaches," she says, "If [large organizations like] TalkTalk and

> **"Most companies acknowledge that if they haven't been breached, they probably will be, or that they have been and just don't know"**
>
> **DAVE CLEMENTE, CYBERSECURITY TEAM, DELOITTE**

Yahoo! can lose customer data with all the resources at their disposal, it's very dispiriting [for smaller companies] when thinking about their own policies."

TAKING RESPONSIBILITY

Larger organizations are increasingly hiring dedicated Chief Information Security Officers (CISOs) to their board in order to have someone directly responsible for defending the firm against cybercrime, and using cloud providers can help too. As Dr Bernard Parsons, CEO of cybersecurity firm Becrypt, points out: "Even the minutest probability of a vulnerability in [larger organizations'] systems translates into a significant risk. At the scale that they operate, even something with a 0.001% chance of happening takes place every hour." For this reason, says Parsons, security budgets for firms like Google or Apple are larger than some countries' GDP, and they're very good at what they do.

But what about firms that don't have a national GDP-sized security budget, and are still struggling to understand the risks? "This is where the technical discussion comes into play," says Clemente. "We need extra security software and layers of defense to mitigate the threat."

The critical element of any security policy, however, is focusing attention in the right places. Companies need to have a realistic plan to deal with data breaches, says Todd. That means identifying the data they hold that is the most valuable and sensitive, and focusing their efforts on protecting and creating strategies to deal with mitigating breaches around that data, using encryption. That's not only a more effective way of dealing with future threats, it's cost-effective too. But the first step is for companies to acknowledge that they are the custodians of their data. "The practical problem if you have multiple providers," says Todd, "is keeping checks on who's doing what." As she points out, any company is only as secure as its weakest point.

Alongside that, replacing static passwords with stronger identity authentication systems, and encrypting data, will help to thwart the hackers. ■

The critical element of any security policy is focusing attention in the right places

RAISING AWARENESS

There are more opportunities for malicious hackers to attack and manipulate data than ever before. Even something as simple as an activity tracker could be a target if it's linked to medical records, for example. To try and raise awareness of the issues and potential damage, and how forensic investigators are fighting back, Gemalto has commissioned its own graphic novel, the *Cyber Investigator Chronicles*.

You can read it at **bit.ly/2gdJYP9**

DIGITAL BANKING BOOSTS INCLUSION AND CONVENIENCE

Around the world, digital banking technology is helping the unbanked gain access to financial services and making money management easier for millions of customers

AUTHOR EILA MADDEN

6

Six major European banks have signed an agreement to develop a cross-border trade finance platform for small and medium-sized enterprises across the continent, using blockchain technology.

Called the Digital Trade Chain (DTC), the platform will record, track and secure transactions by connecting all participants – including the buyer, the seller, their individual banks and logistics transporter – digitally via an online interface and mobile applications.

The banking consortium – which includes HSBC, Rabobank, Société Générale, Natixis, UniCredit and KBC – believes the DTC will help to make the trade finance process more transparent, more simple and more efficient by significantly reducing administrative duties, including paperwork, and speeding up the order-to-settlement process.

Source: tinyurl.com/DTC-platform

13,000

US bank Wells Fargo says it expects to be the first bank to fully upgrade its entire ATM network to allow customers to withdraw cash using just their mobile phones. All 13,000 ATMs are expected to be fully mobile-enabled by spring 2017.

Customers who want to use the service will need to first download the Wells Fargo mobile app. When withdrawing money, they'll need to log in to the app to request an eight-digit access code, which they should enter along with their card PIN to start the transaction.

Wells Fargo spokesperson Hilary O'Byrne said rolling this functionality out across its entire ATM network was a "game changer".

Source: tinyurl.com/wells-fargo-ATMs

GETTY

2017
Wells Fargo's ATMs should be fully mobile-enabled by this spring.

8

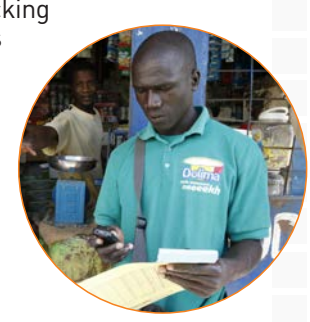
Senegal has become the first West African country to pilot a new digital currency on behalf of the West African Economic and Monetary Union.

The eCFA can be used across all existing payment platforms alongside the bloc's hard currency, the CFA. If the pilot is successful, the eCFA will be rolled out across all eight of the union's member states: Cote d'Ivoire, Burkina Faso, Benin, Togo, Mali, Niger, Guinea-Bissau and Senegal.

With the vast majority of the region's population lacking access to traditional banking infrastructure – such as a bank or ATM – the eCFA could help them leapfrog current barriers to financial inclusion.

The digital currency has been issued by the Banque Régionale de Marchés (BRM) in compliance with the digital money regulations issued by the bloc's central bank. The BRM teamed up with Ireland-based eCurrency Mint to produce the technology behind the eCFA.

Source: tinyurl.com/Africa-eCurrency



GETTY

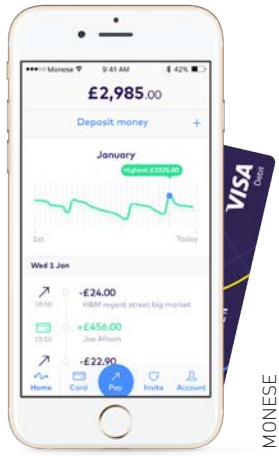
US$10m

Estonian entrepreneur Norris Koppel has raised US$10 million to help expand his London-based digital banking service, Monese, into mainland Europe.

The startup, which was named Best Challenger Bank at last year's European Fintech Awards, targets immigrants who struggle to open accounts with traditional high street banks. Koppel launched Monese in 2015 after first-hand experience of this.

The service promises instant account opening via a mobile app, a current account interface, cheap global payments and a contactless debit card. At the start of the year, Monese had attracted more than 40,000 customers from over 179 countries.

Source: tinyurl.com/Monese-Koppel



MONESE

40,000

The number of people banking with digital venture Monese at the start of this year.

51%

The Bank of Korea (BOK) has launched a series of pilot projects to take South Korea a step closer to becoming a coinless society. The projects will see retailers give shoppers change in the form of top-ups onto pre-paid cards, rather than as coins. The payments will be settled between the retailer and pre-paid card issuer after the transaction.

The pilots are part of the bank's Coinless Society Project, which aims to "ease the inconvenience of using and carrying coins".

The project follows a bank survey that revealed 47% of customers do not carry coins, even when they receive them as change. The main reason cited, by 62% of respondents, was the inconvenience of carrying them. More than half of the 2,500 shoppers surveyed (51%) supported the idea of a coinless society.

However, a BOK spokesperson said the bank does not aim to eliminate coins completely.

GETTY

Source: tinyurl.com/Korea-coins

GETTY

12

The State Bank of India has announced plans to launch its own digital bank. Customers will be able to access its services using their government-issued 12-digit identity number.

SBI Digi Bank is expected to start operating in the first half of 2017 and will be open to new and existing SBI customers. It will offer a range of products, including current and savings accounts, loans, insurance, investment products and personal financial management.

"We are working on a digital-only bank where no individual will be visible to the customer and all transactions will be done with the help of apps, internet banking and mobile banking," an SBI source said.

Source: tinyurl.com/SBI-Digi-Bank

AUTHOR ELLIOT WILSON

In developing and developed markets, technology is proving to be a force for good

REAPING DIGITAL DIVIDENDS

ISTOCK

We are in the midst of the greatest information and communications revolutions in human history. Basic technology has become more affordable and available, even in the most deprived of countries. A 2016 World Bank report, *Digital Dividends*, found that the world's poorest households were more likely to own mobile phones than to have access to toilets or clean water.

But access to technology is not enough. It is what is done with it – how it is corralled by individuals, corporates and governments alike – that truly matters.

Leaders and followers are emerging. In the developed world, Estonia has emerged as a digital pioneer. It became the first nation to launch an encrypted, digital ID card that contains residents' medical information, and allows them to verify and sign documents, pay taxes, pay for goods and services and carry out complex financial transactions, online and from anywhere in the world (visit bit.ly/2kESDxw for more on Estonia's eGovernment revolution).

EMERGING LEADERS

In the emerging world, India is making the switch from follower to leader. Fishermen in the southern state of Kerala saw the benefits of mobile telephony early, using their cellphones to find new buyers, boost profits, and reduce waste. In Bihar, an NGO called Digital Green is issuing tablets to farmers in areas lacking electricity or surfaced roads. Each one contains pre-recorded how-to videos that help farmers rotate in profitable crops and boost yield.

At a macro level, of the world's 196 countries, 192 are building digital ID databases. Each is different. In Britain, the UK Verify scheme, designed to give people a single, consistent way to prove their identity when accessing state services online, has been outsourced

For more on reaping digital dividends, visit Gemalto.com at **bit.ly/2knUuXl**

> This is a big deal. National databases allow governments to channel better services to citizens, and for people to be able to prove who they are"
>
> **UWE DEICHMANN, LEAD CO-AUTHOR, *DIGITAL DIVIDENDS***

to the private sector. Azerbaijan's decision to digitally register every newborn stems from a desire to create a comprehensive national health database. Across the emerging world, the World Bank's Identification for Development (ID4D) initiative, launched in 2014, aims to present 1.5 billion people with an official, legal, government-mandated ID by 2030.

A BIG DEAL

"This is a big deal," says Uwe Deichmann, lead co-author of the *Digital Dividends* report. "National databases allow governments to channel better services to citizens, and for people to be able to prove who they are, to register to vote, and to build up their creditworthiness and medical history." That in turn helps poor citizens in any country to benefit from digital technologies, even when they don't own a mobile phone or a computer.

Governments are working with digital security providers to build secure, trusted vaults that contain citizens' medical, financial, and educational data, for example, and which can be accessed via the cloud (and by the right people) anywhere in the world. When individuals have a digital ID card, they can see what a sovereign authority knows about them, and who has been reading their information.

The integration of new, cost-efficient technologies, many of which were inconceivable just a few years ago, is accelerating development in the emerging world, and transforming the worlds of business, work, and service delivery. Estonia, now one of the world's most digitally interconnected countries, has an economy that is the 40th largest by purchasing power. Public sectors are benefiting too. National ID schemes, for example, can help to save money. Consider Nigeria's e-ID scheme, which revealed the (non-) existence of 62,000 "ghost" workers, saving the state US$1 billion in annual social security costs.

LOCAL BENEFITS

But digital dividends can often be seen more clearly at a local level. M-pesa, a mobile payment system launched in 2007 in Kenya, has since been replicated across sub-Saharan Africa, slashing the cost of sending remittances and paying for goods and services. The for-profit Bridge International Academies, focused on emerging African and Asian nations, create tablet-based education programs that cut the cost of teacher training and improve pupils' exam performance.

New technology is not a cast-iron guarantee of a better world for all. Fears of national databases being hacked by criminals are all too real – though anti-hacking and encryption technology is becoming better and cheaper every year. Workers fear the downsizing effects of automation and clever machines, while higher cellphone and broadband penetration has not led to an attendant rise in the quality of digital government services. "New technology is great, but we also need to work on complementary factors," notes Deichmann. "Employees need to develop new skill sets, while also holding government to account, to ensure that technology pays digital dividends to everyone." ■

Fishermen in India saw the benefits of mobile telephony early, using cellphones to find new buyers and boost profits

ISTOCK

AUTHOR ELLIOT WILSON
ILLUSTRATION RHUBARB RHUBARB

For the latest technology news, check out the Gemalto blog at **blog.gemalto.com**

The 'Industrial Internet' – the seamless integration of a host of technological innovations – is helping companies like Tesla and Apple redefine their sectors

Industry 4.0 will change everything

The telephone acquainted us with direct two-way communication, and the internet with the concept of global interconnectivity. We are now entering a new digital era – called "Industry 4.0" by some and the "Industrial Internet" by others – that will involve the seamless commercial integration of a host of innovations, the names of which are still alien to many CEOs, let alone the working public.

Cyber-physical systems, augmented reality, 3D printing, enhanced automation, connected fabrication, advanced robotics and analytics, artificial intelligence, and the encroachment into our lives of Big Data and the Internet of Things. When slotted together, these transformative ideas – and others yet to be invented – will revolutionize everything from how goods and services are designed, built and delivered to the end-user, to the way we interact with each other at work.

TWO BROAD BENEFITS

No company will be able to avoid the revolution – nor will they want to. Industry 4.0 will deliver two broad benefits – efficiency gains and cost savings – essential to any profitable and high-functioning company. A digitally integrated workplace will help corporates track and trace products, dream up fresh ideas, stray into new industries and product formats, and find new clients. "It's a virtuous circle," says Björn Johansson, Director at Strategy&, PwC's strategy consulting arm. "Pull the digital lever and everything you do improves exponentially."

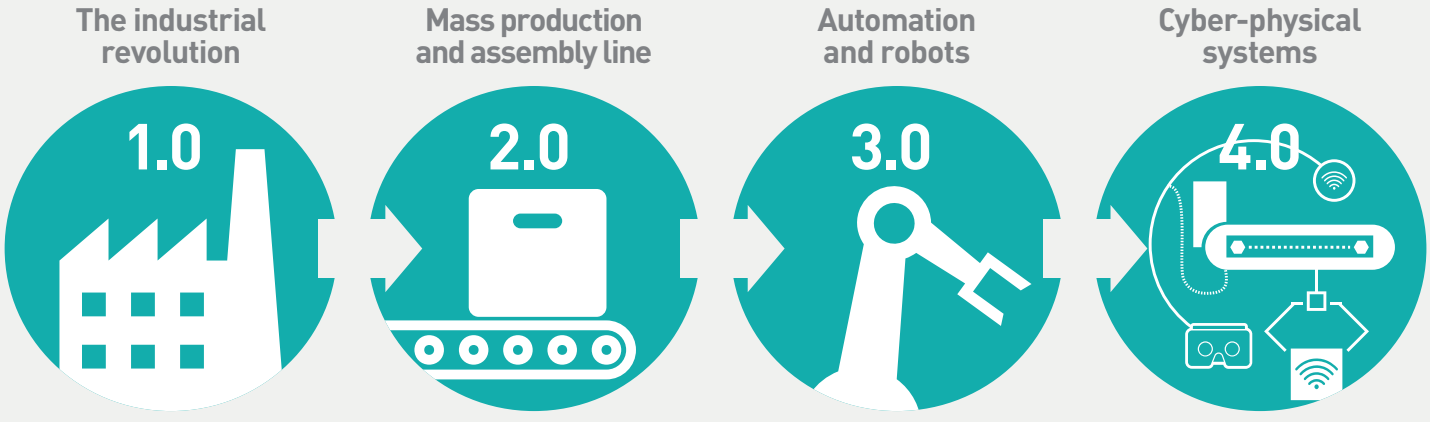
Early adopters stand to benefit most. Take the examples of Tesla and Apple, two US firms that have respectively upended and redefined the world of automobiles and smartphones. Tesla's internal connectivity is well known: its assembly-line robots are "trained" to spot the smallest failure in an engine or electric battery and deliver that data instantly, boosting yield and cutting downtime. Tesla requires its suppliers to provide real-time updates, forcing them to install new technology and processes. Corporates that fail to invest will fall behind.

A SHIFT IN MINDSET

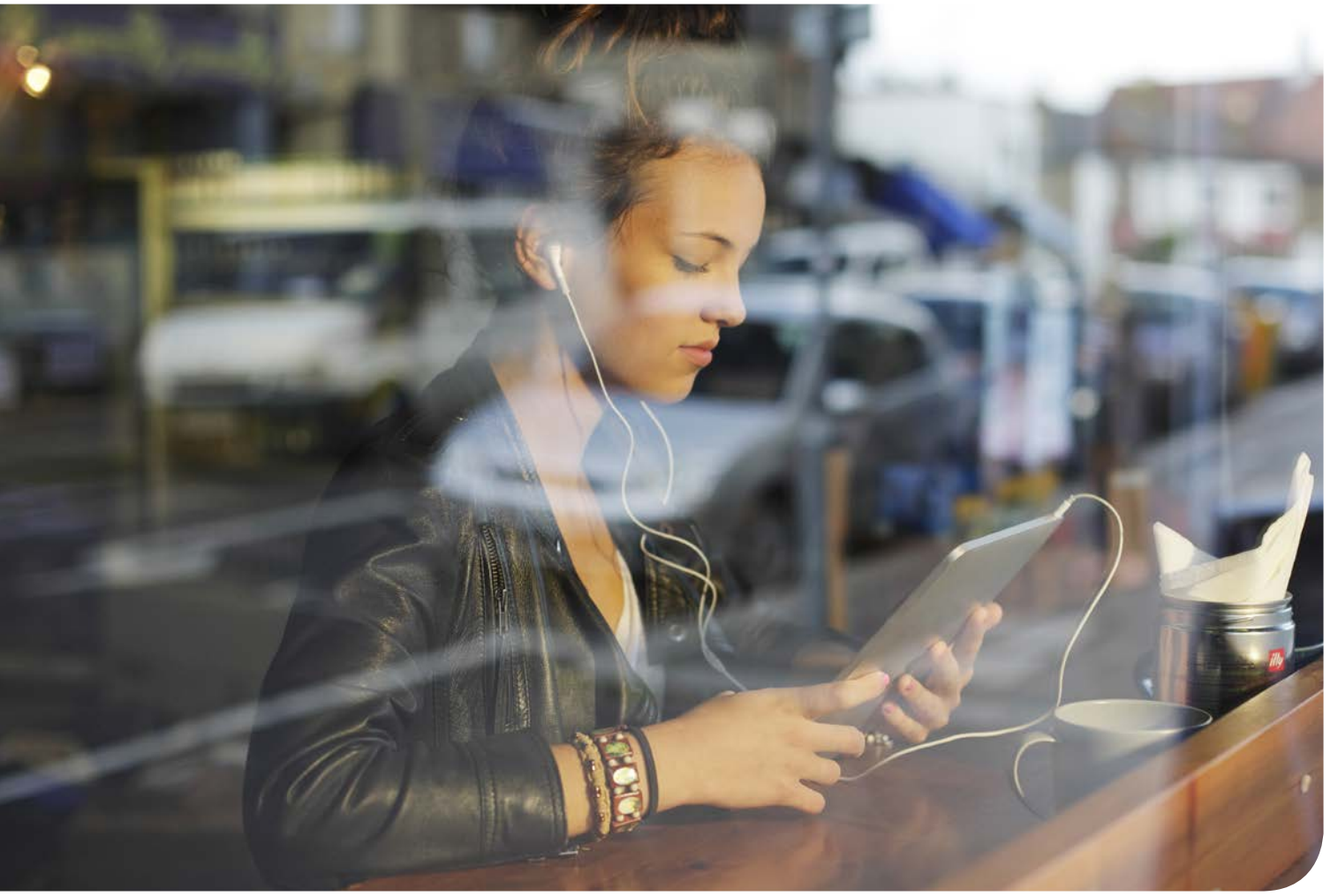
Industry 4.0 will change everything. That's both the good and the bad news. Employees will need to change how they work and think, a radical mindset shift that may be hard for some to accept. Managers and CEOs will have to spend more to bring in the right talent. Middleman-industries that can be entirely digitally operated – the car-rental world for instance – may disappear altogether.

On the plus side of the ledger, the cost of installing new technology is falling as it develops. And those who do invest wisely stand to capitalize. Companies that invest in smart supply chains and interact better with clients will, says PwC's Johansson, "grow faster, leapfrogging peers and becoming profitable disrupters. You don't need to do everything at once. Pick your battles and ask customers what they need. If you're already good, Industry 4.0 will make you better." ■

INDUSTRIAL EVOLUTION



OUT NOW!! READ GEMALTO'S CYBER INVESTIGATOR CHRONICLES



Are you reading */review*?

/review is the online home of *The Review* – and much more besides. The site is regularly updated with exclusive content, infographics and video, as well as extended web versions of stories from the magazine.

For must-share stories and powerful insights from the digital world, */review* should be a regular destination. The site is optimized for smartphones and tablets, so you can access our content wherever you are.

gemalto.com/review

View on all devices

GEMALTO.COM

IN AN INCREASINGLY CONNECTED SOCIETY, GEMALTO IS THE LEADER IN MAKING DIGITAL INTERACTIONS SECURE AND EASY. LEARN MORE AT GEMALTO.COM

gemalto
security to be free