As the public and businesses continue to embrace new security technologies, **John Davies** and **Mike Sussman** predict 2014 will be a year of rapid integration and evolution in the access control market

THE FUTURE O CONTROL

©Yale Locks and Hardware

F ACCESS

2013 saw a big rise in integrated systems in the security sector, and 2014 looks set to follow this pattern with a number of new technologies and trends coming to the fore. The last few years have seen a huge shift in the integration of security, with terms such as PSIM becoming an everyday part of the security specialist's lexicon. But the pace of change is becoming more subtle at the moment, although no less exciting overall. With a range of different security, IT and buildings services coming together, 2014 looks set to be a year of evolution rather than revolution – which from a business point of view ideally places the industry in a strong position to maintain growth.

Customers and installers have become much clearer on the types of security solution they want to use, with the desire to find the right price evenly matched by the need to find systems that offer the best value for money and provide ongoing service and the ability to evolve and upgrade. Technologies and ideas that are fresh but can prove themselves to be cost effective and highly effective have become the real holy grail for security providers. So the list of trends for 2014 might not always be earth-shattering, but many are quietly changing the face of the security industry and look set to become the norm in the not-too-distant future.

One technology that has been promising to do big things for some time is Near Field Communications (NFC). While the technology has been available for some time, NFC's success will be determined by the tipping point from the number of enabled mobile devices and the public's willingness to use them to gain access to secure doorways. The use of NFC has also been spurred on by a number of new compatible stand-alone locks which are especially well suited to access control using a smart device.

At the moment NFC is more popular in the consumer market. For example, residential landlords can send a key to the smartphone of a tenant which can then be activated or revoked as necessary (without the inconveniences of having to immediately issue traditional metal keys). History has shown us that public acceptance of a technology will push its adoption in the commercial market too, as experience of the technology and trust in its ability is cemented. NFC offers exciting possibilities for securing access, and the signs are that the market is poised to increase adoption very soon.

The adoption of cloud-based security is another area that has gained enormous ground in recent years and looks set to continue vehemently in 2014. It's fair to say there were concerns over the security of using the cloud, voiced by some commentators and potential users when cloud-based access control was first muted. These were largely quashed by a wider acceptance of online use of services such as banking or retail, however, which have demonstrated that using IP needn't compromise vital security.

In fact, there are actually security benefits, in that the core systems are physically stored away from premises and can't be directly influenced by intruders in the building. As well as ease of use and installation, cloud-based services also rapidly roll out updates (which is particularly useful in an emergency situation) and there is no need to store large servers onsite (which could be attacked or hacked directly) – freeing space and resources. Additionally, scalability is potentially almost limitless and data can be accessed by authorised mobile users at any time.

The momentum of security integration is unlikely to slow in 2014 – in fact it will continue to be a key market driver moving forward. The benefits are unquestionable, with the drive for efficiency savings being the core proposition. Integration enhances security reaction times – for instance, if a door is forced the combined system will sound an alarm, lock-down key areas and direct the security team to the location of the potential incursion. Integration makes installation and upgrades easier and more cost-effective, and it makes full use of legacy and existing systems. There is a massive growth in the use of BACnet protocols as well, which are adding a new level of software integration which is helping to move away from the remaining proprietary software that was once commonplace in the security industry.

There has been some debate within the security industry lately about the effectiveness and convenience of using passwords (both for physical protection of premises and logical access to IT systems). Integrated security systems allow authorised users to minimise the security details they have to memorise, and are likely to gain further interest this year because of this advantage. The ability of integrated systems to intelligently provide access also means workforce management is much easier. From managing working hours to activating buildings services only when they are needed (and thus saving energy and resources), integration is providing intelligent solutions that will save real money in 2014.

The increase in mobile working and the use of smart devices will also continue to steer security demands, offering convenient and secure access to integrated systems. But mobile devices, by their highly portable nature, also pose a potential risk of unauthorised misuse. Accordingly though, mobile device manufacturers have beefed up handset security and this has offset many of the potential concerns – in some ways echoing developments in the security industry itself. Long promoted as convenient and highly secure, biometrics recently got further mainstream consumer adoption with inclusion of fingerprint readers on iPhones late last year.

This use of biometrics has wider repercussions too. As with mobile devices, experience shows that consumer adoption helps to facilitate business use, so I would expect biometrics to find even greater popularity in 2014. The quality and accuracy of biometrics have rapidly improved in recent years, moving on from

fingerprint readers and now readily incorporating facial recognition (which is very well suited to "clean" areas) and moving towards previously niche and more complicated systems such as palm vein and heartbeat recognition readers.

Like fingerprints or the shape of the human face, heartbeat recognition readers use the electromagnetic signature of the human heart which is unique and offers an ideal way to prove identity. Rather than having to present biometric data at an access point, for example, systems could be attached to the body, automatically sending approval to entry doors and allowing authorised individuals to freely move between unrestricted and restricted areas with a minimum of fuss. Good access control systems have always been as much about making life easier for authorised individuals as they have for guarding against unauthorised intruders – something which is central to the more towards biometric systems.

There is also a continuing move towards PoE, which makes installation easier, quicker and neater – benefiting end users and installers alike by saving costs. This theme is continued with a growing move towards wireless systems. In the past there had been some reservations about using wireless systems with regards to security. The perception by some is that there is a greater risk of systems being hijacked, but as the ubiquitous use of Wi-Fi has shown that, properly protected and configured, systems can happily use encrypted wireless signals, making installation much easier and actually removing the physical vulnerability of running wires around the facility which could be intercepted manually. There is also a growing emergence of hybrid WiFi/wired systems which minimise wireless deadspots but continue to offer the benefits wherever possible.

Energy saving continues to be a welcome added bonus to integrated access control systems, which talks directly to other security and buildings services systems. Having more automated control over the use of resources such as lighting and heating is obviously more cost effective, but there has also been a distinct move recently towards installing access control systems with switch mode power supplies, also saving money on the running costs of the control systems themselves.

Switched-mode power supplies are likely to continue gaining in popularity. Such supplies can offer sizable saving in energy consumption by incorporating a switching regulator in order to be highly efficient in the conversion of electrical power. Unlike a more traditional linear power supply, the pass transistor of a switching mode supply continually switches between low-dissipation full-on and full-off states and spends very little time in the high dissipation transitions (which minimises wasted energy).

As well as the technology, legislation is moving forward to meet the demands of the security industry. In 2014 we will see the publication of IEC 60839, entitled, "Alarm and electronic security systems Electronic access control systems. System and components requirements" – which aims to update the standard to take into account the latest integrated systems. It is being published at the IEC level (World standard) and also published by BSI as a EN (European) standard. As with all new standards, IEC 60839 will have a profound impact on the security industry in 2014 – pushing providers further towards modern integrated systems and ensuring that they adhere to the developing needs of all customers that rely upon them.

©iStock

Widespread use of cloud computing has reassured businesses that the technology is secure

John Davies is Managing Director at TDSI. A graduate in Chemistry from the University of London, John joined TDSi in 2003 and led the management buyout in February 2005. John is active with the British Security Industry Association, having been Chairman of the Export Council, and is also an industry representative on the Security Sector Advisory Group for UKTI DSO.

Mike Sussman is Engineering and Operations Director at TDSi. Mike joined TDSi in 2004, since when he has been responsible for product development and bringing new access control products to market. As Chairman of the BSIA's Access Control Committee and with over 25 years' industry experience, Mike works closely with the association in promoting access control standards for the industry.