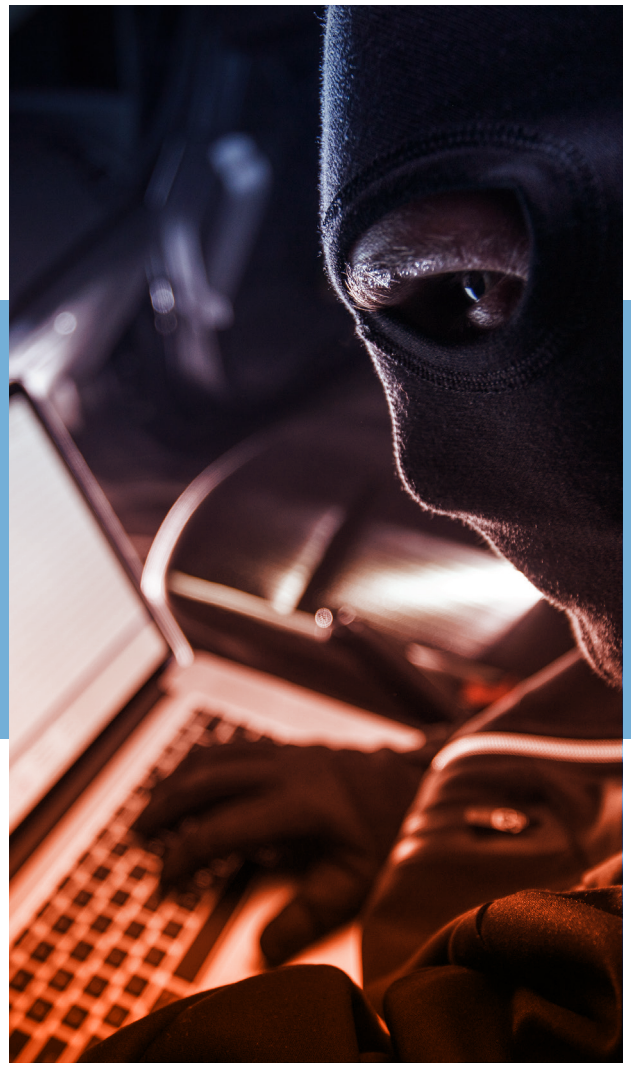
IFSEC INTERNATIONAL

Security sector insights in the age of terror and the cyber-attack

A review of the seminar theatres at IFSEC International 2017.

IFSEC
INTERNATIONAL



Contents

Foreword

Adam Bannister
Content Editior
Ifsec Global

There's more to visiting IFSEC International than seeing the latest cutting-edge innovations in video surveillance, access control and intrusion detection – central though this is to the experience, along with networking and meeting customers or suppliers.

IFSEC is also about education. Across several seminar theatres the London-based event features presentations from respected industry experts on regulatory updates, certification and standards, strategic security advice and how to procure, deploy and maintain security solutions. From installers and integrators to consultants, vendors and, of course, the heads of security and security personnel who protect people and assets. We aim to provide up to date, relevant live content to the entire supply chain.

It's fascinating how the dominant topics and themes have changed in the decades since IFSEC first launched. In recent years we've seen the rise of convergence, PSIM, video analytics and the (ongoing) migration to IP, among others. Dominant buzzwords now include integration, the internet of things and machine learning.

But twin threats loom over the security landscape: hacking and terrorism – potentially in combination. Mindful of the zeitgeist, IFSEC 2017 launched Borders & Infrastructure Expo, reflecting the growing importance of border security and protecting critical national infrastructure.

This round-up of articles, which distil several presentations from the event to their key tips and messages, focuses on counter-terror and cybersecurity – especially in regard to physical security systems – as well as drones, access control trends and CCTV procurement. ■

Calls for greater collaboration as security industry faces "blended threat"

> **Ninety percent of breaches are due to people's mistakes, poor configuration and maintenance**

Recent cybersecurity threats underscore the need for physical and information security teams to work more closely together.

"The threat is blended so the teams need to work together," said Ellie Hurst, Marcomm and Media Manager for Advent IM at IFSEC International. Hurst cited numerous attacks where hackers exploited vulnerabilities found in physical systems.

For example, in December, two individuals hacked into the Washington DC CCTV camera network days before Donald Trump's inauguration. Meanwhile in October, Hangzhou Xionmai Technology, a vendor behind DVRs and internet-connected cameras, inadvertently played a role in wide-scale DDOS attacks against PayPal, Twitter, Spotify and other platforms.

While physical and information security professionals typically work in different departments, they need to find a common language, said Hurst. "Do you know what you have? Do you know what they are built on? What is the life-cycle management of these products and are they patched? From there you can decide whether to accept the risk."

Though rare, some organisations have merged the physical and information security teams, said James Willison, Founder of Unified Security Ltd.

"Symantec has merged their team and Barclays is building one SOC for both cyber and physical security."

All is not lost if your organisation is behind. There are measures every company can take to mitigate the risk, said the presenters at IFSEC.

"Ninety percent of breaches are due to people's mistakes, poor configuration and maintenance," said Steven Kenny, Business development manager for the architecture & engineering (A&E) programme at Axis Communications. "Creating a documented internal policy and increasing employee awareness is important."

Added Hurst: "Training and education is also important. You need to find a training course suitable for those in physical security. At the end of the day, the threat isn't going to go away. You've got to do the training." ■

Businesses have been hacked whether they realise it or not, expert warns

> The most important consideration is an "outstanding" security policy

There are two types of businesses – those who know they've been hacked and those who don't know they've hacked – a leading security expert has said. Stuart Rawling, director of business development at Pelco Schneider Electric, made the stark warning at the event's opening panel 'Current trends and future of the industry'.

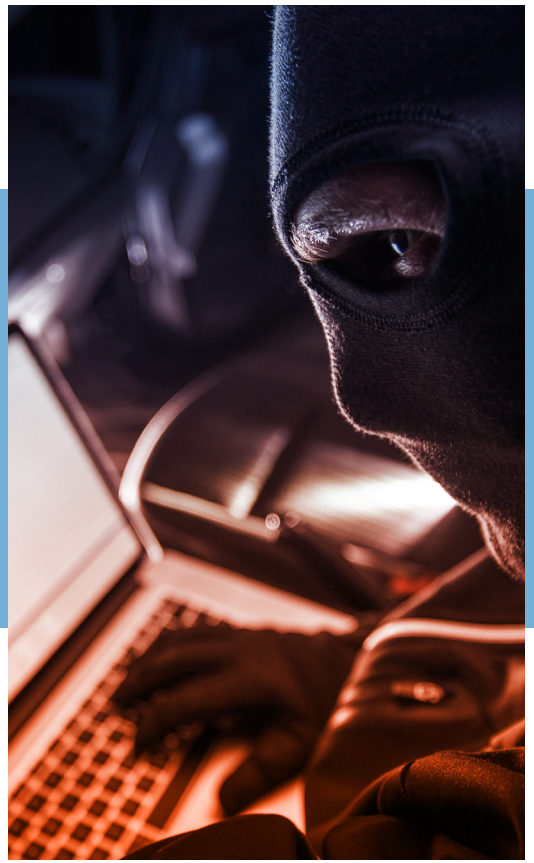
Rawling said businesses must have a solid security plan in place which brings together both human and cyber elements. "There is a risk of getting an antivirus solution and hoping that will solve everything," he said. "An antivirus won't help you against a zero-day attack – by its very definition it's unknown."

The theme that rapidly-advancing security technology cannot be expected to tackle threats without a human element and robust planning was a key element of the session. Professor Martin Gill of Perpetuity Research warned that "leaving it to technology and hoping it will all be OK" is a dangerous path for the industry. "We should be holding on to the human element. I speak to a lot of offenders, and one said to me recently: 'Technology doesn't jump off a wall and arrest you.' I just interviewed 12 heads of retail and 12 loss prevention directors. And when asked what their best security system is, they all agree: their staff."

Rawling agreed, saying he "doesn't see a day coming soon" where a physical security guard is not deployed. "Ultimately there still needs to be a human decision made on what to do," he said. "A response plan still requires a human response. What do you do when something happens? That's where security fails most often – the operating procedure, not the technology."

Fellow panellist Tony Weeks, head of technical services at the NSI, said that technology cannot be implemented without human expertise. "No matter how advanced the technology, you will still need people to configure and look after the systems," he said.

The most important consideration is an "outstanding" security policy which addresses all aspects, the panel agreed. "When I speak to offenders about why they chose their target the answer is always the same: because it was easy," said Gill. "That hasn't changed over 30 years." ■



Cyber awareness is everyone's job

> **People in facilities aren't expected to understand cybersecurity**

Cyber awareness is everyone's job and only through real collaboration can organisations protect themselves from attack. This was the message from Mike Gillespie, managing director and co-founder of Advent IM, on day three of the show.

Gillespie argued that the current thinking is that cyber is an IT function. "I work in facilities and I don't do cyber. He often hears people say it's IT's problem and it has nothing to do with me," he said. "But cyber is so pervasive and interconnected, we can't get away from it. Cyber is everyone's responsibility. You need to know about it and talk intelligently about it. Cyber is going to affect every one of you."

Today the biggest disconnect is communication and collaboration. "We don't have people talking to each other with a common language," Gillespie continued.

One of the biggest problems is security practitioners are not well-versed in speaking the language of business. "Have you sent data to the board or have you sent them something that offers insight and is actionable? If you don't send insight, don't expect them to engage."

As threats become more complex, physical security practitioners need to collaborate within their organisation and among peer groups. In particular, Gillespie told the audience they need to be familiar with things such as the national surveillance camera strategy. "If you have anything to do with surveillance systems, you need to be pulled into this strategy to get ahead of it."

Attendees also need to source new skills and understand the cybersecurity landscape. "Cybersecurity is not a separate discipline and is integral to business and building systems," said Gillespie.

Last, he implored the industry to ensure that their hardware was secure and up to the latest standards. "How much of your security kits goes through penetration testing? Is your firmware being updated to protect against hacks? Are you choosing poor passwords that are hard-coded and cannot be changed? We need to understand the whole of the ecosystem in which the systems sits. If we don't know this, then we can't protect properly. The threat is not going to go away. You really need to get on board." ■

How the GDPR will affect physical access systems

With the GDPR (General Data Protection Regulation) set to go into effect in May 2018, security professionals must have a plan in place for all data stored on physical access systems.

"Most IT departments are forgetting about the access control database because it is owned by security," said Andrew Bull, director of sales for UK&I, Quantum Secure, at IFSEC.

But this could be an expensive mistake as GDPR promises severe penalties for non-compliance. "GDPR has put teeth in the data protection act and, for once, a regulation could hurt if a company doesn't pay attention," said Bull.

Bull outlined some considerations to prepare for the regulation.

Consent: An organisation should have a specific statement in which an employee gives their consent about the data being held in the physical access system database. "This should not be presumed consent," said Bull.

Policy: An organisation needs to define the purpose of keeping data. If an employee leaves a company, when do you delete their information? Is there a legitimate reason to keep the data?

Process assurance: An organisation needs to define who has access to the database and also be able to track where the data is stored. Article 33 of the GDPR says a company needs to report a personal data breach within 72 hours of the breach and report who is affected.

Contractors and visitors: There needs to be a policy and consent form for contractors and visitors. "We rarely ask for consent for visitors but organisations should add a check-in box so a visitor understands their data is being stored on the database and a clear statement about what is being done with the data," Bull said.

Once a policy is set, processes need to be put in place to ensure the policy is executed. Typically, there are gaps between policy and process, said Bull. "My policy says that I store data for two years after an employee leaves the organisation. But how do I track when the two years has expired and delete the personal data the database? Does this apply to everyone? Are your policy and procedures role-based?"

Last, talk to your legal team. The legislation is not written with access control in mind and reading the documents can be tedious, said Bull. Get your legal team involved to help plan for the regulation. ■

How Cisco is using analytics to build better, smarter cities

Ninety percent of all data has been generated within the last two years. With 500 million tweets per day and six billion google searches daily, it's easy to see why.

But these numbers are actually small when you compare them to what lies ahead. Today there are 14.9 billion devices connected to the internet. By 2025 there will be 82 billion, according to market researcher IDC. The task at hand is how to take this data and turn it into insight to benefit communities and the cities of the future.

At IFSEC 2017, Stu Higgins, head of smart cities and IoT for Cisco, outlined a number projects the company is working on to do just that.

At Place de La Nation, Paris is using sensor technology to monitor people, traffic flow, waste management, temperature and air quality, among other things. Cisco is working with town planners on how to make changes to improve traffic. They are also developing other use cases for the data they are collecting.

Glasgow is looking at analytics to improve environmental processes. Currently if a flood occurs, only a police officer can confirm it – usually for hours later. If a citizen could record the flood with their mobile phone and share the video with the government, the amount of time to report the flood is reduced, potentially saving $5bn pounds a year, said Higgins.

A project called City Verve in Manchester is looking to technology to focus on health and care, transport and travel, energy and the environment and the community and public realm. Using a $10m grant, involving 21 technology partners, the project is testing everything from smart parking to smart lighting to a talkative bus stop which encourages people to walk to another stop to get exercise and then get on the bus for free.

Meanwhile in Swindon, the C-ITS Project is taking real-time video and using analytics to spot congestion. Funded by the Department of Transportation, project managers are considering ways to integrate the data with an in-vehicle app. They could also share the data with logistics companies in order to avoid traffic jams.

Last, Project Swift is looking to create a 200-300MB permanent connection on their train from Glasgow to Edinburgh. A real-time, always-connected system has a variety of applications.

Higgins told the audience: "The key is how you pick the bits that are important and spot patterns in that data." ■

The 6 most common cybersecurity mistakes companies make

> **Many think legacy equipment cannot be hacked. This is false**

Cybersecurity risk is one of the preeminent threats organisations face today and the National Cybersecurity Centre (NCSC) is hoping to help, based on insight from 800 incident reports they collected in the past nine months.

John Noble, CBE's director of incident management, told IFSEC attendees about some common mistakes companies make when it comes to cybersecurity.

1. **Companies ignore the basics.** They have outdated anti-virus signatures and patching programmes. What's more, companies do not lock down their system administrators accounts.

2. While companies need to consider the trade-offs of running a business and being secure, many organisations go too far and **ignore the advice of security professionals.** Companies need to take into account the reputational impact of a breach.

3. Because systems today are so complex, companies **misunderstand where the real risks are**. Companies must determine what data is most important in an organisation and put security controls against that data.

4. **Legacy equipment is ignored**. Many think legacy equipment cannot be hacked. This is false. Legacy systems must be patched.

5. **Outsourcing can be source of weakness and risk**. Companies need to ask third-parties about their security controls and carefully look at their contracts and how these third-parties secure their systems.

6. When a company acquires another company, often they **bolt on the acquired network to their network**. By doing so, a company is opening its network to risk.

NCSC's mission is to make the UK the safest place to live and do work online. To achieve this objective, NCSC provides advice to government, individuals and companies about cybersecurity. Part of the GCHQ, the organisation offers confidential advice to companies breached and coordination with other parts of the government in the case of an incident. ■

Community engagement vital to prevent "ripple effect" of terrorism

> "We're seeing the balance between organisational response and the response of the ordinary citizen"

Recent terror attacks show that governments must ensure adequate communication to – and between – communities to protect them against increasingly-sophisticated terror attacks, experts said in the Security Management Theatre.

Speaking in a panel debate, Stephen Mackenzie, director of Mackenzie risk management, said the "whole philosophy has moved" on counter-terrorism following attacks in Manchester and London. "We're trying to make our counter-terrorism strategy much more public and transparent to engage the community. We're seeing the balance between organisational response and the response of the ordinary citizen. With the rise in recent terrorist events we're working to get better information out into the public domain – but we're playing catch-up."

His view was backed by the Canadian perspective of Bonnie Butlin, co-founder and executive director at the Security Partner's Forum. Preparing for the 150th anniversary of Canada has "highlighted the importance of counter-terrorism in a new way," said Butlin. "We're seeing trends for sectors of the economy to start working together like never before. Typically reputational risks are so high that they are a powerful disincentive to sharing information, but if then one business gets hit, it might ripple all the way through for lack of sharing."

Butlin also noted that the lines between physical and cybersecurity are becoming increasingly blurred. "We have discovered a number of IMSI devices, or fake cell towers, which will absorb the calls to emergency services and prevent them responding," she said. "But we don't know who is responsible."

However Dato' Amar Singh Ishar Singh, Kuala Lumpur police chief, Royal Malaysia Police, believes an even more robust policy than community engagement is required. Singh, who deals with the growing terrorist threat in Colombo, said police "must be much more aggressive, rather than waiting for terrorists to come to us".

"You can have all the defensive strategy you want, being ready to respond with the army and police. But we need to be aggressive – we target possible terrorists groups online and in Kuala Lumpur alone we have made more than 300 arrests." ■

Video Analytics: "Oversold and underutilised" – but key to preventing terror attacks

> **Video analytics raises "far too many false alarms, it's not really performing"**

Atul Rajput of Axis Communications, Stephen Jones of Seagate, Jonathan Rickard of Panasonic, and Andy Coles of Hikvision took part in a lively debate about the trends shaping video surveillance.

Video analytics raises "far too many false alarms, it's not really performing," said Jonathan Rickard. "But that is going to change as machine learning and processing power in cameras is increasing. Video analytics can already identify unusual behaviour – like someone in a crowd who is drunk or walking in an usual way."

Analytics can take away the current expectation that a single security guard can monitor 150 cameras, said Rickard. "A guard can see one or two cameras maximum. Even if you give them a screen with 50 cameras, they won't be able to do it. Machine learning is needed to monitor all cameras and then present anything usual to the security guard."

Andy Coles pointed out that artificial intelligence is already built into many surveillance products. "Until now analytics have been used to review an incident after it happens. Imagine intelligent analytics that can interrogate behaviour before it happens. That's where security is going. Deep learning will make a big impact in the years ahead."

Stephen Jones said: "Forensic searches for video analytics are good, but we need to now react in real time. It takes a lot of processing power and technology."

In many incidents, such as the recent Manchester Arena bombing, terrorists conduct a reconnaissance before the bombing. How could video analytics have prevented these attacks, asked an audience member? "If I know a suspect was on a terror list and you could get your VMS platform suppliers for government and businesses joined up, yes, you could spot that," said Andy Coles. "The technology is there, but as everyone is using disparate systems, you can't do anything like that."

In connecting systems, "simplicity is key", Atul Rajput added. "The more complicated systems are, the more mistakes that can be made on installation." ■

Aviation laptop ban: The threat is real and requires new response

The proposed ban on all electronic items larger than smartphones is required because "the threat is real". That's the view of Ian Hutcheson OBE, security advisor at airport security giant L3.

Hutcheson said these complex IED,s which can be disguised as such devices, require more advanced technology than is currently available, also revealing that L3 is currently working on new computed tomography machines to tackle the threats.
However, he also claimed that simply detecting threats is not enough for the role of technology. He said: "It is much easier to measure detection capability than deterrents, but mitigating future risks will require technologies that both deter and detect. Despite this, technology can produce real deterrent value such as PWM scanners at Heathrow. Many people discarded drugs and other contraband because they didn't understand the capabilities of the scanner."

Hutcheson also noted the potentially negative impact that increased response to threats could have to the global aviation industry's core business: getting passengers from origin to destination. "How do we improve security while keeping business moving? That is it we need to find out." ■

We're making life too easy for terrorists: former IATA chief

Governments around the world are "making life too easy" for terrorists, the former head of security for airline body IATA has said.

Speaking at a panel on border security, John Hedley said current regulations are making conditions more difficult for passengers – but not criminals. "There is no international database for list or stolen passports," he said. "Governments don't share that data, so if you have a stolen passport you can use it in any country except your own. Sadly terrorists don't conform to the niceties of data protection. Governments have a list of people on a watchlist. But they do not have the resources to watch them. But if you knew they were travelling you could prioritise them – it would make life difficult for the bad guy.

"But governments won't share the data. It's not rocket science; the technology is there but the political will is not."

Fellow panellist Ian Hutcheson OBE, a former police officer and current security advisor at L3, agreed that the current procedures must be improved. "The appetite for risk in government has diminished rapidly," he said. "Following 9/11 the EU implemented competency for aviation security for its member states, but it allows individual member states to put more stringent measures in place. The UK, being the UK, has more stringent measures than anyone else.

"100% of the passengers are subjected to 100% of the security measures. Probably 99% of them pose no risk whatsoever. We could use data to assess risk – we've suggested to governments that they use risk-based systems."

Although conceding that the issue was highly contentious, Ellie Hurst, marketing manager of Advent IM, queried the "dichotomy" in data usage. "Why is it fine for people to buy an app which knows everything about you, but it's not fine for governments to profile for security?"

Hurst also stated her belief that "there is a great marriage which is needed between cybersecurity and the physical world". The attacks in Lodz, Poland, where a teenager was able to hack the automated tram system causing injuries, is evidence of this, she said. "This was a cyber-attack that caused real physical harm. But it was facilitated by poor physical security – the hacker was able to gain access to the system at a place which should have been secured. There has never been a better time for us all to work together." ■

"It's not rocket science; the technology is there but the political will is not "

Police and security drone use on the rise

> **"The commercial drone industry is growing rapidly but effective regulation is essential"**

A rising number of police forces and security services in the UK are using drones and the figure is set to increase further, according to the managing director of a CAA-approved UAV training provider.

Sion Roberts, the boss of RUSTA and Eagle Eye Innovations, said he started working with officers in Surrey and Sussex in late 2015 and demand for training has steadily grown. "We first trained about 40 officers from Surrey and Sussex to use small unmanned aircraft in their day-to-day policing roles," he said. "Since then we've trained elements of the Metropolitan Police, forensics in Northern Ireland and parts of the Ministry of Defence."

Surrey and Sussex Police initially trained 38 members of staff and in 2016 secured £250,000 to expand its fleet of drones from one to five. In addition to police and emergency services, the use of UAVs is becoming widespread by the film and TV sector, farming and agriculture, surveyors, and search and rescue teams.

However, pilots operating drones commercially in the UK must obtain permission from the CAA. Roberts, who spent 22 years in the RAF, stressed that the commercial drone industry is growing rapidly but effective regulation is essential. "The only way the industry is going to grow is to keep it safe," he said. "Regulation has to carry on evolving. If a drone causes an incident, this fledgling industry could come to a grinding halt very quickly."

But Roberts said the CAA has been "very pragmatic" in helping the industry to advance. ■

Budget constraints mustn't drive CCTV requirements, says Tavcom Training's Peter Mason

A CCTV system diagram helps you assess bandwidth requirements

There are many good reasons to integrate a CCTV system into an existing IP network but spotting the potential pitfalls is vital to ensuring that it works as desired, delegates at IFSEC International 2017 heard recently.

Speaking at the TDSi-sponsored Tavcom Theatre, Peter Mason, lead IP tutor at Tavcom Training, explained the common mistakes when integrating CTTV into an IP network – and offered a rage of tips and troubleshooting advice.

"Most importantly, you shouldn't let the budget drive the operational requirement," said Mason. "The operational requirement has to drive the budget; otherwise you won't get the system you need."

Mason advised the session's attendees that it is essential to create a CCTV system diagram to give greater control over what is happening. This will help to assess the level of bandwidth needed and whether it will saturate an existing network's bandwidth, he added.

Mason also outlined the difference between delay (the delay between transmitting and receiving packets) and jitter (the variations in that delay from packet to packet), explaining that adding routers to a system creates jitter.

Other topics covered by the non-technical training advice seminar included IP addresses, subnetworks, testing security and camera bitrate. ■

Surveillance camera strategy will "drive up standards"

> **"I'm not anti-surveillance; I'm anti bad surveillance"**

The three-year national surveillance camera strategy for England and Wales will help to drive up standards while at the same time balancing threats to privacy, the UK Surveillance Camera Commissioner has stressed. The strategy, launched in March 2017, aims to provide direction and leadership in the surveillance camera community to enable system operators to understand good and best practice and their legal obligations.

Speaking at IFSEC 2017, Tony Porter, whose role is independent of the government, said it supports the Home Office responsibilities to keep the UK safe from the threat of terrorism and to reduce and prevent crime. "I'm not anti-surveillance; I'm anti bad surveillance," he said. "But surveillance is everywhere in the UK. We have six million cameras at the last count. If that figure was accurate three years ago, you could add another 25% on it now."

Porter, a former senior counter-terrorism officer who has just been appointed to another three-year term as commissioner, said there has been a significant increase in body-worn video, drones and automatic number plate recognition cameras in recent years, all of which fall within the scope of the code of practice.

But he explained that a self-assessment tool, launched since he became Surveillance Camera Commissioner in March 2014, is already helping organisations that use surveillance cameras in public places identify if they are complying with the code. The tool has 12 guiding principles and enables users to put an action plan in place if they are falling short in any areas.

Clare Crump, auditor for the NSI, also explained to delegates that the code seeks to strike a "balance of protecting public and upholding civil liberties" and outlined the steps that organisations which voluntarily wish to show compliance need to take.

The trends shaping the future of access control

In a wide-ranging panel debate, a panel of access control manufacturers discussed the trends shaping the access control industry.

Panel chair John Davies, managing director of TDSi, said the major disruption seen five or six years ago things in the CCTV world – when communication was opened between cameras and software – was now happening with access control.

Spencer Marshall of HID Global said that until recently credentials were used on a low and slow frequency, with no memory capability. Encryption hadn't evolved – this was raw data – and a lot of people still used 125kHz technology. However, manufacturers will increasingly use the faster, higher frequency (13.56 MHz) 'handshake' between credential and reader required for encryption.

Davies pointed out that some years ago everyone was talking about NFC. Then Apple locked the NFC technology on Apple pay, which prompted a move to Bluetooth. However, now things are about to change, as Apple has announced that in iOS 11, access to NFC will be opened up.

Marshall explained the differences between NFC and Bluetooth. NFC is near field, close proximity. Bluetooth (BLE) is low energy and draws minimal battery energy. HID have now patented a 'Twist and Go', gesture-based reader using BLE technology, which works at a longer range of 8-10 metres.

Gareth Ellams of ASSA ABLOY identified simplicity as the main innovation driver. hence ASSA developed its wireless, encrypted Aperio locking system, which Ellams said was future-proofed, despite using proprietary algorithms.

Shane Naish of Integrated Design introduced the innovations currently turning the humble turnstile into a speed gate. This is still controlled by simple relay IO, although integration with access control systems using ethernet is key. This will increase functionality and the volume of data gathered. An alarm event can then be specifically identified as 'entry', 'exit', 'crawl'or 'tailgating'. An alarm event can also be shared with a CCTV system so that this tilts, zooms or pans to look at the person involved.

Davies said that access control was moving away from manufacturing in different silos. Open standards are breaking down the differentiators or barriers. New standards are being developed for the credential side.

While Wiegand – only a one-way protocol – is still prevalent, HID is developing an alternative with several other manufacturers called OSDP. open supervised device protocol. This is an open standard with encryption between the reader and panel and bi-directional communication. This means tampering can be detected and the reader easily updated or upgraded.

The cloud is having a huge impact, according to Davies, and represents a paradigm shift: companies are moving away from selling kit and providing an ongoing service instead. ■

Rethink Security

IFSEC International 2018 takes place **19 - 21 June**

IFSEC
INTERNATIONAL

IFSEC International is the world's most renowned security exhibition and conference, bringing together 600 premiere manufacturers and distributors with more than 27,000 senior security buyers, across 3 days at ExCeL London. Showcasing over 10,000 of the latest innovations across all areas of security, including access control, video surveillance, drones, fencing, bollards, cyber, analytics and more, IFSEC International is the only security event that brings the entire security buying chain together under one roof.

Find out more by visiting our website

www.ifsec.events/international/