MOBOTIX AG

Frank Graham, Business Development Manager, UK & Ireland

The video surveillance revolution is possibly the most dramatic change to the security industry over the last quarter century. In 1989, fewer than ten cities in the UK had open video surveillance systems, 25 years later, the technology is deployed in every major city and the majority of towns with estimates suggesting a total of between three to six million public and private cameras across the country.

The grainy, black and white, analogue 0.25 frame per second images of the 1990s have been replaced by full motion video, high definition cameras that have the ability to digitally pan-tilt-and-zoom to create discrete yet powerful devices that have helped to combat crime and promote health and safety.

Some of the most significant changes have been less visible to the viewer. The switch to IP has made deployments flexible and reduced costs by simplifying connectivity and enabling more efficient remote monitoring solutions. And innovation has not stood still in recent years. The current state of the art devices offer built in storage, thermal imaging, analytics and hemispheric technology that can cover an entire large room with just a single camera - all highlighting just how far the industry has come.

Video surveillance has also brought about many cultural changes. The initial fear of “big brother” has subsided with research in 2014 carried out by Synectics showing that 84% of people in the UK support video surveillance in a public space. For pioneers in this space like MOBOTIX, the next 25 years will see advances in artificial intelligence allowing video surveillance to spot dangers without human intervention and integrate tightly into other areas such as mobile applications – the video surveillance revolution is not yet over.

www.mobotix.com

BEYONDTRUST

Brian Chappell, Director, Technical Services EMEA & APAC

25 years ago most attacks came over dial-up connections and were often focused on BBSes (Bulletin Board Systems). 'War Games' dialers were still common, stepping through sequences of telephone numbers dialing each in turn and seeing if there was a modem at the other end. When a system was found it was returned to later and the system explored for access. Common methods of access involved buffer overrun and social engineering to 'guess' passwords, all very manual. The internet still had a capital letter and the web was still very nascent. Fast forward 25 years and hackers now use sophisticated vulnerabilities scanners that step through sequences of IP addresses looking for vulnerable systems with intrusion being achieved through buffer overrun and social engineering.

Seriously though, the IT Security space has evolved with many aspects becoming commoditised. In many scenarios, IT security teams are using the same or similar tools to identify weaknesses in their environments that hackers are using to find opportunities to exploit networks. We have entered into an arms race which each side struggling to gain the advantage, now we are on the verge of intelligent tools that will help automate defences, taking actions based on observed behaviours rather than simple pre-defined sequences of events. Systems that will learn how to better protect our environments against the next generation of tools being brought to bear upon us.

25 years ago we were firmly in the fortress mentality build a big wall at the edge of our networks and we’ll be safe. Now we are truly embracing layered, intelligent security that finally delivers on IT's promise of working smarter rather than just harder.

www.beyondtrust.com

HID GLOBAL

Harm Radstaak - Vice President Physical Access Control

The market’s biggest story of the past 25 years has been the evolution of secure identity technology to combat an onslaught of escalating threats. From prox to smart cards and on to even smarter ID technology, the industry has steadily improved security, improved the value of access control investments, and significantly enhanced user convenience. HID Global introduced its first prox reader in the early 1990s and has since helped usher in a new era of more powerful and versatile smart card solutions that increase security through data encryption and mutual authentication. Another significant development has been the transition to access control technologies based on open standards, enabling organisations to move beyond static, proprietary access control architectures to more secure, open and adaptable solutions.

Improved interoperability has also fostered a development environment in which companies like HID Global can collaborate with partners to embed its technology into many different systems that can all be accessed with the same smart card. Most recently, we are also seeing the growing adoption of new credential form factors that offer a more secure and convenient way to open doors and parking gates. We are seeing a card, phone or “wearable” replacing mechanical keys and dedicated OTP solutions for physical and logical access control. At the same time, physical and logical access control are merging onto both cards and phones.

Centralised identity management systems are being used to manage multiple IDs for multiple uses on multiple devices with multiple lifecycles, while also ensuring security and privacy for online transactions. Plus, using Bluetooth Smart or NFC technology, users can now simply ‘tap’ their smart card to a reader or NFC-enabled device to access facilities, VPNs, wireless networks and cloud-based and web-based applications. We’ve come a long way in the past quarter century, with much more innovation ahead.

www.hidglobal.com

www.securitybuyer.com