



# SECURITY Legacy Systems OR Legacy Thinking?

This article highlights the parallels between changes that revolutionised the computer industry and changes in today's security market. How can knowledge of their impact then, be exploited to our advantage now?

By Keith Bloodworth

Photo by CNL

The UK lags behind other areas of the world in terms of its acceptance of IP-based security systems. This is almost entirely due to the volume of analogue (or legacy systems) which have been implemented over the years. Given that it is impossible financially and logistically to simply throw these away and start afresh, the UK is facing a particularly interesting -- some would say 'challenging' -- time, as organisations consider how best to move their security needs into the new IP-enabled world.

These challenges may be less daunting than first imagined if one looks for parallels in the history of the IT industry. There are lessons in how this sector met the challenges, who succeeded and who failed, which may prove useful to the security industry in a time of transition.

## When Hardware Defines a Market

The security market has its roots in specialist companies offering one particular product to its customers, be it CCTV, fire systems, access control or intruder detection, to name but a few. Over time, major manufacturers such as Honeywell, Tyco and Siemens have established a dominant position in the marketplace by acquiring the smaller specialist players and thus being able to offer a broader spread of security products to a larger customer base.

Quite recently, these organisations have begun to introduce systems designed to provide a single point of access, management and control to all their different security products. The apparent benefits offered by such systems are numerous, not to say tempting: reduced operating costs, the achievement of optimal maintenance, greater productivity, higher reliability and

less downtime. One such system, for example, is EBI (Enterprise Building Integrator) developed and marketed by Honeywell.

Any system that seeks to link together hitherto disparate systems for the benefit of the user must be a good thing? But then again maybe not always the solution needed. Perhaps solving integration issues in this way creates problems of its own. A look over the shoulder to the IT sector is called for.

## Those Who Fail to Study History Are Cursed to Repeat It

The 1970s and 80s were dominated by the major computer hardware manufacturers, with IBM head and shoulders above everyone else. Their systems utilised proprietary protocols: once an IBM system had been purchased, the customer became 'true blue' through and through for all their hardware and software needs, regardless of whether they wanted to be or not. Choice was not an option.

Although IBM customers may have felt comfortable -- even cherished -- being supplied by such a mighty organisation, they paid a heavy price for this. For example, something as relatively simple as a printer would typically cost £3,000 from IBM, whilst the non-branded equivalent would be a mere £500, but unfortunately the latter was incompatible with all IBM hardware.

The arrival of networks later in the '80s signalled a major change and one which would end the one-to-one relationship between computer manufacturers and end users. A host of fast-moving, often small, but always innovative software companies swept into the market. They developed software

and systems -- and started to create new open standards -- enabling users to seamlessly connect equipment from different manufacturers gaining from both cost reductions and performance improvements.

Although the manufacturers such as IBM, Univac, ICL, Burroughs and Honeywell, tried to fight back by launching their own 'cross-platform' integration solutions, these were viewed as neither truly independent nor open. Despite claims to the contrary, they always seemed to favour the manufacturer's own hardware and proprietary systems.

## Change or Die

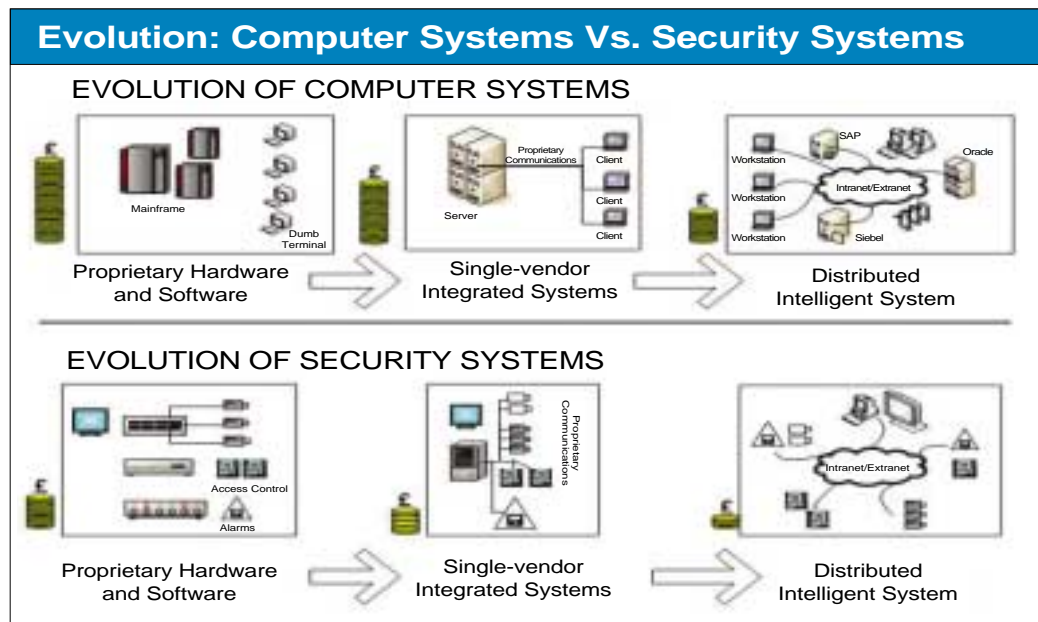
Even though these manufacturers knew that they had to change, their sheer monolithic size made it extremely difficult for them to 'turn around the ship'. These manufacturers had the wrong infrastructure, the wrong people and the wrong skills to meet the demands of the new breed of customers. And where are they now? Gone or adapting to the new markets.

The same challenge is facing traditional security manufacturers and installers. It is extraordinarily difficult to change an organisation which is dedicated to developing proprietary all-inclusive systems which are sold by a regionally-based sales force and supported by a fleet of engineers, more used to climbing ladders than reprogramming software. This is a fundamental challenge to security vendors -- change or die!

## Champions and Best of Breed

The champions of change towards open security systems are today's equivalent of the IT industry's software developers of the 1980s: they are companies whose sole aim in life is to develop -- and sell -- applications which exploit the connectivity between any device and any application. These companies place power and control in the hands of the user, who in turn are no longer tied to a single manufacturer's security system. Now best-of-breed is a user choice -- not a manufacturer's.

In the IT sector, networks -- first LANs then the Internet -- were the further catalyst for change. In the security sector, the same is true. IP networks are gaining ground rapidly and with them come the equally rapid realisation of the benefits of sharing and analysing information no longer locked within propri-



etary, closed systems.

An added benefit is that liberation of legacy applications gives a new lease of life to "old" equipment. IPSecurityCenter, for example, integrates old analogue systems with new digital ones to provide one view of a company's complete security infrastructure and the ability to link and share with other company-wide applications such as HR or Finance.

Already, there are examples of retail organisations exploiting this technology to address not only security and compliance problems but to provide a wealth of customer behaviour activity data for better marketing, category management and merchandising. By combining their CCTV infrastructure with Point of Sale equipment, retailers gain by identifying till fraud and multiple returns, and ensuring compliance with age-restricted sales. With the addition of the ability to track customers through the store to monitor dwell time and flow patterns, it is easy to see how this integration of physical and business data is delivering real business benefits.

## Resistance Is Futile

Although progress towards open IP-enabled security systems is inexorable, and the outcome is inevitable, it will not be a simple journey. Resistance to change will also impact on the smooth adoption of integrated security systems. Many of the UK's independent security consultants -- who wield a considerable amount of influence and power -- will continue to promote analogue, proprietary systems because this is the only world they know and are comfortable with.

Change generates not only resistance, but also fear of the unknown. Whilst the fears regarding new or changing technology are often unfounded, those with a vested interest in protecting existing revenues by maintaining the status quo will naturally take advantage of fear, uncertainty and doubt.

A recent innovation in the world of telecoms provides an interesting parallel with what is likely to happen in the security envi-

ronment. Voice over IP (VoIP) technology delivers voice and data over the same network (rather than utilising separate cabling and proprietary telephone systems). It is proving to be flexible, cost-effective and productive. Yet its take-up has been hampered by concerns about the 'risks' involved in putting all an organisation's communications services across a single network. But still, the trend is unstoppable. According to a recent Infonetics report, as we move deeper into the 21st century it becomes more apparent that IP networks are the next-generation networks for all forms of communication. It's hard to find a carrier not modernising its network with VoIP or planning to do so.

Faced with these massive trends, fears expressed in the security sector about entrusting CCTV, access control and the like to an IP network rather than to dedicated cabling and equipment look naive. Networks today are inherently robust, resilient and stable. Quality of Service (QoS) networks are a reality. But fear of change lingers on, fuelled by misguided statements about poor quality images, massive use of bandwidth and higher risk.

### Drivers for Change

Certainly at the moment, there is no equivalent cataclysmic event to the Millennium Bug which dramatically accelerated the changes already underway in the IT market. The impetus for change in security is coming from organisations who already appreciate that they must find more cost-effective and efficient ways to counter increasingly visible security risks. Terrorism and other high-profile threats continue to highlight the need for

an integrated security solution to manage risk and provide information to all interested parties in real-time. This in turn highlights the inability of traditional security products to deliver the pre-emptive and informed decision support needed by today's security manager.

In this environment, the trailblazers and 'early adopters' for integrated IP-enabled security systems are government bodies -- such as the education sector, health service, police and councils. As they reduce security risk with better IT systems, their results contribute significantly towards increased business confidence as well as demonstrating lower real-life operating costs.

### Total Integration - The IT Way Forward

Any integration solution needs to weave together the experience and expertise of both security and IT professionals. Already major IT vendors such as IBM and EMC are providing computing and storage infrastructure targeted at the security market; CISCO has recently acquired SyPixx to deliver video surveillance as part of an Intelligent Converged Environment. Organisations working in this new arena need to provide a bridge between the security and IT worlds, as well as between the old and new worlds of security systems.

Solutions must integrate the main security applications and provide an intelligent interface between these and 'operational applications' which handle the allocation of resources or the movement of staff, for example, as a result of an incident or alert from a security system. Designed to take advantage of existing powerful IP-enabled networks, this level of integration will, for the first time, allow organisations to operate a seamless, cost-effective -- and reliable -- security operation for the 21st century.

At a recent CEBIT conference, Steve Prentice, analyst and chief of research at Gartner Inc, stated that legacy systems and particularly legacy thinking are the single biggest challenge to transforming business today, with a majority of enterprises still operating ageing systems, which consume a majority of their IT budget in ongoing maintenance costs.

He went on to say that whilst the dot.com threat may have been a mirage, transformational business models enabled by Internet era IT are not. The challenge to established companies will come not from other established players, but from start-up entrepreneurs who will use technology to upset the status quo.

The worlds of security and IT will become ever more inextricably linked over the next few years. The parallels which can be drawn, and the lessons which can be learnt, from some of the major events in the history of the IT sector provide the security industry with an insight into who will win, who will lose -- and how to end up on the winning side.

*Keith Bloodworth is Managing Director of Computer Network Limited (CNL) (www.cnluk.com).*

**CCTV Manufacturer**

SE325i      SE506N

312X IR Camera      High Speed Dome Camera

SE705V      SE506

80M Night Vision      Speed Dome Controller

SE325      SE1604

SEC-EGO Electronic Inc.  
Add: 4-3-982 Sunshine 100 Nankai District, Tianjin P.R.China  
Tel: +86 22 23738362  
Fax: +86 22 23738363

**SE-EGO**  
CCTV TECHNOLOGY POWER

www.alarmtronic.com      sales@secego.com