IFSEC International
SECURING PEOPLE, PROPERTY & ASSETS

The Future of Security is All About Collaboration

IFSEC Global looks at the current level of threat from terrorism assessed as 'severe', it is timely to look at where the major security threats will come from over the next few years and what businesses and public sector organisations need to do now to prepare.

Through Counter Terrorism Awareness Week in November 2015, the Police sought to involve businesses, both in terms of physical and on-line threats. Perhaps the first lesson is that collaboration is key: awareness and preparedness is going to have to be country and organisation-wide.

The problem is too big for the Police to deal with alone. Security will involve not only industry professionals but IT, HR and other teams, up to and including the board.

A further lesson is where organisations should focus attention, and budgets.

The Government is doubling the aviation security budget, primarily on drones, and adding nearly 2,000 new intelligence and security officers. It will also increase the current military budget by £2 billion, to be spent on the Special Air Service (SAS) and other special units.

So the focus by the government will be in the areas of intelligence, technology and specialist services. This is where the security industry will focus too. The current threat requires a response that is strategic and proportionate. Measures need to take account of where the threats originate, with appropriate counter-measures.

Insider threat

Attacks, whether from criminals or terrorists, could come from an insider: an employee or contract or agency staff who has authorised access to your premises, says the Centre for the Protection of National Security.

This is a major security concern, particularly when protecting critical infrastructure: the insider who knows and has access to the key points of vulnerability, such as in transport or utility systems.

The risks are harder to identify and counter than a purely external threat. The insider has the opportunity and time to access critical information, systems and spaces of particular sensitivity. So the cost of downtime from an incident and restoration of services may be huge.

The insider may already be working for the organisation, or may be someone newly joined who has infiltrated specifically in order to get information or exploit the access that the job might provide.

Employee checks

The starting point is to ensure that new employees really are all that they claim to be, in terms of background and credentials.

Employers should use an independent service to check credentials, to ensure they are genuine and accurate. Evaluation requires experience and persistence, to follow up all references and identify when something ‘is not quite right’.

Checks should include: provision of a five or 10 year career history and references; BS7858 standard security references; character references; and other checks in relation to job role and levels of access.

Once employees join a company, monitoring of activity at work will become a focal point increasingly. Security teams, IT and HR departments will need to work with the Police and the Counter Terrorism Internet Referral Unit to monitor internet usage.

Additionally this will include monitoring of data from CCTV and access control systems – to identify where activity deviates from normal patterns of access, time spent in sensitive areas or on specific tasks for the job role.

Store detectives

Store detectives will be seen as critical for the security of large stores, particularly in major conurbations, shopping malls and other spaces which have been identified as having a high security sensitivity.

An experienced detective is trained to recognise if a member of the public or retail staff is behaving suspiciously – but their surveillance exceeds the capabilities of CCTV cameras, through the flexibility to go into areas that are not filmed, or harder to access – or to follow suspects or watch if they are collaborating with staff members.

Effectiveness depends on the size and quality of security teams, and ability to select and rotate detectives to blend in with the socio-economic profile of customers and avoid recognition by criminals.

Also, detectives need to be regularly trained and supported, with an understanding of current local threats and customer behaviour issues, and with daily contact with the Police, so that they are alert to local security warnings.

Vulnerability Testing

Security processes usually fail when people neglect or stop following procedures. The best way to ensure the integrity of security is through an audit process and, secondly, vulnerability testing, with private detectives working undercover.

This is relevant to major retailers but also to high profile corporate sites, such as banks, and public buildings.

The audit process involves independent assessment of security processes including access control, key holding, use of passwords, identity checks, guarding provision and coverage, alarm handling and response times, CCTV monitoring and other issues.

Vulnerability testing is critical to see how processes stand up when undercover detectives check them. Observing the organisation's processes – such as how contractors are dealt with when trying to access restricted areas – can identify weaknesses.

Audits and testing are likely to become as routine as the annual financial audit. It is an opportunity to comprehensively review current provisions and opportunities to upgrade services, as technology or the nature of any threat changes.

Centralise control of security services

A further focus of attention will be the fast communication of security data, response to alerts, and managing of intelligence data. Acts of terrorism around the world have shown the importance of centralised 'hub and spoke' data sharing for the speed of response to an alert. Minutes can make a crucial difference.

So organisations will centralise security monitoring and management: sharing data with the Police and intelligence services, verifying alarm signals and despatching local guarding and repair teams.

CCTV monitoring will move off-site, with increased use of web-enabled security technology. Centralisation offers the potential for standardisation to better quality CCTV and surveillance, more accurate verification and faster response.

The threat of terrorism needs this new focus on centralised intelligence: so that multiple sites in a group are connected to a control network over the internet, for 24-7 security management, communication, reporting and control.

The new intelligence centres will be fully equipped ARCs (Alarm Receiving Centres), monitoring CCTV and managing access control and two-way communication – but also managing building services too, including electrical, lifts and HVAC, for more comprehensive control.

Regular contact by the intelligence centre with Police and security services will ensure that intelligence reports and alerts can be taken into account daily for planning of site security, with extra guards or detectives deployed on a same-day basis.

When the central management team receives an alarmed alert, it can be confirmed quickly, with key managers notified and consulted; and emergency services contacted and guided to the incident, at the precise location.

Scene reports, evidence, CCTV footage can all be collected and managed centrally, for fast and efficient processing and collaboration with the Police and security services.

The technology and services for the intelligence centre are available today: what is taking longer is the cultural shift.