Future Innovations

The global terrorism risk continues to evolve and become more sophisticated in terms of the threat to life and assets. With current threat level from international terrorism to the UK rated as ‘severe’, an attack could take place at any time and any organisation could be directly affected or indirectly disrupted.

To mitigate such threats, organisations need to remain proactive in their defence which will require a constant review and randomisation of security protocol and operating procedures so that security infrastructure cannot be compromised or second-guessed by potential perpetrators. To facilitate this approach we envisage the wider adoption of output security specifications to create lean and responsive security services which will replace traditionally stringent input specifications.

Establishing an effective output specification in security involves balancing the twin focuses of controlling risk and minimising operational disruption. With multiple parallel objectives for the service the most effective approach to defining outputs is a balanced scorecard approach. This enables collaborative weighting of different service outputs to develop a specification which is representative of the risk appetite and wider operational objectives of the client. This form of contract offers strong commercial advantages to clients, as the security provision will fluctuate in accordance with the security environment.

In addition a less mainstream, less prepared for security threat, we believe, is the potential disruption that could be caused by cyber-crime. Also operating within an evolving landscape of continually changing methods of attack, deploying increasingly sophisticated techniques, the threat is now evolving into a physical ‘insider threat’ as an innovative way of circumventing IT security infrastructure.

Every business relies on the confidentiality, integrity and availability of its data; protecting this information is becoming increasingly critical, and increasingly prone to attack. Worldwide, thousands of IT systems are attacked and compromised daily; some purely for the kudos of doing so, others for political motives, but most commonly they are attacked with an aim to steal money or commercial secrets.

ICTS is developing multi-layered security principles to protect against this emerging trend which focuses not only on electronic and procedural data protection (from an IT perspective) but also on more stringent employee screening, attention to employee welfare, utilisation of profiling and screening methods (from an HR perspective), advanced threat detection training and robust contingency planning.

Ashley Bancroft