Frank Cannon

Founding Director, Cannon Asset Protection and fellow of The Security Institute

Frank has documented his learning over 40-years and formed a body-of-knowledge called The CAP Way, which he advocates through his one-man consultancy, Cannon Asset Protection.

The protective security industry is a growing sector, both in size and diverse specialisms. An intelligence analyst, a CP officer, an installation engineer, and a frontline security officer —amongst other disciplines— are all professionals.

The increased access to open-source information, and the continuous evolution of technology, requires those security practitioners to maintain their professional competencies; CPD must be a lifelong journey across the sector. Competence breeds confidence, confidence creates professionalism, professionalism builds reputation, and reputation generates trust.

Validating information through a security lens, to provide intelligence to lead protective security operations, is essential; however, fake news is endemic and difficult to regulate. A curious mind must be employed to seek out truth. Capital investment decisions made on false information can prove very expensive and ineffective.

Security practitioners must deliver excellence whenever possible, and advice given must always be based on meaningful research to provide proportionate and affordable solutions that meet the bespoke needs to mitigate the adversarial risk. Speculative, excessive profit-making, and overengineered solutions should not be part of our tradecraft.

Some would say the answer is always 'yes,' when asked to deliver a protective security service. I would add a nuanced caveat of 'yes, but'. I'm often frustrated when I read a strapline of 'world-leading', 'unparalleled' and 'global-operations' on a website or social media post describing a small to medium enterprise – they can't all be true! I believe in partnerships, networks, and associations between complementary experts to deliver a holistic protective service; leveraging relationships across a wide supply-chain to create a unique solution to unique challenges. One size does not fit all, and no one person knows all.

The sector must build and maintain trust from within our communities and across society. Unscrupulous behaviour by charlatans masquerading as 'world leading' service providers only serve to distract from the collective goal of being recognised as a first-choice profession; therefore, we must all report this conduct to our regulator.

Whilst AI machine learning, and digital analytics can reduce the time and increase the quality of decision making, we must avoid the scenario where the 'computer says no'. Emerging technologies must be aids to support adversarial risk management and service delivery, and not be presented as the panacea or entire solution.

There is an opportunity for future adversarial risk and business resilience professionals to work alongside their peers within organisations to maximise the value they bring to delivering the business plan. Weaving in secure behaviours into existing workplace initiatives will ensure that everyone plays their part to protect the organisation's people, property, and information, whilst understanding how to react, respond, and report undesirable events.

Curiosity and empathy are powerful qualities for all security professionals; egos, arrogance, and Machiavellian behaviours are traits that must be remove from our profession. Unity, shared vision, and humility will help the industry become a trusted partner of the police and a trusted advisor to the government. As President Truman once said, "It is amazing what you can accomplish if you do not care who gets the credit."