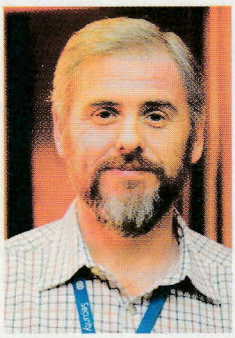
PROTECTING ASSETS:

Awareness adds value

Good employee security awareness adds value to a business, writes Frank Cannon.



About Frank Cannon
He spoke on this subject at the UK Security Expo 2016 at London Olympia. The former British Army man has been working in the oil sector in Kazakhstan the last few years. He's a member of the Security institute and has the CPP qualification through ASIS.

Simply put; it increases the number of people within the organisation who behave appropriately to safeguard the workforce and protect its property. Through enhanced vigilance and informed awareness, the employees identify and report suspicious conditions or people at the earliest point possible thus triggering a proportionate response by others. This early notification helps to minimise the negative consequence of crime and thus saves money.

Why is implementing such a programme 'extremely challenging'?
To be effective, a security awareness programme must have the support of senior executives and then resonate with the workforce. It is necessary to identify a series of key security messages consistent with the security risks but also echo the organisation's beliefs and vision statement. The pitch, tone and proportionality of the security message must compliment the day-to-day working culture of the target audience. There is not a one-size-fits-all programme that can be used to create a security culture but more the need for a cognitive process that requires an informed approach to harness the views of numerous stakeholders. Once initiated, the programme must remain evergreen and adapt to meeting changing work and security risks. The challenge is convincing leaders to invest funds based on the likelihood that an undesirable event will have a negative impact on the business; and convincing the workforce to change their behaviours.

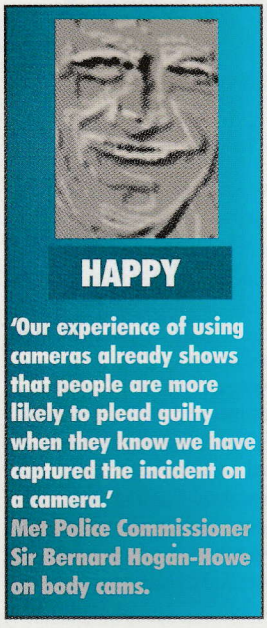
If all the staff are effectively part of the wider security team, how do you demarcate their roles from the roles of security professionals?
A 'team' is a group of people with a common purpose; in this instance, the purpose is to safeguard all those in the team and to protect the property they use or own. Communication is the essence of good teamwork and by encouraging every member of the team to observe, listen and communicate their thoughts it allows others to take action to address any fears or concerns. Non-security professional members of staff become the 'alarm' or information gathers leaving the security practitioners to respond or analyse and plan.

What does such training look like?
My belief is that 'training' is a process to develop skills or practical ability whereas 'education' is the giving and receiving of knowledge or theoretical competence. I believe a security awareness programme is an educational process to help employees observe events or people through a 'security-lens' and help them recognise an abnormal situation that may place people or property at risk. An awareness programme can be delivered through various forms.

What are the main elements?
Prior to the development, the security threats and associated risks against the organisation, its workforce or its assets (property, vehicles, materials, information, reputation, etc) require assessment. It is then necessary create an integrated programme creating a proportionate blend of physical, technical and procedural elements. The security procedures set out behavioural expectations for the employees so that a pre-determined outcome is achieved. Only then, can an awareness programme be developed to communicate with the workforce. A programme consists of numerous methods (or tools) to communicate the security-related expectations, or security strategy; key messages. Each one amplifies specific issues that, when put together, helps to create a 'security culture'. That isn't a tangible asset or outcome but more a way in which routine business is executed. Key messages are developed with the support of stakeholders and complement the organisation's culture, beliefs and operating processes.

What format does the training take (classroom, online, reminders, refreshers)?
Security education is a continually evolving process that takes advantage of opportunities as they appear. Initial induction, promotional courses, trade training, team meetings, periodical workshops and quarterly 'town halls' all provide good platforms to engage the workforce. The location, audience, time and importance of the security message often dictate how and when the security awareness is delivered. This can range from regular (three to five minute) 'security moments' at the start of routine meetings to a full day workshop involving larger audiences. An artisan tradesperson, with little

Pictured this page and next: simple but vivid pictures and short phrases (in Kazakh, Russian and English) put across vigilance messages to non-security staff
Images courtesy of Frank Cannon



HAPPY

'Our experience of using cameras already shows that people are more likely to plead guilty when they know we have captured the incident on a camera.'
Met Police Commissioner Sir Bernard Hogan-Howe on body cams.

БОЛЫҢЫЗ! БУДЬТЕ БДИТЕЛЬНЫ! KEEP AN EYE OUT!

болып жатқан Незамедлительно сообщайте о Immediately report any
немесе әрекет любых подозрительных вещах suspicious item or
Апат или действиях Аварийному activities to the
табарлаңыз: Оператору Org Emergency Operator:

CONTINUED ... FROM PREVIOUS PAGE

access to a computer, will benefit from a 'toolbox-talk' at the start of the day whereas an office worker may learn more through an online e-package. For those with time, or for the more important security risks, a workshop or stand-alone meeting may be the most appropriate forum to communicate security expectations. Or, a well-designed poster may successfully convey the simpler messages. The message being communicated must be *relevant*, *important* and *personal* to the audience. Each recipient must identify with the message and understand a personal benefit for changing an otherwise acceptable behaviour to help increase the levels of protection.

Does the programme include information security as well as conventional physical security?

If the organisation, its management or the security risk assessment identifies a cyber-risk that requires employees to behave in a specific way then information security can be included within the programme. To be honest, anything that adds to the protection of personnel or assets can be included into the programme scope, include; health, safety, environmental or community interaction.

How can you measure the effectiveness of such a programme?

This is challenging and often why organisations tend not to invest in security awareness. It's always difficult to compare workplaces that have a programme with those that do not. I often say that success is when I have leaders or supervisers discussing personal safety or asset protection as part of their routine business. An organisation with an effective programme (or security culture) has 'security' as part of their operational planning process, listed within their job descriptions and part of their standing meeting agenda items. Success will be when employees behave appropriately demonstrating their engagement, participation, commitment and accountability. Success is when employees are routinely reporting suspicious people or events, where employees are willing to participate in workshops or practice exercises (drills), where employees change their behaviours based on advice received, and seek out security awareness materials for use within their own team. The ultimate goal is to have a security incident and injury-free working environment so the 'before and after' incident statistics must support a downwards trend, however; the security risk level can change overnight so incident trends are not always a true reflection on success.

Zero might not be success

When considering the challenge of identifying and mitigating an attack from a motivated and capable adversary it is not always prudent to correlate zero security events with absolute success. Conversely, a high rate of security events or incidents does not always indicate failure as it is almost impossible to predict what the incident rates may have been but for the programme.

Finally, what can you do to help an organisation develop awareness?

It's not necessarily what I can do but more what an organisation can do to help itself. But, maybe the most beneficial element I can bring is to help win over the executive leaders so they understand the need for one to exist in the first place. ❐