The Hybrid Security Conundrum

There is one particular habit that annoys the hell out of us. So many headlines, articles, presentations speak about “security” when they mean “cyber-security”. In nine out of ten cases we’ve found it more helpful to talk about all security in a holistic way. If they have to focus on cyber that’s OK, but any carelessness with words makes people forget about the importance of physical security.

Because physical security IS important.

Frontline security officers are the unsung heroes of the industry and play a vital role in protecting people and property. They are adept at spotting the ‘out of the ordinary’, things that don’t quite fit with normal activities: they know the people, the patterns and routines; and they spot, and act on, the unusual. In the navel-gazing world of business process design, there is a phrase “work as done, not as imagined”. Security officers know what goes on, not what the manuals say should go on, and they know what will work to deal with unwelcome events.

In this article we want to look at how the security officer contributes unseen to cyber-security.

In the past, cars were stolen using a stolen key or brute force, in other words a physical attack. In some notorious cases, remarkably little brute force was needed, but that has been greatly improved. Cars with keyless ignition are now getting stolen by thieves cloning the signals from the remote control to unlock the doors and the ignition. Manufacturers seem to be getting on top of this problem, but it is a good example of a new kind of security threat, a hybrid cyber-physical attack. The cyber attack, cloning the signal, facilitates the physical attack, the theft of the car.

Hybrid attacks work the other way round too: a physical attack enabling a cyber crime. For example, the theft of a laptop or memory stick may enable a criminal or terrorist to gain access to those systems, in other words a hybrid physical-cyber attack. Going back to the car example, imagine the possibilities for vehicle theft or terror attacks when autonomous driverless cars are common.

What may at first just seem like a break-in, an attempted burglary, could be the initial stage of a more complex attack to facilitate a cyber attack, and of course the opposite applies, with a cyber attack on security systems being a means of compromising physical security, or facilitating an attack against people or property.

What can the front line officer do to help? We’re hoping you can tell us. Here are a few examples:

- Spotting the out of the ordinary, a break in where nothing was stolen: could it have been to get access to computer systems or networks?
- Spotting new kinds of hostile reconnaissance, such as wifi repeaters or communications cabinets, cables or devices.
- In offices where screening or bag searches are routine, let visitors see that it is being done thoroughly.

With the increasing use of what the technology industry calls "Artificial Intelligence", more and more physical assets and people will be protected by computer systems: networked CCTV, electronic door controls, identity and pass control systems, alarms, air-conditioning and building management systems, etc. One of the new challenges will be to ensure those systems are themselves protected, so physical protection will become even more important.

The fact is terrorists and criminals are constantly playing a 'cat and mouse' game with those seeking to stop them, and the threat landscape is becoming more diverse and complex. To try to get ahead of the opposition a more collaborative approach to security is needed. It used to be easy to distinguish between physical and cyber-attacks, but we hope this article has convinced you that more complex attack methods are becoming possible in this hybrid world. It's true that many attacks are very simple, but perhaps one of the simplest, using a vehicle to attack pedestrians or ram-raid a building, could in future be done with a remotely-commandeered driverless vehicle. Perhaps we should call these attacks "multi-dimensional" rather than "complex".

It is clear we will need a new kind of vigilance and a new way of working. Security teams tend to work in silos because that is how the organisation manages them; and tend to have their own jargon because that is how the industry speaks to them. Both those barriers need to be broken down, but it is unlikely that we will see a hybrid cyber-physical security team any time soon. Instead we need to create the environment and the forum in which they can work closely together.

We have helped some of our clients establish cross functional **Security Threat and Risk (STAR**) groups. The STAR group pulls together the whole range of security specialists and business managers into a single group to discuss potential threats and how to manage them.

One particular STAR group we know includes police, border control and security patrol officers. We really like that because it includes representatives of the frontline team. They are uniquely placed to pick up warning signals indicating that something is not quite right and they have an eye for practical issues and potential situations that may not be obvious to risk and security theorists.

There's an obvious challenge in such groups. Each specialism has its own language, jargon and methods. To make those meetings really effective, we devised what we call the **"Rude Protocol".** The eagle-eyed amongst you may recognise that term. The Rude Protocol was mentioned in our very first article for the TPSO magazine as a kind of meeting etiquette, a way of promoting clear communication. It has four simple rules:

- If you don't understand what is being said, ask for a fuller explanation without embarrassment
- If you are asked to explain something, do so without patronising or impatience
- If you disagree with what's being said, say so without sarcasm
- If somebody disagrees with you, discuss it without taking offence

Funnily enough, these are rules that will come naturally to many frontline officers who are skilled in defusing confrontation and difficult situations. It may be harder for some of the

other specialists to adopt these habits.

The random-looking ramblings in this article may be a clue to the fact that we are still trying to work it out, to think through what the issues are and how to tackle them. But we thought it would be a good idea to share it early and ask for suggestions or comments from the people that know about security at the sharp end.

Andy Blackwell.

Director, 3DAssurance.
Andy is widely acknowledged as a SeMS and aviation security expert. As Head of Security at Virgin Atlantic, he was the first to implement the SeMS Framework. Now a leading SeMS exponent, Andy has authored numerous articles on SeMS and security, and speaks regularly at international security events.

John Wood.

Director, 3DAssurance.
John was responsible at the UK CAA for developing the SeMS framework, working with and guiding many industry stakeholders. Experienced in design and implementation of effective strategic change in public and private sectors, John has been a lead designer of numerous governance, risk and compliance systems.

www.3dassurance.com