KPMG

FTSE100 conversation about terrorism as a business risk

Audit Committee Institute

A conversation with Sir Bernard Hogan-Howe — Thursday 29 June 2017

Sir Bernard Hogan-Howe provided a fascinating insight into his time as Metropolitan Police Commissioner, the challenges that our police forces face, and the recent developments we have seen relating to the evolving terrorist threat.

Going back ten years, the devastating 7/7 attacks on London brought about some significant changes to how counter-terrorism is organised nationally in the UK. The setting up of counter-terrorism units in major cities, and an enhanced relationship with MI5 resulted in greater trust and information sharing at a local, national and international level. With no land border with mainland Europe, a high level of gun control and relatively better community integration than in many of our European neighbours, we had not seen the extent and volume of attacks suffered in, for example France or Belgium.

However, 2017 has very sadly brought a real step change with the significant loss of life in the attacks affecting Westminster, Manchester, London Bridge and Finsbury Park. "When people start dying, you start to think differently."

Whilst there is no miraculous cure to the threat we face, there are certain steps that can help businesses be better prepared, reassure their staff and customers, and react more effectively in the wake of an attack.

Sir Bernard shared with us his ten areas for businesses and boards to give consideration to:

1. Use security experts well

Give consideration to the physical risk assessment of premises, how could these be enhanced to protect those inside? Could counter-terrorist advisors help provide additional solutions or identify weak spots? How could simple, often inexpensive, solutions provide an extra layer of physical protection? Might, for example, something as simple as large decorative planters deter a vehicle from violating your main entrance?

2. Vehicle access

Is vehicular access effectively controlled and monitored? How are goods deliveries or suppliers managed to mitigate the risk of everyday vehicles being used as weapons? Is the goods-in area a potential open door to a terrorist?

3. Evacuation or stay put plans

Most organisations invest significant time into ensuring staff are well informed and well-practiced in the procedures to follow when evacuating company premises. Does the same follow if the building is invaded and it is safest to stay inside? Are there designated safe areas where people can be protected by physical barriers/fire shutters etc.? Is this well communicated and understood? Has regular scenario-testing taken place?

4. Shared sites

Organisations are often part of a wider infrastructure, e.g. shopping centres, business parks, industrial estates or offices in shared, managed buildings. How joined up are the crisis action plans for each of the occupants? Do security teams liaise effectively as a community and is the approach co-ordinated, or are plans created and executed in silos?

5. CCTV

CCTV and access to video and audio of perpetrators can be hugely valuable in the prevention and detection of crime, when used effectively. Where is the central CCTV control point? Is this known? What access can the security teams gain from outside of the control point e.g. via the internet?

6. Internet and Wi-Fi – friend and foe

Access to Wi-Fi is an everyday expectation now and most companies have a customer-friendly approach to online access. In an attack situation, internet/Wi-Fi access can be a positive thing (e.g., allowing hostages to get a message out), but conversely, it can also provide assistance (or a mouthpiece) for attackers that the organisation may need to interrupt. Can this be done, and quickly if needed?

7. Insider threat

The insider threat has been evident in many post-attack investigations. Cyber-crime is often cited as being committed with insider help (whether active or unwitting) and recent press reports suggest that the recent Manchester Arena attacker had access to hydrogen peroxide, a commonly available chemical. How might a business or industry provide access to products that could facilitate criminal activity? For example, do employees or contractors have access to supplies that could be used for making explosives? What procedures are in place to restrict access to large volumes of dangerous products? Is there easy access to large vehicles? Are opportunities provided that could help individuals carry out extremist activities e.g., fire-arms training?

8. Staff overseas

Does the organisation always know where its people are? What plans are in place to support people caught up in a crisis situation? Is the organisation ready and able to support family members? What welfare support is available? How is this communicated and managed? Do employees know about the help available and how to access it?

9. Statutory duty for health and safety

As a statutory duty, organisations and leadership are required to ensure appropriate health and safety standards are adhered to. But what consideration is given to the security aspects that are inexorably linked to health and safety? For example, if a business handles a dangerous material (e.g., nuclear waste), the safety of how this is handled within the business will be a fundamental part of the organisation's operations – but does the security of the material attract the same level of attention? What is the risk of theft? What are the procedures that prevent criminal access? Are these fit for purpose and working as intended?

10. Exercise, practice and test

Plans need to be rigorously tested. It is important not to make assumptions, and plans may not always survive contact with reality. Testing and practice also serves to reassure staff that the organisation takes their safety and security responsibilities very seriously. However, re-testing is important too. Things change and develop - so regularly revisiting procedures, challenging potential scenarios and executing practice drills are all key to avoiding complacency.

Forthcoming breakfast events

Conversation about cyber risk – a growing threat: Thursday 14 September 2017

Sir Iain Lobban KCMG CB, former Director of the UK security and intelligence organisation GCHQ, will lead a discussion on addressing the growing threat of cyber risk.

Conversation with a chairman: Wednesday 15 November 2017

Richard Burrows, chairman of British American Tobacco, joins us to give a board chairman's perspective on the audit committee.

We will start with tea and coffee at 7:45am, sit down for breakfast at 8:00am and finish our discussion by 9:30am.

Both breakfasts will take place at Number Twenty, Grosvenor Street, W1K 4QJ.

To reserve your place at either breakfast please email us or contact us on 0207 694 8855.

Tim Copnell
Chairman of the UK Audit Committee Institute
T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk

kpmg.com/uk

Produced by CREATE I Document number: CRT084863A