“Terrorism and the corporate world”

Interview with Peter Power, FBCI, MD Visor Consultants (UK) Limited, Chairman of the World Conference on Disaster Management

Key note speaker at the 3rd BCM Forum 2016

By Dr. Marilena Fatsea, Fidel & Fortis

Q. In light of this heightened state of threat awareness, how could companies be involved in the fight against terrorism? What are the main challenges executives and decision makers have to take into consideration to protect their organization?

"All terrorists aim to spread fear, anxiety and panic throughout the wider society by elevating a specific terrorist incident beyond its localized setting, thereby creating a perception that every citizen and business is vulnerable to attack. Thus, when a country is perceived as incapable of preventing such attacks on its businesses, whatever their shape or size, it causes the affected government, organisations and communities to appear inept and incapable of protecting both citizens and the wider economic/commercial environment. We regularly hold realistic terrorist attack scenarios for businesses ranging from an active shooter to bombs, as well as unusual threats such as deliberate water contamination. I believe that nothing is more useful than working through a possible simulated event (see below) and then identifying corporate strengths and weaknesses in the response. After that, adapting Crisis Management (CM) and Business Continuity (BC) plans - which then become the documentation of executive competence - until the next exercise".

Terrorism and BCM

Q. In an article of yours, published in “Continuity” magazine you explicitly say that the consequences of recent terror events (Paris and San Bernardino) will impact on BCM practitioners’ responsibilities. Can you briefly explain, in what ways may these events impact their responsibilities?

"The most recent 'Horizon Scan Report' by the BC Institute reveals that terrorism has jumped the highest number of places to now become the 4th biggest (out of 10) concern for BC professionals. The threat of cyber-attack remains at number one, followed by data breaches and IT/telecoms outages at 2 and 3. Since many cyber-attacks are terrorist inspired, it follows that terrorism is logically a top concern for a great many people with BC responsibility. Within this threat group physical terrorist attacks can have an even more profound impact on any business. Since it's the job of whoever looks after BC to maintain all critical business activities in the event of any incident, it follows that the impact of any terrorist incident such as Paris and San Bernardino will, I suggest, impact on the responsibility of anyone tasked with maintaining BC.”

Q. Based on your experience, what is the terror threat level on the work environment today? Tentative

"To quote the UK Government, the terrorist threat level in the UK is considered as 'Severe' insofar that an attack is believed to be 'highly likely'. This is only one level below the top categorization which is 'Critical', which means that an attack is considered 'imminently'. I believe this to be entirely accurate".

Q. What types of cyberattacks may qualify as cyber terrorism? Can Hacktivism amount to cyber terrorism?

"It's important to note that I am not an expert on cyber security and as you know, I should not be labelled as such. Nonetheless, I am aware that on 1 November 2016 the UK Government announced that it's about to spend £1.9 billion solely on national cyber security. That's the equivalent of 2.1 billion Euro. This colossal investment follows intelligence that attacks against the UK critical national infrastructure are a real threat, as I believe they are against most other European countries. However, in an age of European interoperability between EU nations, how many other countries are taking the threat just as seriously?

The British Government states that "If we want Britain to be the best place in the world to be a tech business then it is also crucial that Britain is a safe place to do the digital business. Trust in the internet and the infrastructure on which it relies is fundamental to our economic future." It follows a warning from MI5 (UK intelligence service) that singles out Russia as possessing an increased cyber-threat. "It is using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways - involving propaganda, espionage, subversion and cyber-attacks," said Andrew Parker MI5 Director General. I find this profoundly worrying".

Q. Do you share the view "that combating cyber terrorism has become not only a highly-politicized issue but also an economically rewarding one"?

"Please see Q 4. Beyond this, when it comes to combating terrorist we really must ask if terrorism is senseless as world leaders repeatedly say? Actually no. It's Calculated Barbarism. Terrorists are pursuing goals that make sense to them - and that's the important bit to remember. To defeat them we must first understand them. Terrorism is not impulsive or the fruit of an instant rage. To achieve its purpose, it requires dedication, planning and training. It is a mixture of drama and dread as a premeditated strategy. Once this is understood reasonable steps can be taken against unreasonable people. Consequently, by demonstrating to potential investors that an organisation has increased its corporate resilience across its critical activities, it then becomes a more attractive to any discerning investor".

Q. How important is systematic information sharing between the private sector and the relevant government authorities, police dept. etc. in the fight against terrorism? Tentative

"The sharing of such information is vital, but the constraints of secrecy can easily and understandably, impede this. In most countries I visit at least 85% of critical national infrastructure is entirely in private sector commercial hands where the pursuit of profit

is the key driver. This fits uneasily with the role of government in any civilised society I suggest, made worse perhaps by the boards of many supplying organisations existing in different countries so that whatever laws might exist within the target country on corporate governance for example, simply might not apply".

Counter terrorism training

Q. What are the most important criteria for good planning and implementation of terror related drills? Who should primarily take part in these drills?

"Recognizing, rehearsing and learning in advance of any disruptive incident is undoubtedly one of the moist critical considerations within the sphere of corporate resilience. This is much more important than just writing a BC plan for example. The use of an outside expert to assist this certainly helps to provide knowledge, objectivity and credibility, but at the end of the day, the organisation itself must take ownership of its responsibilities. Unless the board is both committed and involved, any exercise would not be worthwhile at corporate level (where reputation is vital)".

Crisis management

Q. How important is cooperation in crisis management? More specifically, what are the prerequisites of effective cooperation between different crisis managers from different organizations and cultures in case of a real crisis event?

"Nowadays we exist in an increasingly fragile, bewildering and interconnected society where just about all essential services we rely on are far more entangled than we realise. When something goes wrong the consequences are therefore more sudden and widespread, made worse perhaps by secrecy, scapegoats and silos: we cannot be told, we need someone to blame and in any case, we work separately.

I've been involved with advising and exercising public and private organisations on matters of CM for many years and am also an author of the UK Government standard on CM (BS11200). I was also a small cog within the Institute for Public Policy Research (IPPR) Commission (the resilience subgroup) on National Security that published an aptly named and wide ranging report entitled 'Shared Responsibilities'. This talked frankly about the need for "fundamental changes to Government structures, the strengthening of strategic decision making at the centre and the breaking down of departmental stovepipes….if we remain trapped in the old ways of thinking and the old ways of doing things, the security of our country will suffer".

In my experience, the highest number of disasters are caused by organisations that fail to prevent a crisis from getting worse and then only waking up when things have deteriorated to the point of disaster. Although crisis prevention is considerably more effective than disaster recovery, many organisations are still encouraged to spend a disproportionate amount of time and money on recovery options, without first looking at reducing risks, as well as preparing for the unforeseen.

We also live in world where the extraordinary has become commonplace and the unexpected is now regularly anticipated. Add to that 100s of predatory News organisations, immediate / global communications and hitherto steadfast organisations frequently discredited and ridiculed and you might be correct to assume

we are perhaps more vulnerable to crises than ever before, even though our security and intelligence services have by comparison, never been so well equipped in so called peace time.

That also means of course, that we are more aware of crises, yet at the same time, more unforgiving if those in command do not deliver the solutions we have been lead to expect. An extremely difficult, if not impossible, challenge, for any government or large organisation where for example, speed of social communication would have been unimaginable, even 5 years ago.

Increasingly organisations have first been altered to a growing crisis because of what is written on Twitter, Face book or some other social site(s) tells them so. One reason why BBC, Sky News and other channels have a constant desk in their newsrooms dedicated to monitoring such sites. Chatter soon becomes news and perception quickly becomes reality.

If we fail to share assumptions and ideas CM between organisations, sectors, regions and even countries, we must surely prepare to fail in the future. It's therefore time to climb much further out of our silos and dismantle some of the unnecessary boundaries, especially in an age of unparalleled public sector outsourcing that I referred to earlier".

Published in The Huffington Post Greece
5.12.2016 http://www.huffingtonpost.gr/marilena-fatsea/-peter-power-_b_13425950.html?utm_hp_ref=greece