Crisis Planning: Communications, Management and Response

Threats and Perils

Recent events have proved in the most horrific ways that the world can be a dangerous place. In Barcelona, London and Manchester, restaurants, bars, and leisure venues have been directly affected by indiscriminate terrorist attacks carried out by individuals or small marauding groups. Using small arms, vehicles, or crudely improvised explosive devices, these attacks have aimed to cause mass civilian casualties.

In terms of risk mitigation, these attacks are different from the ETA and IRA terrorism campaigns of the 1970s and 1980s. The landscape has changed and organisations and individuals are facing wide-ranging threats which do not stop at terrorism either. Consider the rising incidence of cyber extortion, with two major and indiscriminate ransomware attacks (WannaCry and Petya) earlier this year, crippling operations in more than 150 countries across the world.

Preparation, planning, and training are all essential to ensure the safety of customers and employees, as well as to help build a culture of crisis resilience within businesses in the face of these new and evolving threats.

To ensure minimal negative impacts in worst-case scenarios, companies in the hospitality sector need to focus on cross-functional collaboration, engaging those responsible for risk, HR, security, IT, communications, finance, facilities and legal to ensure all business continuity, disaster recovery and crisis management plans are both cohesive and coordinated.

The case of the June 2017 London Bridge attack illustrates this need. As employees and customers at bars and restaurants in Borough Market fled, it would not have been clear to managers who was safe, and who may have remained in danger. Employees at larger premises may not have known who was in charge, or what they should do.

Most businesses did not suffer any physical damage during the terrorists’ rampage, but after the event they were inaccessible, trapped behind a police security cordon for many days, unable to trade, at a cost of thousands of pounds and a potential threat to livelihoods.

The greatest danger, therefore, is not usually the crisis itself, but a lack of preparedness in knowing how to react, respond and recover. Unfortunately many hospitality and leisure businesses appear unprepared.

A recent YouGov survey* conducted for insurance and risk management specialist Arthur J. Gallagher found that one in three (31%) UK small or medium-sized businesses in the hospitality and leisure sector surveyed had faced a security threat in the previous 24 months (and it is worth noting that results were collected just prior to the London Bridge attack, Manchester bombing and ransomware attacks). Despite this, nearly two thirds (63%) believed their business was at ‘low risk’ of being impacted by a terrorism incident. Furthermore, less than half (47%) had any insurance in place that would respond to various crises or threats, and yet two in three (66%) claimed to be ‘resilient’. This reveals a clear disconnect between preparedness and perception when it comes to dealing with today’s fast-evolving security threats.

Too Small, Too Busy?

Less than a quarter (24%) of hospitality and leisure businesses surveyed had assessed their exposure to rising UK security threats. When asked why, nearly half (47%) said they believed the risk too small to warrant action, one in five (21%) felt it wasn’t relevant to their

*uk.ajginternational.com/sme-crisis-resilience-report
business, and 14% said they were just too busy. However, an example serves to illustrate the vulnerability of a small hospitality business.

During the London riots in 2011, a local specialist caterer was unable to access her premises in order to collect an order scheduled for imminent delivery to the largest wedding venue her company had ever been asked to serve. Failure to deliver would have had serious consequences: the company risked losing its significant investment in the food that had been prepared, and the crippling reputational impact of failing to deliver would have been difficult to avoid or alleviate.

In this case, however, the caterer was prepared. Crisis consultants, provided under a relatively inexpensive crisis insurance package, were deployed to help. They liaised with local police and escorted the client to her shop, where they secured the premises and safely loaded the foodstuffs. The quick response allowed the caterer to continue as planned, and she even received new business enquiries as a result.

**Anticipate, Prevent, Respond, Recover**

An effective crisis management plan is much more than a written document. It has multiple components, including risk analysis, employee training, security protocols, emergency procedures, and risk transfer. It takes time, effort and the right stakeholders to build rather than big budgets or simply buying insurance. And cross-functional collaboration is critical.

**ANTICIPATE.** The first step is to anticipate crises by creatively considering what threats the business may face. To ensure their resilience, companies should begin by conducting a threat and risk assessment, preferably with the support of a risk consultant or qualified insurance broker. This process will help a business anticipate and understand where their specific vulnerabilities lie.

The risk assessment should include multiple components and cover a wide range of potential threat scenarios. To name only two, it should involve an analysis to calculate the impact and likelihood of low-frequency, high-impact threats such as non-damage business interruption after a terrorist attack (like the ‘denial of access’ that occurred in Borough Market). Each business is unique in this respect. Another component should be a cyber-security audit. This will determine, for example, the vulnerability of payment and online booking systems. It will also consider the company’s preparedness for a ransomware attack such as WannaCry, which affected businesses large and small around the world earlier this year.

**PREVENT.** The next step is prevention. Use risk management and mitigation techniques to prevent, where possible, being caught up in a crisis and ensure security policies and procedures are in place, tested, and robust. All employees should be familiar with them and appropriate training and regular updates are important. Simple communication can often avert a crisis. Consider also the implementation of a safe travel programme. When employees are on the road, for example, they could be required to check in at intervals to alleviate concerns for their safety.

It is vital to construct robust business continuity, disaster recovery and crisis management plans, which should involve the collaboration of all functions of the business, as detailed above. While businesses may not be able to prevent many forms of terrorist or cyber attacks, what they can prevent or mitigate is the severity of the impact.

**RESPOND.** Your organisation must be empowered with the tools needed to respond in the event of a crisis. Ensure you and your people can respond effectively to any security crisis through training and awareness, co-ordinated crisis management planning and appropriate insurance cover. Educate your people on how best to avoid crises. Enlist the support of human resources personnel to coordinate training in areas such as:

- **Evacuation** – the orderly removal of removal of staff and customers from the building usually due to a fire or other incident within the building.

- **Invacuation** – staff and customers made aware of an emergency and moved to the most sheltered areas within the building (away from external windows and other exposed areas) Invacuation is typically employed if moving outside would increase the risk to staff ie. bomb threat nearby, toxic fumes in the air etc

- **Lockdown** – Lock external doors and windows and take immediate shelter in a secure location such as a cupboard or locked meeting room until such time as the all clear signal is raised. Lockdown would typically be invoked as a response to a security incident/threat.

These emergency drills can make the difference between life and death and are relatively easy to write into a policy and rehearse. Simple preventative steps
such as appointing crisis coordinators, and making all employees’ contact details available to them, can make a huge difference. All personnel should be aware of these leaders’ responsibilities. The success of response is again founded in excellent planning. Cool heads should prevail, which is much more likely when delegated individuals – the crisis coordinators - take the lead to ensure everyone follows an agreed crisis response plan.

These plans won’t be detailed for every scenario. Instead the plans should be short, principle-based and stress-tested to enable rapid decision-making and communication at times when there will be a vacuum of information and panic and pressure from stakeholders on all sides. Emergency contacts for insurers, IT providers, and other crisis-response experts should be carried by crisis coordinators at all times.

Response is also where the value of your people training will become clear. In most cases of terrorism, the ‘run, hide, tell’ advice of the UK’s counter-terrorism police should be followed. Every team member with computer access should also be trained in the ways of identifying and responding to common cyber-security threats like phishing e-mails and social engineering ploys. The latter seek to obtain access to systems by scamming employees into revealing sensitive information, or clicking on dangerous links to unwittingly download malware.

**RECOVER.** When events do happen, a key goal is the swift return to business-as-usual. From a financial perspective, recovery requires the collection of indemnities for insured losses such as business interruption, and the swift repair of systems. A relocation plan may need to be executed. If a crisis elsewhere impacts upon supplies, pre-arranged back-up alternatives should be implemented. But, from a people perspective, recovery means ensuring every employee affected has the post-incident help and support they need to recover and return to health and happiness.

### Duty of Care

Protecting people is the most important measure of all. To help satisfy your employers’ duty of care to employees who may be involved in an incident, businesses should take action to:

- Ensure all employees know which colleagues are involved in crisis response, and require them to provide and regularly update their own emergency contact details and personal information;
- Maintain real-time information about colleagues’ movements, and provide them with an effective information flow regarding safety-critical issues;
- Provide situational awareness training, such as what to do if caught up in civil commotion or a marauding terrorist attack;
- Create a robust process and clear awareness of travel emergency response, including medical assistance information, evacuation, and repatriation procedures, together with contact details;
- Offer access to post-incident trauma counselling and other return-to-work support for those negatively affected by security events.

As firms work to anticipate and prevent security threats, they must avoid taking a box-ticking approach. From the top down and the bottom up, everyone must understand the importance of resilience-building measures. Building a culture of resilience is in everyone’s interest.

### Conclusions

All businesses face the threat, however remote it may seem, of incurring damage and losses due to acts of terrorism, cyber-crime, and other malicious incidents. However, the investment of resources including time and a relatively small amount of money can go a very long way to avoiding disaster. This may be even more important for smaller companies: after all, a week’s business interruption through denial of access or a £50,000 extortion demand is much more likely to threaten the survival of a small business than a large multinational.

But the reality of today’s fast-evolving security threats is that organisations of any size, sector or geography can be impacted by incidents like terrorism and cybercrime. No business should shelter under the misconception that they are too small or unlikely to be targeted, as many attacks are indiscriminate. The greatest risk exposure when it comes to terrorism, for example, is through non-damage business interruption, such as denial of access to premises after being caught inside a large security cordon, loss of trade due to people’s nervousness to frequent areas where attacks took place, or unplanned evacuations due to heightened threat levels.

It is imperative that organisations are resilient and adaptable to today’s threat environment. While risk
transfer (ie. insurance) is a key part of this, it is proactive risk management that will help save lives and ensure an organisation can respond and safeguard those to whom it owes a duty of care.

This Management Guide was created by Justin Priestley and Mark Eade of Arthur J. Gallagher. For further information and guidance contact: Mark Eade, Business Development Manager, Hospitality & Leisure Practice - Arthur J. Gallagher:
T 020 7560 3960
M 07810 152034
E mark_eade@ajg.com

Justin Priestley, Executive Director, Crisis management, Arthur J. Gallagher:
T 020 3425 3427
E justin_priestley@ajg.com

Further Resources

Arthur J. Gallagher is the international broking division of Arthur J. Gallagher & Co, one of the world’s largest insurance brokers. The division operates outside of the United States – in the UK, Australia, Canada, the Caribbean, Latin America and Asia. It employs more than 6,850 staff and through the wider Gallagher network offers service capabilities in more than 150 countries worldwide. Arthur J. Gallagher offers specialist insurance broking and risk management. Its dedicated hospitality and leisure practice serves approximately 8,000 hotel clients worldwide, strategically developing and delivering tailored propositions to effectively offset the risks to the international tourism industry.

National Counter Terrorism Security Office has advice and contact details for reporting suspicious behaviour or terrorist-related activity.

New Crowded Places Guidance for the UK was published by the National Counter Terrorism Security Office on 8 June 2017. It includes specific advice for hotels and restaurants as well as leisure and retail premises.

Project Argus is a suite of free workshops designed to inform and advise senior management in preparing a response to a serious event, such as a terrorist attack.
www.gov.uk/government/publications/project-argus

Facewatch is a secure UK online crime reporting and information sharing platform that enables businesses, the public and police to tackle crime. It was created by Simon Gordon, the owner of Gordon’s Wine Bar, London.
www.facewatch.co.uk/cms

The FBI website contains advice on combating cybercrime.
www.fbi.gov/investigate/cyber

The US National Cyber Security Alliance has advice on general online safety for businesses.
staysafeonline.org/business-safe-online

NHS information about post-traumatic stress disorder.
www.nhs.uk/Conditions/Post-traumatic-stress-disorder/Pages/Treatment.aspx

Counselling Directory provides information about post-traumatic stress disorder and how to access professional help.
www.counselling-directory.org.uk/ptsd.html

Mind, the mental health charity, explains what post-traumatic stress disorder is and how to access treatment and support.
www.mind.org.uk

DISCLAIMER

This brief is intended as a guide only. While the information it contains is believed to be correct, it is not a substitute for appropriate professional advice. The Institute of Hospitality can take no responsibility for action taken solely on the basis of this information.