airmic

EXPLAINED

CRISIS MANAGEMENT

A short guide

2018

Good Practice
Guidelines

Gallagher

Insurance | Risk Management | Consulting

Acknowledgements

Gallagher

Founded by Arthur Gallagher in Chicago in 1927, Gallagher has grown to become one of the largest insurance brokerage and risk management companies in the world. With significant reach internationally, the group employs over 26,000 people and its global network provides services in more than 150 countries.

In an increasingly unstable political environment where security threats can cause serious disruption, a robust crisis management and risk control strategy is more important than ever before. Gallagher's Crisis Management team brings together over 100 years of practical operational and insurance market experience in the counter terrorism, kidnap and ransom, recall and political risks fields. This experience allows them to assess their clients' organisations, objectives and the security and operational situations that could put them at risk and develop insurance solutions and crisis management strategies which help to mitigate this risk.

Business Continuity Institute

Founded in 1994, the BCI defined a set of practices for individuals to be able to demonstrate their individual capability in business continuity management. These Professional Practices form the stages of the business continuity management lifecycle and are described in the BCI's Good Practice Guidelines.

The BCI is the world's leading professional association responsible for improving organizational resilience through building business continuity capability and professional development of individuals all over the world.

The BCI vision is a world where all organizations, communities and societies become more resilient.

The BCI core values are professionalism, reliability, and inclusivity. The BCI is built on the principle of professionalising business continuity practice, and continues to be the authoritative and reliable source of information on all aspects of business continuity theory and practice for professionals, and offers a wealth of online resources via www.thebci.org

The Good Practice Guidelines have been revised as part of the BCI's process of continual improvement and ongoing development of our body of knowledge to remain relevant to professionals worldwide.

Gallagher

Insurance | Risk Management | Consulting

Good Practice Guidelines

Contents

Introduction

As trade becomes increasingly global and dependence on digital technology increases, the potential for disruption is rising exponentially. Risks are becoming more complex and more connected, and it's no longer just major organisations or cities that are at risk - events can happen anywhere, at any time.

Threats, such as terrorism, political violence, kidnap and ransom, cyber risks or product recall can cause serious operational disruption, financial loss or adverse publicity that can impact your organisation and its profits. That's why it's important to understand crises and the steps you need to take to manage them.

The British Standards Institution (BSI) defines crisis as an "abnormal and unstable situation that threatens the organizations strategic objectives, reputation or viability" and crisis management as "development and application of the organizational capability to deal with crisis". While you may have an incident response plan, incidents are usually something which can be predicted in advance and can be resolved quickly before long-term or permanent impacts occur. Crises, on the other hand, are unique or unforeseen events and can have dire consequences for your organisation. Failure to respond to a crisis in the correct manner could potentially cripple your organisation and, as this is not something which is part of day-to-day management, you will need to allocate the time and resource to introduce a crisis management plan.

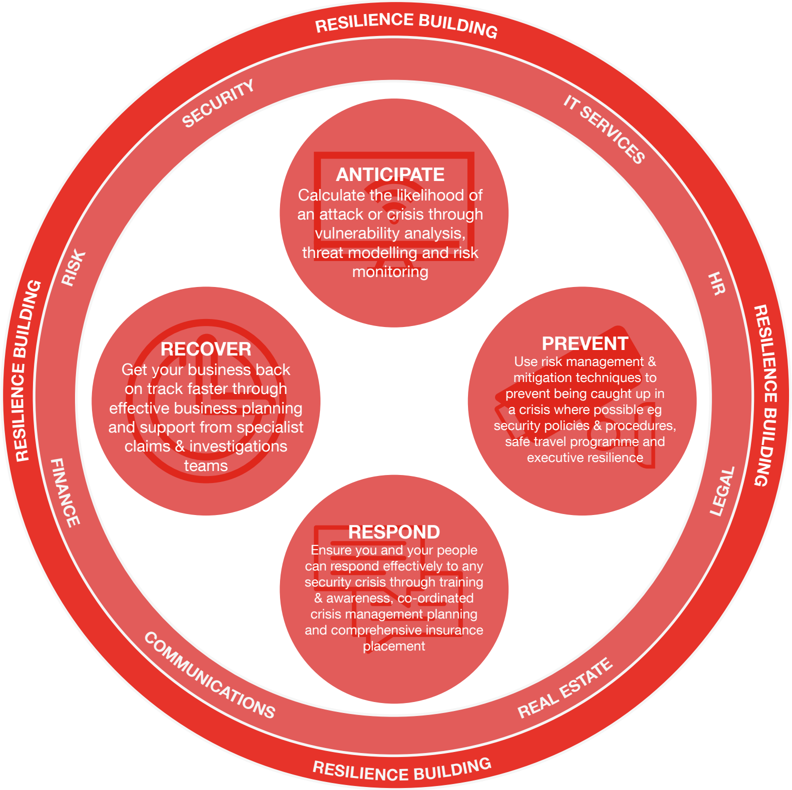
Research undertaken in 2017 by Gallagher, in conjunction with YouGov, shows that UK companies are keenly aware of the need to build a culture of crisis resilience against the main threats their organisations face, but managing and responding to security threats like cyber extortion, terrorism and emergency repatriation is easier said than done. These incidents are low frequency but high impact – increasingly causing damage to brand and reputation, as well as financial loss and personal injury or loss of life.

The key to a successful crisis management plan is to start as early as possible and have a clear strategic direction including clear communication, effective leadership and a detailed record of all decisions taken. Companies need to shift their mind-set and take a comprehensive approach to building effective resilience aligned to four key pillars of activity: 'Anticipate, Prevent, Respond, Recover'.

This guide practically outlines certain key principles in the Airmic 'EXPLAINED: Business Continuity Management' guide, BSI standards publications – 'BS65000: Guidance on organizational resilience' and 'BS11200: Crisis Management – guidance and good practice' as well as Airmic's 'Roads to Resilience'.

The four pillars of crisis management

Effective crisis management 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 this, rather than just big budgets or simply buying insurance.



ANTICIPATE
Calculate the likelihood of an attack or crisis through vulnerability analysis, threat modelling and risk monitoring

PREVENT
Use risk management & mitigation techniques to prevent being caught up in a crisis where possible eg security policies & procedures, safe travel programme and executive resilience

RESPOND
Ensure you and your people can respond effectively to any security crisis through training & awareness, co-ordinated crisis management planning and comprehensive insurance placement

RECOVER
Get your business back on track faster through effective business planning and support from specialist claims & investigations teams

It's also important to place crisis management within the framework of enterprise risk management (ERM) and business continuity management (BCM). The best way to describe this is as a 'continuum' of actions which exist before and after a negative event:

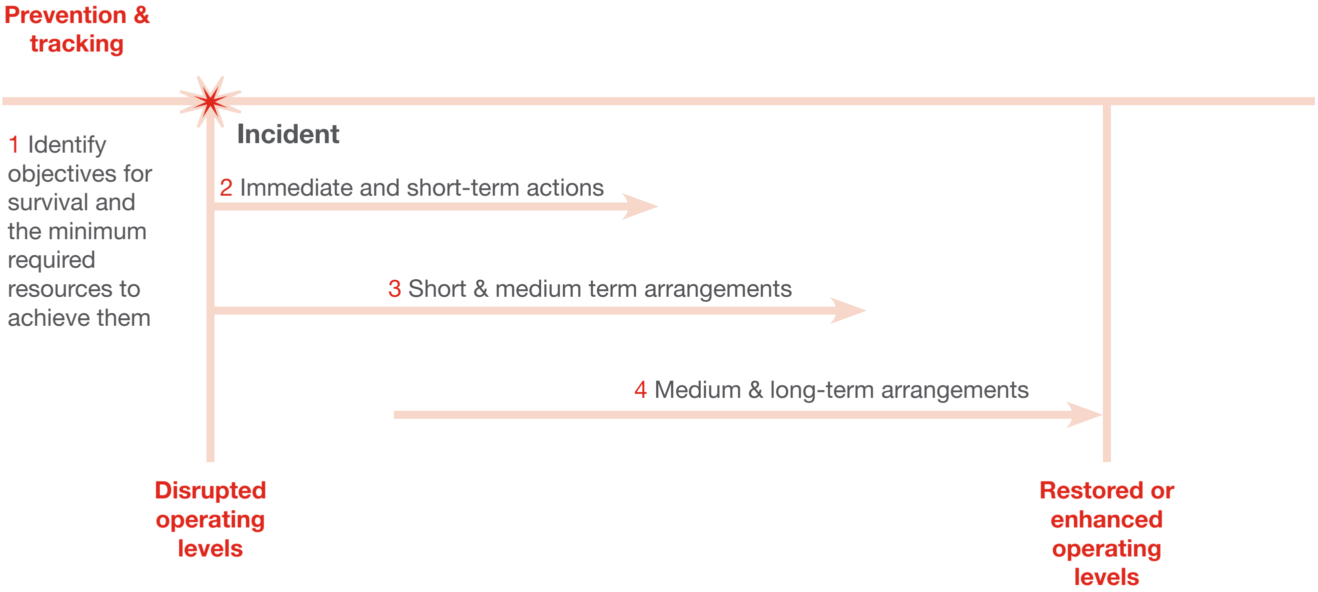

Prevention & tracking
1 Identify objectives for survival and the minimum required resources to achieve them
Incident
2 Immediate and short-term actions
3 Short & medium term arrangements
4 Medium & long-term arrangements
Disrupted operating levels
Restored or enhanced operating levels

Figure 1: **The phases of a business continuity response**

Chapter 1: Anticipate

The first step in effective crisis management is to understand the definition of a crisis and to anticipate those crises in the context of your business or organisation.

What is a crisis?

In BS11200:2014, Crisis management - Guidance and good practice, the British Standards Institution (BSI) define a crisis as an 'abnormal and unstable situation that threatens the organization's strategic objectives, reputation or viability'. While this may immediately lend itself to events such as a terrorist act, product contamination or serious production line failure, there are in fact many types of crises each ranging in severity and requiring a different response.

Types of threat

	SECURITY THREATS	NON-SECURITY THREATS
DEFINITION	A deliberate attempt to incite panic or disrupt day-to-day operations. These threats can also be planned attacks with the aim to extort money or inflict reputational damage on an organisation.	'Acts of god' and other non-man made threats which can inflict serious damage on an organisation. These threats can be hard to predict and can also cause significant business interruption.
EXAMPLES	• Cyber extortion • Terrorist attacks • Product tamper • Assault • Hostage situations • Kidnap and ransom threats	• Flooding • Hurricanes • Storm damage

Why crisis resilience is so important

Changing security threat environment: an example of dynamic change in the global environment

You only need to glance at the headlines to understand why crisis resilience is a hot topic for many companies. The terrorism landscape is changing as remote bombings are increasingly replaced with attacks orchestrated by lone-shooters or cars targeting pedestrians. It is no longer just major cities that find themselves at risk of terrorist attacks. Attacks can happen anywhere at any time and the damage they can cause extends from financial loss to reputational damage and in the worst case scenario, injury or loss of life.

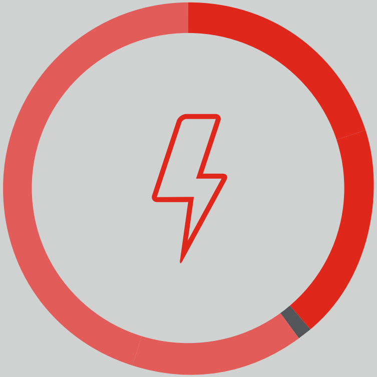
Terrorism remains a very real threat to companies, but they are rarely the direct target and physical damage and loss of life are not the most likely risks they face. What companies need to think about now are non-damage business interruption and denial of access to their premises for both employees and customers, merely by finding themselves on the wrong side of a security cordon. The denial of access caused by events such as London's Borough Market attack in 2017 can have a significant financial impact on your organisation, which without effective BCM appropriate controls including insurance cover, can be difficult to recover from.

Current perceptions

Statistics show that a large proportion of the organisations sampled in our survey[1] have experienced a threat or incident within the last 24 months. Almost twice as many large companies anticipate a risk in the future compared to small and mid-sized organisations (SME)s, highlighting the need for crisis resilience for organisations that fall within this category in particular:

[1] http://www.ajginternational.com/news-insights/articles/news/2017/one-in-four-large-uk-firms-concerned-about-their-crisis-resilience/

Extortion & threats



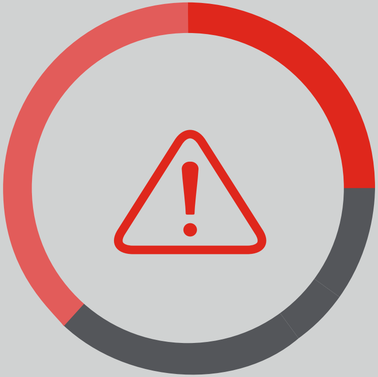
60%

see a risk in the future

38%

experienced in the last 24 months

Physical incidents



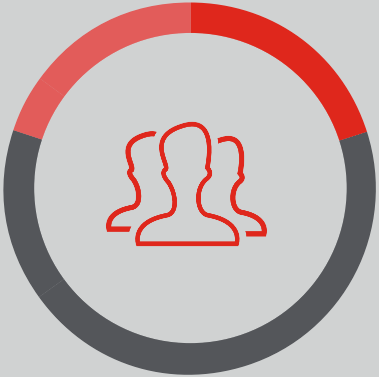
41%

see a risk in the future

25%

experienced in the last 24 months

People risks



20%

see a risk in the future

20%

experienced in the last 24 months

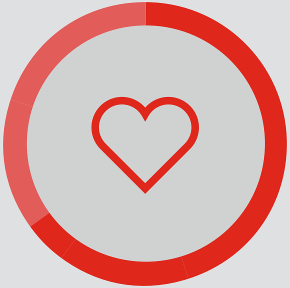
Duty of care

While the risk of an incident in the workplace is very low, the risk in the wider community is increasing, particularly in public spaces. Preparation and planning now might make all the difference.

Organisations have a duty of care to their employees, customers, stakeholders and the general public which is why they need prepare (as best they can) to satisfy their duty of care and take appropriate action to:

- Ensure all employees understand which colleagues control and are part of the Crisis Response team, and have relevant contact details.
- Maintain real-time information of colleagues' movements and provide them with an effective information flow regarding safety-critical issues.
- Ensure that employees update and maintain their own personal information and emergency contacts held by the organisation.
- Create a robust process and clear awareness of travel emergency response, including medical assistance information, evacuation and repatriation procedures, together with contact details.
- Manage accumulation risk exposures and insurance limits effectively – in respect of both travel arrangements and key office locations.

As the Manchester and London terrorist attacks in 2017 showed, no-one can become complacent when it comes to safety during a major incident. In Gallagher's 2017 survey on crisis resilience readiness, over two-thirds (68%) of respondents acknowledge they have a duty of care to employees – but that means a third did not.[2]



68%

of respondents acknowledge they have a duty of care to employees – but that means a third did not

[2] http://www.ajginternational.com/news-insights/articles/news/2017/one-in-four-large-uk-firms-concerned-about-their-crisis-resilience/

Understanding the risks to the organisation

The next step is to anticipate crises by creatively considering what threats the organisation may face. To ensure their resilience, companies should begin by conducting a threat and risk assessment, this is carried out as part of the Analysis stage of the BCM lifecycle, and is preferably undertaken with the support of a risk consultant or qualified insurance broker. This process will help an organisation anticipate and understand where its specific vulnerabilities lie. The risk assessment should include multiple components and cover a wide range of potential threat scenarios.

	Physical risk	Digital risk	Human risk	Reputational risk
Definition	Minimising business interruption risk	Minimising data loss or leak	Minimising loss of life or injury	Minimising damage to reputation
Impact on organisation	Denial of access Loss of revenue Costs for recovery/repair	Reputational damage Loss of customers Financial losses	Loss of resource Issues with PTSD	Financial losses Loss of customers
Analysis required	Calculate the impact and likelihood of low frequency, high-impact threats such as business interruption after a terrorist attack	Cyber security audit to determine, for example, the vulnerability of payment and online booking systems and the company's preparedness for a ransomware attack such as WannaCry	Calculate the impact and likelihood of low frequency, high-impact threats such as non-damage business interruption after a terrorist attack	Calculate the impact of a crisis on the brand and reputation, in particular from digital and human risk situations.
Data available to help anticipate threat	External security intelligence companies Social media International and local media Management information from the security team	Management information from the IT department/ CISO Social media Online digital vulnerability databases Cyber security company notifications and alerts	Management information from the HR department External security intelligence companies	Social media International and local media Management information from the communications team of the organisation Public Relations advisors and the press

Chapter 2: Prevent

Building a culture of resilience

Building a culture of resilience takes time and effort – it's not a quick solution, but it is a comprehensive one. Getting it right means more confidence and trust throughout the company and from stakeholders that risks can be prevented or responded to without damage to people, organisational operations and brand reputation.

By taking a comprehensive approach to resilience and putting plans in place that are regularly tested, most companies are able to reduce the total cost of managing risk. Insurance is an important part of the overall picture, but it is a big spend and may not cover the key risks a company might face and only helps with the recovery process, not resilience. By focusing more on anticipating, preventing and responding to risk, insurance can shift from centre stage and become just one part of a true culture of resilience.

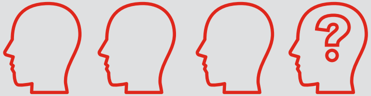
Most companies have some kind of insurance cover for threats such as terrorism and ransom, and they can point to business continuity, disaster recovery and crisis management plans. These are all important tools, but they provide a false sense of security if they are not joined up into a comprehensive plan of action.

That means achieving an appropriate balance between identifying, preventing and responding to risks and getting organisations back to normal. Crisis management plans should be short, principle-based and genuinely stress-tested to enable rapid decision-making and communication when there is a vacuum of information, panic and pressure from stakeholders on all sides.

Enterprise Security Risk Management and Enterprise Crisis Management fall within the wider remit of Enterprise Risk Management: like any element of ERM, an escalated approach to the identification, approval and review of risks contributes hugely to disseminating responsibility for crisis, security, continuity and resilience across the organisation. The graphic overleaf demonstrates how risk can be identified, consolidated and review at each level of the organisation.

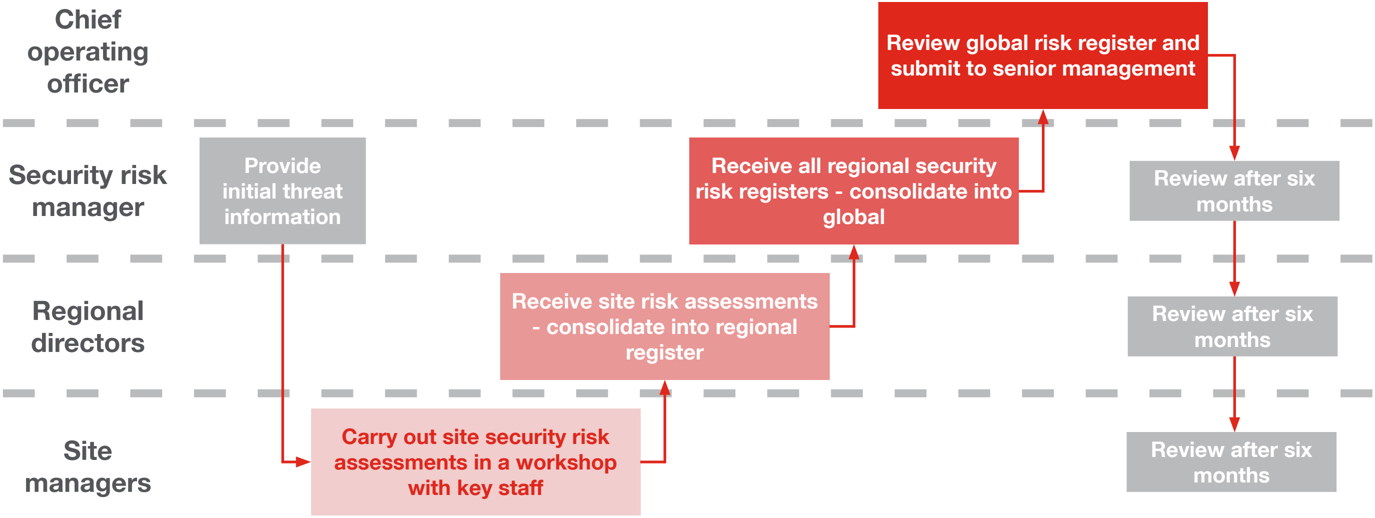
24%

Almost a quarter of respondents were concerned about their resilience or were not sure how resilient their business was



Source: Building a Culture of Resilience[3]

[3] https://uk.ajginternational.com/crisis-resilience-report/


Chief operating officer
Security risk manager
Regional directors
Site managers
Provide initial threat information
Carry out site security risk assessments in a workshop with key staff
Receive site risk assessments - consolidate into regional register
Receive all regional security risk registers - consolidate into global
Review global risk register and submit to senior management
Review after six months
Review after six months
Review after six months

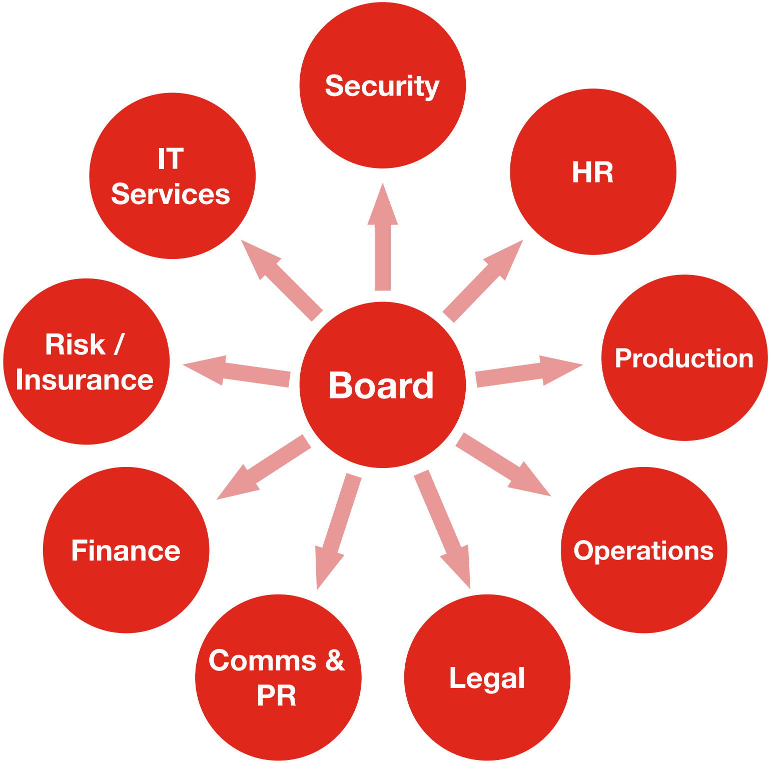
When forming part of an ERM programme, security risks should be presented at senior levels of the organisation alongside the range of other risks that the organisation faces (including health, safety and environment, sustainability, information technology, reputation and brand, and supply chain risk). Integrating the security risk management programme into a wider ERM framework will help the organisation 'compare apples with apples', and will prepare for a range of complex crises in a risk-led way.

> “Resilient organisations are discerning about risks they take; identify the importance of emerging trends; manage the impact and consequences (both beneficial and detrimental); cope with unexpected adverse events; rapidly bounce back stronger from a crisis; constantly adapt to change; and embed the lessons learned into their business enablers”
>
> Roads to Resilience, Airmic 2014

Roles and responsibilities within the organisation

In addition to incident response procedures, your organisation should have a crisis management team which is able to put strategies in place and make key decisions in crisis situations while carrying out a leadership role. Each member needs not only to be clear-headed and calm, but also equipped with the appropriate level of authority, experience and capabilities to carry out their roles.

The size of the team will vary depending on the size of your organisation but it should consist of a cross-section of top management and key organisational area representatives. As far as possible, the team should include the representatives of each key core function who might need to have a say in the process including:



If certain key functions are outsourced, for example, PR, Insurance and Legal, representatives from the relevant organisations should be present at each meeting of the crisis management team.

The team should be responsible for identifying issues, making decisions and implementing solutions as well as continuously reviewing the crisis response plan as a whole. They should also confirm and monitor the internal and external communications should a crisis occur, making sure that the information that is disseminated is consistent and coherent.

After an event they will be in charge of assessing the impact on operations as usual and ensuring that recovery begins as quickly as possible.

There are several characteristics of a great crisis management team:

- They have taken part in regular incident and crisis management exercises as a formed team
- They understand the strategy of their organisation
- They are action-oriented and consider their input into the wider conversation very carefully
- They represent Operations, HR, IT, Communications, Finance, Legal, Security (physical and digital), Risk and Production
- They have the complete buy-in of senior leadership
- They have the mandate to make decisions, engage with outside stakeholders and place accountability on other areas of the organisation to get things done
- They religiously adhere to a crisis management process to structure how they work together, without allowing this to limit their response options
- They understand the specific dynamics of risk to their organisation – without becoming mired in the technical detail

Implementing a strong crisis management strategy

- A consistent cross-departmental approach is required to ensure that the crisis management strategy that you introduce are understood and implemented. To achieve this you should:

Identify and agree:

- Critical organisational processes;
- Interdependencies between these critical processes and other parts of the organisation;

- Recovery priorities for these critical processes; and

- Minimum resources required for the recovery of these critical processes.

After this has been achieved you should:

Establish:

- Incident management and communication lines;

- Business continuity strategies;

- A plan framework, structure and content; and

- The roles of people and priorities to apply.

The better your people understand their roles and responsibilities and who they should report to if they have a concern, the more likely your organisation will be able to mitigate the risk of an incident.

Implementing safe travel policies

Every organisation should have a safe travel policy for business travellers. This should be split into sections including before departure, during the journey, on arrival, while travelling, during your stay and on departure.

You should objectively assess your travel management process: this should apply escalating measures to low, medium and high risk trips. The diagram below shows the types of activities that should be undertaken for each level of trip risk, and some key questions to ask of the entire travel management process.

	Key to all trips undertaken	Key to medium and high risk trips	Key to high and very high risk trips
Carry out a policy and procedure review to assess your existing planning and process	Access to online resources (such as country information) for useful and detailed travel advice	Carry out trip risk assessments based on trip details provided by travel teams or travellers: these should look specifically at the trip to inform the decision to travel, hotel locations, methods of travel, and timings of a trip	Identify specific risk reduction measures from the trip risk assessment: what security measures? What insurance?
	Carry out workshop training and review for all functional managers covering the trip risk assessment process		Senior leadership review and approval of high risk trips, and preparation for managing a possible crisis

Are you receiving notifications/keeping updated on high risk countries your travellers are visiting? Are these timely and detailed enough?

How are you keeping insurance coverage appropriate and consistent? Are your trip risk assessments focussed on the trip itself, not just the country?

Are you clear on when you should activate crisis management plans? Are you getting additional support for long term travellers?

Do you have operations room support in an emergency, if required? Is this already provided by insurance coverage?

Pre-departure

- Make sure that somebody in the office has a copy of your itinerary and contact details.
- Make photocopies of your passport, visas and tickets and keep them separate from your passport, wallet or purse.
- Know the laws of the country you are in and do not break them. Find out if anything, such as alcohol, is banned.

During the journey

- Travel in casual clothes. Do not wear expensive watches or jewellery, or use expensive luggage.
- Carry any sensitive information in your hand luggage.
- Do not use a business card as a luggage label, but do use your business address and phone number.

On arrival

- Arrange to be met when you arrive. Agree a discreet way of identification in advance to avoid the use of signs displaying yours or your company’s name. Confirm the credentials of the person who is meeting you.
- Only use an official and not an independent taxi.
- When you check in, do not disclose your occupation, company name, position, or the name of the organisation you are visiting.

During your stay

- Confirm your arrival to your office and call in regularly.
- Register with your national embassy if required.
- Only leave your passport at reception if required by law, and retrieve it as soon as possible.

While some of this may seem like common sense, it is important that all employees take the correct steps to ensure their safety while travelling to reduce the risk of assault, robbery, kidnap and ransom. These are just some of the things employees should consider while travelling. Your risk management and HR departments should carry out an assessment of the likely risks employees will face and provide suitable advice for your organisation’s individual circumstances.

Implementing natural disaster risk plans

Weather-related crises can be just as destructive as a security threat. They can interrupt trading and require a costly clean up, resulting in a significant loss to your organisation. While the UK is unlikely to experience a natural disaster on the scale of 2017's Hurricane Harvey or the fire damage experienced in California in 2017, flooding can also cause mass damage.

From heavy downpour to coastal flooding, water damage can occur in many ways and it is near impossible to anticipate when a flood will strike. You should double-check that you have the correct insurance in place to protect your organisation should it incur any damage as well as business interruption cover to help you get back on your feet.

As well as the correct cover, if your organisation is located in a high-risk area then a tried and tested flood response plan is also essential should a flooding incident occur. Providing your broker and insurer with a thoroughly prepared water risk response plan, as part of an effective BCM programme, helps demonstrate you appreciate the risk and can respond effectively. It may also enhance your risk profile for a potentially lower premium and may be a deciding factor in securing your cover in a marginal situation. A flood plan should include the following steps:

- Check your existing property cover for exclusions

- Listen to the weather forecasts daily or set up a severe weather warning so that you can prepare for flooding

- Have an evacuation plan and test it regularly – just like you would with a fire drill

- Allocate flood responsibilities such as turning off the electricity, alerting your insurer and speaking to customers and suppliers, making sure you know who is responsible for what

- Document your supply chain including critical vendors, contractors, partners, suppliers and customers

- Document your key equipment or machinery and identify contingency replacements

- Document your key information including finance, legal, banking, HR and insurance files

- Back-up your computer data and systems and store them off-site

- Make a contingency plan including alternative office locations and emergency communications such as a switch to mobile phones

- Communicate and test the plan so that everyone knows what to do and when
- Annually review the plan and revise it where it is no longer relevant

Cyber resilience healthcheck

As a starting point, we recommend you complete the checklist overleaf. Whenever you have answered ‘Yes’ to the questions in bold you may have an exposure. If you have answered ‘No’ to these questions there is less likely to be an exposure so, provided that you are confident in your answer, you can move on and ignore the questions under that heading.

In May 2017, the WannaCry Ransomware virus infected thousands of computers, preventing affected users from accessing their data until a ransom was paid. This included Nissan, FedEx, and critically, the NHS where staff were unable to access patient’s test results, X-rays and records and as a result operations and appointments were cancelled. The amount collected globally was less than $75,000 and it is suspected the impact on the NHS was unintentional. Yet whether or not the hackers intended to cause this damage, out-of-date software allowed the virus to spread at a rapid pace, reinforcing the importance of regularly assessing and addressing any cyber risks.

Heading	Exposures		
Loss or theft of employee or customer information from organisation's computer systems Compliance with the requirements of the General Data Protection Regulations (GDPR)	Do you keep employee or customer information electronically?	Yes	No
	Are customer credit card or bank details kept on your systems?	Yes	No
	Are these details encrypted?	Yes	No
	Do you have an IT policy in place regarding the handling of this type of data?	Yes	No
	Do you have a stable finance team?	Yes	No
	Do you use temps in your finance team?	Yes	No
	Do you update security software as soon as advised?	Yes	No
	Do you have a privacy policy in place governing your collection of private data?	Yes	No
	Are there automated checks and audit trails built into the financial systems?	Yes	No
	Do new supplier bank details need FD approval?	Yes	No
	Are checks made monthly on funds leaving the organisation's account?	Yes	No
	Are there flags set to highlight where and when donor information leaves the system?	Yes	No
Spoof websites - establishment of websites that may look and feel just like yours, but is taking funding away from you	Do you operate a website?	Yes	No
	Do you regularly check for spoof websites, e.g. using Google Alerts?	Yes	No
	Do you have a process in place if someone reports a spoof website?	Yes	No
	Have you discussed what to do with spoof websites with the police?	Yes	No
	Have you discussed what to do with spoof websites with your Internet Service Provider?	Yes	No
	Have you been successful in identifying spoof websites to date?	Yes	No

Heading	Exposures		
Denial of service attacks on websites - resulting in you being unable to collect payments, issue sales invoices, or just provide information to your customers, employees or suppliers	Do you operate a website that provides you with an income or provides your customers with assistance?	Yes	No
	Are you PCI compliant?	Yes	No
	Do you have someone monitoring your website for attacks?	Yes	No
	Do you have a process in place if your website is attacked but the attack is not successful?	Yes	No
	Do you have a process in placeif your website is successfully attacked/corrupted?	Yes	No
	Have you discussed what to do with your Internet Service Provider?	Yes	No
	Have you discussed what to do with the police?	Yes	No
	Is there an established recovery process?	Yes	No
	Has the recovery process been successfully triggered before?	Yes	No
Loss of supporter data by third party suppliers/partners - whether by human error or deliberate act and the release of personal information to your supporters.	Do you permit data to leave your system?	Yes	No
	Do you ghave a contract with a third party that clearly defines what they can and cannot do with your data?	Yes	No
	Do you conduct due diligence to ensure that the contract is being complied with?	Yes	No
	Are you certain that third party staff are well trained on data protection?	Yes	No
	Are you certain that third party staff are all employed and not temporary in nature?	Yes	No

Chapter 3: Respond

Your organisation and people must be empowered with the tools needed to respond in the event of an incident or crisis. Ensure you and your people can respond effectively to any security crisis through training and awareness, coordinated crisis management planning and appropriate insurance cover. All employees should know their roles and responsibilities should a crisis occur and plans should be tested regularly to help reduce panic. Organisations should take a cross-departmental approach where functions such as risk, HR, security, finance, communications, legal and IT work together to understand, prevent and respond effectively to the broad range of threats and risks that exist. Risks need to be modelled realistically and managed well. Educate your people on how best to recognise and respond in a crisis. Your incident and crisis management team should coordinate training in areas such as:

- **Evacuation** – the orderly 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 e.g. a bomb threat nearby, toxic fumes in the air.

- **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. 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 incident and crisis response experts should be carried by coordinators at all times. Response is also where the value of your people training will become clear.

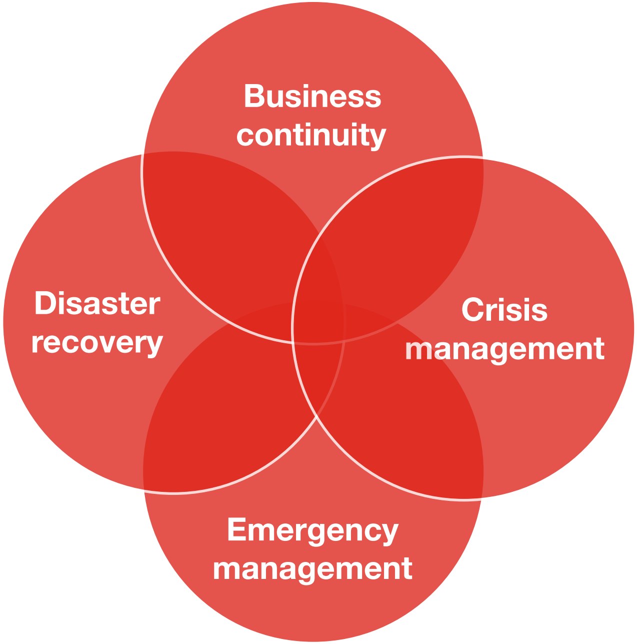
In most cases of terrorism, the 'run, hide, tell' advice of the UK's counter-terrorism police should be followed.

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.

Tools to manage in the event of a crisis

In the event of a crisis, it is important to have a well-rehearsed plan in place which provides guidelines on how to respond to potential threats. With so many varying threats, it is clear that one plan will not be suitable for every circumstance which is why you need to have a number of different plans in place which respond to varying levels of severity.

The key plans you should have in place are:



Business continuity	Crisis management	Emergency management	Disaster recovery
This type of plan aims to anticipate and reduce the risk of an event before it happens. It is normally made up of a number of different approaches including crisis management plans and insurance. The overall aim is to understand how this can impact your organisation and provide a clear method for dealing with potential threats.	Crisis management plans outline how the organisation will respond in the event of a major crisis such as a terrorist or cyber-attack. These events can have considerable impact on your organisation, stakeholders and the public and if poorly dealt with, can incur significant financial and reputational damage.	Emergency management planning outlines ways to coordinate and manage the first response team should an incident or crisis occur. This includes how to staff an emergency response team including how to assess potential performance, how to plan emergency arrangements and how to train your chosen staff.	This plan takes place after an event occurs and is designed to assess what has happened, how it could be prevented in future and how the organisation can get back on its feet.

For each plan you should use the four pillar ‘Anticipate, Prevent, Respond and Recover’ process, taking the time to identify any gaps and ensure that these are accounted for. Once again, each plan should be regularly tested so that everyone is aware of their responsibilities and adapted if it is no longer fully relevant.

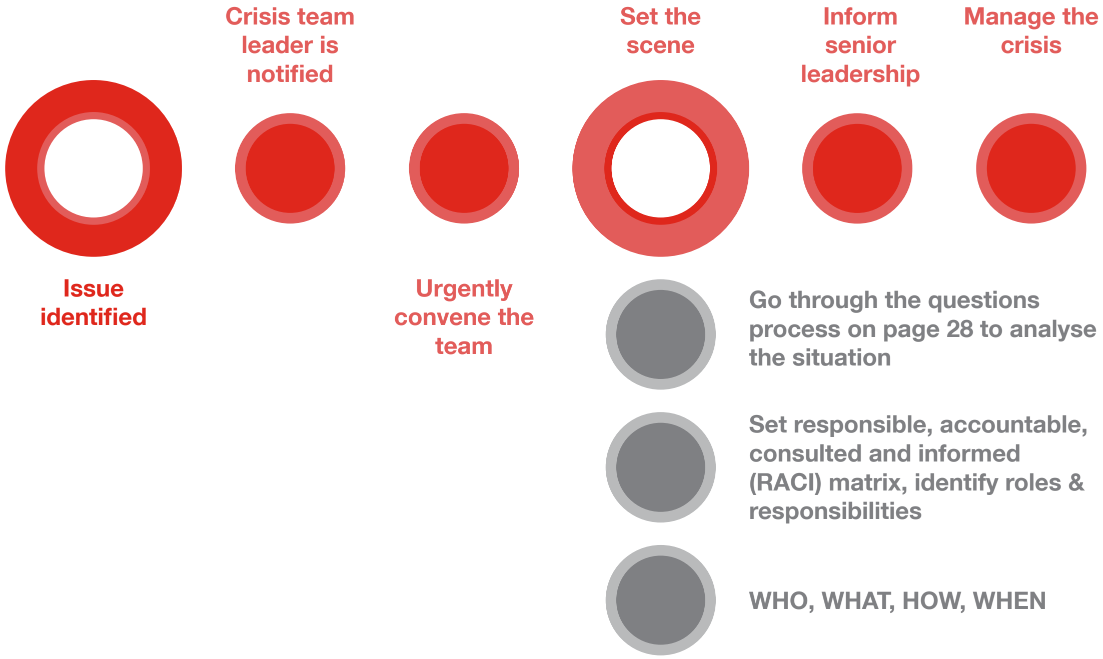
"Communicating internally during an incident can be one of your biggest challenges if you have not considered all of the options and made adequate preparations. Many of the tools you would use to find contact details and send messages will be missing or severely impacted. It's essential you know how to make contact with key people and prepare in a way that's right for your organisation and its culture.

Your communication planning needs to articulate in detail how this will work in practice for the crisis management team as well as how to cascade messages across the organisation in a clear, consistent way. By discussing, documenting, regularly updating and testing this process, you will save time, energy and valuable resources during a time of crisis. Issuing regular communications internally, even when there is seemingly no "new news" will help to maintain a sense of calm, especially when people feel disconnected during an incident, and will allow your crisis management team to focus on other concerns."

Global law firm

The immediate crisis response process

Once the plans have been formulated, the following process should be enacted at the beginning of the crisis and followed through. The diagram below shows how the initial issue which causes the crisis is communicated, and to whom, during its early stages.



Issue identified

Crisis team leader is notified

Urgently convene the team

Set the scene

Inform senior leadership

Manage the crisis

Go through the questions process on page 28 to analyse the situation

Set responsible, accountable, consulted and informed (RACI) matrix, identify roles & responsibilities

WHO, WHAT, HOW, WHEN

Once the Crisis Management team has been convened it should begin to answer some key questions to inform decision-making: this is the point at which teamwork, and the dynamics of the group, will have an important impact on the quality of the outputs and, to a great extent, the overall management of the crisis.

Strategy

How could this issue damage the organisation's strategy

Priorities

What are the priorities of the organisation and crisis management team?

Evidence

What evidence do you have that you know to be correct?

Scoping

Establish the best case, worst case and most likely scenarios

Hypothesis

Identify your hypothesis of what might have happened

Next steps

Identify all the immediate actions you need to take

Audiences

What audiences need to hear your message? How is it tailored?

Messaging

What's the message of the organisation to these audiences?

These analytical questions serve to create four sets of work streams – when put together, they form the core of the roadmap to manage the crisis in a dynamic and pragmatic way. The complex and rapidly changing nature of a crisis means that it is not easily managed using long, verbose plans developed in advance: training and exercising the crisis management team, and carrying out one-on-one mentoring with crisis team members, will ensure they have the confidence to use this analytical process to identify the activities which will have the greatest positive impact on the situation at hand.

Decision points

What decisions still need to be made?

What dependencies?

Who makes the decision?

Actions

What can be done now?

Who does it?

Who resources?

Information

What do we not know?

Who do we know?

Do we have this information yet?

Messaging

What are we saying?

How should this change?

Different for which stakeholders?

Natural Instincts in a Crisis

“Survival training isn’t so much about training people what to do – you’re mostly training them not to do certain things that they would normally think to do,” says John Leach, a psychologist at the University of Portsmouth who survived the King’s Cross fire disaster in 1987. He estimates that in a crisis, 80-90% of people respond inappropriately.

In a disaster, the speed at which we think through our options goes from bad to worse. The brain’s first port of call is to flood with the “feel good” hormone dopamine. This may seem counter-intuitive, but though it’s usually associated with reward pathways, dopamine also plays a crucial role in preparing the body to face danger. It triggers the release of more hormones, including adrenaline and the stress chemical cortisol. And this is where it gets messy.

This cocktail of hormones shuts down the prefrontal cortex, which sits behind the forehead and is responsible for higher functions such as working memory. Just when we need our wits the most, we become forgetful and prone to making bad decisions.

If we can’t rely on our natural instincts, the best way around the mental fallout is to replace unhelpful, automatic reactions with ones that could save your life.

Extracts from an article by Zaria Gorvett 12 July 2017
http://bbc.com/future/story/20170711-what-not-to-do-in-a-disaster

Tools and technologies in action

There are myriad tools and technologies available to assist modern crisis management teams: some of them high tech (such as social media monitoring platforms or shared incident reporting) and some of them low tech (such as whiteboards, posters and pens). A good crisis management set-up should have a mix of these – the only commonality is that any tool should:

- Have a purpose in the overall crisis management plan;
- Be suitable to the organisation's structure and culture;
- Be trained into members of the crisis management team and their supporting staff.

Any crisis management team should have tools prepared to answer the following questions – attempting to come up with ways of working in the middle of a complex incident will only distract from the objectives at hand.

- How are we going to record information in the room?
- How will the team interact with each other?
- How will we communicate securely across the organisation?
- How will we take account of our people?
- How will we communicate and monitor on social media?
- How will we disseminate actions across the organisation in support of crisis management?
- How are we going to escalate to senior leadership or specific functions?
- How will we get access to specific organisational IT systems?
- How are we going to record and preserve evidence which could be needed in court or by the police?

Use the above questions as a tick-list when assessing tools or technologies: how many of these questions does the tool or technology answer? What would be the return on investment given the cost of the tool or technology? If you begin looking at multiple tools or technologies which would have to be used in parallel, ensure there is some kind of interoperability – but this doesn't always have to be technical. A whiteboard will work just fine with a social media monitoring platform, it just means some human effort might be required.

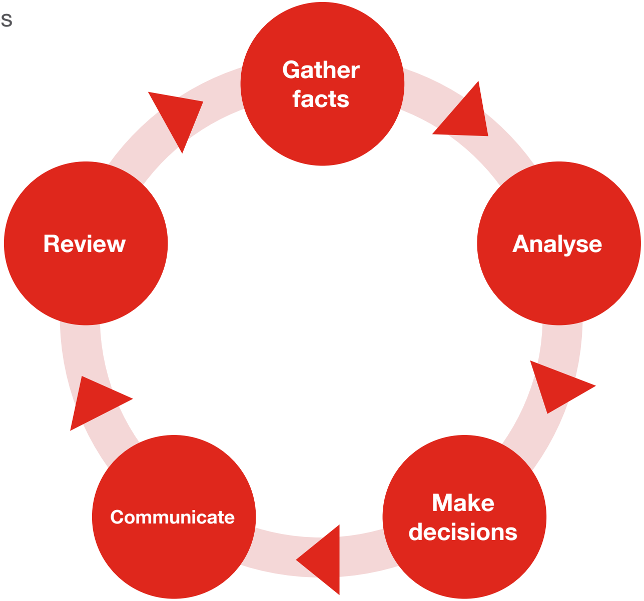
When considering technology solutions it's also critical to assess their resilience: if there is no internet access, for example, how would it be used? Such technologies should always fit into the organisation's broader disaster recovery arrangements.

Media and crisis communications process

In the London terrorist attacks in 2005, mobile phone networks were closed to the public as part of the Metropolitan Police emergency response. That means organisations should also look to other media for their communications channels as part of their response plans to arrange for employees to either request assistance or 'check in' as safe.

An up-to-date list of contacts should be compiled and maintained to ensure that prompt contact with the right people is made in a time of need including:

- Customers (wholesale/retail)
- Transportation companies
- Security Management Consultants
- Crisis Public Relations
- Product Safety specialists
- Laboratory Analysts
- Trade bodies
- Health & Safety Executive contacts
- The Press



Social media impact and uses

Details of the incident emerging on social media from members of the public can have a detrimental impact on how the Crisis Management team navigates the issue, escalate it further and cause longer lasting reputational damage. For much of the 20th century a crisis was managed ‘at the speed of sound’: traditional media such as print, television and radio broadcast snippets of news at easy to expect intervals. Teams had more time to prepare cohesive statements, competently link their message to actions already being taken, and generally had a better understanding of how to engage with a far smaller number of journalists and commentators which set the overall news agenda.

Crises now play out ‘at the speed of light’ and often in public view.

Communications are transmitted globally in a fraction of the time and form part of a constantly evolving storm of opinions, conversations and conflicts which can temper or inflame the message which has been carefully crafted by a crisis management team. Social media can also create new components to the crisis, or transform existing problems faster than an organisation can effectively deal with them.

Conversely, social media is also likely the greatest crisis management tool ever developed. It has democratised the way in which brands can engage with millions of customers, stakeholders and influencers. There's no excuse for a crisis management team to shy away from utilising this tool to tailor its crisis response and spread its message to a much wider audience than was possible previously.

The social media response to a crisis falls into two phases: the 'initial spike', and the 'long tail'.

Phase 1: The initial spike

A social media component to a crisis isn't always guaranteed. Many serious issues faced by organisations remain intensely private and may never generate any media interest: kidnaps are a good example of this. But when the crisis does hit the mainstream news the social media response is almost always immediate.

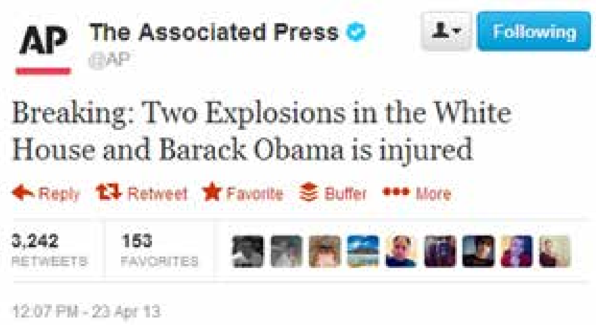
The 'initial spike' is the period where the crisis is under an intense spotlight. Thousands or hundreds of thousands of social media posts per hour relating to the brand and the issue at hand overwhelm corporate communications teams and muddy the already difficult task of navigating the complex issues surrounding a crisis. This is the period in which missteps can have significant initial consequences, and publicly traded companies experience sharp initial drops in share value in a knee-jerk reaction by markets.

The 'initial spike' is characterised by:

- An exponential increase in social media chatter involving the organisation.
- A period of between 12-36 hours.
- Widespread misinformation regarding the crisis, the organisation and its response.
- A very pronounced 'peak' after which social media engagement drops precipitously.

This period does, though, present some key opportunities that any well-trained crisis management team should take advantage of. The vast amounts of information generated on platforms such as Twitter and Facebook can be used by the team to better understand the scope and nature of the crisis it’s facing: physical security incidents, for example, begin to be documented in almost real time through videos, images, eyewitness accounts and live streams. Similarly, this information can be used to tailor the response to reputational crises by understanding popular grievances against the brand.

The two images on the right demonstrate the power of the initial spike: in April 2013, an Associated Press Twitter account was compromised and the attacker used this access to post a false report of an attack at the White House. The reaction was immediate – the tweet was shared thousands of times, and major stock markets like the Dow Jones went into freefall until the situation was resolved.

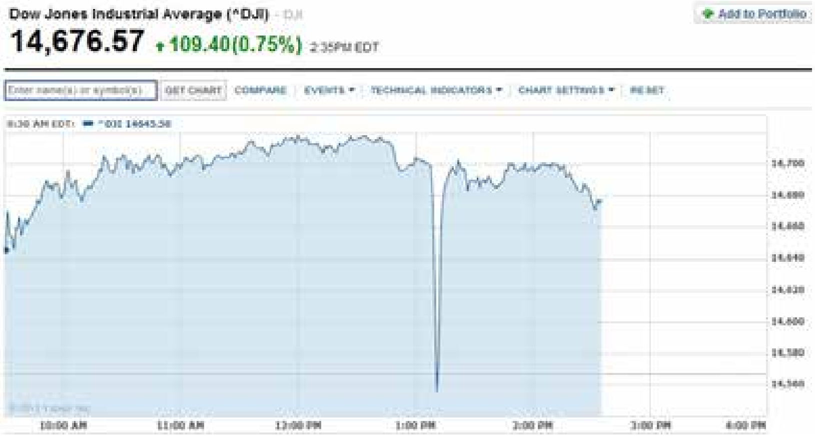


AP The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

3,242 RETWEETS 153 FAVORITES

12:07 PM - 23 Apr 13



Dow Jones Industrial Average (^DJI) - DJI

14,676.57 ↑109.40(0.75%) 2:35PM EDT

Crisis management teams should look to do the following during the ‘initial spike’:

- Ensure that there is a dedicated social media monitoring team that can provide two inputs into the overall process:
    - Specific, operational information sourced from social media (such as eyewitness accounts).
    - An analysis of sentiment (positive, negative, indifferent) towards the organisation and its response, and a summary of popular opinions and grievances which can be used to tailor social media messaging.
- Make social media a key pillar of the corporate communications strategy, and provide regular updates on how the crisis is being proactively managed and what actions are being taken to remedy the problem.
- Ask staff not to share their own inputs or opinions on social media to ensure this doesn’t dilute the message of the crisis management team, and also to avoid a member of staff’s opinion being taken as fact or an official statement.

Phase 2: The long tail

The ‘initial spike’ drops off as quickly as it appeared. Online communities move onto new topics of discussion, the market self-corrects shareholder value, and the news cycle begins to be dominated by other international events. What is left is the ‘long tail’.

In many ways, this period can be the most damaging to an organisation’s reputation, credibility and value in the long term. The ‘long tail’ is a period of heightened interest in the organisation and the issue at hand: social media chatter is not as high as the ‘initial spike’, but it remains at consistently elevated levels for a period of two weeks to one month. This is the phase in which investigative journalists will begin to probe and analyse the response to the crisis and the organisation’s successes and failures: this is where the real judgement begins to take place, and key stakeholders such as investors, suppliers and large B2B customers form lasting opinions of the organisation.

The ‘long tail’ is characterised by:

- Consistent and elevated social media interest in the organisation.
- A reduction in misinformation being shared as influencers such as journalists provide greater context.

- Greater damage being done by leaks from the organisation, possibly outlining a poor or botched response to a crisis.

- Connections being made between the recent crisis and previous actions or decisions taken by the organisation which contributed to or exacerbated the issue.

- The formation of long-term opinions and judgements as to the efficacy of the organisation’s response to the crisis.

This is also the period where organisations experience a false sense of security, as at face value it seems the crisis has ended, and so neglect ongoing social media crisis management activities which could have a real effect on long term opinions. This is the time to be proactive even though overall social media engagement has reduced.

Crisis management teams should look to do the following during the ‘long tail’:

- Provide clear direction on the organisation’s message regarding the crisis itself, and its response to it.

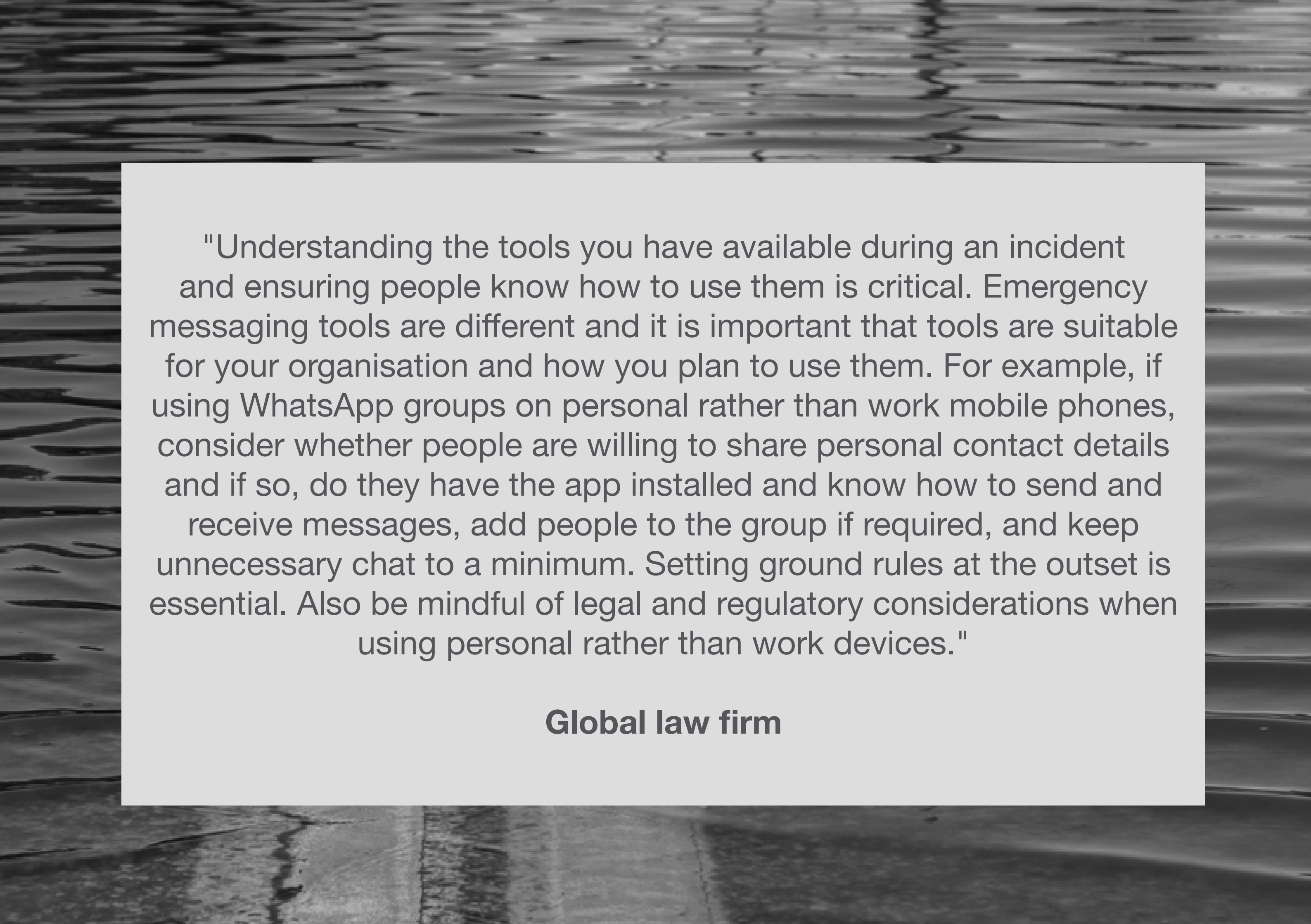
- Ensure there is very close liaison between social media teams and crisis/corporate communications to ensure everyone reflects that message accurately.

- Continue taking concrete actions which can be shared on social media to reassure stakeholders that the organisation isn’t neglecting post-incident responsibilities.

- Begin internal investigations and lessons-learned processes to identify the root causes of the crisis and the effectiveness of crisis management actions.

- Share selected findings from post-crisis investigation and be open and candid on social media about what may have gone wrong, why, and how it will be remedied.

- Engage very proactively from organisational social media accounts with ‘influencers’ who are still discussing and analysing the crisis.



"Understanding the tools you have available during an incident and ensuring people know how to use them is critical. Emergency messaging tools are different and it is important that tools are suitable for your organisation and how you plan to use them. For example, if using WhatsApp groups on personal rather than work mobile phones, consider whether people are willing to share personal contact details and if so, do they have the app installed and know how to send and receive messages, add people to the group if required, and keep unnecessary chat to a minimum. Setting ground rules at the outset is essential. Also be mindful of legal and regulatory considerations when using personal rather than work devices."

Global law firm

We have identified three crises to demonstrate the characteristics of social media response.

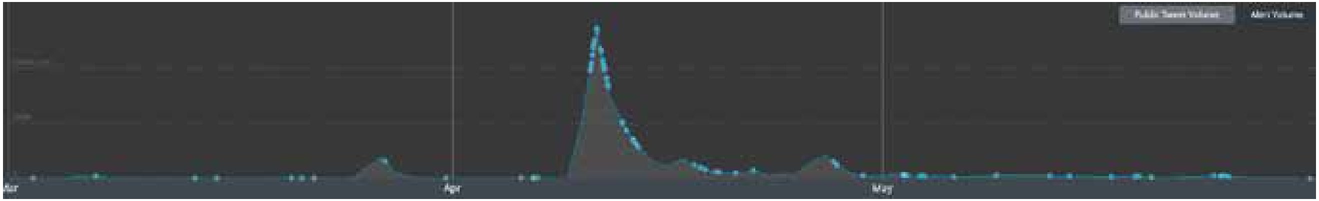
United Airlines – 9th April 2017

A passenger became injured and bloodied after he was dragged from his seat by airport police before a flight departed from Chicago to Lexington, Kentucky. A video of the incident involving the passenger, David Dao, was captured on a video phone by a fellow passenger. The video rapidly went viral and tapped into a broader frustration with major airlines, suspicion of the actions of large corporates, and anger over the actions of isolated law enforcement officers in other parts of the United States.

It was obvious the incident had escalated into a corporate crisis, and United began to experience the power of social media – both the difficult to control 'initial spike', and the even more damaging 'long tail' phase.

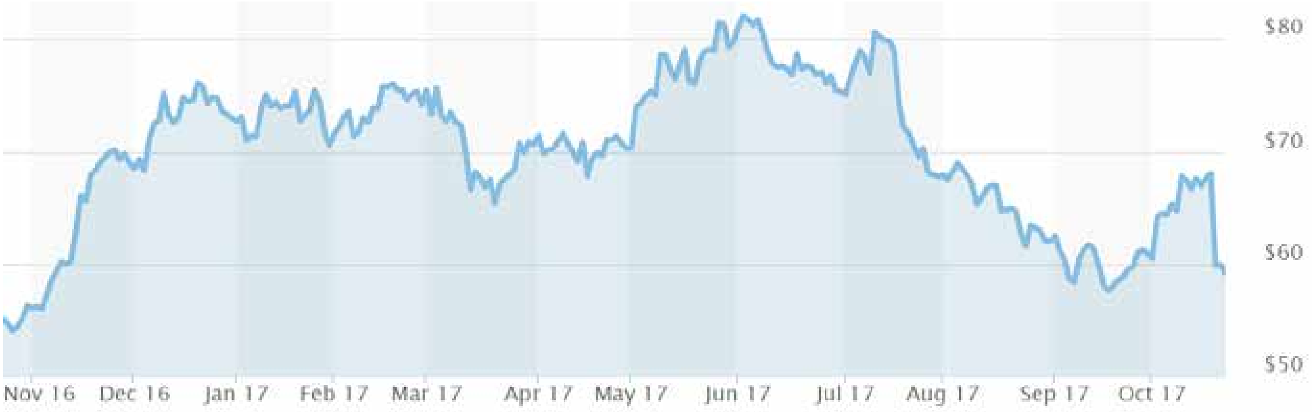
Social media activity:

The graph below shows all Twitter activity one month before and one month after the United Airlines incident, where one high activity peak can be identified and a subsequent three week period where there was heightened social media engagement compared to the norm.



Share price activity:

The graph below indicates how incidents have both short and long-term effects for company's share prices. There was a temporary steep decline in United Airline's share price directly after the incident, though the price soon returned to previous levels within a fortnight, after United laid out fresh plans to shift the policies and culture of the company. However, the graph also shows longer term effects on the price of shares as analysts discovered United was falling short of promises made by management post-incident.

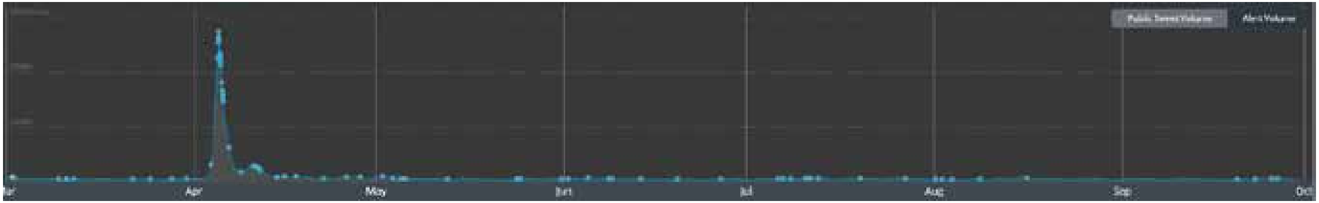


PepsiCo advertisement – 4th April 2017

PepsiCo released a video advert starring Kendall Jenner in April 2017, sparking controversy as it was widely criticised for appearing to trivialise pro-social justice demonstrations and being insensitive to the ongoing Black Lives Matter movement. This is a good example of a purely reputational crisis which was inflamed as influencers began to link PepsiCo's actions to the ongoing, and highly politicised, issue of civil disobedience in the West.

Social media activity:

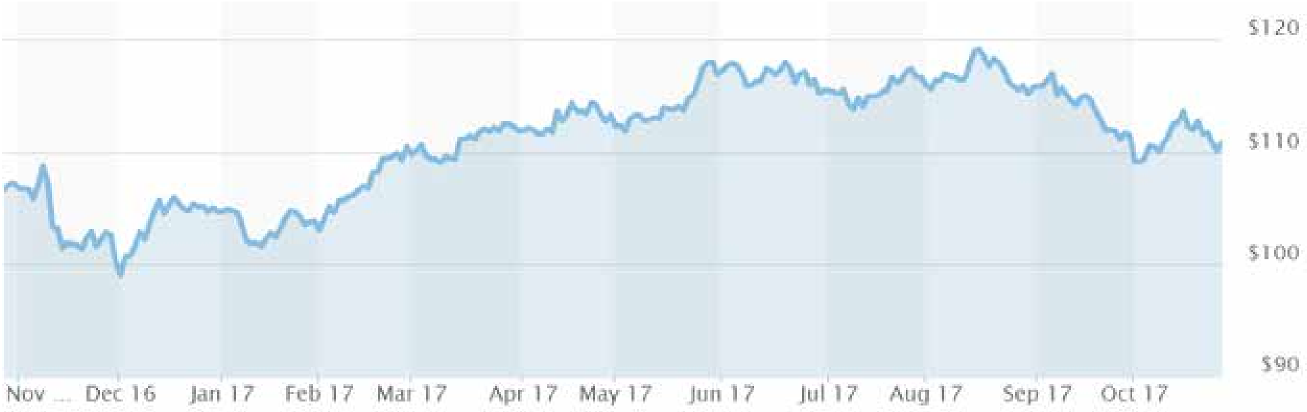
The graph below shows all Twitter activity one month before and four months after the Pepsi advertisement, where one initial spike of high engagement can be identified.



Share price activity:

Pepsi's share price fell slightly in the immediate aftermath of the advertisement's release in April and social media backlash as the markets experienced a knee-jerk reaction to the news. At the end of May PepsiCo Inc were in talks to acquire All Market Inc, causing a related spike of its share price. From this point on the company's value can be seen to fluctuate, until it reached a peak during mid-to late August. On 4th September, Kendall Jenner broke her silence about the advertisement saying, "It feels like my life is over". This brought the topic back into the media and initiated a fall in share prices directly after.

This is another good example of a company's focus on the 'initial spike' on social media which precipitated the crisis in the first place, and was broadly successful, but suffering greater damage in the 'long tail' phase.

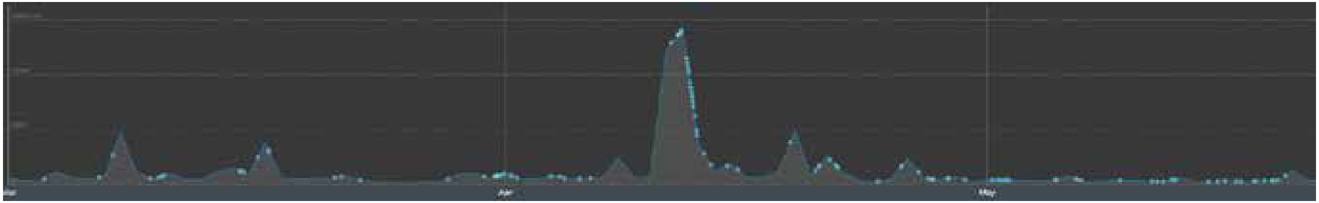


Borussia Dortmund – 11th April 2017

At approximately 7pm local time the Borussia Dortmund football team were traveling to their home Champions League quarter-final match in Germany against Monaco when three explosive charges detonated, injuring one policeman and player Marc Bartra. A Russian-German man was arrested ten days later and accused of carrying out the attack to cash in the inevitable drop in the club's share value. In the hours before the attack the suspect had bought 15,000 'short stock' options for the team, effectively betting on a drastic fall in price.

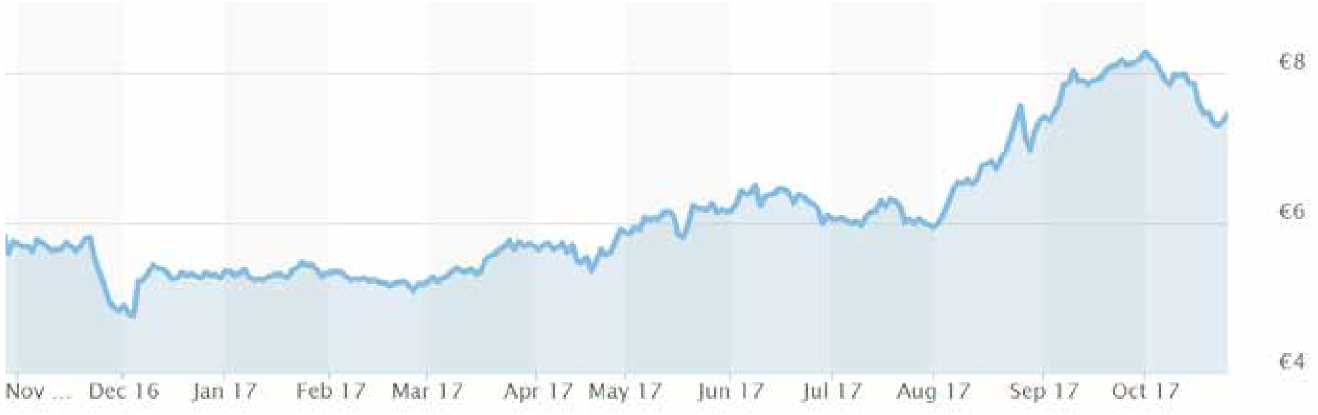
Social media activity:

The graph below shows all Twitter activity one month before and one month after the Borussia Dortmund incident, where one high activity peak can be identified (the 'initial spike') and several smaller subsequent peaks which would constitute the 'long tail'. The initial social media interest in this case stemmed from its connection to football, a professional sport with high levels of social media engagement, and the 'long tail' was generally focussed on the unusual motive of the attacker and did not damage the club's long-term reputation.



Share price activity:

The bombing had the outcome the assailant had hoped for in that it caused an immediate drop in the price of the team's shares. However, after the suspects arrest and news emerged of his motive, the price of shares rose once more to pre-attack levels. The Borussia Dortmund bombing is a unique case: the explicit objective of the attack, to cause a long term drop in the club's share price, meant that it ended up having the opposite effect. The club experienced a surge in solidarity and the bombing had very little long-term effect on shareholder value.



After the Borough Market attacks in London 2017, Cannon & Cannon butchers said that the stock, trade and employment damages they have occurred as a result of the attack were around £30,000. As their head office is located in Borough Market they were unable to trade and as a result they have lost one of their largest supply contracts – potentially putting their entire organisation at risk.[4]

When events do happen, a key goal is the swift return to business-as-usual as far as possible, by use of effective BCM. 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.

Dealing with business interruption

While many organisations have some form of terrorism or crisis resilience cover in place, they are often unaware that it may not extend to losses from business interruption such as those incurred after the Borough Market terrorist attack in July. This is why it's important to have an insurance policy which protects against non-damage business interruption, where an organisation cannot trade due to an event which is not situated directly on

[4] http://www.insure24-7.co.uk/terrorism-insurance-cover-vital-businesses/

their premises.

Most companies recognise its importance, with our survey[5] indicating that 82% of respondents considered BI to be the most important insurance to have in the event of a terrorist attack. For many organisations, however their BI insurance is not adequate. Property and BI policies generally exclude the risk of terrorism and will not respond if the loss is caused by a terrorist act.

Companies need to arrange separate cover specifically for terrorism, but calculating the correct sum to insure can be difficult, with many organisations struggling to get this right due to lack of understanding, poor advice, a desire to save premiums and, often, the belief that it will not happen to them. When calculating insurance gross profit figures, risk managers need to give proper consideration to what costs can be excluded.

Organisations need to ask themselves some serious questions – will they let employees go after a loss and then re-recruit when the organisation is back up and running? Is their indemnity period appropriate, not just to recommence trading but to get back to the same position as before the loss? Organisations may not consider themselves to be at direct risk of a terrorist attack, but they should consider whether they are in the vicinity of a potential target or customers or suppliers to a potential target. If the answer is yes, then they are automatically at a higher risk than they might have thought.

Reviewing plans and processes

While we have discussed this at numerous points through this guide, we cannot stress the importance of developing a programme which responds to a number of different eventualities from risk management to crisis response to recovery. This is not a one-off task; it should be reviewed regularly and edited wherever responses are no longer relevant. The plans should be tested regularly so that should the worst happen, each employee knows their responsibilities and is able to respond in as cool and calm manner as possible. Being prepared and introducing a culture of resilience can make all the difference in case of a crisis.

The role of leadership

As the above information demonstrates, crises can have a significant and sudden impact on a business and so it is crucial that the leadership team deals with these in a timely, informed and objective manner. Whether the “leadership” in a crisis situation comes from the business’ executive leadership team or its crisis management team, it is their role to ensure:

[5] http://uk.ajginternational.com/crisis-resilience-report/

- Plans are in place to, as much as possible, avoid a serious crisis situation, and that all employees are aware of the business continuity and emergency procedures to follow.

- Crisis communications procedures are followed in a timely manner and that all key parties have a thorough understanding of the situation at hand and are therefore able to respond consistently and appropriately.

- Decisions, however complex or stressful, are made and are based on all information available at the time thus removing any potential bias, assumptions or premature actions.

- Strategies, objectives and processes put in place by the crisis management team are followed in each crisis situation, are informed by a cross section of the business and are reviewed on a regular basis.

- Decisions and actions are recorded and reviewed post-incident.

Decision making in a crisis can be extremely challenging and can have serious negative psychological effects, so preparation and training are vital in providing leaders with the tools and techniques needed to make informed, strategic decisions in a situation characterised by uncertainty.

Business Interruption Insurance

You can purchase a Business Interruption policy that insures against loss of profit and increase in cost of working / higher overheads resulting from, for example, fire, storm damage or machinery breakdown. Most Business Interruption policies will include increased cost of operation to provide reimbursement for additional expenditure incurred by you in order to avoid or reduce a reduction in turnover following an insured event. You will need to identify the extra costs that could arise and also determine how long it will take you to get back to business as usual. Finally, you will also need to think about whether all of your customers will return immediately when you get back to normal operation. Losses can seriously disrupt cashflow, and your insurance arrangements will need to provide appropriate protection.

Additional cover is available to protect interruption to your business due to supply chain disruption.

EXPLAINED: Buying insurance and buying business insurance - an Airmic Guide 2016

Office flood – getting the basics right

Pre-planning, rehearsals and great communication and collaboration across business units proved to be key to managing a major flood at a Central London office.

Having key empowered individuals managing the incident and recovery led to a successful outcome

A UK based retailer who has head office facilities in central London suffered a major flood in the basement area of one of their offices - the basement being occupied as office space

The retailer had plans in place for incident reporting, communications and response which ensured that the matter was escalated quickly with local management empowered to make immediate decisions to secure the site, make safe and have operations transferred to one of the retailer's other London offices.

This transfer was possible because of pre-planned contingency arrangements with 'hot desking' and technology solutions which allow flexibility of managed space within the portfolio of the retailer's premises within the Capital.

Emergency contractors and 'salvage' teams were immediately enlisted with the cause of the water ingress quickly identified. Communication with affected colleagues was quick and efficient due to up-to-date contact information and practiced 'call tree' exercises.

The business was not interrupted in any noticeable way and recovery back to normal operations was speeded up due to pre-planning, excellent collaboration across internal and external teams and tasks being understood and actioned without fuss and with full knowledge and backing of senior management.

The internal insurance team was at the hub of the recovery communications and actions with early notification to the premises landlord and identification of the party responsible for causing the water damage - so the costs were minimised and substantially recovered from other parties.

The individuals leading the 'on the ground' emergency and recovery work and the insurance department personnel involved were all experienced incident managers who knew what to do, where to go for assistance and the routes to solving problems – all with clear goals, namely; minimum disruption, clear communication to all and minimum cost.

Conclusions

Recent events have proved that the world can be a dangerous and unpredictable place. From Las Vegas to Barcelona to Manchester and London, indiscriminate terror attacks are increasingly becoming the norm and new technologies mean that anything including vehicles and homemade explosives can be used to incite terror. No organisation should shelter under the misconception that they are too small or unlikely to be targeted, as many attacks are indiscriminate.

It is a sad reality that these fast-evolving security threats can impact organisations of any size, sector or geography and while the greatest risk exposure does come from terrorism, it is actually non-damage business interruption which can wreak the most havoc 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.

This doesn't mean that your organisation cannot reduce the risks you face. Your organisation needs to be resilient and adaptable to today's threat environment and while insurance is a key part of this, so is a robust risk management scheme teamed with a culture of resilience. You should work to anticipate threats wherever possible and put measures in place to help prevent them occurring. In the event of a crisis you should have a plan to help your employees to safely respond to the threats they face including emergency management and evacuation procedures. Finally, you should have a recovery plan in place to help your organisation back on its feet after a crisis and to help your employees recover from any emotional trauma following the event.

In conclusion, a tried and tested risk management plan such as the 'Anticipate, Prevent, Respond and Recover' strategy can help your organisation to save lives and ensure that you can respond and safeguard those to whom you owe a duty of care.

Bibliography and other useful resources

- BS65000: Guidance on organizational resilience. British Standards Institution – 2014
- BS11200: Crisis management – guidance and good practice. British Standards Institution – 2014
- Roads to Resilience – Building dynamic approaches to risk to achieve future success – A report by Cranfield School of Management on behalf of Airmic – 2014
- Roads to Ruin – A study of the major risk events; their origins, impact and implications A report by Cass Business School on behalf of Airmic – 2011
- Building a Culture of Crisis Resilience – A report by Gallagher, in conjunction with YouGov – 2017
- BCI Good Practice Guidelines 2018 edition: The global guide to good practice in business continuity – Business Continuity Institute – 2018
- EXPLAINED: business continuity management – Airmic 2017
- EXPLAINED: risk and managing risk – Airmic 2018
- Travel risk management Guide – Airmic 2017
- EXPLAINED: buying insurance and buying business insurance – Airmic 2016
- GDPR Guides – Airmic 2017 and 2018

airmic

6 Lloyd's Avenue
London
EC3N 3AX

Ph: +44 (0) 207 680 3088
Fax: +44 (0) 207 702 3752
Email: enquiries@airmic.com
Web: www.airmic.com
EXP-0012-0218