



Gallagher

Insurance | Risk Management | Consulting

SME Crisis Management: A guide to security threats



Contents



Introduction: Why crisis resilience is so important

You only need to glance at the headlines to understand why crisis resilience is a hot topic for many businesses.

Mass shootings, increases in workplace violence, the changing nature of terrorist attacks and the widespread riots of 2020 have demonstrated that it is no longer just major cities that find themselves at risk of significant security threats. Threats can come from 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.

Riots, looting, violent attacks, terrorism and extortion are becoming ever present threats to businesses of all sizes. From grocery stores to real estate offices, the threat is very real, but these businesses are rarely the direct target of physical damage. What businesses should be considering is 'non-damage' business interruption and 'denial of access' to their premises for both employees and customers as a result of a security incident in their neighborhood.

If your block is closed off because a security threat has happened nearby this can have a significant financial impact on your business, and without effective crisis management plans in place, including insurance coverage, it can be difficult to recover from.



The scale of the problem

\$500k

Then the cleanup following a shooting can take up to a month, depending on the case. Not counting BI issues, costs can reach \$500k.

APPROX

52%

of employees have experienced a workplace violence event (threats, assaults, robbery).

\$3m

is the indicative cost of a violent case going to a jury trial.

Post-event employee turnover rates can exceed

50%

per occurrence depending on the incident.

100%

of shootings should expect go to litigation.

The site of a shooting can be shut down from

8-72

hours depending on severity.

For public companies, stock can drop around

9%*

depending on crisis management, the market and other factors.

Types of threat

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

Security Threat

Insurance 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 organization.

Examples

- Cyber extortion
- Protests and riots
- Terrorist attacks
- Active Shooter
- Assault
- Hostage situations
- Kidnap and ransom threats.

Non-Security Threat

Insurance Definition:

'Acts of god' and other non-man made threats which can inflict serious damage on an organization. These threats can be hard to predict and can also cause significant business interruption.

Examples

- Flooding
- Hurricanes
- Storm Damage
- Disease/ Pandemic.



Your crisis plan

Crisis management plans should be short, principle-based and tested to enable rapid decision-making and communication when there is a vacuum of information, panic and pressure from stakeholders on all sides.

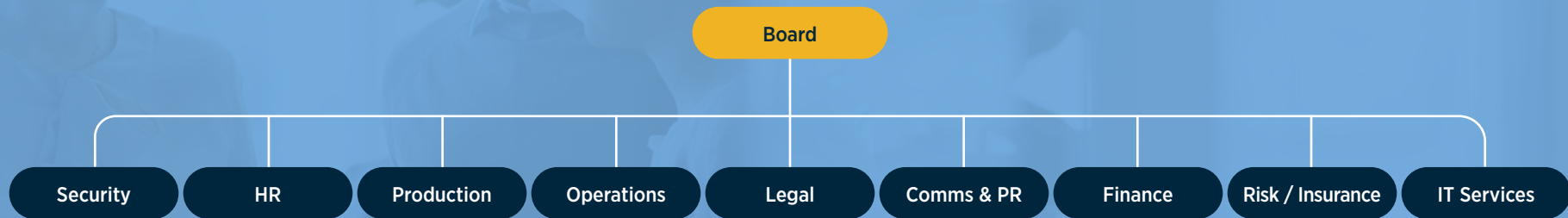


Step 1

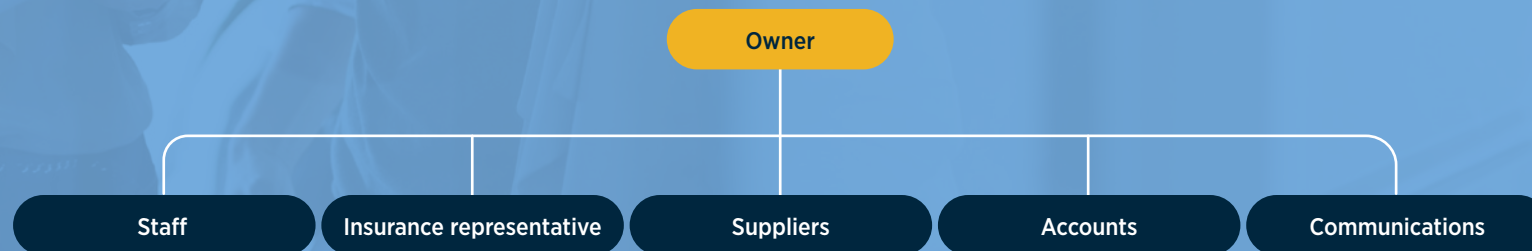
The team

If you can, create a crisis management team.

The size of the team will vary depending on the size of your business but it should consist of a cross-section of top management and key organizational area representatives such as:



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



If it's just you running the show, make sure you know who the relevant parties within the business are and what they need to know. Have it written down somewhere accessible so you can react in an emergency and let your staff, suppliers and insurance company know what's going on.

Step 2

The analysis

Conducting a risk assessment will help you anticipate and understand where vulnerabilities lie.

Depending on the size of your business, it's helpful to conduct the risk assessment with the support of a risk consultant or qualified insurance broker, but you can also do a basic version yourself. The below table shows the different types of risks you should consider.

You need to identify and agree:

- Critical business processes
- Interdependencies between these critical processes and other parts of the business
- Recovery priorities for these critical processes
- The minimum resources required for the recovery of these critical processes.

	Physical Risk	Human Risk	Reputational Risk	Digital Risk
Definition	Minimising business interruption risk	Minimising loss of life or injury	Minimising damage to reputation	Minimising data loss or leak
Impact on Business	<ul style="list-style-type: none"> • Denial of access • Loss of revenue • Costs for recovery/repair. 	<ul style="list-style-type: none"> • Loss of resource Issues with PTSD. 	<ul style="list-style-type: none"> • Financial losses Loss of customers. 	<ul style="list-style-type: none"> • Reputational damage • Loss of customers • Financial losses.
Analysis Required	Calculate the impact and likelihood of low frequency, high-impact threats such as business interruption after a riot.	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.	Cyber security audit to determine, for example, the vulnerability of payment and online booking systems and the preparedness for a ransomware attack.
Data available to help anticipate threat	<ul style="list-style-type: none"> • External security intelligence companies • Social media • International and local media Management information from the security team.	<ul style="list-style-type: none"> • Management information from the HR department • External security intelligence companies. 	<ul style="list-style-type: none"> • Social media • International and local media • Management information from the communications team/ Public Relations advisors. 	<ul style="list-style-type: none"> • Management information from the IT department • Social media • Online digital vulnerability databases • Cyber security company • Notifications and alerts.

Step 3

The plan

With so many varying threats, it is clear that one plan will not be suitable for every circumstance which is why you should have a number of different plans in place which respond to varying levels of severity.

You need to establish:

- Incident management and communication lines
- Business continuity strategies
- A plan framework, structure and content
- The roles of people and priorities to apply.

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

Business Continuity

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.

Emergency Management

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.

Crisis Management

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.

Disaster Recovery

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.

Step 4

The response

Gather the team, or yourself!

The complex and rapidly changing nature of a crisis means that it is not easily managed using long, plans developed in advance, keep it simple and make sure your staff know the plan. Ask yourself or your team the following questions.

Decision points

- ✓ What decisions still need to be made?
- ✓ What dependencies?
- ✓ Who makes the decision?

Information

- ✓ What do we not know?
- ✓ Who do we know?
- ✓ Do we have this information yet?

Actions

- ✓ What can be done now?
- ✓ Who does it?
- ✓ Who resources?

Messaging

- ✓ What are we saying?
- ✓ How should this change?
- ✓ Different for which stakeholders?

Communication

As ever, depending on the size of your business the individual responsible for communicating about the security will vary, but the process stays largely the same.

Be it your Head of Corporate Communications or yourself as the business owner, 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:

- Staff
- Customers
- Suppliers and Transportation companies
- Security Management
- Trade bodies
- The Press.

These days communications are transmitted globally in real time and form part of a constantly evolving storm of opinions, conversations and conflicts. Social media can also create new components to the crisis, or transform existing problems faster than a business can effectively deal with them.

Conversely, social media is also likely the greatest crisis management tool ever developed. It has democratized the way in which brands can engage with millions of customers, stakeholders and influencers. There's no excuse for your business not to utilize social media in a crisis.



Gallagher Crisis Protect

Gallagher Crisis Protect is an insurance policy that covers companies for a range of security threats. Included with the policy is access to security consulting support.

Clients can call an emergency number 24/7 for immediate on the ground assistance, and the policy also provides funds for pre and post incident risk management.

The policy helps companies by removing the challenge of trying to plan and mitigate for a wide variety of changeable security perils, and with the provision of crisis consulting, also helps ensure companies are complying with legislation around duty of care and workplace safety.



The consulting support

Gallagher Crisis Protect includes a comprehensive crisis consultancy package that helps build resilience and address duty of care.

In the event of an incident, you have the support of some of the worlds leading crisis consultants, available 24/ 7/ 365 by calling one number. The solution supports clients during the three phases of a crisis; pre-incident, during the incident and post-incident.

That means you get immediate value from the policy even without an incident occurring.

One

Pre-Incident

- ✓ Online crisis management portal that provides information and templates for increasing resilience during security-related crises.
- ✓ A dedicated secure group, private to you, that you can brand to your own organisation. You have full control to add and manage access for a group of your colleagues, where they will be able to take advantage of the training and awareness information, as well as manage and share access to their own plans, procedures, documents and guidance, available anywhere at any time with a secure internet connection.
- ✓ Document library including thought leadership papers and awareness guidance.
- ✓ Active shooter (vicious attack) online awareness videos.
- ✓ Quarterly webinars on key issues and topics.
- ✓ “Ask the Expert” - hints, tips and ideas, now including access for COVID-19 related security questions and concerns.

Gallagher Crisis Protect

Two

During the incident

- ✓ 24/7/365 emergency response number to get immediate advice and support in a crisis
- ✓ Consultancy support from a panel of retained response consultant companies that are leaders in their field, all coordinated through a single emergency response number.
- ✓ Access to live incident log via the online crisis management portal (ensuring key decisions and actions are captured as part of duty of care and audit purposes, especially important in the context of any future potential litigation).





















Three

Post-Incident

- ✓ Post-incident information guidance and advice including lessons identified, counselling advice (PTSD) and legal support.
- ✓ Incident log summary case file for audit and records.

The insurance

What security threats does the policy cover?

 Assault	 Blackmail	 Civil Commotion	 Deprivation	 Detention	 Disappearance
 Emergency Repatriation	 Employee Dishonesty	 Extortion	 Hijack	 Hostage Crisis	 Kidnap
 Radicalization	 Sabotage	 Stalking	Consultant Costs Only		
 Terrorism	 Threat	 Vicious Attack			
			 Cyber Extortion	 Product Tampering	

Gallagher Crisis Protect

We will cover losses to your business, in up to five locations, up to a total of USD1 million.

We will cover losses and liabilities to third parties, up to USD100,000.

You will have access to a 24/7 crisis consulting helpline.

You will have up to a value of USD1 million of crisis consulting costs covered by the policy.

Cyber Extortion and Product Recall incident crisis consultancy costs covered up to USD25k

FAQ's

Doesn't my regular business insurance already cover these risks?

No. Some business insurance policies might cover some security threats but you would still have to purchase separate policies to get the same level of cover across all the threats.

Why is this policy better than others on the market?

This is the most comprehensive security insurance available globally. No other products covers as many security threats perils within one policy, plus crisis consulting services, all for a flat annual fee.

How much does it cost?

If your business has a revenue of less than USD250 million the premium is USD2,000.



This note is not intended to give legal or financial advice, and, accordingly, it should not be relied upon for such. It should not be regarded as a comprehensive statement of the law and/or market practice in this area. In preparing this note we have relied on information sourced from third parties and we make no claims as to the completeness or accuracy of the information contained herein. It reflects our understanding as 01.01.2021, but you will recognize that matters concerning COVID-19 are fast changing across the world. You should not act upon information in this bulletin nor determine not to act, without first seeking specific legal and/or specialist advice. Our advice to our clients is as an insurance broker and is provided subject to specific terms and conditions, the terms of which take precedence over any representations in this document. No third party to whom this is passed can rely on it. We and our officers, employees or agents shall not be responsible for any loss whatsoever arising from the recipient's reliance upon any information we provide herein and exclude liability for the content to fullest extent permitted by law. Should you require advice about your specific insurance arrangements or specific claim circumstances, please get in touch with your usual contact at Gallagher.

Get in touch

Email: Crisis_Protection@ajg.com

 [linkedin.com/gallagher-global](https://www.linkedin.com/company/gallagher-global)

www.ajg.com

Insurance brokerage and related services to be provided by Arthur J. Gallagher Risk Management Services, Inc. (License No. 0D69293) and/or its affiliate Arthur J. Gallagher & Co. Insurance Brokers of California, Inc. (License No. 0726293).

©2021 Arthur J. Gallagher & Co.



Gallagher

Insurance | Risk Management | Consulting