



Security Resilience

Who, What and Why?





Security Resilience:

Who is it for?

Security Resilience is a strategic crisis response consultancy for business owners and those responsible for the well-being of businesses and their employees. It is ideal for the boards of small and medium sized businesses in all industrial sectors. Security Resilience is activated by a host of potential crises facing their business – helping stakeholders protect their people, their property and their reputations.

Security Resilience is offered in collaboration with our global security and crisis response partner [Crisis24](#).



An immediate expert 24/7 response to a host of crises



Act of Terrorism



Assault



Blackmail



Civil Commotion



Cyber Extortion



Deprivation (Denial of Access)



Detention



Disappearance



Emergency Repatriation



Employee Dishonesty



Extortion



Hijack



Hostage Crisis



Kidnap



Product Tamper



Radicalisation of Workforce



Sabotage



Stalking



Threat



and many more





Security Resilience:

What does it do?

Security Resilience provides immediate 24/7 access to expert security consultants to guide stakeholders through the optimum response to a crisis from prevention and mitigation, to crisis management and crisis recovery.





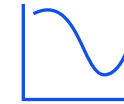
Crisis prevention and mitigation

Help in assessing the threats, selecting and training the company crisis management team members, and validating contingency plans through practical exercise.



Crisis Management

Expert, on-the-ground support in the event of a crisis, guiding and advising the crisis management team through to a successful conclusion.



Crisis Recovery

Post-incident support to help the impacted business recover its trading position and minimise damage to its reputation.

Security Resilience services are tailored to the particular crisis facing the business and may include:



Immediate assessment and initial guidance



Stakeholder liaison
eg police, authorities



Identification of legal implications



Personnel impact assessment



Investigation services



Help setting up crisis management team



Management of crisis communications



Surveillance and counter surveillance management team



Victim witness debriefing



Deployment of consultant to location





Security Resilience:

Why do businesses
need Security Resilience?



Business headaches: instant response

We know from experience that the major security worries of many businesses relate to some form of radicalisation and terrorism, some form of violent crime (whether against employees, in the workplace or travelling overseas) or some form of company cyber crisis. Knowing who to call whenever these issues appear, which may be any time of the day or night, can be problematic.

Security Resilience gives stakeholders immediate 24/7 access to security consultants, all experts in their field, to guide them through the optimum response to a crisis.

Business's 3 major security headaches:



Source: Security Exchange









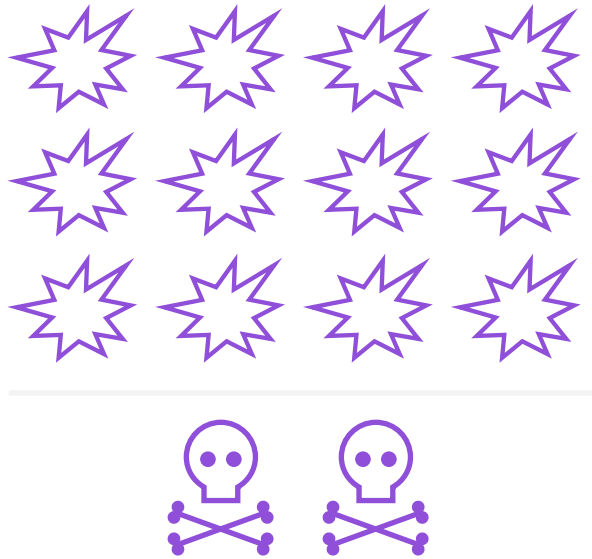
Business headaches: terrorism

As well as the risk of being a terrorist target themselves, businesses also risk facing the impact of a nearby attack. A number of clients affected by nearby terrorist incidents have suffered restricted access to their premises with concerns about staff safety, business continuity and the suitability of planning for future incidents. (In fact the operations centre has received several requests about contingency planning from businesses that have never been impacted either directly or indirectly, but are nevertheless concerned about the possibility)

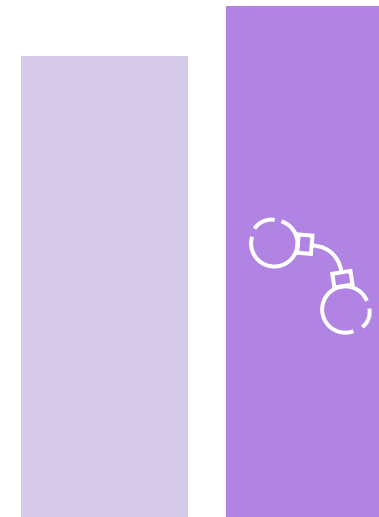
Typical response measures

-  Short (two hour) desktop walkthrough exercises
-  Advice on stakeholder communications
-  Assessment of staff trauma and recovery
-  Effective crisis management to foster swift business recovery





12 UK terrorism incidents
in 2021 = 2 fatalities



203 terrorism-related arrests
in UK year ending 30 June
2022, an 11% increase



Business headaches: radicalisation

Many clients, especially those with substantial numbers of manual workers have expressed concerns about the possibility of radicalisation, either through online conversion or through friends or relatives returning from Jihadist activity overseas and exerting influence. In one case, where a former employee was involved in a lone act of terror using a vehicle as a weapon, the company was (unfairly) criticised for not having picked up the individual's radical tendencies in their vetting procedures.

Typical response measures



Explore and develop early warning systems



Adaptation of existing whistleblowing facilities to encourage the reporting of any unusual behaviour.










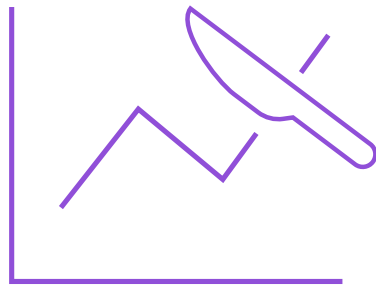
Business headaches: violent crime

Businesses, concerns about Violent Crime are reflected in the increasing threat of knife crime, violence in the workplace, sexual assault or online trolling as well. Meanwhile concerns about threats to lone travellers (from the threat of street robbery to assault in a remote hotel) are driving more requests especially from lone travellers for pre-trip advice. Even in first world countries, police and government forces are hard pressed to cope with the volume of incidents so companies are increasingly having to resort to self-help measures.

Potential response measures

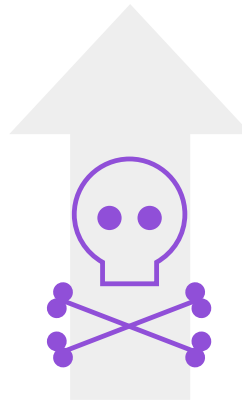
-  Snapshot briefings to improve traveller awareness
-  Incident investigation and threat containment
-  Liaison with the relevant law enforcement agency
-  Ensure proper medical treatment and safe location for victims
-  Review company staff safety procedures





10% increase in crimes involving knives and sharp instruments in the UK year ending March 2022.

Source: Office of National Statistics



25% increase UK homicides year ending March 2022

Source: Office of National Statistics)



688,000 Incidents of violence at work in UK 2019/20 – 299,000 assaults and 389,000 threats

Source: Health and Safety Executive





Business headaches: cyber-extortion (denial of access)

With personal and corporate data being stolen on an industrial scale, the chances of a company being targeted by hackers or extortionists are increasing along with directors' concerns about the possibility. Many of our clients have reported receiving demands via their company email threatening to close the system down if a certain sum is not paid to the perpetrator's anonymous virtual account.

Potential response measures



Advice on how to handle the demand and how to prevent further attacks



Importance of response planning for an attack



Short desktop walkthrough exercise to promote awareness and prevention.





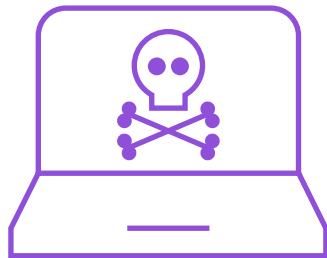
UK Computer misuse increased 89% to 1.6 million offences year ending March 2021

Source: Office of National Statistics



18 UK ransomware incidents in 2022 required a nationally coordinated response

Source: NCSC Annual Review 2022



61 percent of fraud incidents in the UK year ending March 2022 were cyber-related (up from 53% the previous year)

Source: Office of National Statistics



38% of UK micro and small businesses identified a cyberattack in the last year.

(82% of these reported phishing attempts, and 25% identified more sophisticated attacks: denial of service, malware, ransomware attacks)



Public expectations and directors' duty of care

Directors' headaches are reflected in the British public's anxiety about security. This is at an all-time high, according to research by Unisys, especially around war and terrorism which has shown an 84% increase in the index of security concerns in the last 3 years.

Against the background of intensifying exposures, Security Resilience helps directors demonstrate they have taken responsible precautions by going outside their company to put expert independent measures in place.





Financial efficiencies

For many small and medium sized companies, resourcing an in-house security team may not be feasible, while the financial costs of funding an outsourced security service may be prohibitive. Security Resilience is a highly efficient and effective alternative.

Security Resilience gives the board of directors the reassurance of knowing that they have immediate access to an affordable, full-service up and running crisis operations centre ready to respond, whenever and wherever it is needed.



Public authorities and a rapid response

Companies who have not experienced a crisis may believe the best response is to alert the police or government agencies (like the FCO). But a potential crisis that is a top priority for the business, may not be for the police – who may also be more focussed on apprehending perpetrators than on post-incident issues facing the business.

Security Resilience provides an immediate 24/7 response not only to help prevent, mitigate and manage a crisis, but also to help the business protect its reputation and recover its trading position afterwards.





Preparation and prevention

In our experience it isn't just crises that have taken place that give Boards cause for concern, but also possible eventualities that haven't happened yet. Over 90% of the calls received by the operations centre requested advice and guidance about potential threats (such as an upcoming activist demonstration in the vicinity or an increased terror threat).

Crisis Concierge provides immediate advice from security experts to help businesses prepare for a crisis and if possible prevent it from materialising in the first place.



Crisis Concierge: Scenarios

A small business is forced to close temporarily and some of its staff are traumatised following a terrorist attack in the area.



Consultant deployed on-site and advises on business recovery



Financial contribution to support the business's post-incident recovery

After a computer system is hacked an anonymous caller demands a bit coin payment in return for reinstated access



Consultant guides the board through the initial crisis response: ensuing correct procedures for assessing the threat, for communicating with key stakeholders and for establishing a robust and effective decision making process.

A services firm is fearful of a potentially violent demonstration planned close to its office.



Consultant advises on the safe movement of staff and customers entering and leaving the premises



Consultant liaises with police and emergency services to establish the scope and extent of the demonstration



Consultant advises on external communications to customers and suppliers

LONDON

58 Fenchurch Street
London EC3M 4AB
Tel: 020 7954 7000

BIRMINGHAM

Embassy House, 60 Church Street
Birmingham B3 2DJ
Tel: 0345 600 5678

CROYDON

2-8 Altyre Road, Croydon
Surrey CR9 2LG
Tel: 020 8681 2556

GLASGOW

Centenary House, 69 Wellington St
Glasgow G2 6HJ
Tel: 0141 303 4400

MANCHESTER

4th Floor, 201 Deansgate
Manchester M3 3NW
Tel: 0161 832 8521

www.aig.co.uk

American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions and other financial services to customers in approximately 70 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: [@AIGinsurance](https://twitter.com/AIGinsurance) www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference herein.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions and coverage is subject to underwriting requirements and actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

American International Group UK Limited is registered in England: company number 10737370. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. American International Group UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 781109). This information can be checked by visiting the FS Register (www.fca.org.uk/register).

