



The role of critical event management software in protecting commercial buildings & corporate estates.

E-book

'Secure today, for a safer tomorrow'

zinc
SYSTEMS





Contents

- Page 3** Introduction
- Page 5** Examples of major and smaller critical events that could occur
- Page 6** Impact of the 'Terrorism Protection of Premises Bill' (Martyn's Law)
- Page 8** How a Critical Event Management (CEM) system can help support you
- Page 10** Scenario 1: Marauding terrorist attack (MTA) attack
- Page 12** Scenario 2: Unauthorised access involving URBEX
- Page 14** Scenario 3: Medical Incident
- Page 15** Summary & benefits of a CEM system
- Page 17** Contact

Safe spaces, secure futures.

The importance of commercial buildings and corporate estates extends beyond their economic & social contributions; ensuring the security and safety of its people, assets and brand is equally critical.

This aspect is fundamental to maintaining the integrity of these spaces, protecting assets, and ensuring the well-being of occupants and visitors. Here are several reasons highlighting the importance of security and safety measures in commercial properties

Protection of assets

Prevention of theft and vandalism:

Effective security measures deter criminal activities such as theft, vandalism, and other forms of property damage. This is crucial for preserving the value of the assets and the businesses operating within these premises.

Data security:

For office buildings and commercial spaces that house technology and data-centric companies, cybersecurity measures are vital to protect sensitive information from breaches.

Safety of occupants and visitors

Emergency preparedness:

Implementing safety protocols and emergency response plans ensures that commercial buildings are prepared for unforeseen events such as fires, natural disasters, or medical emergencies, thereby safeguarding lives.

Health and environmental safety:

Ensuring buildings are constructed and maintained according to health and safety standards protects occupants from hazards such as poor air quality, structural failures, or exposure to toxic materials.

Security and safety are crucial for commercial properties because it safeguards assets, reduces liabilities, enhances reputation, ensures compliance, mitigates risks, and contributes to long-term value and sustainability.

Business continuity and reputation

Minimising downtime:

Robust security and safety systems help in quickly addressing incidents, minimising downtime for businesses affected by emergencies or criminal activities.

Reputation management:

A safe and secure environment enhances the reputation of commercial establishments, making them more attractive to tenants, investors, and customers. It signals reliability and professionalism.

Legal and compliance obligations

Regulatory compliance:

Commercial buildings must comply with local, national, and international safety and security regulations. Failure to adhere to these standards can result in legal penalties, financial losses, and reputational damage.

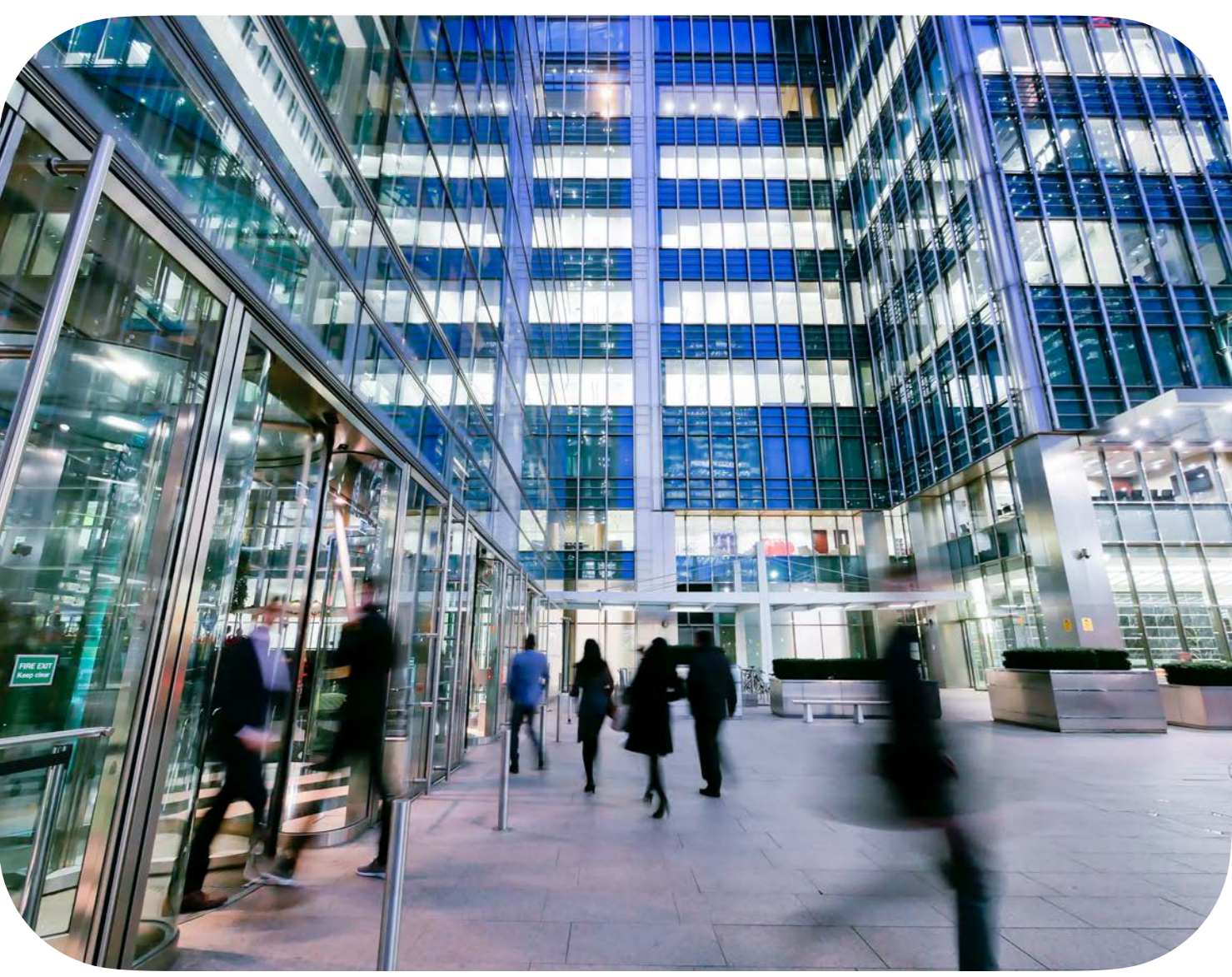
Liability reduction:

By implementing effective safety and security measures, property owners can mitigate liability risks in the event of accidents or incidents on their premises.

Enhancing the value of properties

Investment attraction:

Properties with state-of-the-art security and safety features are more attractive to potential investors and tenants, thereby enhancing the property's market value.



Core service teams and their responsibilities

A Control Room or Security Operations Centre tends to serve as the nerve centre for monitoring and managing all building risks, operations and systems. Highly trained operators respond to emergencies, centrally managing and coordinating incident response and critical communications through pre-authorized, automated operating procedures.

Critical Events

Security

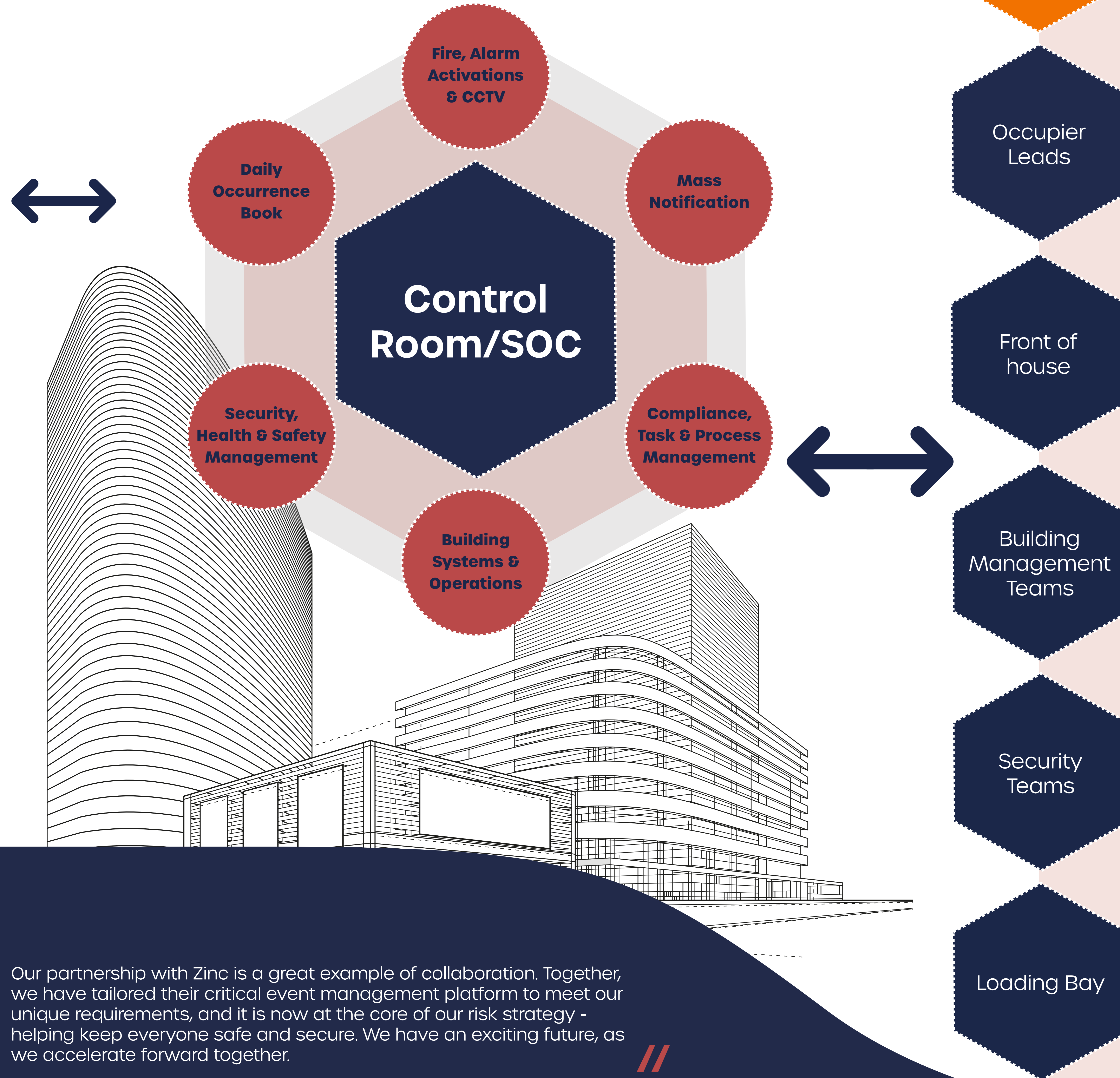
- Activated Alarms
- Access Control Incidents
- Civil Unrest
- Confiscations
- Daily Occurrence Book
- Evacuation & Invacuation
- Theft, Robbery & Burglary
- Building / Criminal Damage
- Product & Stock
- Patrols Management
- Security System Failure
- Suspicious Activity
- Terrorism
- Unacceptable Behaviour
- Unauthorised Access
- URBEX
- Violence & Abduction
- VIP

Health, Safety & Environment

- Accidents
- Dangerous Occurrences
- Extreme Weather
- Flooding/Water Leaks
- Fire
- High Risk Activities
- Lift Entrapments
- Missing Person
- Near-Miss
- Pest Infestation
- Safety Observations
- Serious Illness
- Suicide / Self Harm
- Unclean Area
- Vehicle & Transport
- Vulnerable Person
- Waste & Pollution

Operations

- Complaints
- Deliveries
- Loading Bay DOB
- Lost & Found
- Mechanical & Electrical
- Requests
- Visitor Logs
- Checks & Assessments
- Asset Checks



The Gold Commander serves as the overall incident commander during emergencies receiving escalated incident alerts and issue tasking. They coordinate response efforts, allocate resources, and make critical decisions to ensure the safety of occupants. Their role is crucial in managing complex incidents such as fires, evacuations, or other emergencies.

Occupier leads in tall buildings play a vital role in tenant safety and satisfaction. They liaise with building management, ensuring that tenant needs are met, safety measures are followed, and evacuation plans are understood. They also facilitate communication during emergencies and provide valuable input for building operations and security improvements.

The role of front of house in a commercial building encompasses managing the reception area, greeting and directing visitors, handling inquiries, and ensuring a welcoming atmosphere. They play a crucial part in security by monitoring entry points and may also coordinate mail, deliveries, and maintain the appearance of the lobby area.

Oversee operations, maintenance, and tenant services, ensuring smooth functioning and occupier safety and experience. Teams include Engineering, Housekeeping/Cleaning, Logistics, Post Room and Lobby. Teams receive critical alerts with linked instructions, role specific incident reporting (i.e. lift entrapments or unclean areas) and the allocation of incident-related tasking.

Responsible for safeguarding people, assets and brand. Their assignment instructions vary from monitoring access, conducting patrols, responding to incidents, medical emergencies, enforcing policies and completing standard/emergency operating procedures (SOPs/EOPs) when required. Their role ensures a secure environment for occupiers and visitors contributing to overall safety and well-being.

A critical role in facilitating the smooth transportation of goods - managing incoming and outgoing deliveries, ensuring efficient loading and unloading processes. These teams are responsible for maintaining safety protocols, controlling access to the loading area, and preventing congestion - contributing to uninterrupted building activities, tenant satisfaction, and minimising disruption.

Our partnership with Zinc is a great example of collaboration. Together, we have tailored their critical event management platform to meet our unique requirements, and it is now at the core of our risk strategy - helping keep everyone safe and secure. We have an exciting future, as we accelerate forward together.

Iconic Commercial Building, London



Both major and impactful smaller incidents occur in all types of commercial buildings worldwide:

While major incidents often draw significant attention due to their scale, smaller events can also have a substantial impact on building operations, occupant safety, and the overall reputation of the building, contracted security firm, facilities management (FM) provider and managing agent. Addressing and mitigating all impactful incidents are crucial for maintaining a safe and efficient building environment.

Smaller critical events include:

Elevator malfunctions:

Given the reliance on elevators in commercial buildings, malfunctions or breakdowns can cause significant disruptions and safety concerns. Regular maintenance and quick response to such incidents are necessary.

Theft and vandalism:

Goods or deliveries left unattended can be targets for theft or vandalism. High-value items or packages left unsecured are particularly at risk.

Vehicle-related risks:

Vehicles entering and exiting the loading bay can pose risks, including accidents, collisions, or intentional vehicle-related threats like ramming attacks.

Water leakage:

Water leaks or plumbing issues, even if localised, can cause damage to multiple floors, impacting occupant comfort and requiring immediate maintenance.

Security breaches:

Instances of unauthorised access or security breaches, though smaller in scale, can compromise building safety protocols and require immediate attention to prevent future occurrences.

Communications failures:

In the event of communication breakdowns, such as phone or internet service disruptions, coordination of emergency responses and communication among occupants and emergency services can be challenging.

Minor fires or false alarms:

Even small fires or false alarms can cause evacuations, disrupting normal operations and raising concerns about fire safety systems.

Potential major critical events include:

Fire:

All commercial buildings face significant fire risks due to the number of occupants, complex infrastructure, and potential for rapid spread. Fire safety measures, including sprinkler systems, fire-resistant materials, and evacuation plans, are crucial.

Structural failure:

Any compromise in the structural integrity, whether due to design flaws, construction age, natural disasters (such as high winds), or construction issues, can lead to catastrophic consequences.

Power outages:

Loss of power can disrupt essential services like elevators, lighting, and HVAC systems. Backup power generators are crucial to maintaining basic functionalities during outages.

Medical emergencies:

With a high density of occupants, medical emergencies like heart attacks or accidents can occur. Having trained personnel, medical kits, and easy access for emergency services is vital.

Natural disasters:

Buildings in earthquake-prone areas face risks of structural damage. Floods, hurricanes, and other natural disasters can also pose threats, requiring specific safety protocols and building designs to mitigate these risks.

Protests, activism & civil unrest:

Can impact a building by disrupting operations, posing security challenges, potential damage, hindering access, and raising safety concerns for occupants, affecting the building's reputation and value.

Terrorism:

Locations can be targets for terrorist attacks, including bombings or deliberate plane crashes. Security measures and emergency response protocols are essential to mitigate such risks.

Is your location prepared for an unpredictable World?



29%

Average decrease in stock price due to a significant security event.



\$1 Trillion

Revenue was lost in the last year due to physical security incidents.



5-10x

The cost of a critical event is underestimated by five to ten times the actual cost.*



83%

Companies said physical security threats will increase next year.

Terrorism: How will the 'Terrorism Protection of Premises Bill' (Martyn's Law) impact commercial buildings?



The Legislation (UK)

Following a series of terror attacks in public spaces, including those at Manchester Arena and London Bridge, government plans to introduce new legislation to improve safety and security at public venues.

Known as 'Martyn's Law' in memory of Martyn Hett, a victim of the Manchester Arena attack, the legislation, that is expected to become law in 2024, will introduce a statutory duty for the owners and operators of publicly accessible locations (PALs) to take appropriate and proportionate measures to protect the public from terrorist attack.

UK Government remains committed to introducing this important piece of legislation to Parliament, as was reaffirmed by the Terrorism (Protection Premise) Bill's announcement in the King's Speech on 7 November 2023. It is anticipated that the legislation will gain all party support and become law within the current term of this parliament.

Through Martyn's Law, premises will be better prepared and ready to respond in the event of a terrorist attack, by mandating, for the first time, those responsible for certain premises and events to consider the terrorist risk and very importantly how they would respond to an attack. Simple steps save lives.

Who will be affected by the new legislation?

The legislation covers all sites, permanent event space and temporary events or pop-ups where capacity may exceed 100 people. The Bill will require certain venues to fulfil necessary but proportionate steps according to their capacity to mitigate the impact of a terrorist attack and reduce harm. It will also require them to put measures in place to mitigate the threat, including implementing security systems, staff training, and clearer processes.

There will be different requirements depending on capacity; It is important to note, a location can move to Enhanced Tier according to the activities being held. i.e. if a building holds an event of 800+ people then the security expectation increases to Enhanced Tier.

Standard Tier: 100 to 799 people

Organisations will need to complete a templated Emergency Action Plan provided by the Home Office and put appropriate and proportional measures in place based on this assessment.

Undertake low-cost, simple yet effective activities to improve preparedness - activities could include the completion of an action plan to embed practices, emergency operating procedures (EOPs) and information sharing within a CEM system, supported by staff training with ACT Awareness.

Enhanced Tier: 800+ people

This will require organisations to complete more detailed risk assessments, security planning and staff training - and a proportional response which will be articulated in the legislation.

High-capacity locations will need comprehensive risk assessments to inform the development and implementation of a thorough security plan, developing a vigilant security culture. A CEM system with built-in controls, processes, measures and integrations including CCTV & alarms will be key.



During 2017, the UK suffered five serious terrorist attacks:

22 March - Westminster Bridge

Five individuals were killed in the attack with many more seriously injured.

22 May - Manchester Arena

Twenty-two people were killed, including a number of children and teenagers. Over 100 others were injured.

3 June - London Bridge attack

Eight people were killed in the attack with many more injured.

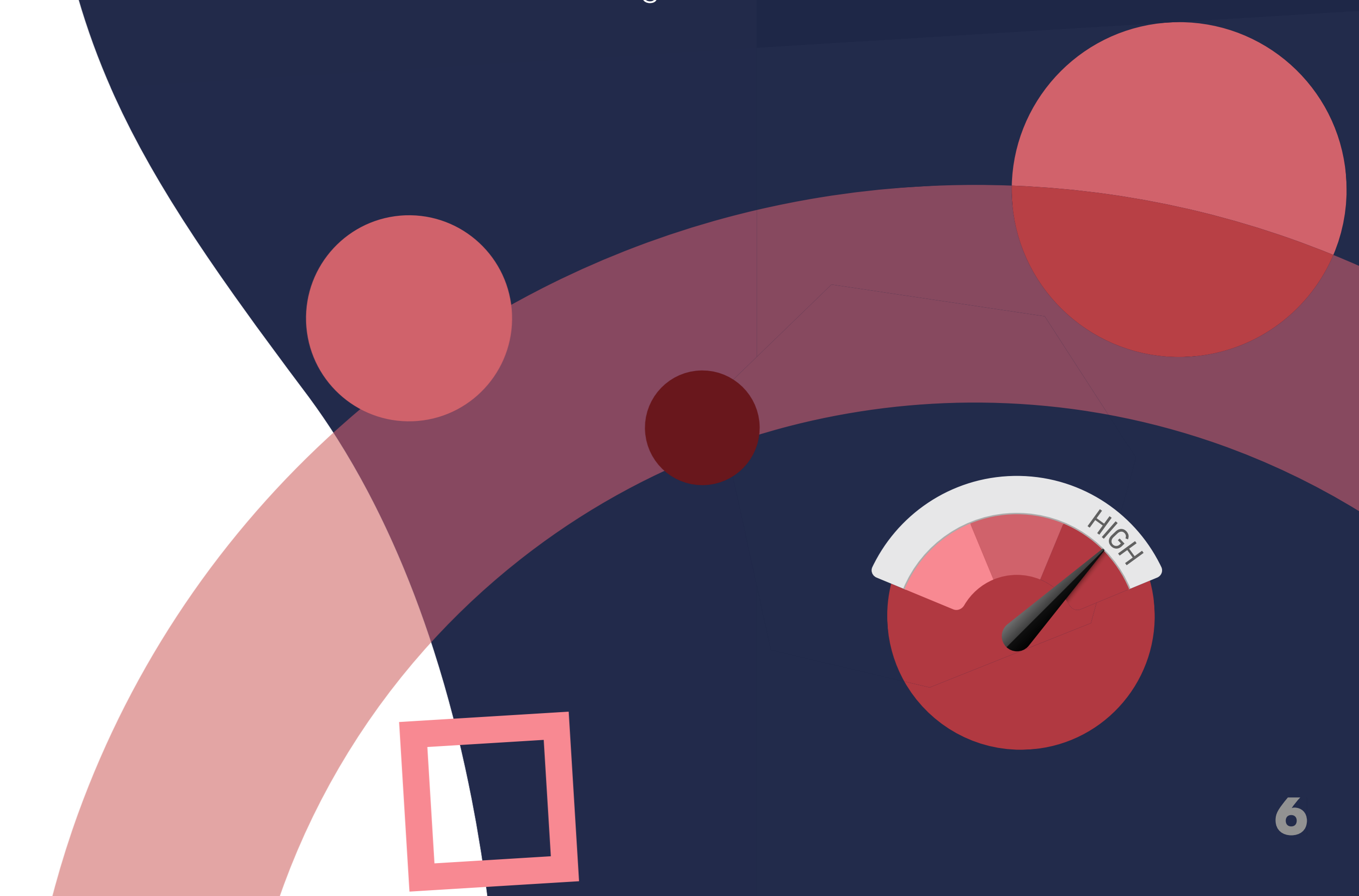
19 June - Finsbury Park attack

One person was killed and ten others sustained serious injuries.

15 September - Parsons Green station

Twenty-three people sustained burn injuries as a result of the partial explosion whilst 28 people suffered crush injuries as crowds surged to exit the train.

Source: Intelligence and Security Committee of Parliament
The 2017 Attacks: What needs to change?



Requirements will vary between buildings and may include activity beyond the assessment of terrorism related risk;

- Understand the risks associated with the location or the planned event.
- Develop a full bespoke incident plan.
- Have measures in place to respond effectively in the event of a terrorist attack.
- Have robust communication channels, escalation protocols and effective record keeping.
 - Evacuation – how to get people out of the building,
 - Invacuation - how to bring people into the premises to keep them safe, or move them to safe parts of the building,
 - Lockdown - how to secure against attackers, e.g. locking doors, closing shutters/barriers to prevent access,
 - Communication - how to alert staff and customers and move people away from danger.
- Be fully prepared with strict response protocols in the event of a terrorist attack.
- Provide training and awareness for those involved in the event including their responsibilities.

One simple step to help you manage the above challenges is the use of Critical Event Management (CEM) software in your organisation.



The passing of the legislation into law should not be the light-switch moment that businesses are awaiting, before considering their preparedness to deal with a terrorist incident. Right now, business can take simple preparatory steps. Following implementation, it is expected that Martyn's Law could feature prominently in insurance tenders going forward from both liability and property perspectives.

Safety & security should never be an afterthought.

In the next 12-18 months owners and operators of Premises, Event Space and Events could find themselves subject to new security and safety requirements;

What are the potential benefits of Martyn's Law?

The fundamental benefit is that undertaking the outlined preparedness steps will help ensure people accessing a venue or event are kept as safe as reasonably possible from the threat of terrorism. The foundations of Martyn's Law cannot be forgotten in this goal; the loss of 22 lives and injury to hundreds more at Manchester Arena, contributed to, in part by failures in security preparedness and prevention.

Benefits of compliance with Martyn's Law legislation will not only be restricted to the threat of terrorism, which fortunately is not a regular occurrence. Basic preparedness steps can help in deterring more regular, malicious activities that businesses often face, such as criminality and anti-social behaviour, or even be of use during non-malicious incidents such as a first-aid incident. Ultimately, the law prepares businesses to be resilient and prepared, which is applicable to a variety of scenarios (terrorism or non-terrorism related).

Martyn's Law compliance could quickly become an issue of business reputation and success, alongside consideration that implementing basic preparedness measures is far cheaper than the potential financial penalties of non-compliance or potential legal liability following a terrorism threat.

Insurance policies can often have some element of terrorism cover included. The insured party and their broker should review their policy to ensure there is sufficient cover in the event of a terror incident. Risk surveys exploring how organisations are meeting requirements can help insurance underwriters to make more informed decisions.

How can Critical Event Management (CEM) software help you reach new heights in safety & security management?

CEM is the practice of establishing measures to ensure incidents and events are resolved quickly and effectively. It's closely linked to all emergency planning and influenced by existing response protocols across corporate entities.

A CEM system provides a consistent framework for planning, responding, and recovering from all types of incidents, disasters, crisis, and disruptions. It plays a crucial role in enhancing the effectiveness of a security service by supporting them through the entire lifecycle of preparation, response and recovery as well as business-as-usual operations for incident preparedness.

Its aim is to keep the whole team following the same plans, communicating on the same system, and viewing the same operating picture: maintaining and enhancing business resilience.

A CEM system will deliver and manage key issues such as:

- Improving communication and inter-departmental coordination, establishing key stakeholders with priority actions including Mass Notification
- All security and emergency operating procedures are automated, ensuring actions are compliant, easily visible, and rapid.
- The technology can help organisations manage the complex process of returning to the workplace and other public spaces post event
- Data is stored securely in one place, recording key metrics and statistics that can provide valuable insight into your operations and protection against litigation.
- Teams can utilise reporting features to manage day-to-day incidents and allow better situational awareness into routine operations, thus improving resilience and your organisation's ability to keep its employees & the public safe.
- Ensure audits, checks, risk assessments are scheduled and tracked
- Post-incident analysis can really aid the management of vulnerabilities which can highlight both successes and failures.

A CEM system is one key solution that will support your journey to adhere to legislation, especially in the requirement of having a robust communication channel, escalation protocols and effective data audits. In the UK, a CEM is based on the Joint Emergency Services Interoperability Principles (JESIP), a programme designed to improve the way police forces, fire, rescue services and ambulance trusts work together when responding to major multi-agency incidents. government

A CEM system also provides a unified data source - a 'single pane of glass' that enables the prioritisation of all safety and security events. This ensures proactive risk management and mitigation, reducing the likelihood of emergencies and their potential impact. Neglecting safety and security data provides increased vulnerabilities, and, in worst cases, catastrophic consequences.



A CEM system will support safety and security leaders who manage commercial buildings & corporate estates by providing;

Connected teams and occupiers:

Provides a consistent and integrated approach to communication enabling security team to effectively manage communication and provide rapid guidance during an incident.

The gift of time and control:

Does the heavy-lifting and gives back the 'gift of time and control'. The digitalisation and unification of critical events, drives compliance and efficiency in the prevention, detection, response and recovery of an incident.

Peace of mind:

Instils confidence in the location's ability to respond effectively to emergencies, fostering a sense of security among staff, occupants, tenants & visitors.

Proactive and reactive safety & security management:

Provides an integrated framework for resilience planning, scheduling, early detection, rapid response, control, communication, collaboration and resource allocation.

Data effectiveness:

Demonstrates the effectiveness of your safety and security measures in a building by presenting the following data*

- Hotspot locations & trending analysis (time, level, activity)
- Incidents reported to the police or building security
- Completion of patrols, audits and checks
- False alarms (fire or intruder)
- Successful fire or evacuation drills (audit trail of time and actions)
- Interactions with occupants (including complaints and requests for assistance or advice—an indicator of the readiness of tenants to contact security).

*Source: ASIS Foundation: CRISP Report
From the Ground Up: Security for Tall Buildings

“ Congrats for constantly developing Synapse, day-by-day your platform is becoming more powerful and best product on the market.

Control Room Manager, London UK

Preventative actions: Verified audits, checks, assessments & patrol activities

A CEM system can support a proactive security and safety management for commercial buildings. This involves comprehensive measures implemented before incidents occur to prevent, mitigate, and respond effectively to potential risks. Here are key components:

By adopting a proactive approach that combines technology, comprehensive planning, continuous evaluation, and community involvement, buildings can significantly enhance their security and safety measures, mitigating risks and ensuring a safer environment for occupants and visitors.

Risk Assessment and Planning:

Conduct thorough risk assessments to identify potential security and safety vulnerabilities. This includes evaluating the building's structure, its location, surrounding environment, and historical risk factors. Develop comprehensive plans based on these assessments to address identified risks.

Patrol management and verified activities

Involves the supervision and coordination of security patrols to ensure effective monitoring and protection of a specific area. Effective patrol management is critical for maintaining security, deterring incidents, and responding promptly to potential threats or anomalies within a designated area or property.

Scheduling and deployment:

It involves setting up checkpoints, routes, planning and scheduling patrols to cover designated areas at specified times, ensuring optimal coverage and visibility.

Route Planning and optimisation:

Determining patrol routes based on risk assessments and optimising them for efficiency to cover the entire area effectively.

Asset maintenance:

Regularly inspect and maintain the building's structural integrity, including its façade, elevators, stairwells, and emergency exits. Ensure compliance with building codes and standards.

Communication and coordination:

Facilitating communication among patrol teams, security personnel, and control centres to relay information, receive updates, and coordinate responses efficiently.

Verification:

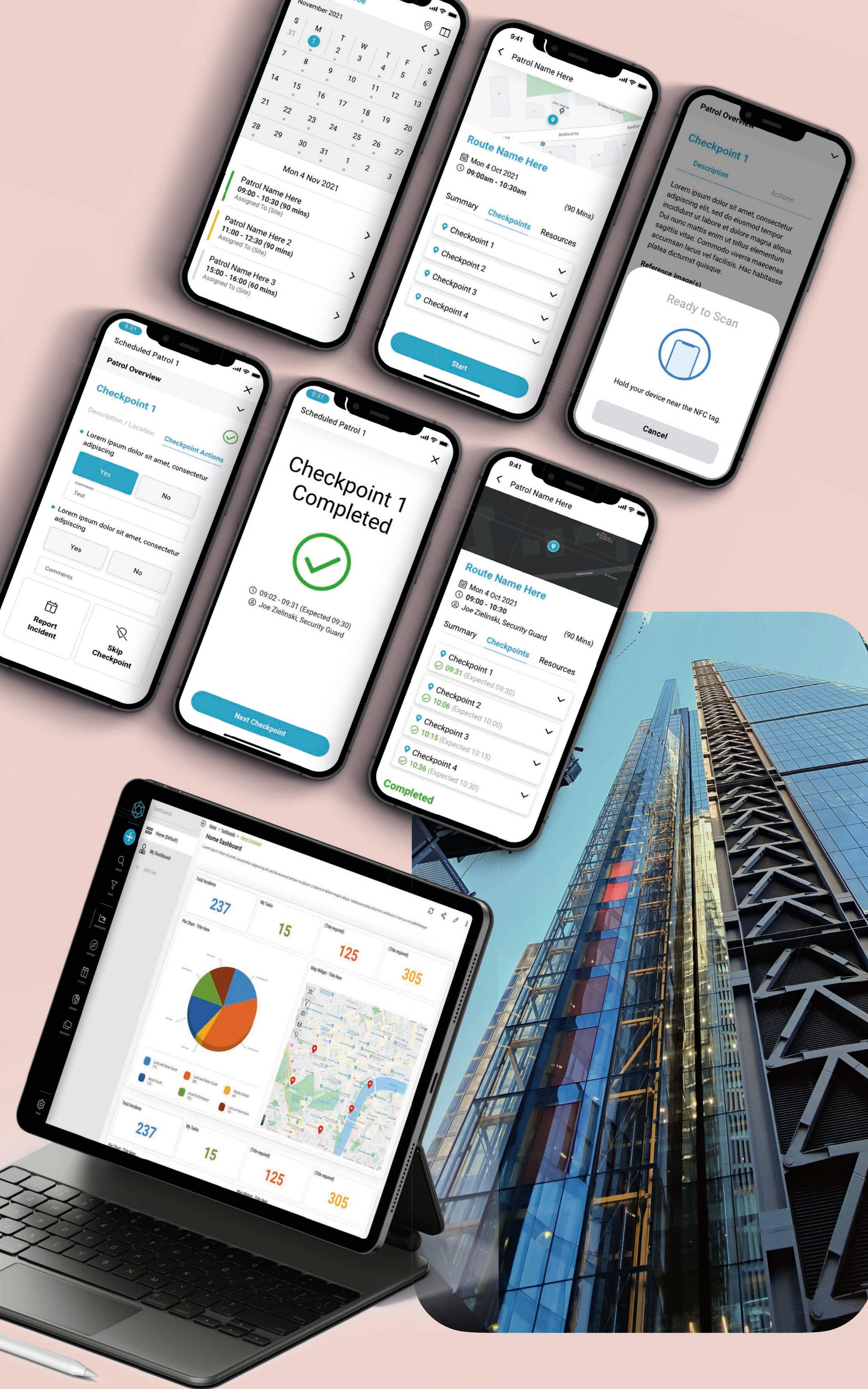
Implementing verification like GPS tracking, QR, Barcode, META extraction, RFID or NFC to enhance patrol checkpoint confirmation, accuracy, effectiveness, data collection, and reporting.

Monitoring and supervision:

Access to live performance reports to oversee patrols through various means like GPS tracking, CCTV, or communication systems to ensure patrols are conducted as scheduled and any late returning can be dealt with swiftly to safeguard individuals.

Incident response and reporting:

Managing responses to incidents encountered during patrols, documenting observations, and generating reports for incidents or anomalies detected with integrated audit trails.



Keep reading to learn how a CEM system operates in real life scenarios...



As new terrorist threats continue to emerge, it is more important than ever that your organisation is aware of the heightened risks and adequately prepared for any potential attack.

Why should a building prepare?

Commercial buildings are unlikely to provide an effective response to a terrorist incident unless Security Control Rooms (SCR) are provided with the appropriate technology, equipment, policies and procedures, necessary training and time to practice and exercise the response.

- Attacks, while rare, can be devastating.
- Simple things to help prevent & lessen their impact.
- Take responsibility for planning your emergency measures
- Measures taken are likely to have additional benefits when dealing with other threats and hazards.
- Completing risk assessments and making records of your planning will ensure resources are allocated appropriately, plans are implemented on a timely basis, provide a future record of your actions and your action will reassure staff that their safety matters.

National Protective Security Authority's (NPSA) research has shown that SCR operators are often unclear on what tasks need to be completed and whose responsibility each task is, resulting in duplication of effort and essential tasks. In addition to preventing loss of life, being adequately prepared for a potential attack will:


- Improve the response capability for other security incidents.
- Increase awareness and reduce fear.
- Enhance cooperation between neighbouring organisations, landlords and emergency services.

A marauding terrorist attack (MTA) is a fast moving attack where assailants move through a location aiming to find and cause harm to as many people as possible. In many cases an MTA may be preceded by a hostile vehicle attack. What appears to be a traffic accident outside your site may be the start of an attack.

Sources:
 - National Protective Security Authority (NPSA) - <https://www.npsa.gov.uk/incident-response-command-control>
 - 22 Bishopsgate, Counter Terrorism Ground Situation Briefing


Scenario 1: Terrorist attack

1 Initial Alert



13:00 hrs
 A member of the Window Cleaning Team, reports an incident via the App that there is a potential vehicle accident near the building involving a van versus pedestrians.

2 Incident Response



13:01 hrs
 Duty Security Manager (DSM) situated in the Security Control Room deploys a Security Medical Officer (SMO) to assist with the accident

3 Initiated Localised Lockdown



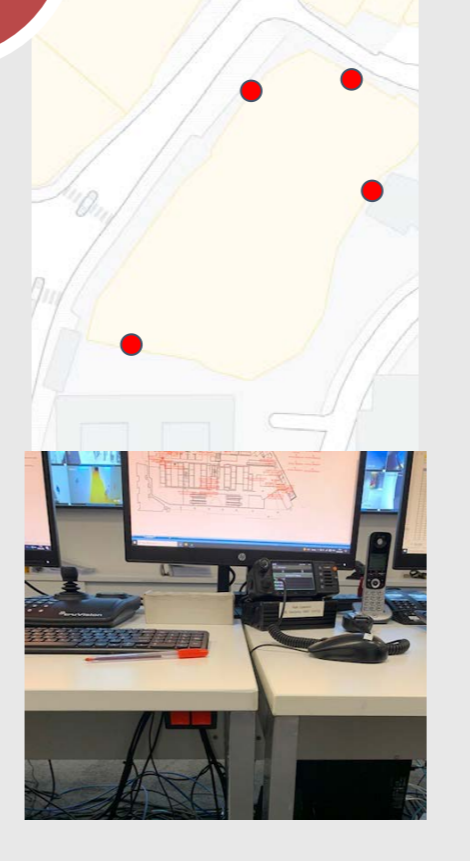
13:03 hrs
 A Security Officer (SO), posted at the West entrance (after viewing the alert), witnessed people running past, some covered in blood. The SO immediately initiated a localised lockdown.

4 GOLD Command Alert



13:03 hrs
 The on-GOLD Commander automatically is notified based on severity escalation.

4 Dynamic Risk Assessment & Crisis Management

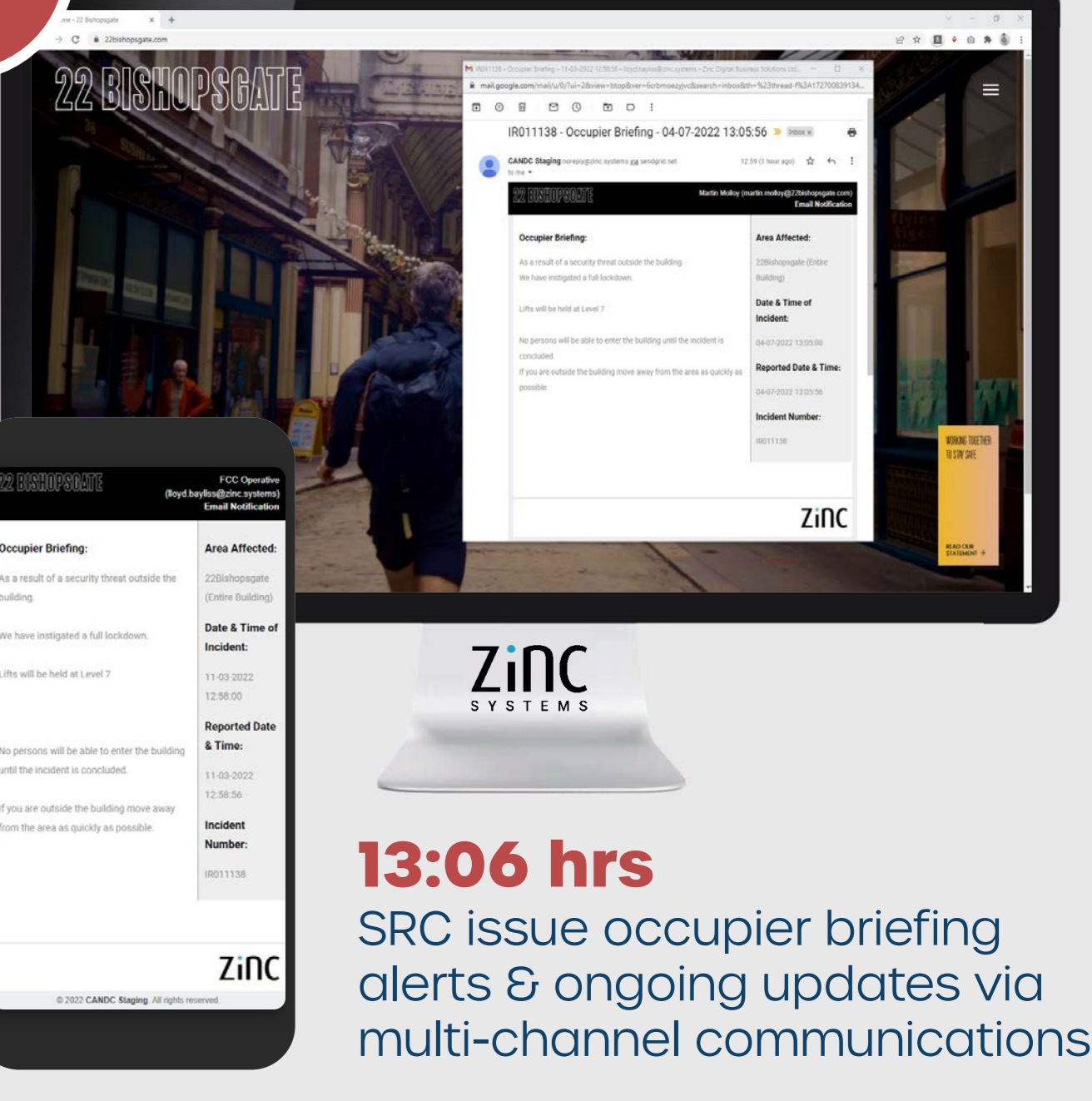


13:05 hrs
 Body worn cameras & building CCTV in the SRC witnessed at least one male seen running towards the South entrance of the building. A second male veered off carrying a rucksack and was stabbing pedestrians as he went.

DSM having carried out a dynamic risk assessment has initiated a full lockdown. Emergency Operation Procedures (EOP) automatically issued:

- SRC to issue critical communications to occupiers
- SRC locked down doors and secured environment
- Terrorist function instigated on the lifts to level 7
- No persons allowed in or out the building

5 Critical Occupier Briefings



13:06 hrs
 SRC issue occupier briefing alerts & ongoing updates via multi-channel communications

6 Threat Alerts & Intelligence



13:06 hrs ongoing...
 SRC conduct automated threat monitoring alerts posted to stakeholders, Police and intelligence partners covering:

- Neighbouring buildings alerts
- Situation briefs
- Building updates to teams
- Travel updates

7 Police Response



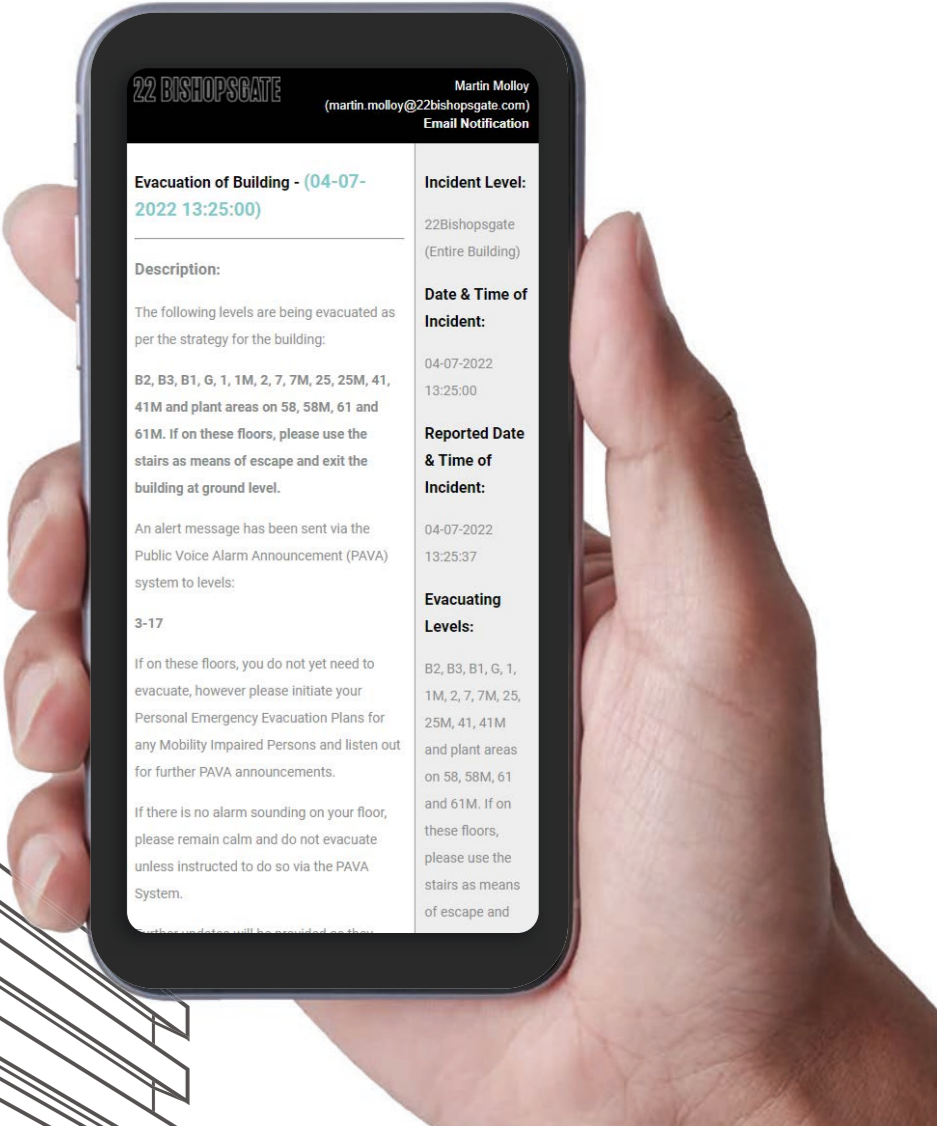
13:07 hrs
 Police officers on scene have put a cordon in place around a van as canisters are located in the back.

13:06 hrs ongoing...
 Armed Police officers neutralise two male terrorists and confirm no further threat.

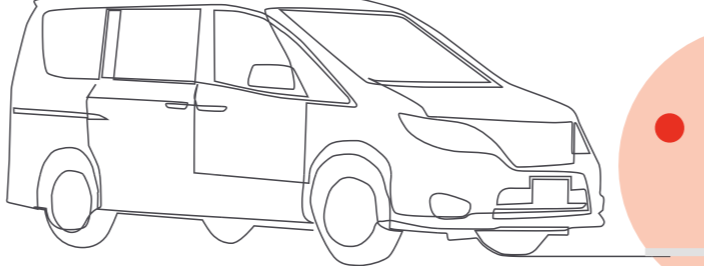
8 Evacuation Procedure

13:11 hrs
 Due to the cordon, a phased evacuation is initiated with automated level management, routes, communications, crowd management and auditing.

9 Post Critical Event & Closure Report



Phased return instructions, post analysis review covering areas for improvement and lessons learnt, evidence report collation for authorities and colleague support plans.



Building objectives

- Minimise the risk and maximise the safety of occupiers and visitors
- Minimise the risk and maximise the safety of the public
- Secure and preserve evidence
- Develop intelligence whilst being in a position to contain the threat
- Protect the reputation of the building and it's occupiers



Terrorist attack: Learn how a CEM system is pivotal in commanding, controlling & communicating.

Rapid alerting and notification:

The CEM system immediately sends alerts to designated stakeholders, including security teams, law enforcement, building management, and occupants, ensuring swift awareness and action. Pre-built templates and automations are setup ensuring critical alerts are instantly sent and received.

Coordination and communication:

The system facilitates seamless communication among response teams and relevant authorities. It establishes dedicated communication channels to coordinate operations, share critical information, and manage resources effectively.

Whether a lockdown, evacuation or invacuation response has been issued, the 'STAY SAFE' principles of RUN, HIDE, TELL provide simple actions for an individual to consider at an incident.

CEM systems enable real-time communication with occupants via various channels like mobile apps, SMS, emails, digital signage, or even in-building speakers. This allows for immediate dissemination of critical information.

Customised Messages:

The system allows for tailored messages based on the nature of the event and the location of occupants within the building. For example, directing people to use specific stairwells, avoid certain areas, or provide alternate routes based on real-time safety assessments. In addition, different groups of contacts can receive different messages and instructions - a security officer will have a different message /action compared to the role to a fire marshal or gold commander etc.

Resource management and allocation:

The system assists in managing and allocating resources effectively, such as medical supplies, emergency personnel, evacuation routes and support services, optimising the response efforts.

Evacuation and crowd management:

CEM systems provide guidance for evacuations or shelter-in-place directives along with managing and directing large crowds within a building. To ensure a systematic and safe evacuation process a CEM can be configured with different evacuation procedures if different parts of a commercial building require unique processes such as phased or linked levels. A CEM system can provide specific instructions to occupants in each area, guiding them with specific routes, lift and exit locations through pre-defined processes.

Emergency operating procedures (EOPs) & plans:

CEM systems often store detailed EOPs and response plans, enabling teams to automatically access predefined protocols for various types of attacks, ensuring a structured and organised response. Complete mobility is available to ensure EOP tasks are available anytime, anywhere - ensuring a compliant and resilient process is completed. This enables better accountability, tracking of progress, and reassurance for individuals in the affected areas.

Real-time updates and situational awareness:

By integrating with cameras, sensors, threat intelligence and other systems, the CEM system provides real-time updates on the situation's development, aiding decision-making and resource allocation.

Integration with external agencies:

The system can communicate or integrate with external agencies, such as law enforcement, emergency medical services, and local safety/intelligence groups, streamlining information sharing and enhancing collaboration during a crisis.

Post-incident analysis and recovery:

Following the attack, the CEM system aids in conducting post-incident analysis by capturing data, feedback, and lessons learned. Complete end-to-end auditing is available and analysis helps in refining future response plans and security measures.



If an attack occurs, the CEM system serves as a central hub for command and control - ensuring swift information dissemination, awareness, coordination, and response.

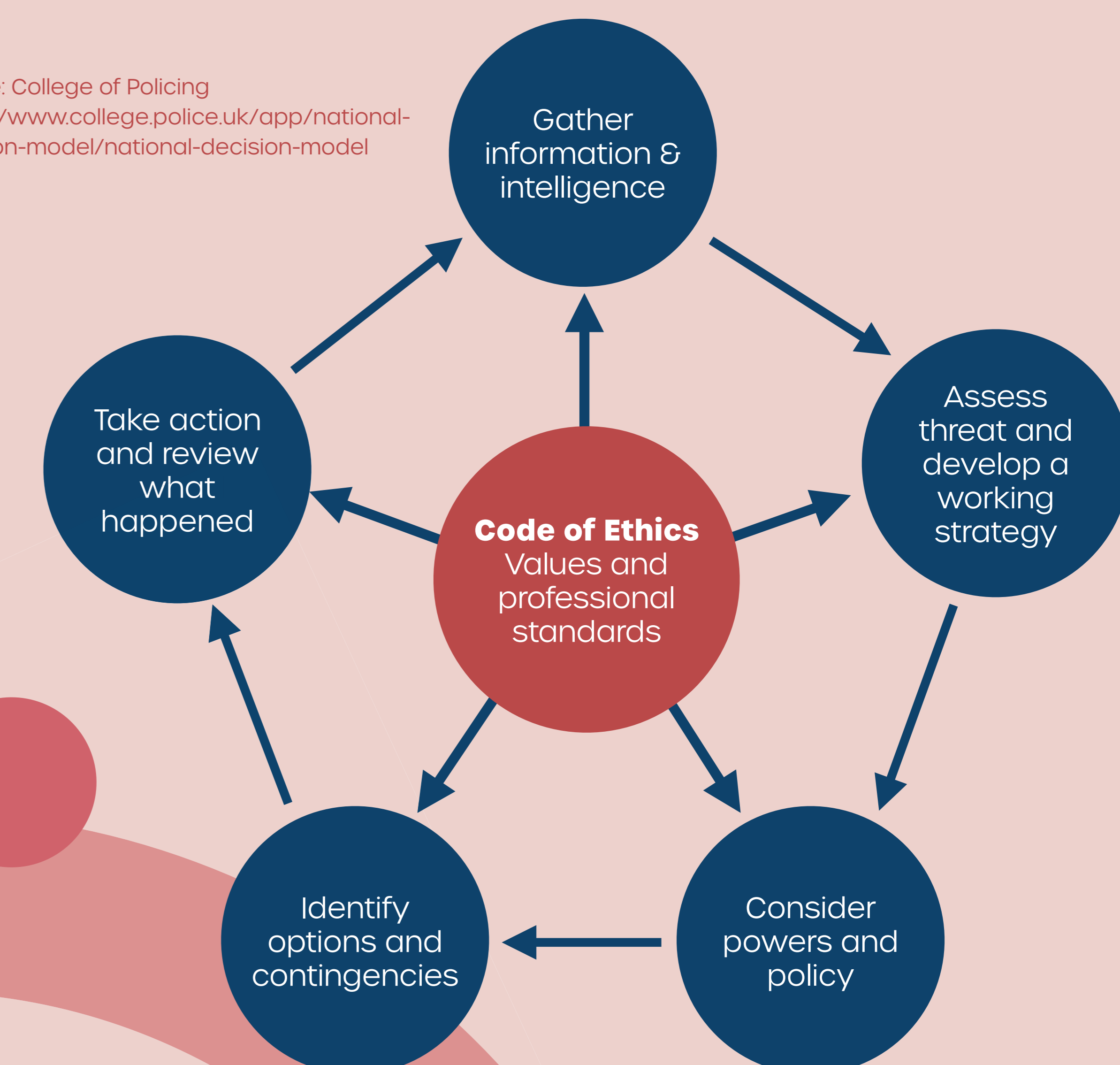
A CEM system has integrated decision models

Decision making is often complex - difficult circumstances due to incomplete or contradictory information.

22 Bishopsgate, London, utilises the National decision model (NDM) - a model that has at its centre the Code of Ethics as the touchstone for all decision making. Using the model encourages security officers and staff to act in accordance with the Code and it reduces risk aversion and weighs the balance of resourcing against demand, threat and risk.

In a fast-moving incident, the main priority is to act with integrity to protect people. With a CEM system, decision makers will receive the support from their organisation in instances where it can be shown that their decisions were compliant, assessed and managed reasonably in the circumstances existing at the time.

Source: College of Policing
<https://www.college.police.uk/app/national-decision-model/national-decision-model>



“ I would describe our relationship with Zinc as a partnership, where both parties have worked together to develop a product that was as unique and sophisticated as the building that it has been deployed in. The Zinc Team have been exceptional in tailoring the product to our ever evolving needs, supporting our journey from practical completion, introduction of different amenity spaces to the mobilisation and activation of Europe's highest viewing gallery

Martin Malloy, Head of Security, 22 Bishopsgate

Scenario 2: Unauthorised access, involving Urban Exploration (URBEX)

URBEX is an extremely dangerous activity and over the past 10 years has resulted in the death of at least 14 people worldwide.

URBEX is a significant and growing problem for iconic buildings and a relatively recent activity in which individuals (typically teenagers and young adults) make video recordings of themselves, which are uploaded to social media platforms - many URBEXers have significant numbers of subscribers/followers on social media (a few in the UK have over a million).

Although often dangerous, URBEXers are well informed concerning their legal rights and rarely commit criminal offences to avoid the risk of arrest/prosecution. However, typically their activities do involve trespassing on private property.

Their objective is to gain access to secured or restricted areas such as mechanical rooms, roofs, elevator shafts, abandoned floors, and other unseen parts of a working building to complete activities such as 'roof topping', 'in-out challenge' and 'overnight challenge/24 hour challenge', posing significant risks to the building.

There are several other risks associated with this activity:

- URBEXers may carry cameras and drones which are often not tethered and could cause a risk if dropped.
- Some URBEXers have high profile social media accounts attracting a lot of young and vulnerable followers, who may aspire to copy these individuals who are in some cases receiving endorsements from companies as well as selling their products.
- A potential terrorism risk in terms of social media posts to vulnerabilities of buildings and premises, the use of Counter Uncrewed Aerial Systems (C-UAS) commonly called 'drones'.
- Concerns surrounding online hostile reconnaissance, from the information URBEXers widely post and share via social media.
- Security Teams may be taken away from their roles in protecting the buildings, assets and people.
- Real or perceived distress of team members, occupiers or visitors.
- Security teams and premises owners may be liable, if they do not take all available actions in pursuit of carrying out their responsibilities in relation to duty of care.

By leveraging the technological capabilities within an agile CEM system, you can leverage customised processes and security measures to help mitigate URBEX risks, ultimately safeguarding the building & its occupants.



In the UK, there is a multi-agency and industry partnership approach to URBEX and is outlined in a staged response supported by an evidential process without automatically having to obtain injunctions.

The ambition is to provide an agreed and consistent stage response from all parties involved in the process, with the primary focus of deterring URBEXers from committing such acts, which can be severely detrimental to themselves, others and building owners.

1. Put in place Banning Notices, which identify individuals as Trespassers.
2. Police serve a Community Protection Warning (CPW) that an individual's conduct may have a detrimental effect.
3. Police serve a Community Protection Notice. If Individual fails to abide by (CPW). If they breach the (CPN) they can be arrested or issued with a Fixed Penalty Notice.
4. Utilise the offence of Aggravated Trespass Section 68 Justice and Public Order Act 1994. If entering customer property after being served a Banning Notice.
5. Arrestable Offence. Provide evidence where they INTENTIONALLY:
 - Disrupt Teams, Occupiers, Public and Police from carrying out their lawful duties.
 - Intimidate Teams, Occupiers and Public which would deter them from carrying out their lawful duties.
6. Obtain Section 9 Statements evidencing the above from Client property team, Occupiers and Police.
7. Put in place a process where banning notices, statements and photographs can be recorded centrally and disseminated to partners, in this case - the use of CityINTEL, a product designed by Zinc.
8. Senior Police Officer Present, consider Using Section 69 Failing to Comply with Direction of a Police Officer, an Arrestable Offence.
9. Implement Safeguarding Principles where juveniles are identified.
10. Engage with the CPS to provide a best evidence case against key individuals.
11. Consider Obtaining Injunctions against unknown and specific individuals
12. Once we have evidence of criminal acts, engage with Social Media companies re their duty of care and funding criminal activity and potential breach of their T&C's
13. Provision of training and packs to Police, venues, Security Companies, Magistrates
14. Consider Private Prosecution - These are initiated against individuals if statutory bodies do not take action.

Full document and further details available from the City Security Council.

Sources

- HighRig Group – Urban Explorers, Way Forward publication, Jan 2024
- National Business Crime Centre / Revo Community

How a CEM system provides an end-to-end solution for protecting against URBEXers.

A Critical Event Management (CEM) system can aid in managing unauthorised access incidents and specific localised threats, like those involving Urban Exploration (URBEX) explorers - who often engage in exploring high risk off-limit areas.



Early detection and monitoring:

CEM systems can integrate with building security cameras, motion sensors, and access controls if required. They can identify unauthorised access or movement in restricted areas, triggering alerts for security personnel to investigate potential URBEX activity.

As an example, integrating with Access Control systems to automatically push true access control or tailgating alerts directly into Zinc Synapse for rapid dissemination and management.

Security patrol management

CEM systems have integrated patrol management tools. Providing detailed reports to prove security patrols are performed regularly and on time, identifying the locations, levels and checkpoints visited, the guard performing the patrol, and recording any incidents or actions that occur whilst on duty.

Offender libraries & banning registers

Storing a library of known URBEX offenders to enable visitor lookups and practice security management. In addition, issuing a banning notice to prevent the person from entering the building again (whether or not they comply with the visitor guidelines).

An example of this is CityINTEL (developed by Zinc) - CityINTEL is a collaboration between the City of London Police, the City Security Council and private security companies enabling the intelligence sharing of URBEXers.

- A database to capture individuals who have carried out URBEX activity at a location
- Descriptions and images of that person
- Violence or other notable markers
- Details of incidents they are connected to
- Banning notice copies linked to them
- Links to other incidents and individuals

Where the identification can not be obtained, all available information identifying the person can be stored including a full description e.g. headshot photo, hair, height, gender, ethnicity, tattoos, marks, CCTV/body worn footage to support future prevention and action when detained in the future.

Immediate alerting and notification:

Upon detecting unauthorised access or suspicious activity, the system can generate immediate alerts to security teams. These alerts can include real-time video feeds or location information to help security respond promptly.

Geofencing and restricted area alerts:

Geofencing technology within a CEM system can create virtual boundaries around restricted zones within the building. If URBEX explorers breach these boundaries, the system can trigger alarms and notifications to security, enabling quick intervention.

Record-keeping and evidence collection:

CEM systems can log incidents, including timestamps, camera feeds, and other relevant data. This information serves as valuable evidence for investigations or legal proceedings related to unauthorised access or damage caused by URBEX explorers.

Social media monitoring

Many URBEXers have significant numbers of subscribers/followers on social media (a few active in the UK have over a million). Open Source Intelligence (OSINT) web crawlers can be targeted to provide alerts on any suspicious posts directly into a CEM system.

Neighbourhood communication

Automatically communicate with neighbouring buildings, alerting them of URBEX activities and supporting intelligence. If required, the CEM system can communicate with local policing, networks and enforcement agencies, providing them with real-time updates and necessary information for swift action.

Process and protocol implementation

CEM systems enables authorised staff to build protocols and procedures for handling security incidents involving URBEX explorers. This includes workflow management, form building, evidence processing, information sharing and ensures a standardised and efficient response to such events.

Post-incident analysis and improvement

CEM systems also facilitate post-incident analysis by capturing data and providing analytics. This information helps in understanding patterns of URBEX activity, identifying vulnerabilities, and improving security measures to prevent future incidents.



Scenario 3: Medical Incident

A well-implemented CEM system serves as a backbone during major medical incidents in a commercial building - enhancing response efficiency, coordination, and ultimately, the care provided to those affected.

Incident reporting

A CEM system can provide rapid reporting via a mobile App to notify relevant medical personnel, responders, and stakeholders about the incident, enabling prompt response and resource allocation.

Logging of injuries

Injury forms capture specific details, injury type(s), affected person's personal information, location, date/time, medical facilities, and contributing factors, aiding analysis and prevention.

Collaboration and coordination

It helps in efficiency triaging the incident to different departments of an organisation, managing medical resources like ambulances, medical supplies, and personnel by providing real-time information on availability and requirements. Staff emergency contact details can also be stored and referred to.

Emergency protocols & continuity of operations

CEM systems can disseminate established medical emergency protocols and procedures, ensuring that responders follow standardised practices, minimising errors and streamlining care as well as implementing continuity plans.

Communication with the Public:

It facilitates timely and accurate communication with the public, providing guidance on seeking medical assistance, evacuation procedures, or any necessary precautions to take.

Data protection and access restrictions

CEM systems can limit data access to authorised individuals, minimising exposure, and safeguarding personal data to designated stakeholders.

Evidence and case management

CEM systems provide secure evidence collation involving the gathering of witness statements, linked incidents and CCTV footage - organising and uploading this data for investigations, ensuring comprehensive documentation and analysis.

Legal and litigation protection:

Having a robust health and safety system in place provides legal protection for the organisation, demonstrating due diligence and adherence to safety regulations in case of legal challenges. A CEM system can also support uninsured losses by showcasing compliance and evidence that if not handled correctly would not be covered by insurance policies.

Compliance & Regulation

A CEM system maintains compliance with health and safety regulations and ensures proper documentation of incident reports, providing crucial data for escalation to regulatory bodies. Examples can include; RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations, UK) and OSHA (Occupational Safety and Health Administration, USA) - these external bodies oversee and mandate the reporting of work-related incidents, diseases, and dangerous occurrences for safety monitoring.

Post-Incident Assessment

After the incident, the CEM system assists in conducting a comprehensive review and assessment of the response, identifying strengths and areas needing improvement for future incidents. Regular assessments and audits as part of the health and safety system allow for ongoing improvements, lessons learnt and refining protocols and procedures.



Bring multiple systems into one provides a clear return on investment:

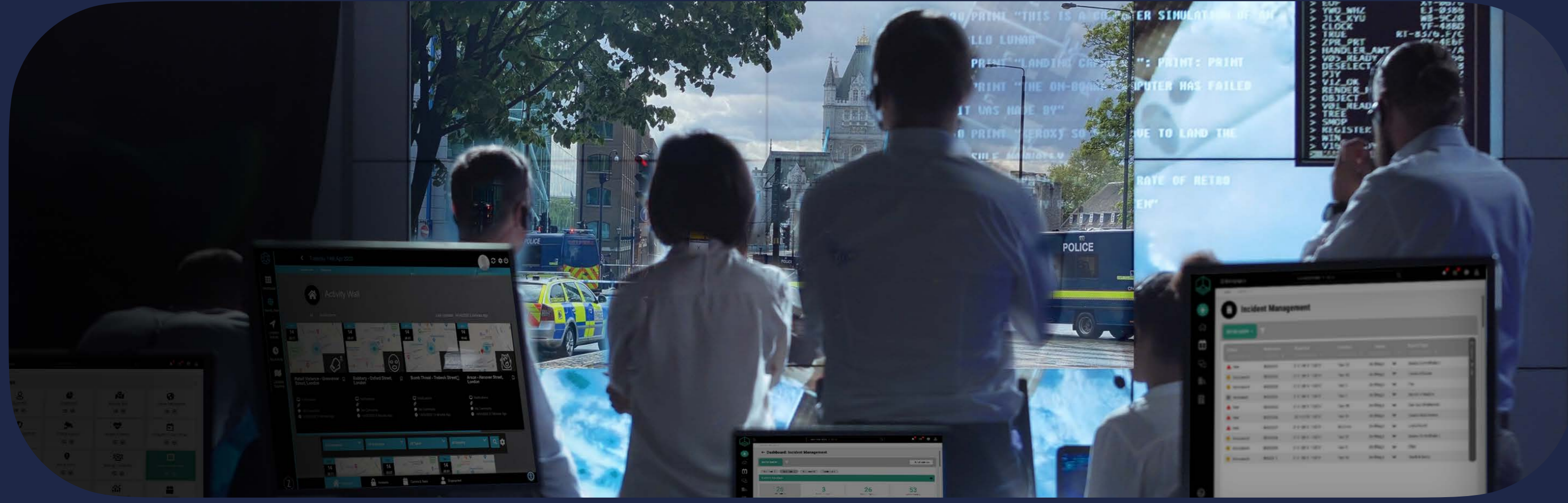
1. Incident management
2. Mass notification
3. Security management & operations
4. Health & safety
5. Patrol management
6. Compliance & task management
7. Case management



Combining systems provides an holistic framework for comprehensive risk mitigation and rapid response. Ultimately, this consolidated approach bolsters preparedness, enhances response efficiency, and fosters continuous improvement, safeguarding both physical security and the well-being of individuals within the environment it serves.



In summary, what are the overall benefits of a CEM system?



A CEM system addresses ineffective and fractured 'tech stack' structures. Too often, these are critical activities (incident reporting, compliance and communications) managed through a combination of manual processes, siloed multi-systems, systems that are not fit for purpose and so complex an IT degree is required, as well as poor process. All leading to multiple points of failure and risk.

A CEM system provides an integrated approach to the management of critical events. It will support teams in the preparation, response, and recovery from events that impact continuity, operations, and safety. In this way, a CEM system intersects incident management, emergency response and communications, risk intelligence and management, as well as crisis management and business continuity.



Early detection & threat identification:

Allowing security teams to proactively address and mitigate risks, preventing them from escalating into major incidents.



Rapid response & decision-making:

Acting as a centralised hub for data collection and analysis, decision-making is more effective, preventing harm and minimising damage.



Improved communication & collaboration:

Seamless communication and collaboration ensure that the right people have access to the right information at the right time, enhancing coordination and response effectiveness.

Resource allocation & deployment:

Security personnel, emergency responders, and assets can be deployed where they are needed most, optimising the security response.

Enhanced situational awareness:

Gaining situational awareness by aggregating data from multiple sources provides security teams with a comprehensive understanding of the evolving situation to make informed decisions against.

Business continuity and resilience:

By identifying vulnerabilities and preparing for critical events, you can minimise disruptions to operations and recover more quickly.

Regulatory compliance:

Helping the location to meet these requirements by pre-defining process, documenting incident response procedures and maintaining records.

Insurance claims:

A CEM system enhances responsiveness, efficiency, transparency, and collaboration - ultimately expediting and supporting a smoother claim and loss adjustment process for insurers.

Continuous improvement:

Allowing the institution to learn from past events and improve their security protocols and become more resilient over time.

Security system & building management system integrations:

A connected eco-system will deliver a unified response to an event, enable the automation of process, and provide data in one place for action and insight.



"Security is paramount in such dynamic environments, and SYNAPSE's capabilities in incident and case management, crisis communication, and organisational resilience are crucial.

We are proud to have such innovative solutions like SYNAPSE fortifying the security infrastructure here to ensure security, resilience and continued success"

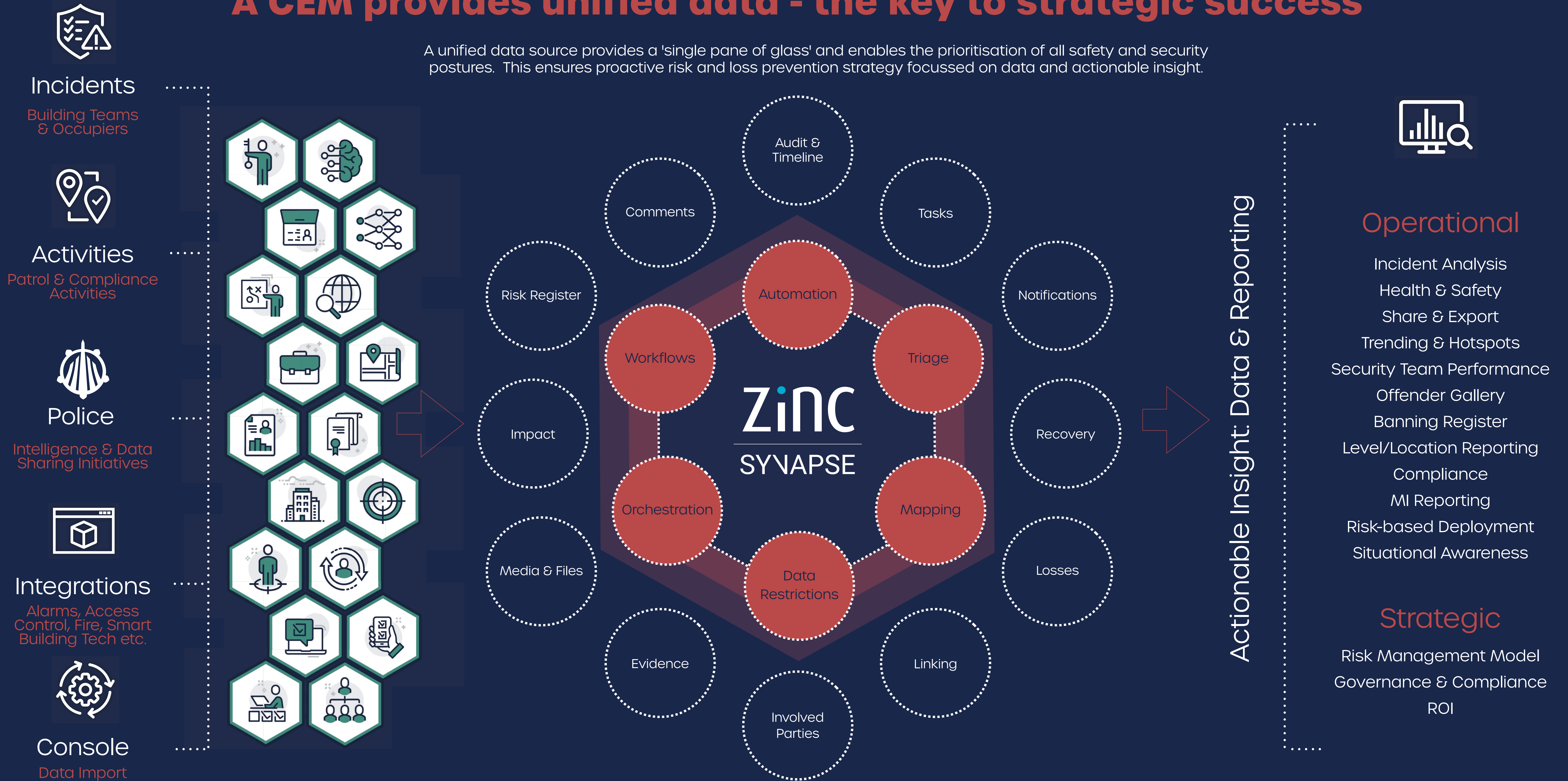
Tony Chebrika, Head of Security
The Peel Group and Media City

Everyone deserves to be safe.



A CEM provides unified data - the key to strategic success

A unified data source provides a 'single pane of glass' and enables the prioritisation of all safety and security postures. This ensures proactive risk and loss prevention strategy focussed on data and actionable insight.



Report

Manage & Investigate

Analyse

Zinc Synapse provides a comprehensive approach to improving security and safety by enhancing a building's ability to identify, assess, respond to, and recover from critical events or incidents that may pose a threat to people, assets, operations, or reputation. It combines processes, technology and communication strategies to minimise the impact of these events.

Zinc provides a framework for early detection, rapid response, communication, collaboration, resource allocation, and resilience planning. By integrating these capabilities, buildings can enhance their ability to mitigate risks, protect assets, and maintain the safety and security of their people and operations.



It is time to unlock the potential.

Resilient buildings, informed teams,
controlled operations.

With risk and technical landscapes both evolving at pace, it's clear to see that the cost of doing nothing or simply not doing enough, is one that can have catastrophic impacts.

Get in touch to learn how Zinc Systems can support your business to achieve high standards of control during critical events and how our Critical Event Management system 'Synapse' delivers a unified, consistent and seamless process, within a user centric design, tailored to an organisation's priorities, process and strategy.

Act now if critical events occur in your location and discover that the price of a CEM system is surprisingly affordable.

Find out more at: www.zinc.systems

Key Contacts:

Joe Zielinski, Chief Executive Officer - joe.zielinski@zinc.systems

Sophie Malone, Chief Commercial Officer - sophie.malone@zinc.systems

ZiNC
SYSTEMS

