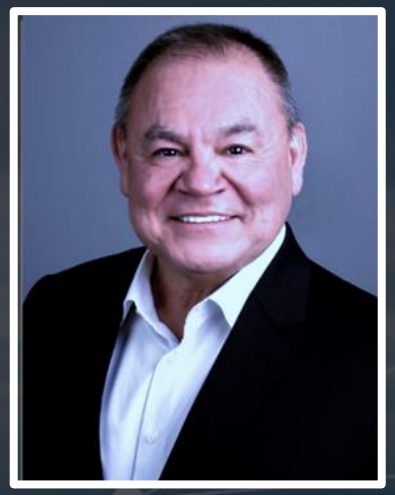

ALLIED UNIVERSAL®
RISK ADVISORY AND CONSULTING SERVICES
There for you.
PHYSICAL SECURITY STRATEGIES
PENETRATION TESTING & CRISIS MANAGEMENT
RISK ADVISORY AND CONSULTING SERVICES: THERE FOR YOU.®

©AlliedUniversalRISKADVISORYANDCONSULTINGSERVICES



ART FIERRO, CISM, CPP

VICE PRESIDENT, GLOBAL INVESTIGATION PRACTICE

ALLIED UNIVERSAL® RISK ADVISORY AND CONSULTING SERVICES

Art.Fierro@aus.com | 972.209.6931

- Corporate Security Executive for F500 Corporations (Fox Entertainment Group, International Paper & Blue Origin) in various global industries
- Expertise in Critical Incident Management, Business Continuity, Threat Management, Physical Security, Investigative Programs, Security Business Analysis, Enterprise Security Risk Management Strategy
- Former FBI Supervisory Special Agent – managing Violent Crime, White Collar Crime, Cyber and National Security matters
- Certified Information Security Manager (CISM) and Certified Protection Professional (CPP)

© Allied Universal

PHYSICAL SECURITY

CONCENTRIC CIRCLES OF SECURITY

© Allied Universal

PHYSICAL SECURITY

PENETRATING TESTING

- A physical penetration test sets out to uncover weaknesses in your physical security.
- Also known as physical intrusion testing, attempts to compromise perimeter security, intrusion alarms, motion detectors, locks, sensors, cameras, mantraps and other physical barriers to gain unauthorized physical access.
- There are globally accepted industry-standard frameworks for physical penetration tests. At a minimum, the testing framework ought to be based on the NIST Special Publication 800 Series guidance and Open Source Security Testing Methodology Manual OSSTMM.
- A physical penetration testing is intended to uncovers real-world vulnerabilities in the physical barriers and the systems that support them, meant to protect employees, sensitive information, and expensive hardware.

© Allied Universal

A THOROUGH PHYSICAL PENETRATION TEST HAS

MANY STAGES

Passive Reconnaissance

Information gathering about the target's surroundings and environment, perhaps using a tool such as Google

Active Reconnaissance

Obtaining information through telephoning, emailing or otherwise directly querying target staff or vendors

Attack Planning

Use what's been learned about vulnerabilities, exit and entrance points, cameras, guards, fences, company technology, staff members, and more

Infiltration Exploitation

Carrying out the planned attack

Open-Source Intelligence

Taking advantage of freely available information about the target as well as its people and specifics about the environment

Covert Observation

Stakeouts, drones, and covert photography help identify physical security controls and monitor staff as they are coming and going

Pretexting

Ensuring the testing equipment, transportation and personnel are ready to roll

Post-Exploitation

Penetrating further into the environment and setting up to maintain a persistent backdoor

© Allied Universal

PHYSICAL PENETRATION TESTING

WHAT'S INCLUDED?

- Doors & Locks
- Sensors & Cameras
- Security Guards
- Physical Barriers
- Biometrics
- Situational Awareness
- Door Bypass & Lock Picking
- On-Site Reconnaissance
- Covert Infiltration
- Overt Operations
- Character Impersonation
- ID Cloning

© Allied Universal

PHYSICAL PENETRATION TESTING
DETAILS

- **Bypass Doors:** If the building uses an electronic key or combination lock, a clone a badge may be used, leverage widely available master keys, or may use special tools on improperly hung doors to gain access. If doors or windows are left propped open or are unlocked, those may be leveraged as an easy method to gain access.
- **Bypass Physical Barriers:** If a location has fencing, gates, or other physical barriers, consultant may climb the fence, leverage gaps in the fencing, or bypass gate controls using publicly available techniques.
- **Identify Ways to Steal Information:** Once consultant has gained access to a location, the penetration tester will observe ways to obtain confidential or sensitive information. This could include identifying unattended computers with active sessions, abandoned access cards, computer screens with confidential data facing common areas, or sensitive information in the trash.
- Consultants do not remove equipment; they will take a photo as evidence of damage that could be done.
- **Network Jacks in Public Areas:** The consultant may attempt to connect to the company network by connecting their device through network jacks in community areas (i.e., conference rooms, break rooms) to identify opportunities to harm.
- **Gain Access to Sensitive Areas:** The consultant may attempt to gain access to sensitive areas of a building, including server rooms, executive offices, or other identified locations. If a bad actor gained access to this room, they could easily disable the machines. They might also use unattended peripherals to steal data or introduce a virus.
- **Check the Trash:** The consultant may look into the types of materials that employees discard and whether the company has a shredding policy and available shredders. If this kind of information makes it to a dumpster, criminals will find it easy to steal.
- **Social Engineering:** Social engineering techniques could be leveraged to gain access to a location by tailgating or leveraging a pretext to mislead employees and convince them to allow access to the building or sensitive information or locations within the building.

© Allied Universal

RISKS

CIVIL UNREST THREAT

EMPLOYEES

Recent civil unrest events have proven that **employees attempting to prevent criminal activity** can be harmed. It's best to close and send employees home as soon as you're aware of civil unrest in your area.

PROPERTY

Criminal activity such as **theft, looting, and arson is more likely to occur after dark**, particularly in urban environments where there is easier movement between areas. Response limitations on law enforcement personnel have the potential to exacerbate this situation.

REPUTATION

Recent trends indicate that reputational risk with financial impact can be caused **when a business or its key leadership is associated with a political party or candidate**. The specific threats from social media call for boycotts.

INFRASTRUCTURE

The biggest infrastructure risks will likely be to **private property and retail storefronts which are in or near protest areas** and not necessarily a focus of law enforcement.

© Allied Universal

DETERRENCE

SECURITY POSTURE

- Minimize presenting facilities as a soft target for opportunistic criminal activity.
- Visible Security officers and off duty Police Officers
- Decommissioned PD vehicles parked onsite
- Visible CCTV Cameras covering outer perimeters
- A proactive plan (Crisis Management Plan) in place can deter criminal activity and aid in protecting employees and assets.
- Intelligence Collection ability

© Allied Universal

PREPARE

SECURITY/EMPLOYEE TRAINING

- Crowd Control & Special Event Security
- Civil Disturbance Situations
- Media Management
- Strikes, Pickets & Crowd Control
- Difficult People or Situations
- Situational Awareness
- Emergency Preparedness
- Threat Management Team

© Allied Universal

PREPARE

BUSINESS CONTINUITY

Make necessary arrangements in advance for repair and recovery resources to clean up and restore damaged sites and resume revenue resumption.

© Allied Universal

PREPARE AND RESPOND

CRISIS MANAGEMENT PLAN

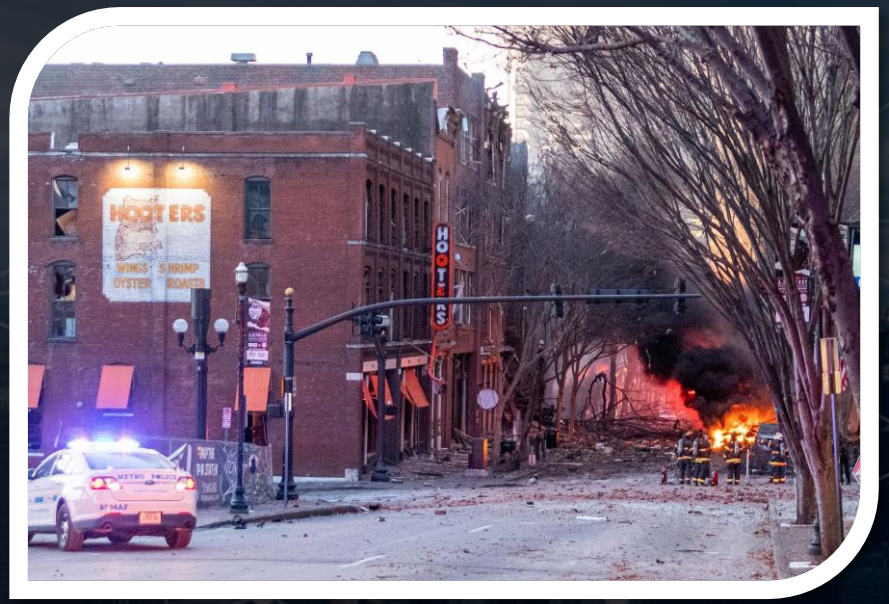
Conduct tabletop exercises for security and GSOC operators to ensure they are fully prepared for potential threats and emergency situations.

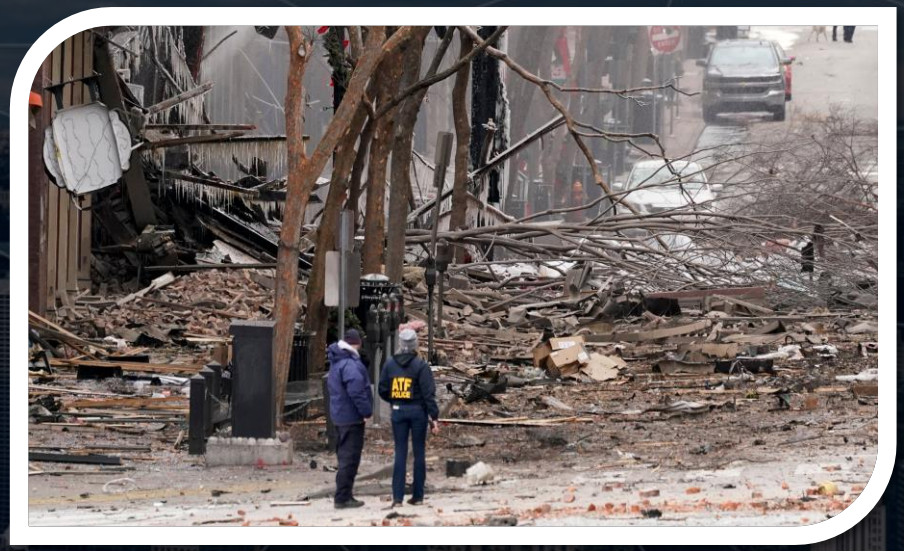
Command (manages)	Operations (does)	Planning & Intelligence (plans)	Logistics (cares)	Finance (pays)
• **The team: Legal executive liaison, Communications, safety and security chief** • **Manage overall crisis response** • Determine priorities and objectives • Direct and control group • Obtain resources • Coordinate with executive leadership • Settle disputes and conflicts • Take direction from the incident commander.	• **Handle the tactical operations in the crisis response** • **Perform initial damage assessment** • **Oversee frontline responders** • **Establish control over the situation** • Compile status reports • **Business Continuity – at end of CIM process**	• **Gather, analyze, and share information on the crisis** • **Assess status reports** • **Recommend action** • Business continuity, **corporate communications, legal,** investor relations, representatives of key lines of business	• **Support human needs,** such as food, shelter, transportation, medical care, and counseling for the crisis team and the organization • Team includes representatives from HR, travel department, meeting services, and employee assistance program	• **Track and document all costs and expenditures of the crisis response** • Handle payroll, emergency purchase orders, cash needs, and purchasing cards • Coordinate with insurance on claims and worker's compensation • Provide administrative support • Team includes finance, risk, insurance, payroll, treasury, and procurement functions

© Allied Universal

CRISIS MANAGEMENT PLAN

HELPING WITH THE UNEXPECTED



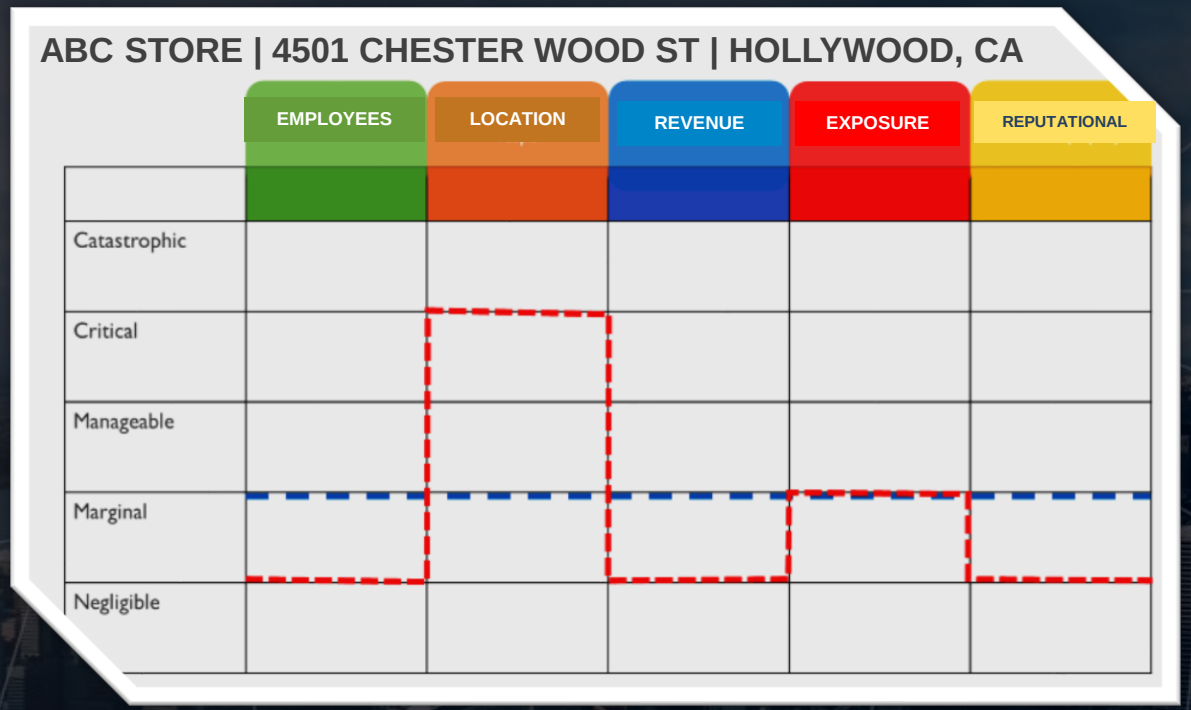


2020 NASHVILLE CHRISTMAS DAY BOMBING

© Allied Universal

PREPARE

PRIORITIZE & RANK YOUR RISK



- Establish what the critical assets are
- Map your risk
- Overlay your business and assets over your risk
- Have a standardized risk scoring methodology that can easily be applied right through EVERY layer and function
- There may not be an exact formula that fits every organization

EMPLOYEES	Score
1 – 20 %	1
21 – 40%	2
41 – 60%	3
61 – 80%	4
81 – 100%	5

LOCATIONS	Score
1 – 20 %	1
21 – 40%	2
41 – 60%	3
61 – 80%	4
81 – 100%	5

Revenue	Score
1 – 20 %	1
21 – 40%	2
41 – 60%	3
61 – 80%	4
81 – 100%	5

Exposure	Score
Negligible	1 – 5
Marginal	6 – 10
Manageable	11 – 15
Critical	16 – 20
Catastrophic	21 – 25

Risk	Score
Insignificant	
Low	
Medium	
High	
Extreme	

Risk Score will help you prioritize security spending

© Allied Universal

PREPARE

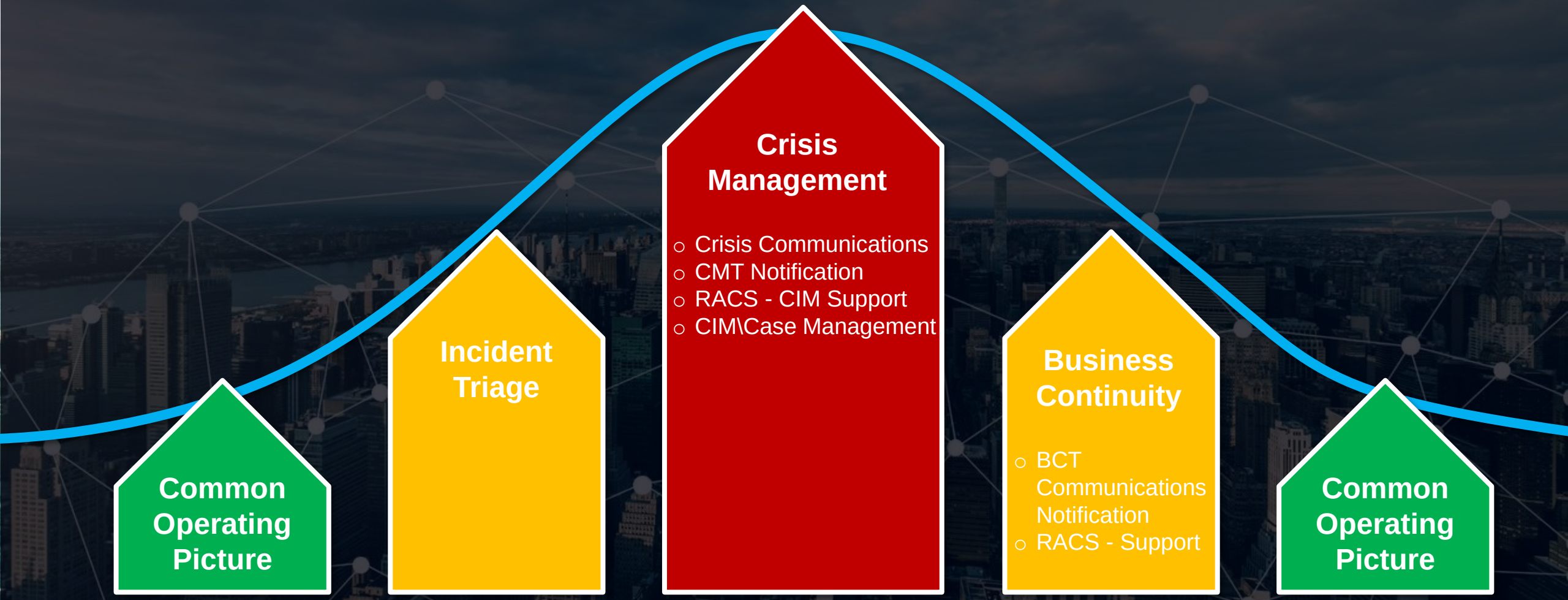
TRIGGERS

EMERGENCY (MANAGEABLE)	TRIGGERS	CRISIS (CRITICAL)
Serious injury to single employee. (A fatal injury on site would by its nature immediately become a crisis).	Medical expert suggests injuries may be fatal Informational that further persons are involved	Multiple injuries / single fatal injury on site.
Fire, quickly contained, building able to be occupied soon after fire has been extinguished.	Fire spreads	Fire out of control, rendering building or buildings uncopiable for more than 4 hours.
Power outage.	Report that issue cannot be resolved Business continuity measures fail	Information coming forward to say that power will be down for more than 4 hours.
Servers all down.	IT has no understanding what's wrong	Information coming forward to say that servers will be down for more than # hours –impact dependant on type of business.
Minor infrastructure malfunction (flood, storm damage, etc).	Environment agency report more rain due	Loss of control of premises (flood inundation, etc).
Criminal/civil breach causing minor disruption – control of premises remaining in company hands.	Police report increased civil unrest Social media suggests that large gang near to infrastructure	Criminal/civil infraction causing significant disruption - control of premises out of company hands.

© Allied Universal

PREPARE, DETER, DETECT, RESPOND, RECOVER

CRISIS MANAGEMENT CYCLE

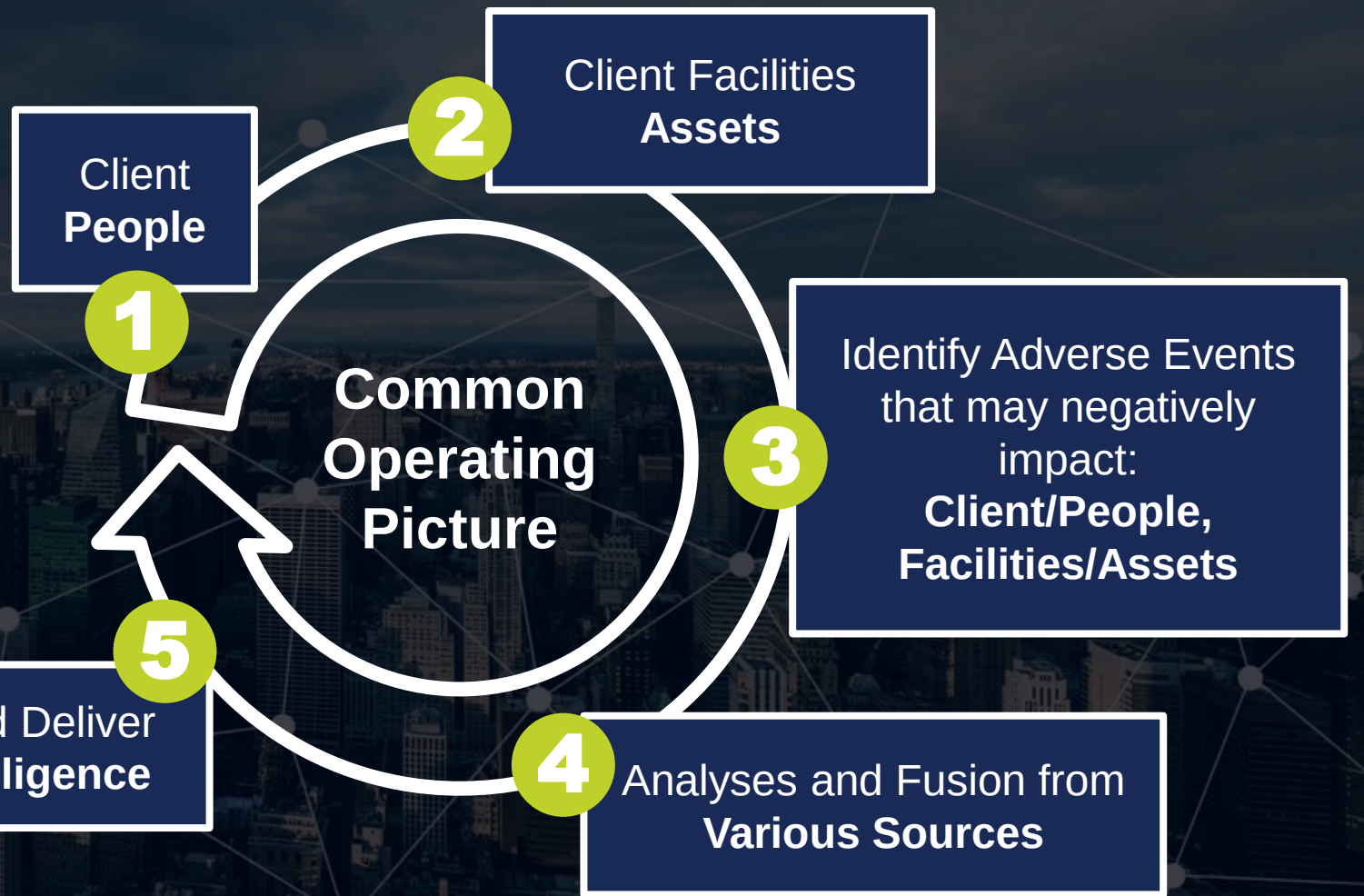


© Allied Universal

DETECT & RESPOND

INTELLIGENCE CYCLE

Intelligence support during a time of unrest (Crisis Management) will also allow local operations to have a near real-time overview of the local climate and operating environment should tensions rapidly escalate.

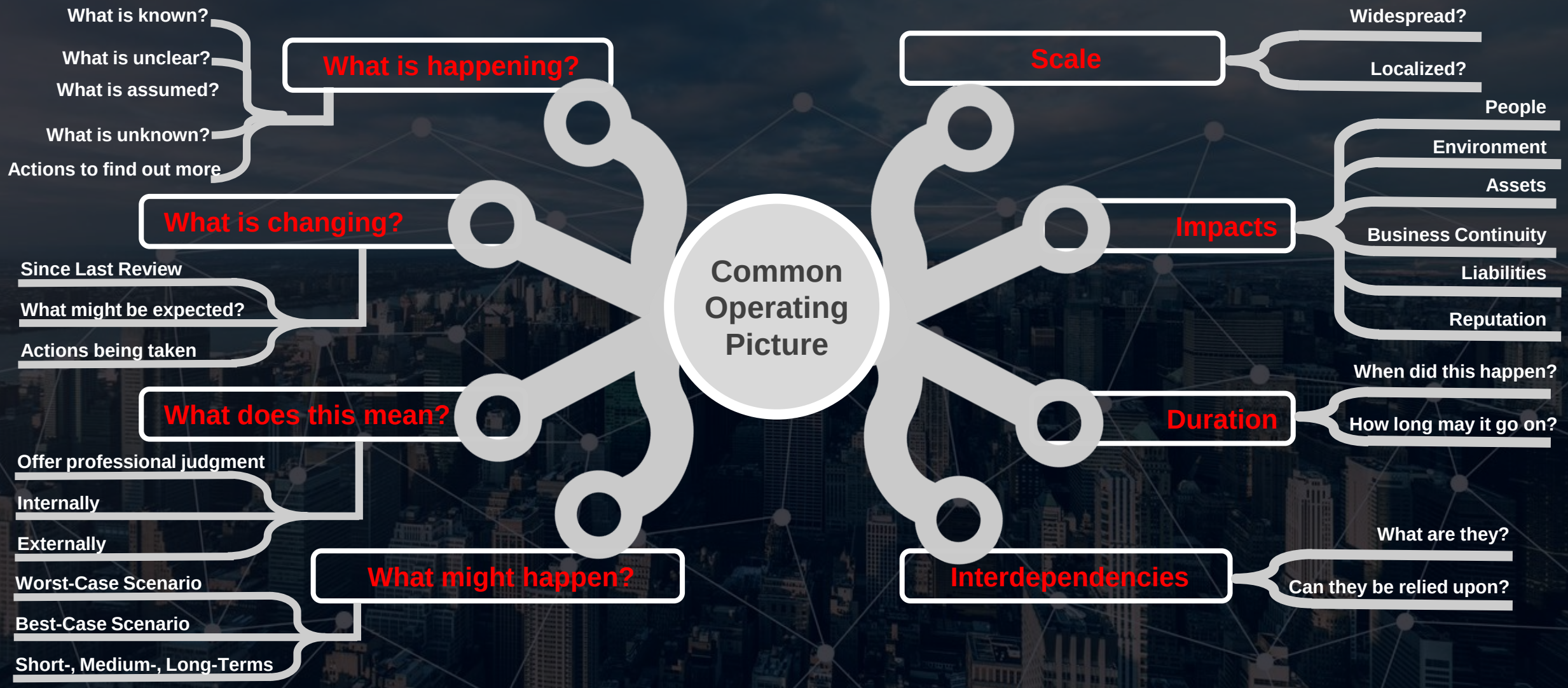


Dissemination of threat information to client:
Timely
Actionable
Relevant

© Allied Universal

INTELLIGENCE FOR RISK AWARE DECISIONS

COMMON OPERATING PROCEDURE



© Allied Universal

DETECT

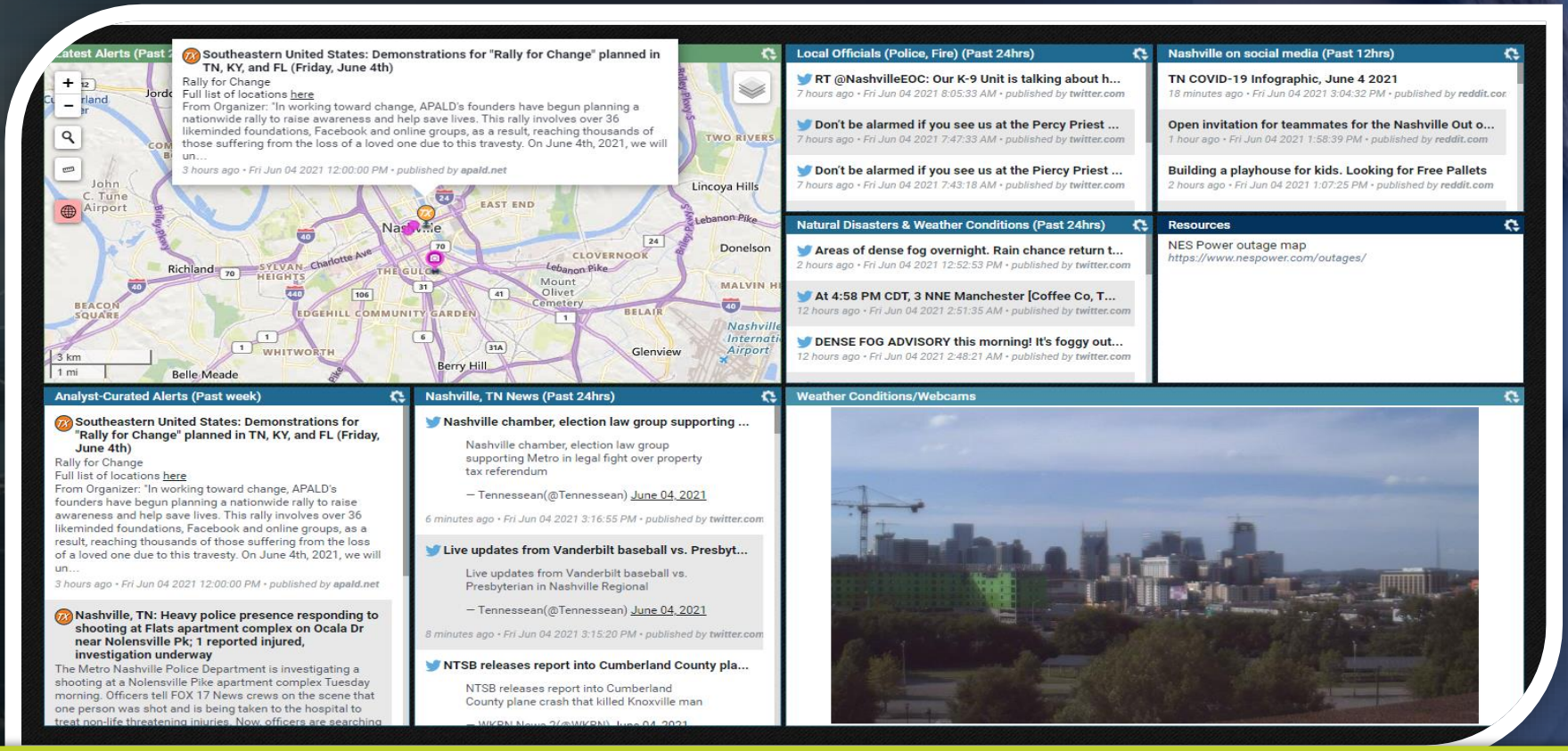
ROBUST INTELLIGENCE CAPABILITY

Intelligence during a time of unrest is a view into oncoming threats. Allow for near real-time view of the local climate and operating environment should tensions rapidly escalate.

© Allied Universal

DETECT & RESPOND

TECHNOLOGY ASSISTANCE



Geospatial commercial services that use information overlays from a variety of services pushed to you. Help make sense of a fast moving adverse event.

© Allied Universal

RESPOND

INTELLIGENCE MONITORING

LOCATION & BRAND THREATS

Opportunists criminals continue use social media to communicate, coordinate, and disseminate information. These individuals use simple words or phrases to create a “trending” topic that allows others the ease of access to current information ranging from demonstration locations to police responses.

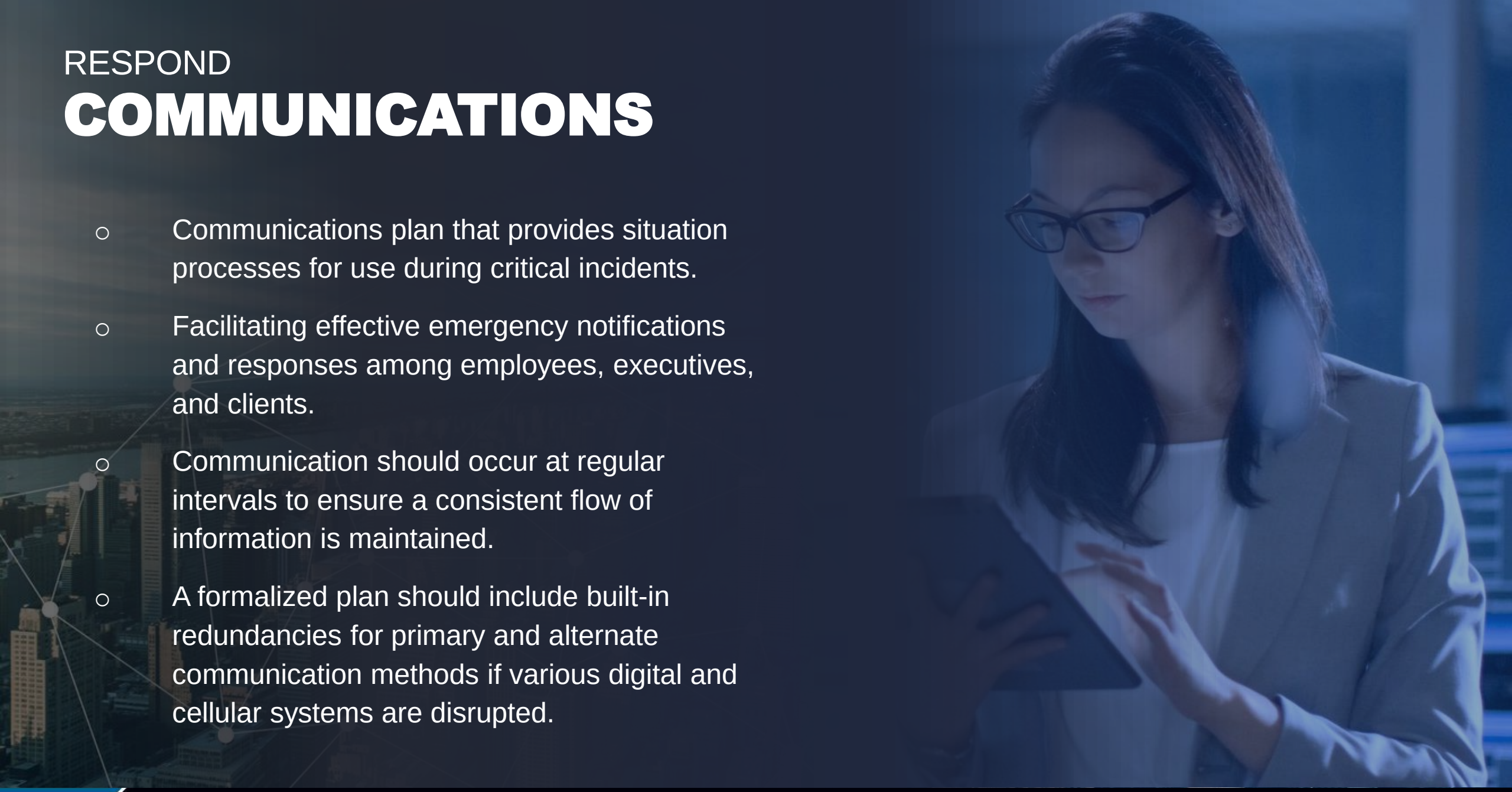
- Monitoring social media or online forums and acting upon credible threats and trends will allow security details and site managers to adequately prepare to deter any threats.
- Subscribe to local, state, and federal governmental outreach programs and intelligence products such as OSAC, DSAC, state intelligence fusion centers, etc.
- Use your liaison contacts with local, state, and federal law enforcement personnel for intelligence and information sharing.
- Participate in business alliance groups for intelligence and information sharing.

© Allied Universal

RESPOND

COMMUNICATIONS

- Communications plan that provides situation processes for use during critical incidents.
- Facilitating effective emergency notifications and responses among employees, executives, and clients.
- Communication should occur at regular intervals to ensure a consistent flow of information is maintained.
- A formalized plan should include built-in redundancies for primary and alternate communication methods if various digital and cellular systems are disrupted.



© Allied Universal

RESPONSE COMMUNICATIONS

OPERATING RHYTHM

© Allied Universal

PREPARE

BUSINESS CONTINUITY PLANNING

TRANSPORTATION

Routes should be reviewed, contingency plans made include alternative routes, particularly if the primary route travels through areas likely to encounter civil unrest.

SECURE RESOURCES

Securing resources prior to crisis events will be critical to success. When planning for coverage, a minimum of two security personnel should be stationed at a location where security will be needed.

SECURITY SYSTEM TESTS

Check all CCTV, security, fire, and alarm systems are operational. Ensure process for either mechanical or electronic lock-down of perimeter doors is in place. Companies should also consider retaining video footage for a minimum of 30 days.

OUTSIDE INSPECTION

No high-value objects next to the front door or visible through windows and the proper security storage of high-value assets. Remove objects that could be used for blockades or projectiles.

© Allied Universal

ALL TOGETHER NOW

THREE IMPORTANT FUNCTIONS

© Allied Universal

WELFARE

CRISIS MANAGEMENT TEAM

- A crisis places exceptional demands on managers and their support teams
- CMT members should ensure that they take into account the need to sustain a response at high levels of intensity
- They should also anticipate the needs of staff that may be working at extraordinary levels of activity
- Prepare for after-action crisis management team support (EAP, etc.)

© Allied Universal

ANY QUESTIONS?

David J. Blake, CPP
Sr. Director
Allied Universal® Risk Advisory and Consulting Services
Florida | Mid-Atlantic | Southeast - Market Lead

615.521.4148 | david.blake@aus.com

© Allied Universal