Military Processes for Crisis Management

- How they can be applied to a Civilian environment using technology.

INITSYS

Military Processes for Crisis Management - How they can be applied to a Civilian environment using technology.

Following processes printed on a piece of paper is a thing of the past. Automated Scripting eliminates mistakes and allows operators to focus on the important things. In both a Military and Civilian environment the processes behind managing a crisis have become critical, and in this article we will look at how automated scripting and making the very best use of the technologies available can vastly improve and speed up Crisis Management in a Military and Civilian environment, as well cut out errors and the element of doubt.

In the Military, a failure to prepare is simply not an option. Plans must be put in place for every eventuality, including what to do if those plans fail. As such, Armed Forces from all over the globe have developed processes for dealing with a Crisis that can be applied to a Civilian environment. They can help how your business might deal with a major incident, or even something as seemingly menial as a burst pipe in your village. In this article we can take a look at some of the processes developed in the Military and how technology can help you to translate those into more everyday scenarios.

The recent wars in Iraq and Afghanistan, and the type of warfare experienced by militaries of many nations in those conflicts, have created a need to develop crisis strategies to deal with events of varying severity.

Recently, I published an article in the Crisis Response Journal about how Merlin deals with the very modern threat of terrorism. In this article, we will look at how technology can be applied to some of the crisis strategies developed by the military to deal with incidents of varying severity on the front lines or bases, and how the same principles could be applied in the civilian world. To our benefit, former service personnel of various nations have written documents on how they dealt with crisis management in a military environment. We can look at these documents to see common trends on how significant incidents would be dealt with and how Merlin can be used to help manage those incidents.

In the first instance, we can look at the input of former British Army officer Lieutenant Colonel Mark Wenham and former U.S. Army Colonel Jimmy Blackmon who both inevitably look at planning and preparation as the first step. At this stage, it is necessary to analyse the nature of a crisis and what risk it presents, and to whom. Though it is impossible, especially in a military environment, to identify every single potential threat, there are many that can be planned simply by identifying those more obvious and as a result of conducting After Action Reviews and analysing lessons identified. Jimmy Blackmon, a former Task Force Commander in the 101st Airborne Division, provides us with a great example to which we can use some of the available technologies to demonstrate how the software can help in these sorts of scenarios (Leadership In Crisis – 5 Steps of Crisis Management. April 13 2020). As a Task Force Commander, Colonel Blackmon was in charge of a force of soldiers stationed at an outpost in Nuristan Province, Afghanistan, accessible by air only. This meant that all supplies, including ammunition, rations, and medical equipment, had to be delivered by helicopter. It also meant personnel had to be flown into and out of the outpost in the same way.

For Blackmon and his team, this represented a significant risk. Under any large-scale attack, his Task Force would be completely cut off and dependant on their abilities to deal with the situation. In this scenario, this meant having plans to deal with the care of casualties, the distribution of supplies, and, if necessary, a procedure to call in a relief force or medical evacuation. Colonel Blackmon and his team therefore had to determine what threats could present themselves and how to deal with them from the moment an incident starts to the moment it is filed as complete. Much of these processes were in a hard copy format, held in files with duplicate copies stored at secondary locations. Many businesses may have similar plans outlined in the event of a crisis, and whilst the nature of that Crisis might differ to those experienced by Colonel Blackmon and his team, the principles behind it remain the same. Some of the key points from phase 1 of Blackmons strategy include:

- Who is in your plan? – It may sound obvious, but you need to determine who is involved in your plan, and at what stage. You simply cannot, at any point in the process of handling a major event, not have critical information such as who to contact next available to you at your fingertips. This may include key personnel from the emergency services, security officers, primary liaison with your customer, anyone that may be affected as a result of the event, and any employees of your own that may be at risk. Remember, the technology is now there to store this data, and automatically handle making contact with them from the moment an event takes place

- ·What are their roles? - Do you know the role the each person will take in handling this event? With the Technology now allowing for different stakeholders to receive different information relevant to their role, it is no longer simply a case of identifying someone and calling them with generic information of the event, the technology can take these individuals to temporary flash pages, with all the data they would need to carry out their role to the letter. In a military world this may be information sent to medical teams, but for your business it could be the teams that will secure a building after a significant break-in, or those that evaluate any losses.

- ·What are your processes? In Tony Jacques Relational Model of Crisis Management he argues that Crisis Management is not “a linear process of sequential phases in which you manage one issue at a time.” I believe that Jacques is correct. The technology now allows for multiple processes to be handled autonomously and to change depending on the way an event might evolve. It is no longer acceptable that a process consist of “Do this, do that”, it must ask questions and change the way it reacts dependant on how those questions are answered. Consider your process, do you have every eventuality covered?

- Discuss the threat, your plans to react and train your staff – It is essential that the threats identified and your processes for handling them are reviewed regularly. Changes in technology might allow you to handle the incident differently or previous incidents might not have gone as well as you hoped. Stay proactive in your approach to handling these events and ensure that the processes are run-through and that all stakeholders are fully trained in their roles.

Once a crisis has been analysed and how it might best be handled, it is possible to look at how the technology can be alerted of this crisis and how those processes can be put in motion. In Blackmon’s example, the technology presents several options in terms of how this can be achieved. Firstly, we can consider how the threat of an attack can be passed to what Blackmon refers to as the CAC, or Crisis Action Centre. In a military sense, this might be Task Force Headquarters or Brigade H.Q. Crisis input terminals can be fine-tuned by its users to allow events to be raised by the click of a button, putting a process into motion. For example, a crisis input terminal could be located at each Combat Outpost (COP), allowing personnel in these positions to alert the CAC in the event of an attack immediately.

Crisis input would allow those stationed in those positions to determine the attack's key details, such as the number of enemy combatants and information on any weaponry they are bringing to bear on the COP. Having received this information via Crisis Input sent by those on the ground, the direction from which the attack is taking place will be known, allowing a specific set of procedures to be put into action to counter the threat. It will also be possible for those within the CAC to send alerts to other COPs, both manually and automatically, warning them of the attack. In such a scenario, it will be possible for those manning observation posts or checkpoints away from the point of attack to confirm whether something is also taking place at their location. This information is vital to determining how best to deal with the situation. How can the same methods of triggering an event be used in a civilian environment? Take away the battlefield, and consider how the threat of terrorism could be handled in the same way at a concert venue or sports arena.

In his article (Leadership and Teamwork in Crisis Management: A Military Perspective), British Army Officer Mark Wenham speaks of the need to clearly define roles and responsibilities based on an individual's competence in a particular position. This information can be added to the processes so that specific jobs or roles can be passed on to the individuals to which they have been assigned. Again, the terminals found in the COP's and medical facilities or other facilities can alert the personnel stationed in those areas that they are needed elsewhere or to prepare for the potential influx of casualties. In a civilian environment those processes need not be any different. The technology can be used to alert first aiders or additional security officers, and help in the allocation of resources depending on how the event evolves.

Through the process flow, it is possible to define these tasks to reduce or eliminate the element of doubt about what steps should be taken next. It also provides flexibility that will be required in these circumstances to allow those processes to evolve depending on how the situation changes. For example, suppose the COP begins to incur casualties, and it becomes necessary for wounded personnel to be medically evacuated. In that case, through Merlin, the Medical Emergency Response Team (MERT) could be activated. If a protocol allows for it, the process of sending off for medical aid or air evacuation can be entirely automated via both calls to an external command post or via messages sent to terminals at those locations. This automation allows for personnel in the CAC to continue to deal with the procedures that require human interaction.

Using the information received from a terminal at the beginning of the attack, the technology can also provide the CAC with direct links to any CCTV situated in the area where the attack occurs, allowing them to monitor the situation as it evolves. This CCTV will be recorded, and all footage saved to the database to be used later as part of the post-event analysis or within After-Action Reports (AAR's). These reports are vital, and Colonel Blackmon defines the After-Action Review as Stage 5 of his process. In a Civilian world the it is unlikely you will call it an AAR, but the same method should be applied. As broken down by Blackmon:

1. What did we say we were going to do?
2. What actually happened?
3. Why did it happen?
4. What did we learn?
5. What will we do to prevent it from happening again, or do we have a new best practice?

In many instances, scenarios like that detailed above would be dealt with using more standard forms of communication such as radios and procedures in paper form. It is also necessary to consider that the primary CAC may not be able to deal with the incident locally due to the nature of the attack. Therefore, it is necessary for other CAC's, perhaps at a higher H.Q., to receive the same signals from the COP so that the same procedures can be put into motion regardless of where that CAC happens to be located. In a civilian environment, this may be classified as Force Majeure, which can be defined as interrupting the expected course of events and preventing participants from fulfilling obligations.

It is also possible to apply some of the technology to a military environment that may not necessarily be in a warzone. For example, if we look at military bases situated in the U.K., such as airfields or army barracks, we can see how that technology may improve and speed up the process with which some crises are handled that are quite similar to incidents that may occur on a civilian premises.

Royal Air Force Officer Jon Short believes that there is enormous potential in using software like Merlin to handle situations in which Duty Guards or Military Police stationed at checkpoints or gatehouses can quickly and efficiently call in more personnel in the event of an incident taking place. Again, we can look to a crisis input application and terminals stationed at these checkpoints to alert many personnel without the need to physically contact each one separately, as is currently the method. Flight Lieutenant Short called to example the moment the news reached military campuses in the U.K. of the passing of Prince Philip. In this instance, several Senior Officers needed to be alerted to the news, each of which had to be contacted individually by phone.

Using one of two features within Merlin, this could have been achieved automatically, either via a call from a text to speech application, or by sending a notification to a custom-built mobile or tablet application. In both cases it is possible to determine whether that message or notification has been received. It can also, if necessary, seek a response from the individual to determine the next course of action.

The same can be applied to instances where there is a physical threat from a terrorist or otherwise. Again, Crisis Input can be used for personnel stationed at strategic locations to immediately alert a control room in the event of a significant crisis. As described above, many of these steps can be automated, including the mobilisation of additional forces or the closure or evacuation of various areas of a campus.

In all examples of crisis management within the military, one of the more key stages is the after-action review or post-event analysis. In-depth reporting features means that every step taken when the event was live is recorded to the database, from the moment it is reported to when it is closed. This includes the actions of personnel key to the event, such as those who raised it, those who dealt with it, and those who were contacted. Audio recordings of any communication made through the system and complete footage from any associated CCTV are recorded in the database. This information is all exportable as graphs or presentable PDF reports that can be used in post-event reviews to determine how well the situation was dealt with and what lessons could be learned. These reports also allow commanders or team leaders to assess their staff's performance and fine-tune any future training to ensure that any similar event in the future is dealt with more efficiently.

www.initsys.net

0845 3301 445

20 - 22 Wenlock Road, London, N1