How Belfius Bank's response to the terrorist attacks in Brussels helped embed business continuity in the company culture

Ludo Jappens

Received (in revised form): 1st August, 2017

Belfius Bank Belgium, Rogierplein 11, Brussels 1000, Belgium
Tel: +32 (0)2 222 67 36; E-mail: ludo.jappens@belfius.be

***Ludo Jappens** is a business continuity and crisis management coordinator at Belfius Bank Belgium, where his team won the European and Global Award for 'BCI Continuity and Resilience team' in 2016. He has been an active member of the Belgian chapter of the Business Continuity Institute since it was first established. He has a degree in applied economics.*

Abstract

Until 2015, major terrorist incidents in Belgium were considered a 'black swan'. However, the suicide attacks in Paris on 13th November, 2015 provided a wake-up call. Investigations revealed that the raid was prepared in Belgium by jihadists who grew up in Brussels and was coordinated by Belgian ISIS fighters in Syria. In an instant, it became clear that terror had been embedded in Belgian society and could erupt at any moment. At Belfius Bank Belgium, the subsequent months were a rollercoaster ride of terrorist-related events. Business activities were strongly affected, as the company's head office is located in the centre of Brussels. This paper focuses on the way Belfius responded to the events and how the lessons learned have helped to improve its business continuity and crisis management capability.

Keywords: Brussels, terrorist incidents, response plans, resilience

Ludo Jappens

THE FIRST TERRORIST EVENT: THE BRUSSELS LOCKDOWN OF NOVEMBER 2015

Belgium uses the Coordinating Body for Threat Analysis (OCAD) indicator to express the level of terrorist threat, ranging from '1 — low' to '4 — very severe'). Level '4' means that an attack is imminent or has already struck. Figure 1 shows how the OCAD indicator was influenced by the terror-related incidents in Brussels.

The day after the Paris attack (13th November, 2015), OCAD raised the threat level to '3 — severe'. This was the trigger for Belfius Bank to think seriously about preventative actions. An important criterion for the raised vigilance was the finding that Salah Abdeslam, the jihadist who did not blow himself up in Paris, had returned to Belgium and disappeared somewhere in the Brussels area.

On Saturday morning, 21st November, OCAD uncovered decisive evidence of an increased terrorist threat and raised the OCAD level for the Brussels area to '4'. Brussels was immediately transformed into a no-go zone: schools closed their doors, public transport suspended all traffic, and mass meetings were cancelled.

On Sunday, 22nd November, television, news sites and social media broadcasted

Journal of Business Continuity
& Emergency Planning
Vol. 11, No. 2, pp. 117–127
© Henry Stewart Publications,
1749–9216

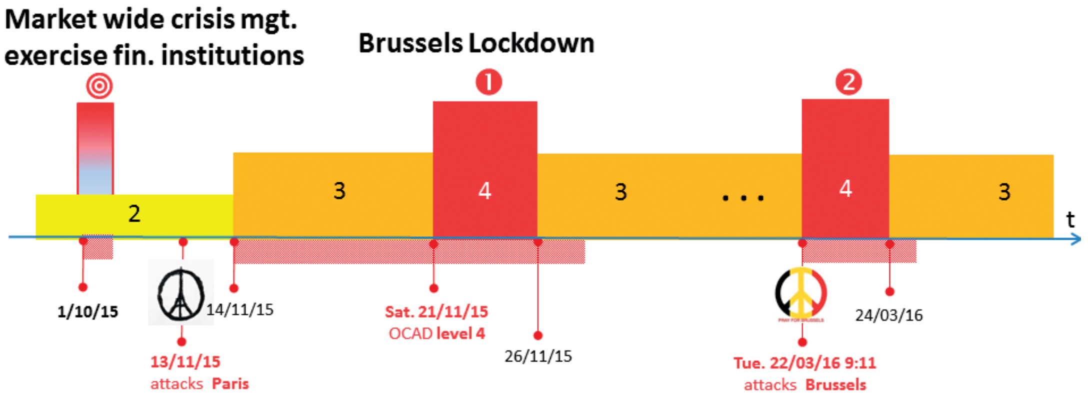

Figure 1 Timeline of the terror-related incidents in Brussels

Source: Belfius presentation material

pictures of soldiers and police patrols on duty in the deserted streets of Brussels. The authorities insisted on more discretion regarding the filming of police invading suspicious houses, fearing that this would harm their actions. Social media responded with an inventive proof of self-control: the exchange of cat photos instead. The perception of danger rose to unbearable heights. By 8.00 pm, every citizen was convinced that going to work in Brussels on Monday would not be a good idea.

BELFIUS BANK'S RESPONSE TO THE LOCKDOWN

The international press identified the Brussels borough of Molenbeek as the breeding ground for terrorism in Western Europe. Businesses located in the city got nervous during the course of that Sunday evening and activated their crisis teams.

Belfius Bank, however, had already moved to a status of 'raised awareness' the day after the Paris attack of 13th November. In the subsequent week, tactical teams covering human resources, communication, facilities and business continuity decided on preventative actions. This 'preliminary stage' involved the crisis management organisation switching to a stand-by mode.

Activating the tactical and strategic players as soon as OCAD raised the terrorist threat level to '4' was achieved in a minimum amount of time. One downside to overcome was the fact that all crisis actors intervened remotely from home. This complicated collaboration somewhat, but did not lead to any insurmountable difficulties thanks to the cushion of a gradual deployment with little time pressure. The critical day to plan for was the next Monday. The decision to encourage Belfius staff to work from home was taken and prepared on the Saturday morning, although notification was postponed until 10.00 pm on the Sunday. Belfius expressed itself as the first major Brussels company to communicate about a comprehensive response plan.

THE SECOND TERRORIST EVENT: THE BRUSSELS TERRORIST ATTACK (22ND MARCH, 2016)

The second terrorist event was of a different nature. Belgium was mightily relieved when Salah Abdeslam, the suicide attacker who had escaped from Paris, was arrested on Friday, 18th March, 2016. The arrest prompted a false sense of security, however, and matters deteriorated sharply a few days later.

Terrorist cells preparing attacks in the Netherlands and France, felt hunted by the security intelligence services and improvised attacks in Brussels instead.

On Tuesday, 22nd, March, two simultaneous suicide attacks caused 14 deaths and more than 100 wounded persons in the terminal building at Zaventem airport, with a further 21 dead and over 100 injured in the Maalbeek metro station, 2 km from the Belfius headquarters.

BELFIUS BANK'S RESPONSE TO THE TERRORIST ATTACKS

Belfius went into crisis mode as soon as it learned of the attacks, this time with the crisis team members physically present at the head office. The scenario for a 'terrorist attack in Brussels, during working hours, without damage to the building', prescribing a lockdown of the headquarters, was put into effect. No one was allowed to enter the building and likewise no one was allowed to leave until there was sufficient evidence about safety outside. The Brussels bank branches closed their doors to all unscheduled visits, opening them only to those with scheduled appointments.

The situation in the city became chaotic. The mobile network collapsed. Every staff member went online on internet, trying to find images and breaking news about the event, saturating the internet pipeline. Social media were still available with a 3G or 4G connection. Traffic and public transport in Brussels quickly came to a halt.

Official information and guidance was quite blurred, while hastily published press releases contradicted each other. Belfius consulted with other companies to check what measures they had taken; however, its primary concern was its staff: carpooling arrangements were made to get everyone home. Arrangements were also made to guarantee business continuity over the next two working days.

RISK AND THREAT ASSESSMENT OF TERRORIST INCIDENTS

One can, of course, draw something positive from a crisis. Such events help to determine the probability, severity and/or mitigation scores of risk and threat assessments. They reveal structural weaknesses and highlight the necessary interventions to overcome them. Where mitigation does not match the risk potential (probability × severity), it is important to focus on threats.

Based on the OCAD level as an objective assessment of the terrorist threat, Belfius had to adjust the probability score in its risk and threat analysis. Historically, the bank considered the likelihood of a major terrorist incident in the Brussels region as 'unlikely' to 'possible'. Now, the probability level had escalated to 'almost certain' on multiple occasions.

For compliance reasons, dealers are not allowed to work outside the controlled dealing room. Closing down the primary premises automatically means a fall-back to the external relocation site.

Business relocation providers apply a 'first come, first served' policy: the first caller acquires exclusive rights over the shared desks. Until this point, Belfius had never had a problem with that principle. In a regional lockdown situation, multiple companies tend to start their business continuity plan simultaneously and in all likelihood will claim the same shared desk capacity at the common external relocation site.

Following the first terrorist incident, Belfius was the first to activate its relocation site, blocking those customers who responded later. These companies learned their lesson and subsequently adopted the official OCAD level as an automatic trigger to assure the availability of their disaster recovery plan (DRP) site, even without planning a real relocation.

As a result, Belfius could not resume dealing room activities at the desired capacity level after the second terrorist incident. It was therefore important to recognise that the mitigation measures previously put in place were less reliable than originally planned. As such, threats previously considered as 'under control' were escalated to 'action required'. Consequently, the shift to a dedicated DRP site entailed few arguments.

Predictably, when the 'BCI Horizon Scan Report 2016'[1] was published, 'acts of terrorism' had moved up to fourth place in the list of most worrying threats, up from ninth position in 2015. Nevertheless, perceptions changed once more after the dust had settled. In the 2017 report,[2] the terrorist threat had dropped back to a more reasonable seventh position. Organisations responding to the survey reported negligible disruption to their normal business activities.

But the regional comparison revealed one notable exception: in Belgium, 'acts of terrorism' remains in the top three for threats, as well as for disruptions.

VULNERABILITY ASSESSMENT AT THE BRUSSELS HEADQUARTERS

The Belfius headquarters is — like several major companies — housed in the heart of Brussels, where large-scale incidents and mass demonstrations are common. The majority of the bank's staff travel to work by public transport. As such, strikes and city lockdowns affect their ability to get to work. In the past, Belfius has been faced with national and/or local union actions and situations causing travel in Brussels to be badly affected and even discouraged by the government.

The terrorist threat adds a new dimension, because of the multitude of soft and hard terrorist targets in the vicinity. These include the Brussels-North railway station, metro lines and city boulevards, the square in front of the building connected to the City2 shopping mall and the Nieuwstraat/Rue Neuve, a popular shopping street where soldiers have patrolled since the attacks.

The extensive coverage of successful terrorist acts in the media often leads to copycat behaviour. The number of bomb hoaxes in the Brussels area tripled in a year. Every event is taken seriously by the police and may affect business activities locally.

On Monday, 21st June, 2016, during the morning rush hour, a man walking down Nieuwstraat/Rue Neuve with a fake bomb belt forced the police to set up a security cordon. In the same month, a fan zone for the European Championship football was set up on the square in front of the Belfius building. Intelligence services dispelled an attack, planned for the first match broadcast.

Belfius Bank's buildings were not designed to shut people out, but rather to welcome visitors in large entrance halls. Extra guards were posted at the outside entrance gates for a long period. One of the first action points to deal with these circumstances was the provision of an alternative secured personnel gate so that the entrance hall can be locked easily when a major physical incident happens outside the building.

The awareness of extreme vulnerability influenced the management board to close down the headquarters building after the March attacks for the rest of the working week. This was a calculated risk, because management had confidence in the resilience capability, demonstrated successfully during the previous crisis deployments.

Mobile working (thin clients, software in virtual sessions) and the practice of structural and *ad hoc* remote work/home-working underpinned the reduced demand for floor space. It also enhanced the flexibility of the business continuity and resilience strategies. However, the terrorist incidents also highlighted awareness of the pitfalls involved with concentrating critical operations in a single location from business continuity perspective. On the positive side, however, it sped up the strategic decision to opt for a dual office strategy.

In a dual office configuration, one particular business activity is carried out at the headquarters as well as in one or more regional offices. In the event of a daytime business continuity deployment, the workload shifts from one location to another, which enables an instant continuity.

This strategy will help Belfius to comply with the guidelines of the Belgian regulator, which has imposed a recovery time objective of two hours instead of four hours for 'system-relevant activities', beginning on 1st July 2018.[3]

CRISIS MANAGEMENT FRAMEWORK

In every crisis management deployment, Belfius applies the same framework (Figure 2), with clearly outlined roles and responsibilities. Training courses and simulations are useful, but 'the proof of the pudding is in the eating'. With that in mind, the bank's participation at the market-wide crisis exercise for Belgian financial institutions, organised on 1st October, 2015, was the perfect opportunity to sharpen the bank's crisis management skills.

The visionary theme was a terrorist attack, targeting the financial system. Looking back, it turned out to be the perfect rehearsal for the incidents that occurred later, despite the fact that the

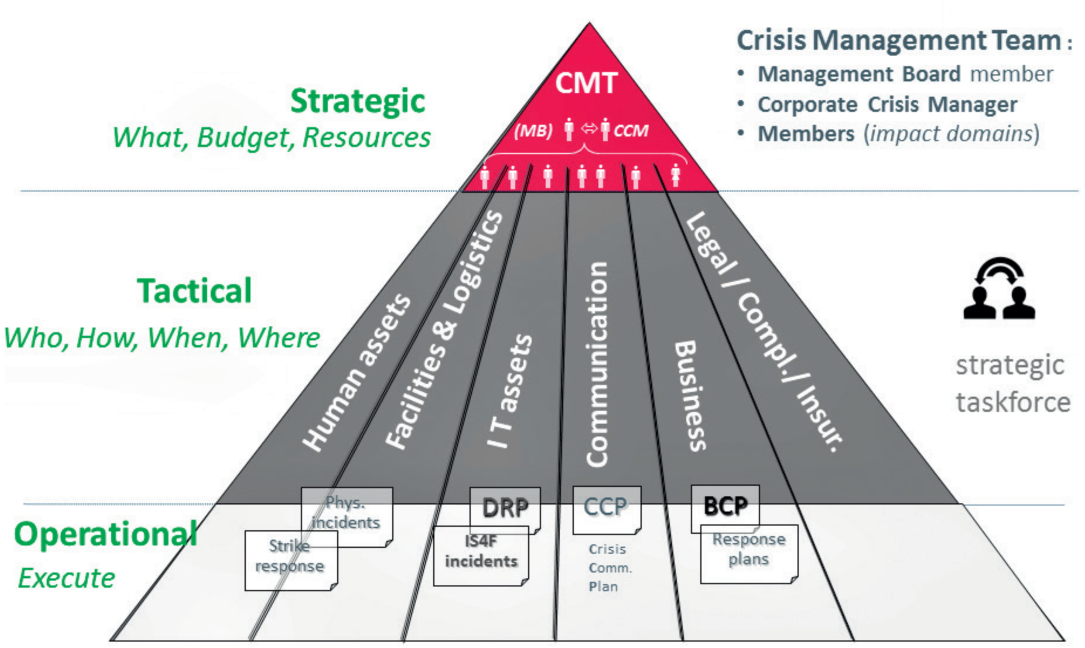

Figure 2 Belfius Bank's crisis management framework

Source: Belfius course material

signature of the attacks by fundamental ISIS fighters is completely different in nature: their objective is not to dismantle the financial system by hitting symbolic institutions, but to kill and maim as many innocent victims as possible.

In both terrorist events, the management board was consulted to approve major decisions prepared by the strategic crisis management team, although crisis management leadership remained with the corporate crisis manager all the time. In November, the management board was staying at an external location, which complicated communication and collaboration.

Even though the three horizontal layers of its crisis management framework (strategic, tactical and operational) prescribe specific responsibilities, Belfius observed that key crisis players were sometimes too distracted by trivial operational issues.

It was also considered that additional guidance about understanding responsibilities and crisis management principles was necessary.

For this purpose, Belfius organised refresher courses for potential crisis actors, using the November crisis deployment as a reference. In doing so, greater maturity was observed in the March 2016 incident.

'Practice makes perfect'. The crisis management actors gained further confidence with every subsequent crisis deployment and the principle of the crisis management framework became more and more familiar.

OFF-THE-SHELF RESPONSE SCENARIOS

Auditors and regulators often recommend a specific scenario for every potential threat.

Belfius maintains three typical business continuity scenarios (overnight, daytime and planned deployment), relying on the same business continuity data, using common roles, but with appropriate tools and reports to meet the specific requirements. Table 1 highlights the distinct features.

In November 2015, Belfius invoked an overnight deployment on the Sunday to secure the premises, to safeguard employees and to ensure the continuity of critical business activities on the Monday. In March, Belfius opted for a planned deployment to survive the next two working days. The daytime deployment is tested at least once a year, embedded in a comprehensive evacuation exercise.

The specific response scenario for 'terrorist attack Brussels, during working hours without damage to our premises'

Table 1: Main business continuity deployment scenarios

	1. Daytime	*2. Overnight*	*3. Planned*
Decision	Embedded in evacuation	Crisis management decision	Crisis management decision
When	Evacuation event	Outside working hours	During working hours
RTO	Resume within the agreed RTO	Next working day RTO = 0	Start of the critical day RTO = 0
Notification	—	SMS, intranet, hidden internet page	SMS, intranet, broadcasts
Tools	Call lists and list of remote workers	Call tree, call cascades, call lists (private data)	Attendance tool: operators assigned to critical activities for following days
BCP scope	Roll-out as designed and trained	Survive next day with very critical business activities	Survive the critical period (type of activities, relocation places, no. days etc)

was developed in response to the lockdown incident in November 2015. In addition, Belfius has specific response scenarios covering events such as IT incidents, strikes, pandemics, power outages, brown-outs, bomb alerts, demonstrations etc.

It is better to maintain only a limited number of up-to-date generic response plans, tailored to worst-case scenarios, than writing specific scenarios for every potential threat. Depending on the circumstances, Belfius can always reply with a mix of components taken from different response plans.

'When the facts change, you have to change your mind'. On the Sunday evening in November, the dealing room operators became reluctant to come to Brussels as agreed in the call tree procedure earlier that day. Consequently, Belfius deployed its external relocation site and overruled the previous strategy.

COMMUNICATION AND COLLABORATION AS KEY SUCCESS FACTORS IN CRISIS MANAGEMENT

In a terrorist event, every employee must be informed in the most appropriate way and via the most effective communication channel.

The business continuity plan contains the private contact details of crisis management actors and candidates assigned to the critical business activities. However, this covers only 20 per cent of the overall staff.

Every internal staff member also has the option of entering, on a purely voluntary base, his or her private mobile number in the secured personnel application. In November 2015, only 60 per cent did so — partly from ignorance, but also because there was no sense of urgency.

Through a merger of these two data sources, the bank was able to reach 65 per cent of its personnel to advise them to work from home the next day. Following an awareness campaign, coverage was quickly expanded to 95 per cent. Of course, handling such private data requires a security protocol.

At the time of the terrorist attacks, Belfius used a very simple notification tool, restricted to SMS messages of 140 characters, without a reply option. To obtain more information, message recipients had to log on and consult the company intranet. One of the first suggestions was the creation of a hidden web page to enable direct internet access.

It was soon recognised that the notification process needed to be improved through the implementation of a more sophisticated and flexible tool, as well as by providing better support for collaboration within teams.

Press bulletins commended the bank's recommendation to work from home as a good practice from a business perspective. This media interest not only helped to spread the message to those employees who had been unreachable, but it also woke up other people. Belfius scored positive comments on social media, as people were wondering when their employers would finally take some action. In a way, the bank's strategy set the standard for other companies.

Belfius uses two official languages to communicate to its staff: Dutch and French. Messages and guidelines, often written and validated in one language, must be translated into the other one before they can be sent. This takes time and effort. In the first terrorist event, Belfius created the cushion of a gradual deployment, but the second one involved operating against the clock. The challenge of creating a correct and concise message of 140 characters led to slightly different interpretations within the two language communities. For the specific business continuity communication to a select group of actors, time and efficiency were gained by using English as a unique language. In the post-processing stage, the need for a new set of ready-to-use pro forma texts was expressed.

AVAILABILITY OF CRISIS DOCUMENTATION

In 'the golden hour' immediately following a crisis event, the crisis management actors need immediate access to call lists and procedures, even if they are not in a position to log on to the systems. At the same time, it is important to avoid confidential or business-sensitive information circulating on unsecured media, such as paper and memory sticks or private e-mails. It is also important that people are not unwittingly relying on obsolete call lists.

The November crisis prompted Belfius to investigate what the ideal communication platform might be. As all strategic crisis actors were already using a fully-secured app on their mobile devices in order to consult their work e-mail and diary, it seemed sensible to exploit additional features on the same application suite. From now on, centrally stored and maintained critical documents can be consulted in a secure way from a mobile device. The most critical files can be replicated in a secure folder and used offline, avoiding any possible disruption to the central IT systems. For business continuity reasons, all communication tools and data are stored in the cloud, completely independent of the central IT systems.

In addition, a digital version of the call lists and other reports is maintained on a secured local area network drive. As a last resort, the entire document library is copied to a secure memory stick. This means that in all circumstances it is possible to locate a version of a key document. A trade-off that takes availability, freshness, preparation time and data volatility into account determines which source is the most appropriate.

To support the tactical actors, Belfius now uses an app with secure lockboxes, enabling the replication of guidelines and procedures without the need to send attachments to private mail addresses.

ORGANISATIONAL RESILIENCE

The bank's organisational resilience benefits from a reliable and robust remote access capacity. All of the prerequisites were fulfilled, step by step, including management endorsement, ample gateway capacity, a digipass for every staff member, scripted software and enlarged bandwidth for the internet pipeline (used by internet banking customers as well). Remote working is now familiar to everyone and also enables a reliable recovery strategy in the event of planned or overnight deployment.

No matter where staff connect to the system (at the office or remotely), they can always start up a virtual session in a secure way. From a business continuity perspective, a software-based solution gives a major advantage over a hardware-based remote solution with fat clients. Indeed, the bank's research found stories from similar companies where their remote work strategy required staff to collect laptops from their corporate headquarters before transporting them to private addresses.

The multitude of strikes disrupting transport to Brussels over the years had convinced the majority of employees to request a digipass.

An important impulse came from senior management, who promoted *ad hoc* remote work as a widely accepted work regime. The driver was not a business continuity requirement as such, but a financial consideration. Free seating, universal workstations, centralised software management and remote work are all effective measures for reducing the cost of ownership of office floor space.

Business continuity management endorsed the principle as a welcome relocation strategy.

While the internet is an enabler, it could also turn into a potential single point of failure, as internet traffic can collapse, a distributed denial of service (DDoS) attack can cut off central systems or the internet gateway may become saturated. Over the three days of the March incident, barely 150 working days were lost, as almost every volunteer employee was able to work. An internet collapse, however, would have been catastrophic.

To control the remote capacity, Belfius relies on a monitoring system that watermarks the number of open remote work sessions. The bank has also developed a proprietary reporting system that lists the active sessions and their location (in-house or remote). If, for some reason, the remote access is limited in terms of connections or server capacity, it is possible to restrict the scarce available sessions to individuals on highly business-critical activities only.

The remote access statistics, combined with physical presence reports generated by the building access control system, delivers precise information on the total occupancy rate on critical days and helps to check the extent to which the critical business activities are adequately covered. In the post-processing stage, this information is processed as a key performance indicator measuring the effectiveness of the crisis management approach. Figure 3 shows the trend for open remote sessions in November 2015, indicating a considerable increase due to the terrorist event.

Voice still imposes many restrictions, although voice-over-IP (VoIP) enables a connection to and from any standard device within the secured site. Staff members may forward their incoming calls to a private device at any time, but 'voice recording', 'group cascades' and 'call centre applications' still remain uncovered features in the standard home-working setting. The need for a smooth integration of all VoIP features into the new workplace architecture has been expressed as a business continuity requirement. While this is still awaited, there is a need to provide in-house relocation desks or distribute mobile VoIP devices to *ad hoc* remote workers.

LESSONS LEARNED

As a learning organisation, the bank continuously looks at improvement points for its business continuity and crisis management capability.

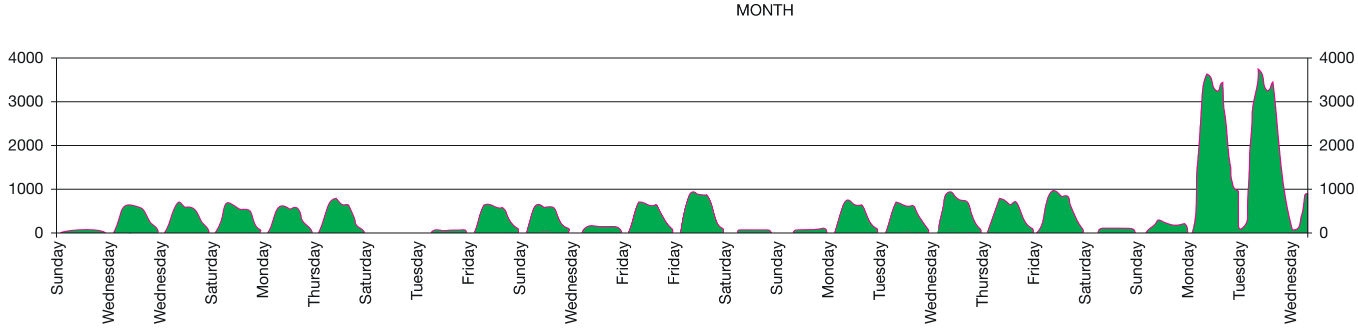

Figure 3 Organisational resilience relying on remote work (November 2015)

Note: The graphic depicts the number of remote sessions, with a peak of 3,500 simultaneous connections on Monday (versus of 800 the week before). On Sunday there was a slight increase by users who were looking for more information on the intranet.

Source: extract from Remote Access monitoring tool

The debriefing from the November 2015 crisis delivered several action plans, each assigned to a specific division to handle.

Most of the lessons learned had been addressed previously. The focus was placed on the communication issues with measures to improve the accessibility of staff members outside working hours and the search for effective communication channels to inform personnel at home. Initiatives were launched for decentralisation to regional buildings and to reduce the vulnerability of the central Brussels building in the event of a city lockdown. Other improvements were sought in the crisis management process, as well as in physical security and in the enhancement of home-grown tools.

All action plans were officially endorsed by the management board and followed with the same sense of urgency as audit recommendations to underline the importance and enforce engagement. On 22nd March, 80 per cent of the improvement points from the November events had been solved and contributed clearly to better crisis management.

The lessons learned from the second terrorist incident gave rise to a new set of action plans. In view of the different nature of the incident and the time pressure, other crisis management skills were tested and new unexpected shortcomings occurred on the surface.

Relocation strategies and contracts needed to be tightened up. Restrictions in the field of telephony prompted Belfius to seek bypass solutions.

The action plans also provided the drive to explore innovative technologies and apps on smartphones to improve collaboration between key actors.

Not all of the recommendations have led to the desired outcome. Financial or technical considerations and risk appetite may counteract structural solutions.

Belfius certainly benefited from the momentum to obtain additional budget allocations for new plans and to speed up emerging projects. On the other hand, it had to inhibit spontaneous, but well-meant initiatives, launched here and there, because they interfered with other actions.

CONCLUSION

Business continuity professionals have a simple mission: prepare a resilience capability to overcome doom scenarios which, according to staff members, only happen to others. Quality and effectiveness need to be validated through exercises, structured walk-throughs, simulations or audits.

When a major crisis event really hits, it is up to business continuity professionals to prove that their preparatory work yields an expected pattern of success, not failure.

Every crisis deployment is on its turn an opportunity. Success stories can be used to strengthen the embedding of business continuity and crisis management into the company culture, to persuade stakeholders (regulators, management board, direct reports and labour unions) of the in-house expertise and to demonstrate the added value of a comprehensive business continuity management programme.

It seems as though the Belgian media have suddenly discovered business continuity as a new discipline in response to the terrorist events.

Social media, newspapers and business magazines have all praised the decisiveness of Belfius Bank's crisis management and emphasised the need for a good business continuity plan, illustrated with best practices from the governance at Belfius. Invitations to share the bank's experiences at national and international conferences have followed.

The story of Belfius Bank's successful approach during the Belgian terrorist events and the way it implemented good practice in all stages of the business continuity life cycle was the key to the bank receiving the European and Global Award for ‘BCI Continuity and Resilience Team of the Year 2016’.

References

(1) Business Continuity Institute and BSI (2016) ‘Business Continuity Horizon Scan Report 2016’, Caversham, Business Continuity Institute.

(2) Business Continuity Institute and BSI (2017) ‘Business Continuity Horizon Scan Report 2017’, Caversham, Business Continuity Institute.

(3) Nationale Bank van België (2015) ‘Additional prudential expectations regarding operational business continuity and security of systemically important financial institutions’, available at: https://www.nbb.be/en/articles/circular-nbb201532-additional-prudential-expectations-regarding-operational-business (accessed 23rd August, 2017).