Business Resilience Communications

Planning and executing communication flows
that support business continuity and operational effectiveness

whispir

Whispir have spent the last 14 years helping organisations to manage their business critical communications. This guide collects the lessons we've learned along the way, exploring the role of effective communications in mitigating the business impact of incidents. We've also observed how the proactive use of communications technology to streamline business processes has become a technology-driven source of competitive advantage.

Quick statistics:

- **61%** of businesses reported experiencing at least one critical incident over the past two years[1]
- **52%** of IR staff lack visibility into system or endpoint vulnerabilities[1]
- For the Fortune 1000, the average total cost of unplanned application downtime per year is **$1.25 billion to $2 billion**[2]
- The average cost, per hour, of an infrastructure failure is **$100,000**[2]
- The average cost, per hour, of a critical application failure is **$500,000 to $1 billion**[2]

Business resilience

Business Resilience is the ability of an organisation to respond and adapt to dynamic changes in the operational landscape – opportunities, demands, disruptions or threats – and continue functioning with limited impact to the business in the short and long term.

Understanding the impact

The challenges are significant - a recent global study by the SANS Institute[1] (see Figure 1.1 below) showed that 61% of businesses reported experiencing at least one critical incident involving a data breach, unauthorized access, denial of service or malware infection over the past two years. The largest percentage of respondents (48%) experienced up to 25 incidents.

Effective business resilience preparation goes beyond Crisis or Incident Management, and involves planning for a wide spectrum of potential scenarios that can effect organizations of all size, from small to medium business, large enterprises and government departments.

Starting over the page, we'll discuss some of the common scenarios. The three key areas of discussion are Crisis Management, IT Incident Management, and Operational Resilience.

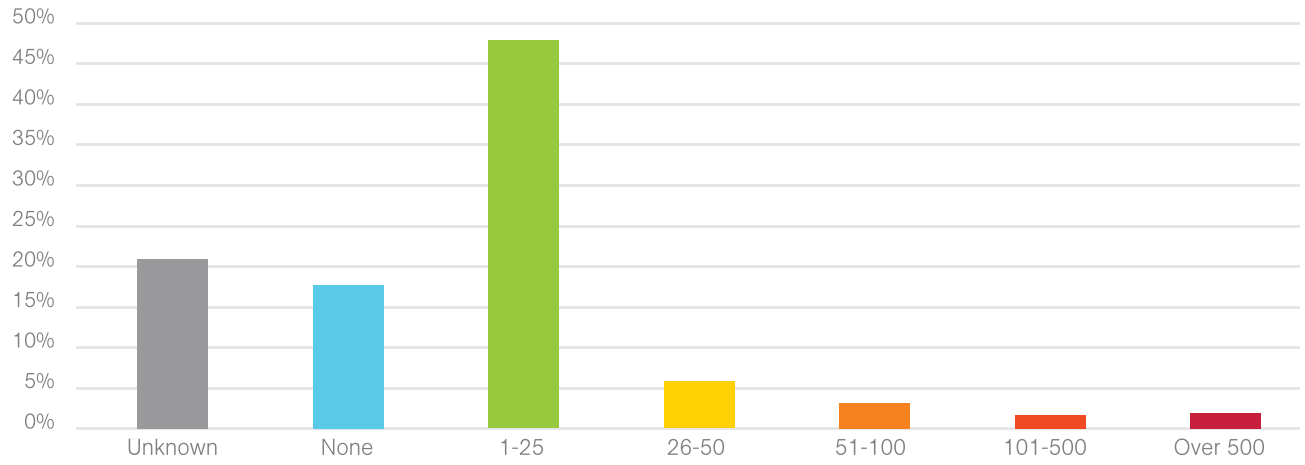

Fig 1.1: Critical IT incidents requiring response, per organisation, 2012-2014.
Source: SANS Institute

[1] - https://www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342

[2] - IDC "DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified." Stephen Elliot. December 2014, IDC #253155.

Crisis Management is the response an organisation needs to take in the event of unforeseen emergencies or disasters to minimise the harm to the organisation, its stakeholders, or the general public.

These events can include natural disasters like floods, fires, or earthquakes; industrial incidents such as oil tankers leaking; technological crises such as data breaches, and a range of other possible scenarios including malevolence, terrorism and other man-made disasters.

The common outcome of all of these situations is financial loss, reputational harm, and potential risk to human life.

An effective and well executed communications strategy is required to help minimise the impact. In summary, planned, open and effective communication is the key to coping with a crisis - and we've included deeper detail below.

Leverage technology to deliver planned, multichannel, two-way communication streams that orchestrate rapid organisational response, while keeping stakeholders informed.

Crisis communications framework:

- **Have a plan.** A written plan should be in place, which includes specific actions that will be taken in the event of a crisis. The key objectives during any crisis are to protect any individual (employee or public) who may be at risk, ensure that all stakeholders are kept informed, and that ultimately the organisation survives.
- **Identify a spokesperson.** A key spokesperson needs to be identified, prepared and kept as up to date as possible to ensure that the media, staff, customers and the public are kept informed with a clear, consistent message.
- **Be honest and open.** In our connected age, it's no longer possible to hope that information can be kept from the media or general public, so a policy of openness and transparency is essential to maintaining trust. This transparency must be projected through all communications channels: news interviews, social media, internal announcements, etc.
- **Keep employees informed.** Employees are the main conduit to keeping communications flowing between all relevant stakeholders, so it's essential to keep the workforce informed with all relevant up to date information to prevent the circulation of incorrect rumours and potentially negative statements.
- **Customer and supplier communications.** Information on any crisis should reach your customers and suppliers directly from you, and not from the media. Part of the crisis communications plan needs to include these vital stakeholders, and how to keep them updated throughout the event.
- **Update early and often.** Be proactive and early with sharing news, even when the whole picture isn't clear. It is better to over-communicate than to allow rumours to fill the void. Start with summary statements on whatever is initially known, and provide updated action plans and new developments as early and as often as possible to stay ahead of the 24/7 news cycle.
- **Social media.** Ensure that all the channels that your stakeholders may be using are covered, not just the traditional areas in which critical statements were released, such as press releases or the company website. Nothing is more damaging than incorrect information being live tweeted without your ability to see and respond with facts and the appropriate damage control.

Case Study: **Qantas**

Rapid organizational response to an unplanned event

Improving response times

Qantas, like many organisations that operate in fast-paced, time-critical environments, are constantly looking for methodologies that improve response times from staff right across the business, should an incident occur.

Adopting an appropriate communications platform that enables the standardisation of protocols and speaks to multiple stakeholders in a variety of channels is imperative for global airline operators. The choice of the correct platform can improve response times, ensure greater staff, ensure greater passenger and staff safety, reduce risk of brand damage, and mitigate impact to the bottom line.

Managing the outcome

When a potentially major incident occurred, Qantas was able to respond quickly via the Whispir platform.

By activating pre-defined communication workflows, Qantas was able to make contact with a variety of stakeholders simultaneously, who would all serve different purposes.

On the ground, staff were rallied to enact repair activity and provide guidance to the pilot, the executive team were able to put together communications internally and externally to alleviate concerns and passengers were able to be informed of changes to schedule. The Whispir platform coordinated all of these communications and importantly provided real time situational awareness.

The ability to notify the appropriate people quickly and therefore put in place adequate responses meant that Qantas was able to turn a potentially damaging situation into a well-managed engagement. Customer concerns about rescheduling could be planned for, impacts to the share price could be mitigated through timely external communications and brand impact minimised.

whispir

IT Incidents are the result of service failures or unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer. Incident Management is often referred to as the way that the Service Desk puts out the 'daily fires.'

ITIL® Incident Management Lifecycle

Incidents are a daily occurrence in most businesses, and rather than try to eliminate them altogether, most organisations work to resolve these on a staged basis.

The "Incident Management Lifecycle", derived from ITIL® (Figure 2.1, below) is a good indication of a standard framework to follow when your business faces an IT incident.

Fig 2.1: The typical incident management lifecycle for an organisation.
Source: AXELOS ITIL

whispir

ITIL® provides a series of recommended steps for management of IT incidents. We've included a quick list of them just below, plus an examination of the potential challenges. A case study follows overleaf.

Major incident management steps

- **Identify and log.** A service manager recognizes a major incident and logs in the system.
- **Categorize and prioritize.** The type of incident is determined, and prioritised by potential impact.
- **Engage.** The service manager steps outside the regular incident process and alerts the major incident managers on duty.
- **Respond.** The major incident manager who accepts the case determines whether the alert is a false alarm and what the incident is. Depending on severity, the incident might be further escalated, or immediately resolved if the current team has the capability to implement a fix.
- **Closure.** The final stage is to review the actions that took place during the incident to identify improvements that can prevent a similar incident from occurring again.

Incident communication challenges

High impact events need to be treated with appropriate urgency. Incidents are categorized by severity, (e.g. High, Medium, Low) based on impact and urgency, and resolved accordingly. Low impact incidents can be de-prioritized and dealt with when resources become available.

The real issue with this approach is the overwhelming deluge of notifications flooding the inbox of IT staff every day. These notifications range from basic updates and progress reports to maintenance updates and outage warnings, **making it entirely possible to miss the major incident warnings** that do need urgent response.

The other major challenge is the problem of **identifying the right person, and bringing all of the team together** who need to manage the response.

According to the SANS Institute, more than one-quarter of Incident Response (IR) professionals (26%) are dissatisfied with their current organization's IR capabilities, calling them ineffective, while only 9% categorize their processes as very effective.

Solution: 68% of respondents to the SANS Survey projected that improvements in their IR capabilities and processes would come from Automation and Security Information & Event Management (SIEM) integration tools that increase visibility into threats and how they apply to their environment, including scoping and remediation capabilities.

State of the art incident management systems are built around an automated communications platform, which allows interactive two-way cross-channel communications, comprehensive reporting and message delivery status transparency for key staff and senior stakeholders.

Messages need to be automated and integrated with monitoring systems, providing rapid crisis team activation and scenarios via a template-based solution across voice text-to-speech, SMS, mobile web apps, and email to ensure faster task allocation and resolution.

Case Study: **StarHub**

Improved response time during an IT emergency

Effective team mobilization

StarHub required a solution that provides elevated cut-through beyond existing IT Service Management (ITSM) notifications.

Operations support engineers were at risk of missing notifications during service disruptions – especially after office hours. Additionally, the business continuity management team's internal call-tree system required upgrade to support complex rule-based escalation management.

Improved transparency for stakeholders

StarHub uses Whispir to improve telecommunication service management, reducing response times, and for staff business continuity communications (e.g. fire drills, staff recalls) enterprise-wide, from the one platform.

The interactive two-way cross-channel solution provided comprehensive reporting and message delivery status transparency for key staff and senior stakeholders.

The outcome from Whispir's communication platform, provided rapid crisis team activation and scenarios via a template-based solution across text-to-speech, SMS, and email, ensuring faster speed of task allocation and resolution.

whispir

As noted previously, Business Resilience goes beyond dealing with crises or incidents, it can also be a source of competitive advantage. We'll explore some of the ways that communications technology can improve an organisation's general operations here.

Production updates

Downtime can be one of the largest costs in business, whether that's IT production resilience, logistics, or distribution. It's vital to ensure that supplies and components are ordered and delivered on time to allow the production cycle to continue uninterrupted.

Solution: automated technologies can leverage machine to machine (M2M) communications and deliver multi-channel messages including SMS, voice, mobile instant apps or email to create work orders at short notice.

This ensures that the correct people are kept notified, including service staff, customers and suppliers, and can also give investors visibility into the efficiency of the operation.

Diverse stakeholder management

A diverse range of stakeholders are impacted by every business event, which can include government or regulatory bodies, executive teams, management groups, customers, partners, suppliers and shareholders, who all require different, yet timely and accurate information on subjects ranging from shift timings, to marketing, operations, legal compliance and finances.

Communicating all of this information with all of these people in a timely and effective manner is a constant challenge.

Solution: combining all of these communications streams into a single platform, with a central reporting dashboard improves cut-through in the delivery of messages. It provides a mechanism for tracking all critical communications, gives recipients a way to respond appropriately, and then allows informed, real time decisions to be made based on the feedback gained from these conversations.

Executive communications

As businesses grow, it becomes increasingly harder to reach employees, and maintaining contact between the executive team and all the layers of the organization can be a real challenge, especially when dealing with different branches, departments, geographically dispersed locations and even international operations.

Solution: dispersed communications work best when delivered through a centralised delivery platform, which has the capability to schedule the timing, and send messages on all of the channels needed to make sure the entire team is reached, including SMS, voice, mobile web apps or email.

Communications should be easily segmented, with pre-defined templates that can be quickly adapted to suit the message, and a response tracking mechanism to keep track of inbound and outbound message flows. This provides a single view of all communications workflows, to and from stakeholders, regardless of the channel used.

"Combine all of these communication streams into a single platform"

In summary - the best defence is a good offence. Incidents affecting business operations are a daily occurrence, and without proper management and communications, incidents can escalate into critical events that could put an organization's survival at risk. The integration of automated communications technology into day-to-day processes ensures you are always prepared.

Resilient communications - best practices:

- **Communications planning.** Having a clearly defined plan in place for communicating in different scenarios cuts down response time, improves accuracy of contact, and ensures the right people are able to be reached in a timely manner.
- **Global multi-channel message streams** Messages should be sent on the appropriate channels needed to make sure all stakeholders are reached, including SMS, voice, mobile web apps, social media, web, or email.
- **Message templates.** Message templates should be prepared with specifics which can be rapidly altered during incidents, thereby saving time by providing pre-defined communication and response options.
- **Message automation.** Where possible, communications platforms should be integrated with monitoring systems, allowing details to be auto-populated into message templates. Tickets can be raised automatically and sent directly to the resolution team members.
- **Two-way conversation flow.** It's not enough to just send messages. There needs to be a system in place to track receipt, allow the receiver to respond as needed, and escalate when required.

whispir

Effective planning and global communications reach are the keys to mitigating operational risk, and the day-to-day application of automated communications can turn changing circumstances into opportunities for building new processes that become a source of sustainable, technology driven competitive advantage. The Whispir Integrated Communications Model combines all of these processes into one platform.

Fig 4.1: The Whispir Integrated Communications Model.

About our platform

Whispir takes a holistic approach to communications, and our platform has been engineered as a cross-channel, automated communication solution which is designed to be robust, scalable and customisable enough to meet the most stringent messaging requirements.

We are the trusted communications provider for more than 350 leading enterprises, including Telstra, Qantas, Westpac, BHP and IBM, as well as government agencies, including Australia Post and V-Line.

Our customers use the Whispir platform for critical communications such as crisis response, emergency management, community notifications and IT incident management, and other business enablement services ranging from customer service & engagement to general operational communications.

whispir