DERDACK White Paper – “Business continuity and the role of communication”

Matthes Derdack discusses new perspectives on business critical events that should influence the way we look at business continuity planning. While business continuity measures are usually derived from known threats and risks, new in-sights point to a planning that is based on the potential impact of critical events and to implementing the ability to rapidly respond to unknown scenarios. In this light, communication and automated communication systems play a much important role in handling critical situations.

1 PLANNING FOR WHAT EXACTLY – PREDICTABLE VERSUS UNPREDICTABLE EVENTS

Business Continuity often fails. The reasons are manifold. If no business continuity plan exists, any response to emergency situations depends on the capabilities and action of solitary individuals and is basically random. In particular, for large-scale events this does of course not work at all.

But even an existing business continuity plan is no guarantee for safety as it might be outdated, poorly drilled and exercised, or even badly designed. There is also the danger that a business continuity plan is too much based on a risk assessment or threat and risk analysis (TRA). In such a case it is derived from predictable or highly probable events and situations only.

However, many rare events are not predictable. There might be signs but they are usually overlooked. The reason is described in the concept of the "black swan" developed by Nassim Nicholas Taleb in his book "The Black Swan". "Black swan events" are highly improbable but their impact is huge – but mostly and heavily underestimated. This is due to our human way of thinking leading to a wrong correlation between probability and impact. Rare events are associated with small impacts.

Additionally, we are mistaken by getting probability wrong. There might be even a fundamental flaw in the quantitative assessment of potential risks and it is a much criticized exercise. Imagine your business has been running without a major incident for 50 years. That can mean that your business will be able to avoid a disastrous incident for the next 50 years. But, it can also mean that disaster strikes the very next day. The probability of a disastrous event on any given day is essentially the same regardless of when the last disastrous event struck. Additionally, the "Black Swan" theory suggests that the cause of a potential disaster is always unknown. So, business continuity planning derived from known causes and their impact is dangerous and impossible for 'black swan' events. They wouldn't be 'black swan' events any more.

There is a lot of criticism on "Threat and Risk Analysis" (TRA). "Black swan" events are entirely invisible for TRA but event know events are highly difficult to seize in their probability and impact. Sometimes this is just wild guessing and additionally, probably and impact change constantly and drastically.

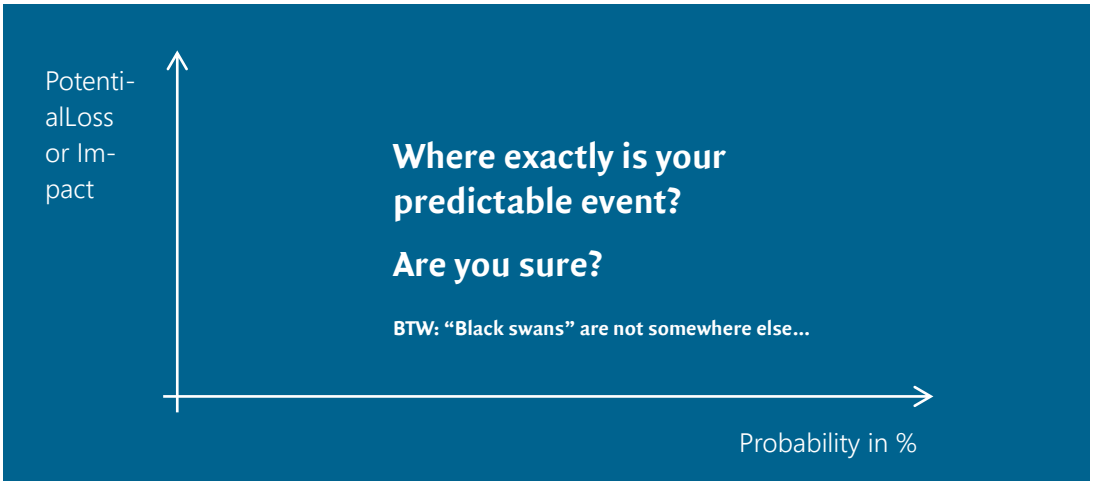

Figure 1: TRA - How good is your guessing?

Unfortunately, rare "black swan" events are the worst and often result in disaster. Prominent examples include the Deepwater Horizon Oil spill in 2010, the Fukushima nuclear power plant disaster in 2011 or the sinking of the "Costa Concordia" cruise ship in 2012.Though Fukushima is a typical example of a disaster caused by a large-scale Tsunami event, one of the characteristics of many bad incidents is their non-linear

development - a small malfunction (typically handled by low-level troubleshooting) is ending up in an emergency situation or disaster. Accepting this "event continuum" is essential in order to understand why business continuity planning needs to span from low-level malfunctions to disastrous events.

> According to a recent survey more than 40 percent of all companies that experience a disaster do not reopen, and over 25 percent of those that do reopen close down for good within two years.(Source, Ezine Magazine)

2 MAINTAINING BUSINESS CONTINUITY

One of the core principles of maintaining business continuity is to ensure that there is an effective response to disruptions in place which minimizes the impact on the organization. That is why organizations design business continuity plans. They typically include various measures at different frontiers:

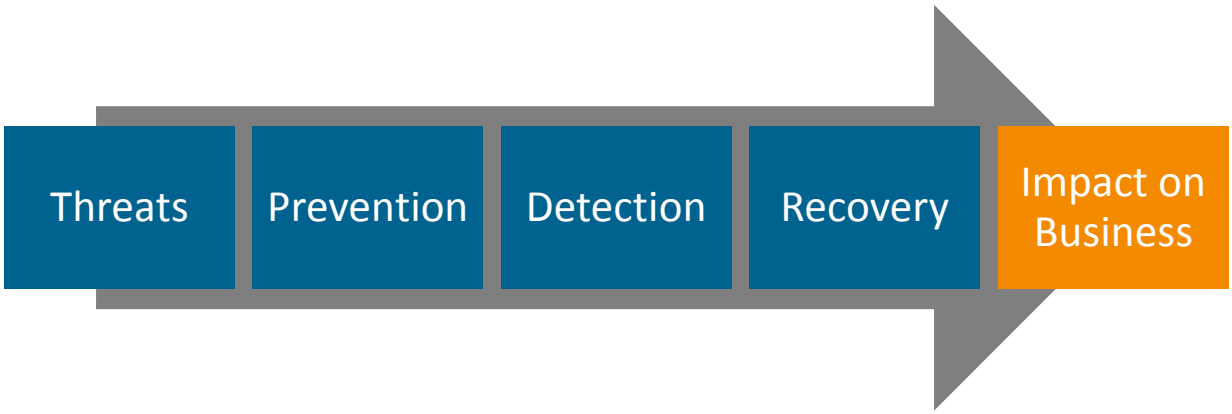

Figure 2: Measurements to ensure business continuity (Source: BSI and Loomans & Matz)

Organizations are facing a multitude of threads to their business continuity. A large aspect of preventing major incidents is Prevention. Organization set policies, e.g. for using IT, accessing important information and so on. They implement security systems, firewalls and campus fences, etc. If Prevention fails, incidents need to be detected. In IT this task is handled by monitoring systems. Their job is to detect any deviation from "normal" and signal it effectively in order to ensure a swift response to an incident. If incidents remain undetected or if the response fails, an organization might end up in an emergency situation or even worse. For such cases business continuity planning also covers emergency response teams and disaster recovery plans. But all being not handled successfully, e.g. elongated downtimes of IT or loss of data, forms the impact on the business.

The German BSI ("Bundesamt für Sicherheit in der Informationstechnik" – Federal office for security of information technology) categorizes incidents in the following way:

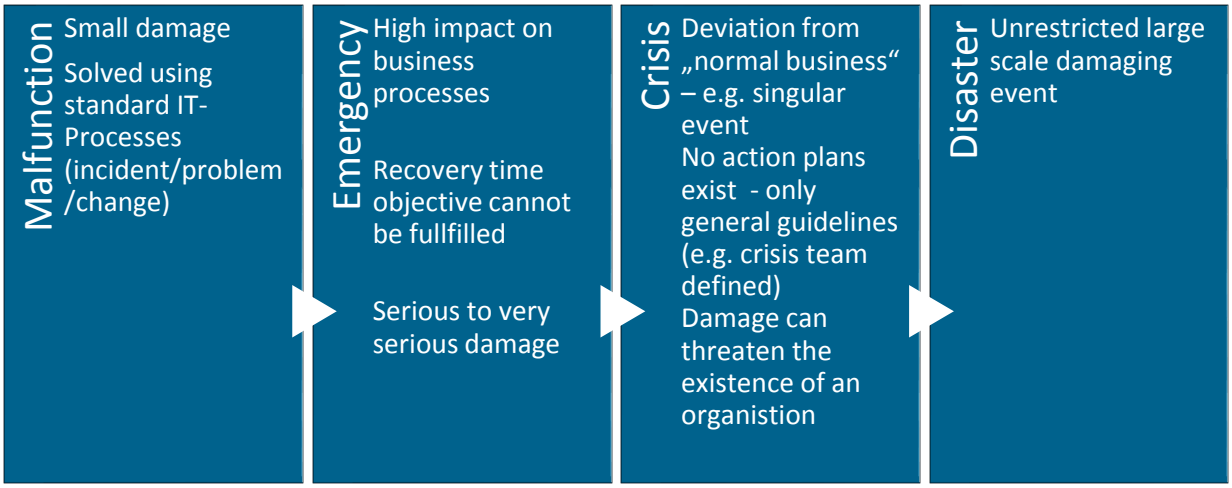

Figure 3: Categorization of Events (Source: BSI, Loomans & Matz)

Due to the non-linear nature of disaster evolvement, each malfunction, if poorly handled, already has the potential of ending up in a disaster. Hence, a disaster not always starts as a disaster right from the beginning. This can be called "Event Continuum" and it requires a diligent handling of all events, even the smallest malfunctions.

Figure 4: Event Continuum

3 THE ROLE OF COMMUNICATION

Failing business continuity often starts with poor communication. Notification of malfunctions and critical incidents might be too slow , ineffective or reaches the wrong people. Involvement of C-level executives happens too late to benefit from their access and command over resources to successfully prevent an evolving disaster. So, communicating the right information to the right people at the right time and in time is essential in dealing with threats to business continuity.

After their investigation of the Deepwater Horizon Oilspill the National Committee came to the conclusion that:

> "In light of the potential consequences, it is no longer acceptable to rely on a system that requires the right person to

be looking at the right data at the right time, and then to understand its significance in spite of simultaneous activities and other monitoring responsibilities."

This forms a strong pledge for effective alert notification and alarm management systems. Alert notifications represent an essential contribution to maintaining business continuity, in particular in the area of successfully detecting and responding to incidents. But there are additional areas where effective communication comes into play. Let us look at a typical IT emergency process:

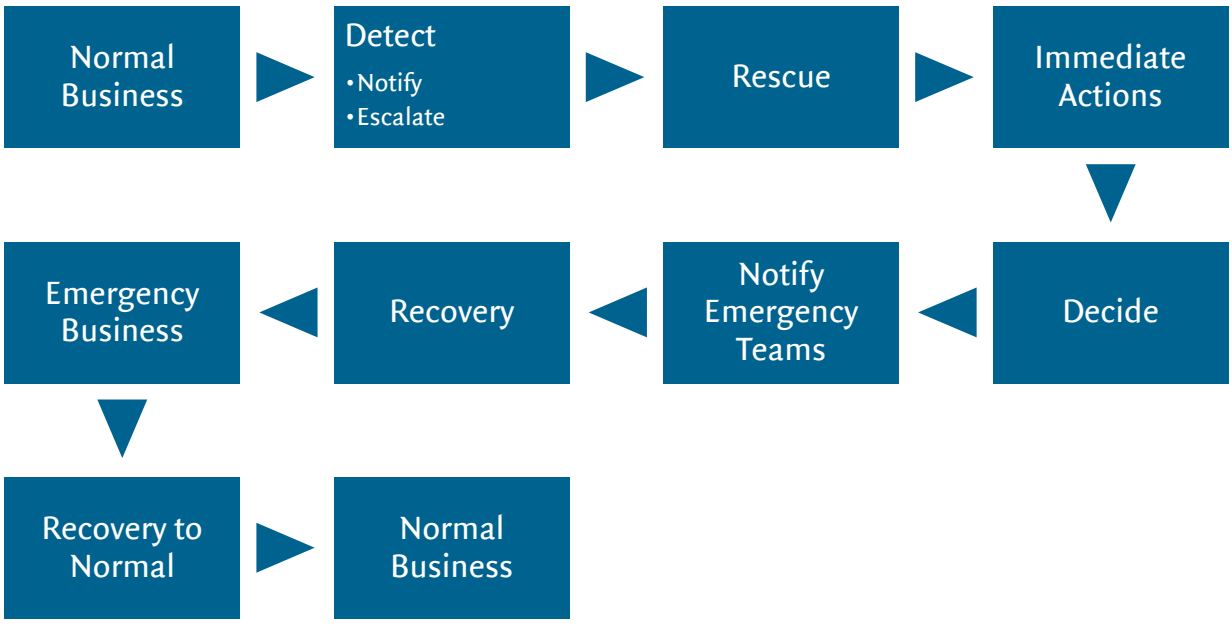

Figure 5: IT Emergency Process (Source: Loomans & Matz)

Effective communication is essential in almost all stages of this process.

Detect:
The moment of detecting a malfunction or critical incident contains a strong pledge for effective communication. This is the glorious moment of automated notification systems like Enterprise Alert®. People who are responsible for troubleshoot a problem or for taking remediation actions need to be informed – reliably and rapidly. But more than that – they also need to receive sufficient information to evaluate the criticality and to take the right actions. In emergency situations crisis teams need to be informed effectively.

Immediate Actions:
To execute immediate actions people need to be informed of what to do and communication between them to coordinate actions is the key.

Decide:
In order to take the right decisions people need to have access to sufficient information. First line operators need to gather information from their peers to create a complete picture of what is happening. Instant communication, e.g. through phone and conference calls, can be crucial.

Notify Emergency Teams:
If the critical situation cannot be contained, emergency teams need to be notified. Again, notifications systems can play an important role as they automate formerly manual call-out tasks and thus free operators from spending crucial time on trying to reach and inform members of the emergency team.

Emergency Business:
If the organization enters a state of emergency business it is advisable to inform employees, suppliers and, above all, customers about that state. A pro-active incident-forward communication can be essential to ensure retaining of valuable customers.

Recovery to Normal:
Once a critical situation has been resolved pro-active information can again be valuable to ensure productivity returns to normal as soon as possible. Imagine, for instance, information that employees can return to the facility and start working again or that the use of an IT application is safe again because newly entered data won't get lost.

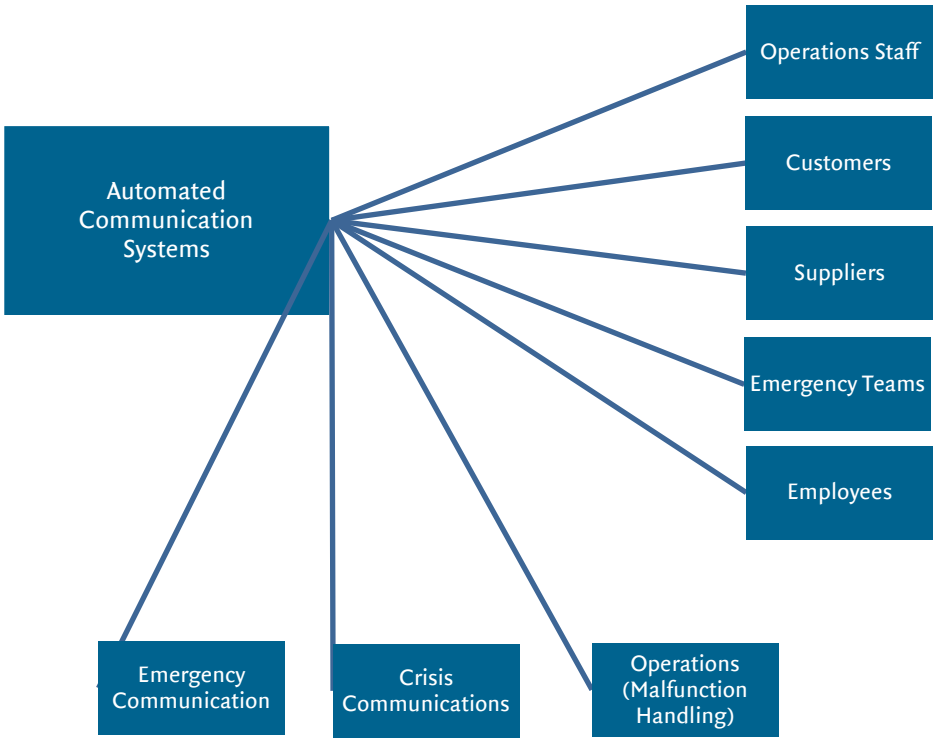

Figure 6: Impact and Relations of a Communication System

4 CONCLUSION

The challenges in even assessing potential threats, their probability and their impact, not to talk about "black swan" events question several paradigms in today's business continuity planning. It becomes obvious that deriving BCP from predictable events and not considering the dynamics of events leads to a serious threat of business operations and survival.

> **Being able to respond rather than being able to forecast, facilitates the ability to effectively react to the consequences of an event. (*Geary W. Sikich)***

Modern systems and software for automating communications and relieving operators from time-consuming communication tasks can have a significant impact on the ability of organizations to swiftly and properly respond to critical events.

> **"Enterprise notification software should be a cornerstone of the effort to maximize systems uptime and minimize disruption to business continuity and service availability."**
> ***PAC Berlecon analyst Dr Andreas Stiehler***

In order to benefit from such systems most they should be applied to the complete "event continuum" which also results in a continuous usage equivalent to permanent testing and maintenance.

5 ABOUT THE AUTHOR

Matthes Derdack is CEO of Derdack and responsible for the vision and the strategic direction of the company. He writes a regular blog at http://blog.derdack.com and is the author of a number of publications in IT magazines.

You can contact Matthes via email: MDerdack@derdack.net or follow him on Twitter: @matthesderdack

Derdack designs software for mission-critical alert notifications and anywhere incident response. Derdack's EnterpriseAlert® supports IT & business operations of large enterprises and global services organizations in over 50 countries. It provides customers with the ability to reliably distribute critical information to the right people and to respond to critical incidents and emergency situations before they can impact business continuity and customer service levels.