CIONET

DISCUSSION SUMMARY

BUSINESS CONTINUITY

Business

Everyone has a plan, until they get punched in the face! Just ask Mike Tyson's opponents.

On 17 October 2024 the Telenet Business Leadership Circle, organised and moderated by CIONET and Hendrik Deckers at the invitation of Telenet Business, took an in-depth look at the role and importance of business continuity. A diverse panel of CIOs shared their insights on what they consider best practices and how they cope with the challenges of business continuity. Using concrete scenarios to prepare for every eventuality is crucial, but it's not enough. Above all, focusing on business continuity also means coping with the unexpected must become instinctive.

In early 2008 there was a local outbreak of the chikungunya virus in Southeast Asia. Strict quarantines of patients – especially in Singapore – prevented the further spread of the virus. At the time, anyone who was paying attention probably thought the chance that the outbreak would lead to a long-term pandemic was pretty low. Yet a good decade or so later, the Covid-19 pandemic put the business continuity of almost the entire global economy to the test.

This reveals the biggest challenge to safeguarding your business continuity. You can prepare for all kinds of scenarios – and it makes sense to do that – but how do you prepare for events that no one thought were possible? Widespread lockdowns and mandatory working from home during the pandemic are a good example. Who could have foreseen that? Staff who went into lockdown armed with a laptop, experience using Teams and a high-performance home internet connection were a happy fluke, not a key pillar of a visionary business continuity plan.

Planning and communication

Yet planning remains essential, as does timing. And of course your IT team must take this on board. If you implement a software update on Friday afternoon and then leave for the weekend, you're simply asking for trouble. Planning means looking to the future, and preferably beyond the boundaries of your own team.

According to our panel, clear communication is paramount when it comes to business continuity. This involves more than just having a proper communication structure in place so that the right people can reach each other quickly. Practical interventions are also needed, such as SIM cards from different networks for key managers, so you can still reach decision-makers even if an entire network goes down.

Who makes the decisions?

Communication is often also linked to a mandate: who makes the decisions around communication? During a crisis, it must be clear who can and should make the necessary decisions. Is it the business? Or does IT decide? A crisis team must be activated, and the team leader should be authorised to make decisions. It's important to task someone with recording and time-stamping all discussions and decisions. If you end up facing a claim for damages or a lawsuit, that information will be crucial. Also, it will be a great resource when it comes to learning lessons after the fact.

The impact of an incident on business continuity can manifest in very unexpected ways. When the shops were closed during the lockdowns, there was a peak in online sales. People bought practically everything online, from bags of cement to barbecues. This created major, unforeseeable challenges for sorting centres, courier services and postal workers.

Well-being

Another area that's often ignored in traditional business continuity planning is the well-being of employees. Especially in situations where a company is facing a long recovery, it's important to distribute the heavy lifting wisely across the available troops. Recovery often requires a sustained effort, day and night. This Trojan effort must be workable for the entire team, so that you don't lose people to burnout.

Conclusion

The conclusion is clear: prepare as well as possible but keep in mind that you can never foresee everything and will inevitably have to improvise to some greater or lesser extent. Black swan events, no matter how rare and unexpected, will always happen. That being the case, it's all about finding the right balance between planning, documentation and pragmatism.

Luk Bruynseels
Chief Product & Technology Officer

Telenet: dealing with the things you can't predict

Luk Bruynseels is Chief Product and Technology Officer at Telenet. His team's field of action includes cybersecurity, physical security and business continuity, in addition to many facets of the operational management of the networks. "We adhere to the ISO 22301 standard," Luk says, "following to the principle of continuous improvement. Every new risk assessment leads to concrete initiatives to optimise the environment."

Telenet is structured in tribes. As a result, IT is highly decentralised. IT is as close as possible to the users, so employees are more aware not only of the importance of IT as a whole but also of the specific software needed to create the right customer experience.

Incident management is an important point of attention for Telenet Business. And it has to be: the company not only manages its own IT environment but also a fixed and mobile network with national coverage. Millions of customers also have a Telenet modem or decoder at home. "So we're well organised when it comes to following up on incidents," Luk adds. "We categorise incidents from simple to major, critical and business critical."

The terrorist attacks on Brussels Airport and in the city's metro on 22 March 2016 were a very serious external incident. Within a short time, the mobile network became completely saturated. At moments like this, all the planning kicks in and a decision is made as to how network usage is controlled. "The most important thing during critical incidents is that certain communication flows are given priority."

What if your data centre explodes?

An example of an internal business critical incident occurred on 1 April 2021, when an explosion blew out an external wall of a Telenet data centre. "The chance of something like that happening – that your data centre explodes – is almost zero," says Luk. "And yet it happened. You can deduplicate as much as you want – with two times two fibre connections on each side of the data centre – but if your data centre explodes, everything stops."

Telenet's response was first and foremost pragmatic. "Initially, we erected a tent over the affected area to prevent additional damage from rainwater. We also put physical security in place to prevent anyone from entering the data centre." Telenet then decided not to simply switch off the entire data centre. In particular, the non-redundant services in the data centre were migrated one by one, an approach that wasn't foreseen in any of the business continuity scenarios.

And the most important lesson that Telenet learned from the incident? Sometimes the impossible happens. "In addition to scenarios, training and other preparation, as a company you must above all develop a reflex to deal with events that you could never have predicted. It's important to have a solid communication structure within your organisation, so that you can reach the right people very quickly."

Gert De Laet
Enterprise Architect

Digipolis: time-consuming recovery after ransomware attack

Digipolis is the company responsible for the city of Antwerp's IT services. With a team of 300 employees and 150 contractors, the company provides support to 10,000 staff affiliated with the city of Antwerp. These employees suddenly lost access to their data during what has since become known at Digipolis as "The Incident".

That incident was a ransomware attack on 6 December 2022. The hackers managed to steal a password via phishing and gain access to an Exchange server, which was well secured via SSL. They then placed executables wherever possible. The Digipolis network wasn't segmented, which allowed the hackers to penetrate all of the systems and disable security and monitoring.

After that first phase – which lasted six weeks and during which the hackers remained undetected – they copied all the data and encrypted every file. Digipolis employees could only find files with the extension .play on their systems. When they clicked on a file, only an e-mail address appeared. Eventually Digipolis received a message from this e-mail address, saying that the decryption key would be provided after payment of a ransom. The company immediately decided not to respond to the demand.

Restoring critical systems

"We had a business continuity plan," says Gert De Laet, Enterprise Architect at Digipolis. "However, in light of the attack, the plan turned out to be too theoretical and, more importantly, inadequate." Digipolis put together a crisis team. "We put our egos to one side and prioritised the citizens of Antwerp. Our goal was clear: to chase the hackers out of our environment and restore the critical systems as quickly as possible."

As a result of the attack, none of the city's applications were working, from libraries and swimming pools to container parks and traffic monitoring – you name it. "We drew up a priority list and started with the vital applications, such as the medication lists of care home residents." To get the staff back to work, Digipolis made a drastic decision. "We ordered a new laptop for every single user – 8,000 units. Then we decommissioned all the old devices."

A roadmap was drawn up for the hundreds of applications that Digipolis had developed for the city – and that ran on-premise in the Digipolis data centre. The company decided to standardise on Microsoft, with Ometa as middleware. This allowed the data to be kept in the source systems. In the second phase, Digipolis placed everything in Azure. "We had citizens' data that was being sold on the dark web removed by a specialised take-down service," says Gert. "But the city didn't pay the hackers a penny in ransom."

Lesson learned

"Of course we learned a lot from the attack," Gert continues. "We invested in risk management, with all the associated plans and scenarios, including communication." The IT budget of the city of Antwerp has doubled since the attack. Another important lesson relates to the well-being of the employees. "At one point, we had to send people home to rest." The attack affected many employees personally, and the response demanded such an enormous amount of work that people were at risk of dropping out. "You obviously want to avoid that, precisely because it is such a big job. Even two years after the attack, the environment still hasn't been fully restored."

About CIONET

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.

cionet.com

About Telenet Business

Telenet Business, part of the Telenet Group, is so much more than connectivity. As a managed service provider they help Belgian companies turn their digital challenges into business opportunities. They support and unburden, large and medium-sized enterprises as well as small entrepreneurs. You can count on them for high-quality managed services such as internet, telephony, solutions to collaborate and communicate digitally, cybersecurity and smart displays.

telenet.be/business