CIONET

DISCUSSION SUMMARY

PLANNING FOR THE UNEXPECTED

Business

This article looks at what was discussed during what proved to be a truly fascinating evening, dedicated to exploring business resilience and sharing insights in that topic. The event was organized and moderated by CIONET and Hendrik Deckers at the invitation of Telenet Business.

In today's volatile world, building a robust business is more important than ever. With that in mind, 12 IT leaders from major companies came together to share their thoughts, experiences, and insights. The roundtable kicked off with each of the 12 sharing their worst nightmare, from their experience in business. Unsurprisingly, it immediately became clear that the worst-case scenarios were different for everyone, ranging from natural disasters or sudden shifts in the market, all the way up to cyberattacks and even espionage. With this is mind, is it possible to define a set of rules for making every business resilient? And is it even possible to be 100% resilient?

But first things first. It is of course a good idea to draw a clear distinction between business resilience and business continuity. The two are clearly related, yet there are distinct differences, mainly in terms of what's required of an organization. Business continuity focuses on the ability of companies to continue operating during a crisis, falling back on a set of processes and procedures. This is essentially a responsive approach. Business resilience implies the organizational ability to overcome unexpected business disruptions — such as the examples mentioned earlier — and recover to the point of being able to continue operating.

Resilience by design

In an ideal world, these are things that need to happen from the early stages of any business's development. This is what we call business resilience by design, a concept and vision that applies across industries today, regardless of the field they're operating in. Of course, this isn't something that can be achieved in an instant. Giving shape to and designing resilience involves multiple elements. First of all, business resilience requires investment. Business and IT leaders face a critical dilemma here: the cost of investing versus the cost of doing nothing. An additional constraint is the fact that investment must be as cost neutral as possible and that the budget provided is usually insufficient to realize everything.

This is where setting up a dedicated governance structure comes into play, as investing in business resilience requires risk analysis, ideally conducted by an audit committee. In this context, the liability of the managerial board to decide certain matters is an important dynamic. But the most important aspect of bringing resilience by design to an organization is adopting the right culture and mindset. Resilience must be to the forefront of everyone's mind: young and old, internal and external.

Christophe Grégoire
Director Technology
& Operations, COO
ASTRID

Business resilience — an increasingly complex story

You could say that ensuring business resilience and continuity in times of distress is at the core of what ASTRID does. The specialized telecom operator for Belgian emergency and security services has a network of 600 masts, covering the entire country and ensuring connectivity at any time and any place. “Monitoring quality, setting up architecture,managing end-user relations, and integrating services through a managed service model is our core business,” says Christophe Grégoire, Director of Technology & Operations and COO at ASTRID.

He argues that ensuring business resilience has become much more complex compared to 20 years ago. “The threats have become more diverse in nature. Everything was simpler in terms of service requirements 20 years ago, with less complexity and less mixed legacies compared to today.”

However, increased complexity goes hand in hand with the need to invest in business resilience. “Risk analysis is more important than ever and comes down to a simple choice: the cost of investing versus the cost of not investing. The path to success lies in acknowledging the importance of resilience and taking action to build a business that can survive and thrive during times of uncertainty.”

Resilience drift

Threats are not set in stone — they evolve over time as they take on new forms, and new threats keep emerging. But one thing is for sure: business resilience demands far more from companies today than it did 20 years ago. From an IT and cybersecurity perspective, this results in an increasingly complex framework, which is not free of legacy. This is where companies must guard against an important side effect of the pursuit of resilience, which is the mixing of legacy and new technologies, as well as the stacking of technologies. Not only does this resilience drift increase complexity, but companies also run the risk of neglecting the basic requirements of business resilience today. What used to be resilient may no longer be so, when we take into account today's needs and threats.

Many IT leaders feel that in the long run companies are building even more legacy on existing legacy IT infrastructure. From the moment the legacy infrastructure is due to be replaced or upgraded — or even just patched — problems start to emerge. The thought leaders on our panel pointed out that they expect systems will continue to fail at the time of updates or patches. From this point of view, one can measure resilience by the agility of IT infrastructure. For some sectors, like the telecom sector, this is of even greater importance, since agility has a direct and immediate impact on customer experience and satisfaction.

Reviewing the cloud

Organizational abilities are the crucial foundation for business resilience in the long run. But when a cyberattack occurs, the key priority is to restore production or services as fast as possible. This is especially true for manufacturing companies, since production is their main source of profit. From this point of view, it's important to reconsider which business controls (i.e. hardware, software, and data) to keep on premises and which to move to the cloud. Over the past few years, moving to the cloud has been the dominant dogma.

However, when a threat materializes, it's important to have a "wall" between the actual data and the operational technologies in order to kickstart production as fast as possible. For production, this means that keeping all OT infrastructure and data on premises offers more protection, as this enables operations to continue offline. In the event of a cyberattack, you can buffer orders manually and keep production running even if the breach hasn't been found, as long as OT infrastructure, such as a WMS and DNS servers, are kept on premises. In this regard, network segmentation proves to be a best practice.

Philip De Bie
VP IT & CIO
Picanol

Ensuring business continuity

When we talk about business resilience, we're talking about a wide range of threats that can have a major impact on production continuity and therefore also business continuity. Cyberattacks are an example of just such an ever-present threat. Philip De Bie, VP of IT & CIO at Picanol, argues that threats like these have an even bigger impact on manufacturing companies.

"For us, it's all about ensuring production continuity, since that's the only value driver underpinning our business." To keep the risk of falling victim to a ransomware attack low, De Bie says it's of vital importance to protect OT infrastructure by keeping it separate from the IT side of things. "Cyberthreats should make everyone reflect on the importance of keeping production controls on premise at all times, away from the net and the cloud."

This of course also raises questions about the IT architecture of the future and the place of fully integrated stacking in that architecture. "Engaging in these essential trade-offs is a routine practice for manufacturing companies, aligning with their approach of paying only the necessary expenses to ensure the continuity of production."

The backup lifeline

Backups play a vital role in the resilience of businesses, not least in the event of a cyberattack. When backups become compromised, you lose your lifeline and become a sitting duck. A simple backup to disk no longer suffices. A three-stage backup should be the standard practice. That means local backups, which are then replicated on a central server and then manually taken offline again. As long as you can rely on your backups, you can try to mitigate the attack.

It should be noted that backups themselves are of little importance to cybercriminals. What matters are the records and data they can exploit or make public. Triple-extortion ransomware attacks are becoming increasingly popular, with cybercriminals not only encrypting and exfiltrating company data but also actively targeting employees, customers, or patients. Any form of extortion likely pushes up the percentage of companies that pay ransoms, which currently stands at a staggering 75%.

Knowledge supporting culture

We've already mentioned the importance of installing a culture of business resilience and resilience in IT and OT infrastructure. Only in this way can an organization and its employees properly absorb ideas around, for example, cybersecurity. But culture without knowledge is pointless. With building a robust business being more important than ever, preserving knowledge should be a key priority as well. This is vital to establishing resilient business architectures and designs.

This is a particular challenge for the IT service sector, which is heavily reliant on consultants to bring in the latest knowledge. It goes without saying that this is more difficult for employees who have been working for the same company for 30 years, especially in an area that's evolving as fast as the IT service sector. The panel's thought leaders noted that this challenge is less prominent in the telecom sector, since it's a smaller industry undergoing a more stable evolution and has fewer partners involved.

Blago Gjorgjievski
VP of Network & Wholesale
Telenet

Why there's even more at stake for telcos

In today's interconnected world, telecommunication services play a critical role in keeping society functioning, especially during times of crisis. Natural disasters, such as hurricanes, earthquakes, floods, or wildfires, can severely disrupt the infrastructure and operations of telecom companies. That's why the importance of business resilience can't be overstated, as it directly impacts the continuity of communications and essential services.

During the Telenet Business Leadership Circle organized by CIONET, Blago Gjorgjievsky, VP of Network & Wholesale at Telenet, explained why business resilience is so important to the telecom sector: "Our purpose is to serve the public, anytime and anywhere." This is the most important KPI for the sector. "Not delivering means we lose customers. A single minute without connectivity is a disaster, and just rebooting our systems is not an option."

This is why continuous improvement and transformation is so important to remaining competitive and to continuing to provide services. But there's a dark side to this according to Gjorgjievsky: "In the process of continuous improvement, you tend to rapidly build on legacy IT infrastructure. However, regular modernization of IT infrastructure is crucial, as it allows you to be agile in times of great need. In the light of the war for talent, telecom businesses need more T-shaped profiles than specialists."

Conclusion

During the roundtable discussion, it became clear that building a robust organization is more important than ever and requires a proactive approach, especially in the face of threats that are evolving faster and becoming more diverse. Everyone has to deal with this. However, after hearing the thought leaders sharing their experiences, it became clear that everyone looks at these challenges from their own perspective, and tackles them accordingly. This is reflected, for example, in the way we look at the connection between IT and OT infrastructure.

Building a culture of resilience requires repetition to the point of boredom and has to start at the top. In essence, business resilience can be seen as a drive toward robustness much more than a drive toward efficiency and continuous improvement. It's about installing a culture of holding the handrail, without people having to think about it.

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