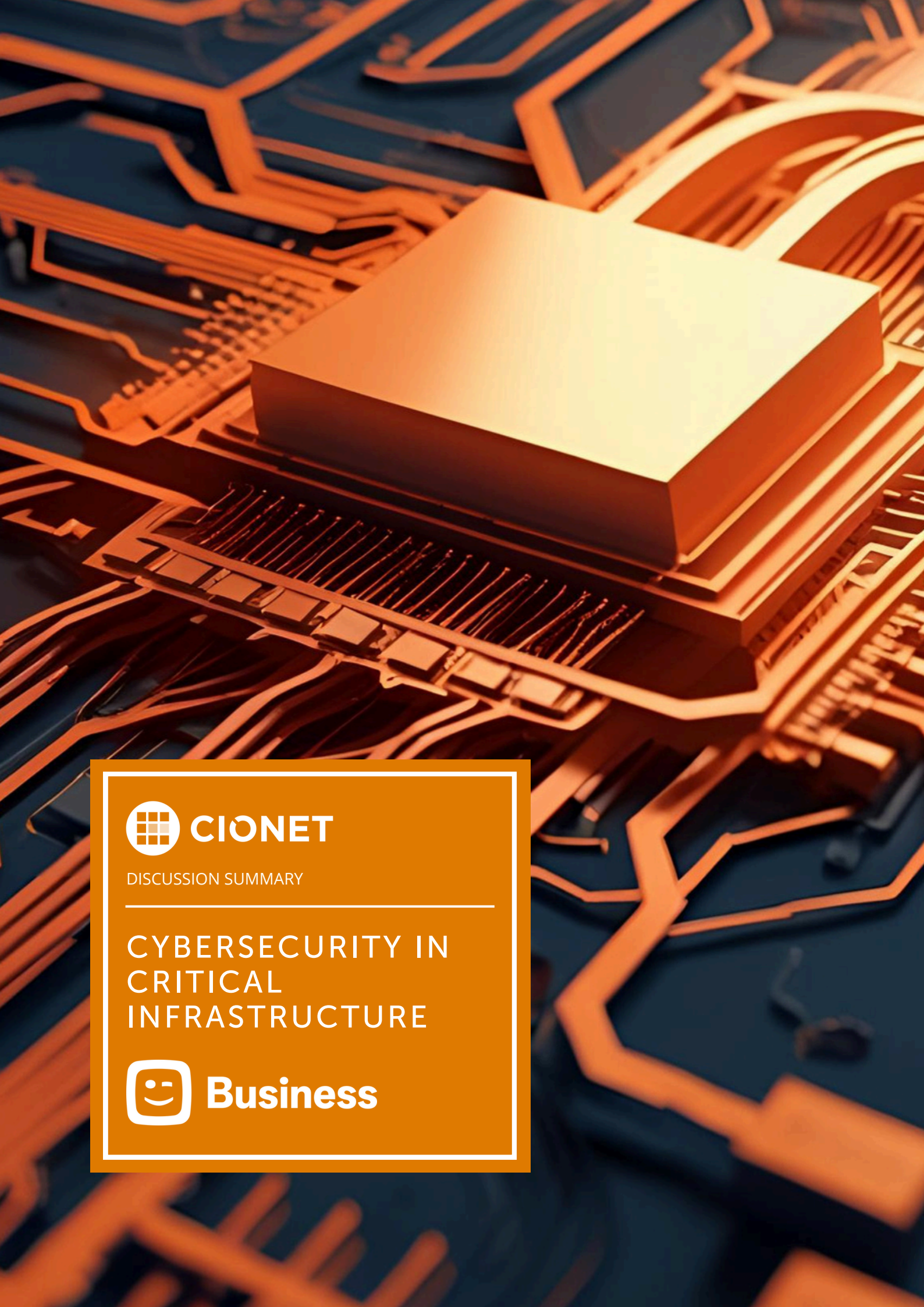

CIONET

DISCUSSION SUMMARY

CYBERSECURITY IN CRITICAL INFRASTRUCTURE

Business

On 5 June 2025, 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 cybersecurity in critical infrastructure.

Geopolitical tensions have dominated the headlines for over two years now. In this context, the cyber threat landscape is also evolving rapidly. The protection and security of critical infrastructure – both physical and digital – is becoming increasingly important.

Critical infrastructure includes processes that are so vital to society that failure or disruption can lead to serious social upheaval and pose a threat to national security. This includes national energy and water supplies, internet connection and telecommunications, financial transactions, the operation of emergency services, etc.

All these processes increasingly rely on digital components, and it goes without saying that they must be adequately secured. In the context of cybersecurity, however, what we see is that threat actors are no longer merely targeting the applications involved, as they did in the past; instead they are going after cybersecurity infrastructure itself, such as that used to secure critical infrastructure.

Focus on security assets

This shift in tactics is changing the way critical infrastructure managers view security. On the one hand, it's about focusing on the security assets, in an environment where the reliability of the security solution providers is becoming more and more relevant. On the other hand, in recent years, the emphasis has shifted from rapid detection and response to resilience.

The priority is to recover quickly, minimise damage and resume activities as quickly as possible.

MARK VAN TIGGEL
Director Security & Cyber Resilience at Telenet

Telenet: availability and security in balance

As a key provider of a network that's essential to internet and telecommunication connections in Belgium, Telenet is part of the national critical infrastructure. "Availability is very important in our sector," says Mark, Director Security & Cyber Resilience at Telenet. "Other critical infrastructure, such as hospitals and airports, depend on it and must always be able to count on connectivity."

Of course, networks must also be secure, and security measures often affect availability. "It's therefore important to keep availability and security in balance," says Mark. "Of course you want to avoid cyber incidents, but security can also have a negative impact on the service provision, for example because it puts extra pressure on the systems, reducing capacity or delaying reponse times."

Threat intelligence

Telenet achieves this balance by focusing on threat intelligence, which allows the right decisions to be made around security. The approach is based on two pillars. On the one hand, it gathers as much information as possible about active threat actors. On the other hand, it has mapped out its own attack surface in detail, by listing which targets those threat actors are most likely to come after.

"This resulted in a list of the most important threat actors and their possible targets," says Mark. "We then built our strategy for the security of our critical infrastructure around this: a combination of best practices from the past and the most up-to-date information on possible risks and threats." Telenet then rigorously tests its techniques and solutions using the same tactics as the potential attackers.

Collaboration is essential

"We regularly exchange information with our peers too. These are not only other telecom operators, but also other managers of critical infrastructure, such as banks, as well as the telecom regulators," says Mark. "Moreover, there may be room for an approach based on the Scandinavian model, in which more work is done based on real-life threat models and simulations, across the various sectors."

Mapping risks and threat actors

The emphasis on resilience critical infrastructure managers are abandoning classic detection and response. They continue to actively collect information about their potential adversaries. Very often, but certainly not always, this involves so-called state-sponsored threat actors, including usual suspects such as Russia, China and North Korea.

Alongside open source intelligence, commercial cybersecurity specialists and integrators are also a great source of data. The major challenge is that the landscape is constantly changing, which makes staying up to date a challenge. In any case, a response plan must be in place for every risk. When a cyber incident hits, there's no time for discussion. You must know in advance what actions need to be taken.

Safety throughout the supply chain

Another major area of concern is the risk to the supply chain. Infrastructure operators are not only reliant on their partners' technology – they are themselves a link in broader chains. The European Union, for example, is now actively moving away from the use of Chinese technology, even though the alternative is usually significantly more expensive. And since President Trump returned to the White House, our dependence on US technology, including public cloud platforms, has been increasingly called into question.

A breach anywhere in the supply chain can compromise the entire system. As a result, critical infrastructure managers try to map and monitor the security level of their suppliers as much as they can. This requires a lot of time and resources, as it turns out, and the onboarding of partners in particular has become a demanding process.

MARIO BECCIA
Deputy CIO for
Cybersecurity NATO

NATO: cyber resilience requires a new mindset

NATO protects the security of its 32 member states in Europe and North America, which together are home to more than a billion people. But while the battlefield was traditionally contained within physical borders, cyberspace has evolved into a new military domain, where cyber weapons have replaced military hardware. "This presents new challenges," says Mario Beccia, Deputy CIO for Cybersecurity at NATO. "Because in cyberspace, contrary to on land, at sea and in the air, it's not possible to guard borders or carry out patrols."

Threat actors are now targeting cybersecurity infrastructure, which is driving the growing importance of cyber resilience. It is vital to anticipate attacks, but also to get ready for recovery and learn lessons from incidents. "First of all, you have to prepare thoroughly," says Mario. "You must have insight into the weak points of your infrastructure." That forms part of the basis of cyber resilience – ensuring the continuity of your activities despite its vulnerabilities, even when an incident occurs.

Restore and learn

If your organisation is hit by an attack, the goal is to resume activities as quickly as possible, and thus keep the damage contained. "So make sure you have a backup of your communications that you can consult, even when e-mail and telephone are down. Also make sure you have backups of your data." That seems like a no-brainer, although in practice it often involves difficult decisions. "You don't want to perform a restore with a backup that's also infected. So what date and time should you go back to? That's often not easy to determine."

Finally, it's important to learn lessons from the incident. "Review the whole thing," says Mario, "so that you know exactly what you need to change – in the systems, with the people, in the culture – to prevent a similar incident in the future." It's an approach that diverges significantly from that of traditional security. A striking element is the geographical dispersion of data and assets, using different technologies, different partners, different clouds and so on. Surprisingly, the public cloud – often considered lacking in terms of security – makes a contribution here, demonstrating once again that cyber resilience requires a different mindset than classic cyber security.

Humans remain indispensable

The rise of AI offers new possibilities in terms of protection, but it also creates new risks. "In a single year, we saw a hundred times more new types of ransomware emerge," says Mario. "This indicates the use of AI, because it's not possible to do that manually." At the same time, we must keep the trend in perspective. "It is indeed a substantial increase, but it remains an evolution rather than a revolution." A greater risk is probably the fact that AI is now built into everything, and we have no control over the use of data in the training of AI."

"Generally speaking, AI isn't yet sufficiently mature to use in the area of critical infrastructure or defence," says Mario. "In the context of agentic AI, a lot of automation has become possible, but full automation remains out of reach. AI still cannot replicate the experience and gut feeling of humans. The human factor therefore remains indispensable."

The right balance

In today's IT security context, the main thing is to strike a workable balance between robust security and compliance. And even though you can measure various elements that tell you a lot about the security level and the security culture, there isn't a KPI that tells you when you've achieved the optimal balance between security and compliance. This also turns out to be the major challenge with cyber resilience. Is that even something we can measure? The answer is simple: no, there is no KPI for resilience. What an organisation needs is a culture that supports security.

Compliance, too, can be a subjective concept. Much depends on the eye of the beholder. An organisation that's confident in its security might still be non-compliant in the eyes of another. That presents a particular challenge. Only a real-world incident truly reveals how well a company can respond and what lessons it will learn. That's why simulations – a kind of security fire drill – are valuable learning tools.

Build transparency, remove barriers

But, as was discussed at the event, the supply chain can provide a distorted picture. In fact, you need to consider resilience across the entire ecosystem. That's not only a highly complex exercise, it's also a somewhat delicate matter. Because even if all parties are prepared to "open the kimono", they must do so in an environment of trust, where it's understood that no one is perfect and that the drive to do better every time is key.

At the same time, the cyber team must be wary of becoming blockers. If that happens, and security begins to hinder the efficient functioning of the organisation, the bar will inevitably have to be lowered. It might be smarter to come at the problem from the other direction. First set the security and resilience bar low and then gradually raise it, avoiding the temptation to "boil the ocean" and instead taking an incremental approach.

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