Securitas

Navigating the shift from regulation to real resilience in critical infrastructure.

Securing what matters

The new rules of critical infrastructure security

Contents

Introduction

Today's critical infrastructure runs on interdependence. Power, water, transport, banking, digital platforms, public administration, and other services are now so tightly connected that disruption in one area can ripple quickly across many others. That interconnectivity delivers efficiency—but it also magnifies risk. A local act of vandalism at an unprotected node can trigger regional consequences. The January 2026 Berlin power grid arson attack is a case in point: one incident with thousands affected and multiple services disrupted.

Against a backdrop of heightened geopolitical tension, threat actors have diversified and professionalized. Hybrid attacks that blend the digital and physical, from site sabotage to cyber intrusion and drone overflight are increasingly designed to overwhelm detection and response.

Critical infrastructure organizations also face into a new security chapter with the European Union Critical Entities Resilience Directive (CER) obliging member states to identify critical entities by July 2026 and setting out increased security requirements. According to analysis, there are set to be over **15,000**[1] designated critical entities in Europe by 2027, up from just **100** under the former directive.

As regulatory requirements increase and threats converge across physical and digital domains, business leaders must adopt a more integrated, intelligence-led approach to security. This shift requires ownership at the highest organizational level. Critical infrastructure is the backbone of societal resilience and economic stability; protecting it is therefore not just an operational concern, but a shared responsibility with consequences beyond individual organizations.

Contributors

Mike Evans
Director, Risk Intelligence Center
Securitas

Benedikt Meyer
Public Affairs
Securitas Germany

Claus Fibiger
Country President
Securitas Denmark

Morten Krohn Sommer Mikkelsen
VP Solutions Offering
Securitas Europe

Gaspard Fierens
Head of Security Advisory
Securitas Europe

Marc Moris
Group Prevention & Protection Lead
Proximus

1 Implementing the European Directive on Critical Entity Resilience (CER Directive): Status, Challenges, and International Context - EU-CIP

Borderless and blended – a new horizon of evolving threats

Global geopolitical confrontation, including the first major European conflict in over 70 years, has heightened threat levels for critical infrastructure providers – NATO[2] now classifies **critical infrastructure** sabotage as a top threat to security. Hybrid or 'blended' attempts to disrupt critical infrastructure are part of a fast-moving trend.

Hybrid attacks move across borders as quickly as data and media flows. Digitalization has expanded the attack surface, yet physical risks have also become more sophisticated—from perimeter breaches to unmanned aerial systems targeting substations and remote assets. Mapping dependencies, diversifying supply chains and building redundancy are essential, but they only work when paired with integrated security and risk management that can detect, verify and respond in real time.

Mike Evans, Director, Risk Intelligence Center, Securitas says, "Today, every single threat actor type is motivated to target critical infrastructure – even rudimentary acts of sabotage and theft can cause severe outages. Some threats are now truly borderless due to the interdependence of modern infrastructure. Threats to critical infrastructure do not respect geography. The speed at which issues spread is a risk factor in itself. Our advice to business leaders is that they need to make real-time monitoring of regional risks a top priority."

> "Threats to critical infrastructure do not respect geography."
>
> **Mike Evans**
> Director, Risk Intelligence Center
> Securitas

Marc Moris, Group Prevention & Protection Lead at ICT and digital services business Proximus, warns of the need for organizations to be proactive and agile. He says, "Preparations for prevention and protection against evolving risks are still insufficient in many cases – critical infrastructure companies need to conduct comprehensive risk assessments to ensure adequate preventive and protective measures and to assess risks more dynamically."

Mapping dependencies and diversifying supply chains are priorities for organizations working to mitigate disruption and avoid downtime, as is building redundancy into critical systems. But this needs to be paired with **integrated security and risk management** to tackle multifaceted threats.

Morten Krohn Sommer Mikkelsen, VP Solutions Offering, Securitas Europe highlights the importance of supply chain evaluation and says, "Critical infrastructure lives inside long and highly interconnected value chains. Every supplier, subcontractor, and service provider becomes part of the resilience equation. If one link in that chain is fragile, the impact doesn't stay contained; it spreads. That's why choosing suppliers is no longer just a commercial or procurement decision. It's a resilience decision."

Evans says, "Situational awareness is more important than ever for critical infrastructure, but the ability to gain a meaningful understanding of blended threats in real-time is what will set organizations apart and enable them to stay one step ahead."

Situational awareness is therefore a decisive capability. Organizations that merge physical data such as video surveillance, access logs or patrol data with cyber signals and external threat intelligence can achieve faster verification and escalation, reducing operational and societal impact.

While digitalization and connectivity

2 https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence?

CASE STUDY

On-site guarding and thermal camera technology for electricity producer

A leading private energy producer – specializing in the delivery of thermal, hydroelectric, solar, and wind power plants – required a security update to improve perimeter protection, renew electronic security and ensure the potential to scale across multiple sites.

An integrated solution was implemented, combining on-site guarding, remote video and analytics, thermal cameras, loudspeakers, and bodycams.

Fire and safety services were also included in this bespoke solution, increasing security robustness and efficiency.

Building a resilient security program

From understanding risk to measurable outcomes in 5 steps

Most operations and assets within a Critical National Infrastructure Environment (CNI) are highly critical, unlike other operators.

1. UNDERSTAND
IDENTIFY WHAT MATTERS

Map critical assets such as people, sites, equipment, and processes. Assess potential consequences to understand how incidents could affect life safety, continuity, financial loss, or reputation. Create a shared understanding of priorities and risk acceptance.

2. ASSESS
DETERMINE THREATS AND VULNERABILITIES

Using open-source intelligence, proprietary data, and local insights, identify relevant threats and determine how their likelihood varies across regions. Assess existing controls across people, processes, and technology.

3. MITIGATE
APPLY THE RIGHT CONTROLS

Combine quick wins with longer-term improvements across three areas – People, Process and Technology.

4. GOVERN
EMBED IMPROVEMENTS

Governance should include reviews and tracking KPIs such as incident types, response times, system uptime, and training compliance.

5. EVOLVE
KEEP PACE WITH CHANGE

Threats and vulnerabilities shift as organizations grow and environments evolve. Monitor emerging trends, update procedures, integrate lessons learned, and revise risk roadmaps twice a year.

Source: Securitas Global Clients Europe – Security Advisory

Integrated physical and digital protection for resilient critical infrastructure

While digitalization and connectivity have increased attack surfaces on the one hand, **physical threats have also become more sophisticated, and organizations are looking for ways to mitigate those**. Critical entities in key sectors will need to conduct formal risk assessments, develop resilience plans, and implement technical measures to mitigate disruption. CER emphasizes the importance of physical security – from access controls and site protection to redundancies and emergency procedures.

Benedikt Meyer, Public Affairs, Securitas Germany, says "What we are now seeing is a concerted, integrated push towards holistic physical and cyber security architectures, and that investment in things like robust perimeter protection, video surveillance, and risk analysis is becoming an expected, auditable minimum standard."

Security technology is also evolving to provide innovative solutions to protect organizations. Claus Fibiger, Country President, Securitas Denmark says, "There has been increasing interest for technology to mitigate risks to critical infrastructure organizations. We have seen more interest in drone detection capabilities in Denmark and across Europe, and at the same time, interest in robotic security patrols for remote assets is growing."
Threats facing critical infrastructure today don't come in neat, separate categories. Mikkelsen says, "Physical risks and digital threats are increasingly blended, and security breaks down where they are still managed in silos. Real readiness comes from integration, linking physical protection, technology and intelligence, with the ability to act in real time. The human element in this chain remains vital to mobilize response to act on incidents."

CASE STUDY

Guarding and remote services help Nordic energy operator respond to drone overflight risk

A major energy transmission operator in the Nordics was exposed to drone overflight at large perimeter substations.

An assessment of the threat determined that security combining static guarding and mobile intervention teams to handle escalation, with intelligence and coordination enabled by a Securitas Operations Center (SOC), would enhance security at these locations.

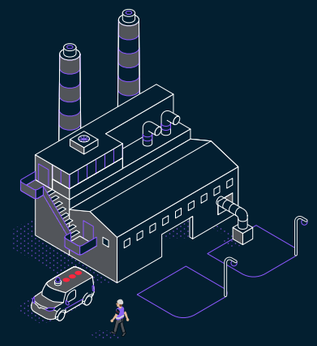
This integrated solution has resulted in significantly faster threat verification for this important operator and simultaneously improved the organization's compliance alignment for future CER and Network and Information Security (NIS2) requirements.

Main sectors impacted by the Critical Entities Resilience Directive

The Critical Entities Resilience Directive (CER) is an EU-wide framework targeting 11 sectors – energy, transport, banking, financial markets, healthcare, drinking water, wastewater, digital infrastructure, public administration, space, and food.

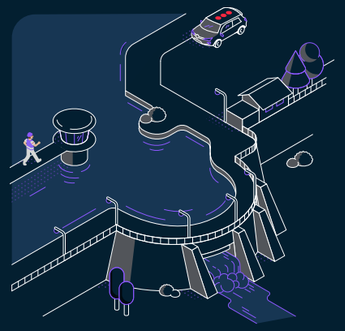
EU member states are required to conduct a national risk assessment to define all critical entities by July 2026, after which organizations may have as little as 10 months to demonstrate compliance with resilience requirements.

Essential requirements include conducting risk assessments, implementing technical and organizational resilience measures, and reporting incidents. The directive seeks to ensure operators are able to prevent, withstand, respond to, and recover from a range of disruptions.



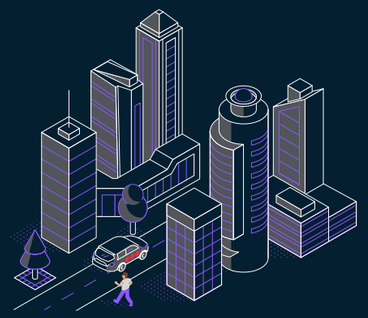
ENERGY SECTOR

Electricity production and energy storage.



WATER SECTOR

Drinking water supply, drinking water distribution and waste water collection, treatment and disposal services.

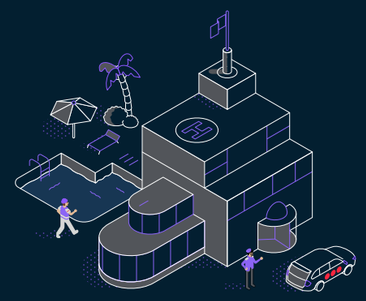


FINANCIAL MARKETS AND BANKING SECTOR

Services such as the operation of trading venues and of clearing systems including banking with essential services such as taking deposits and lending.

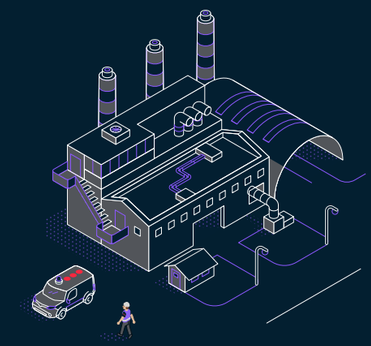
DIGITAL INFRASTRUCTURE SECTOR

Services such as the provision and operation of internet exchange point service, domain name system, top-level domain, cloud computing and data centers.



HEALTH SECTOR

Distribution, manufacturing, provision of healthcare, and medical services.



PRODUCTION, PROCESSING AND DISTRIBUTION OF FOOD SECTOR

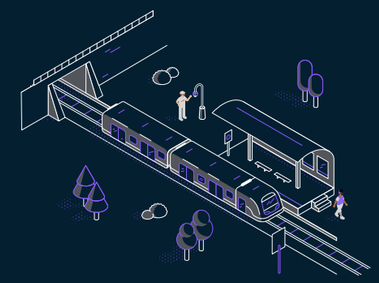
Large-scale industrial food production and processing, food supply chain services and food wholesale distribution services.

CASE STUDY

Risk intelligence informs transport sector organization's operations

A company in the transportation sector operates several sites and depends on reliable situational assessments to inform security strategy. The operator regularly receives risk intelligence information on relevant developments in the vicinity of its sites, such as protests, disruptions, or other potential risks.

The intelligence has enabled them to identify potential threats at an early stage and adjust security measures, improving operational readiness and strengthening resilience.



TRANSPORT SECTOR

Services such as the management and maintenance of airport or railway infrastructure.

PUBLIC ADMINISTRATION SECTOR

Compliance and control - a board-level imperative

The CER Directive and other frameworks have a significant role to play in the evolution of critical infrastructure security. They are transforming resilience from a voluntary ‘best practice’, into a legally mandated leadership and governance obligation. In light of these dynamics, resilience has shifted from a technical measure to a strategic, board-level priority.

Fibiger says, “It’s important that CER is seen as wider than compliance. Directives are not just regulatory burdens - they are strategic drivers shaping board level decisions and investments. It is a question of leadership, risk awareness, and long-term competitiveness. Organizations that understand their role within the value chains they operate in can use resilience as a position of strength—rather than viewing it merely as a regulatory requirement. When resilience is embedded into management practices and operational thinking, it becomes a strategic asset.”

While high levels of resilience are more common in sectors like energy, robust security, and implementation of security controls, can be inconsistent across sectors and incident preparedness lacking. Across Europe, the regulatory environment is tightening the focus with national implementations of the CER Directive coming into force - a prime example being Germany’s KRITIS Umbrella Act[3].

CASE STUDY

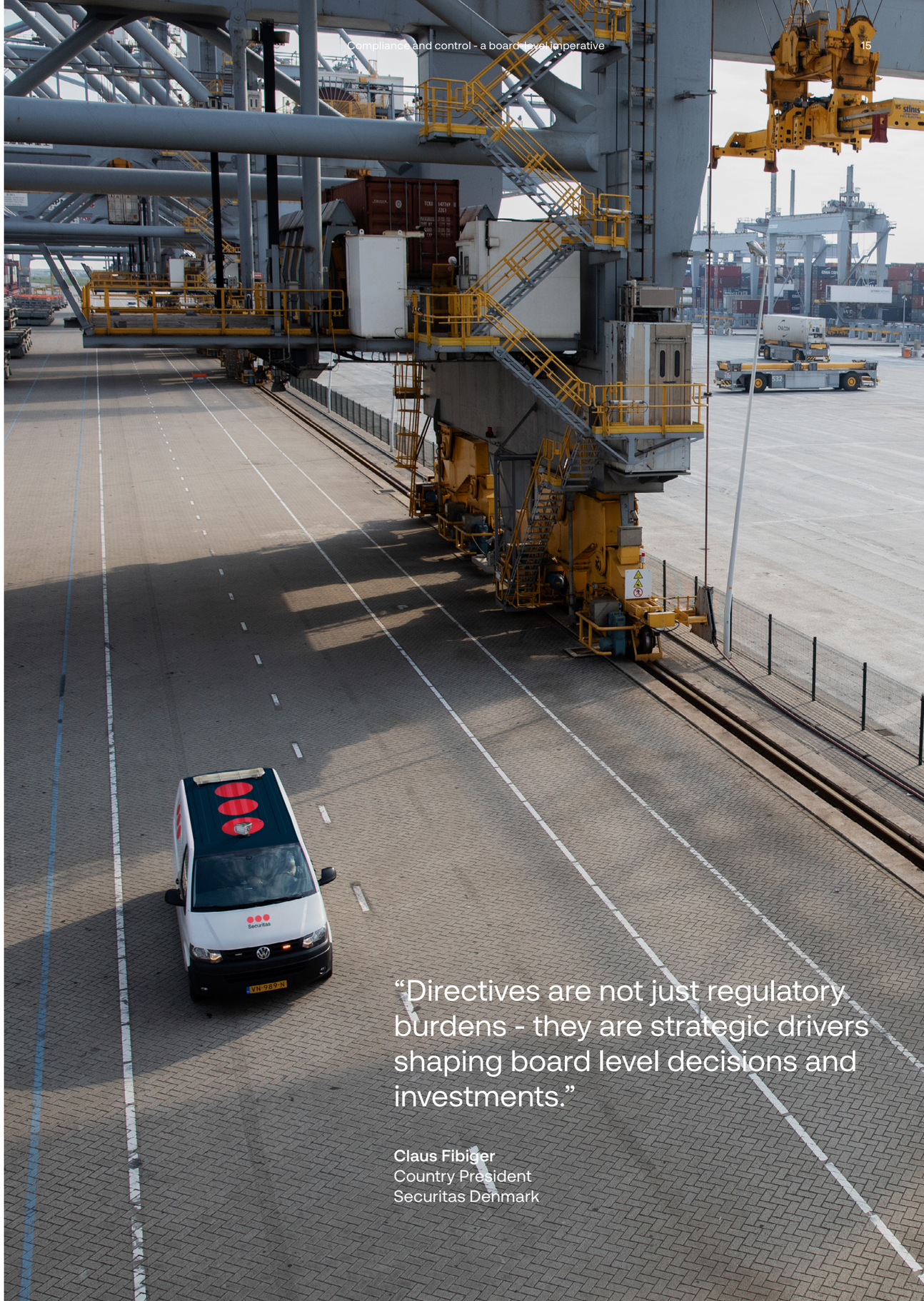
Mobile video security solution secures a critical infrastructure construction site

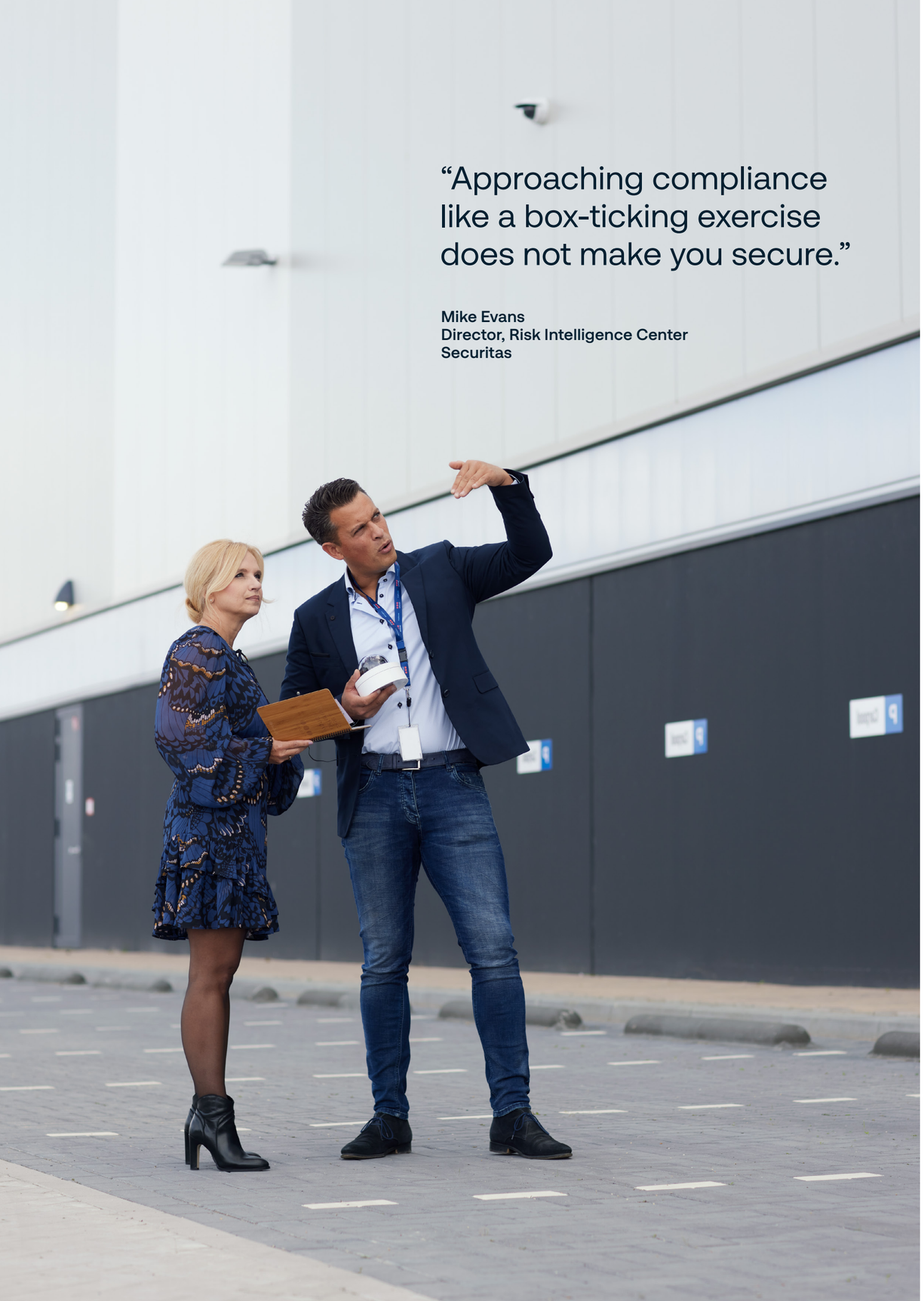
While planning a major railway infrastructure modernization project, two large gas pipelines were discovered that interfered with the planned construction. This unexpected hurdle had to be addressed urgently to keep the project on track. The existing gas pipelines needed to be redirected by the national gas company, and security was needed to protect the site throughout the process.

A mobile video solution featuring embedded video analytics was deployed, and a remote connection to the local Securitas Operations Center was established. This enabled heat accumulation and the perimeter to be monitored continuously, with SOC operators on hand 24/7 to respond to alarms in real time.

In the event of an incident, operators would coordinate the appropriate response forces and could make on-site announcements using SOC-connected horn speakers.

3 https://www.bundesregierung.de/breg-en/news/cabinet-kritis-umbrella-law-2404992





“Approaching compliance like a box-ticking exercise does not make you secure.”

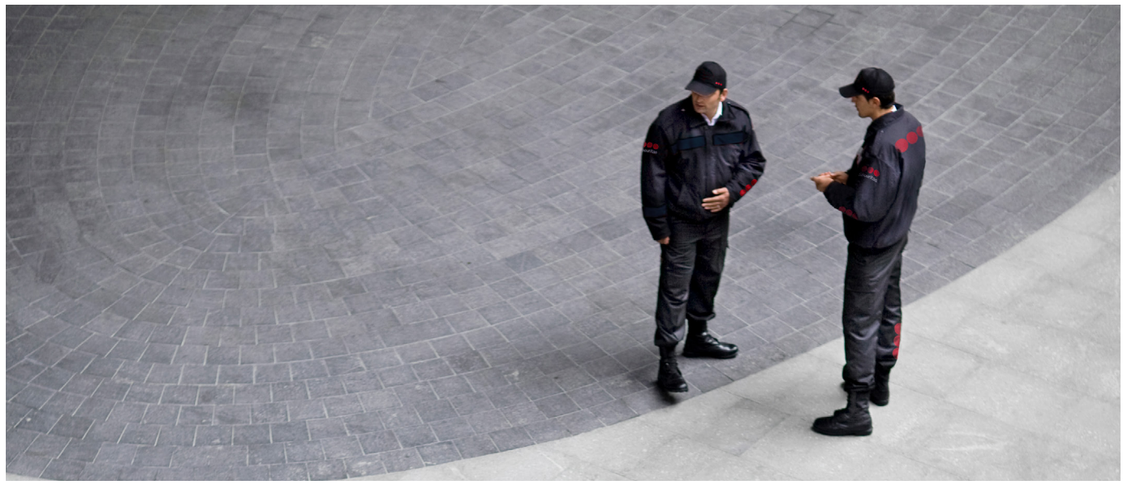
Mike Evans
Director, Risk Intelligence Center
Securitas

The framework is intended to identify critical entities first and foremost, with organizations serving over **500,000** people identified as KRITIS. Players within this category must report incidents within 24 hours, with non-compliance potentially resulting in fines of up to **€1 million**.

Physical security is central to compliance with legislation like CER and the KRITIS Umbrella Act – the importance of adequate perimeter security, access control, surveillance and monitoring, guarding, and alarm systems is emphasized by these frameworks. Meyer says, “Legislation enforces mandatory risk analysis, reporting obligations, and physical security requirements – but importantly, we also see that compliance is marking a major step towards comprehensive, cross-sector critical infrastructure protection.”

Moris says “Europe has excelled in developing new legislation, but compliance must not become an end in itself for critical infrastructure organizations. Business leaders need to remember that criminals operate outside legal frameworks and that risks should be assessed continuously.”

Evans adds, “Compliance is essential, and these evolving frameworks are a rising tide helping to lift all boats. Approaching compliance like a box-ticking exercise does not make you secure. It should be seen as just the start when it comes to critical infrastructure security – not the endgame.”



CASE STUDY

Real-time monitoring and intelligence empowers global financial institution

A global organization at the forefront of the financial services industry was facing increasing incidents, with threats impacting staff, resources, and crucial business operations.

Shortcomings in the existing reporting system to track threats were identified– a limiting factor both for resilience and future compliance.

A tailored custom intelligence service, built on real-time live monitoring was set up, featuring 24/7 alerting, early warnings, and crisis support – enabling a predictive approach to threats and robust response.

Regular intelligence updates were set up to provide ongoing threat landscape visibility. Executive protection screening was put in place to safeguard personnel facing targeted threats. A Dedicated Request for Intelligence (RFi) service was also established, where they could call on specialists to provide information on specific threats.

These customized, integrated services have helped mitigate property damage, threats against staff, and potentially disruptive protests. With greater control and decision-making clarity, the financial services organization reported improvements in global operations.

Security priorities for business leaders: from compliance to continuity and recovery

The response to the convergence of physical and digital threats is a top priority for critical infrastructure leaders. Surveillance, intelligence and response capabilities need to be unified as part of a concerted security approach. Preventing every act of sabotage, insider threat, and system failure has become unrealistic, emphasizing the importance of layered resilience and effective responses.

Evans says, “In a world where blended threats are being designed with the intention of maximizing societal impact, integrated security that spans both the physical and digital layers has never been more important.”

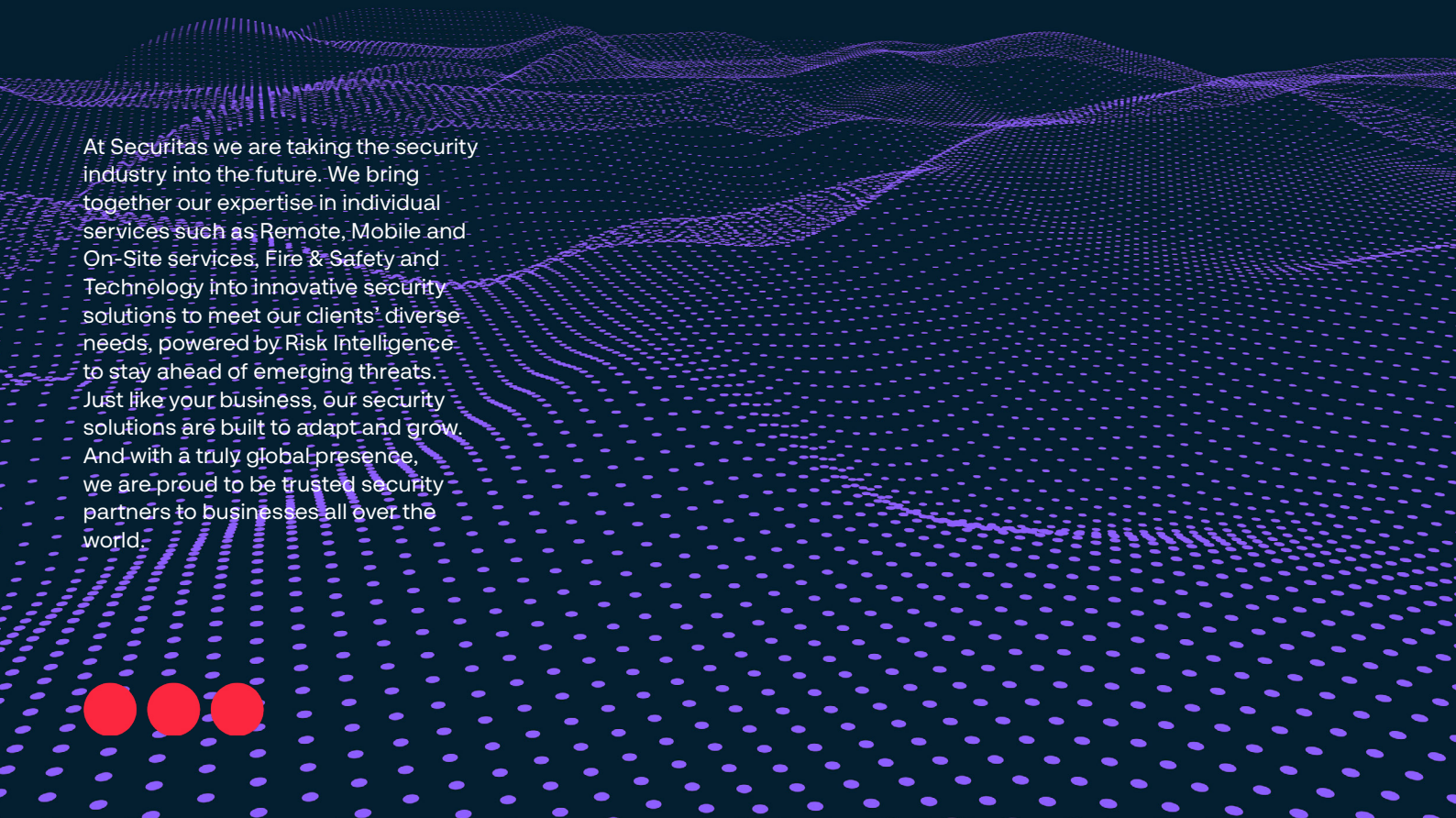
Collaboration and alignment among stakeholders are also important factors, Moris says, “Collaboration must extend beyond any public-private divide to include partnerships within the private sector, leveraging expertise, resources, innovation, and alliances among companies.

Alignment between critical infrastructure operators, service providers, and public authorities remains essential. Security providers play an integral role in mitigating and managing major incidents.”

Regulation and frameworks such as the CER Directive should be seen not merely as compliance obligations, but as **strategic opportunities to strengthen preparedness and long-term competitiveness.**

Fibiger concludes, “Being at the forefront of preparedness allows companies to respond more effectively as requirements tighten. The best-prepared organizations emerge stronger—more credible in customer dialogue and more reliable in operational delivery.“

Organizations that embrace this mindset—integrating security, partnering effectively, and using regulation as a lever for resilience—will be best positioned in an increasingly volatile risk landscape.


At Securitas we are taking the security industry into the future. We bring together our expertise in individual services such as Remote, Mobile and On-Site services, Fire & Safety and Technology into innovative security solutions to meet our clients' diverse needs, powered by Risk Intelligence to stay ahead of emerging threats. Just like your business, our security solutions are built to adapt and grow. And with a truly global presence, we are proud to be trusted security partners to businesses all over the world.