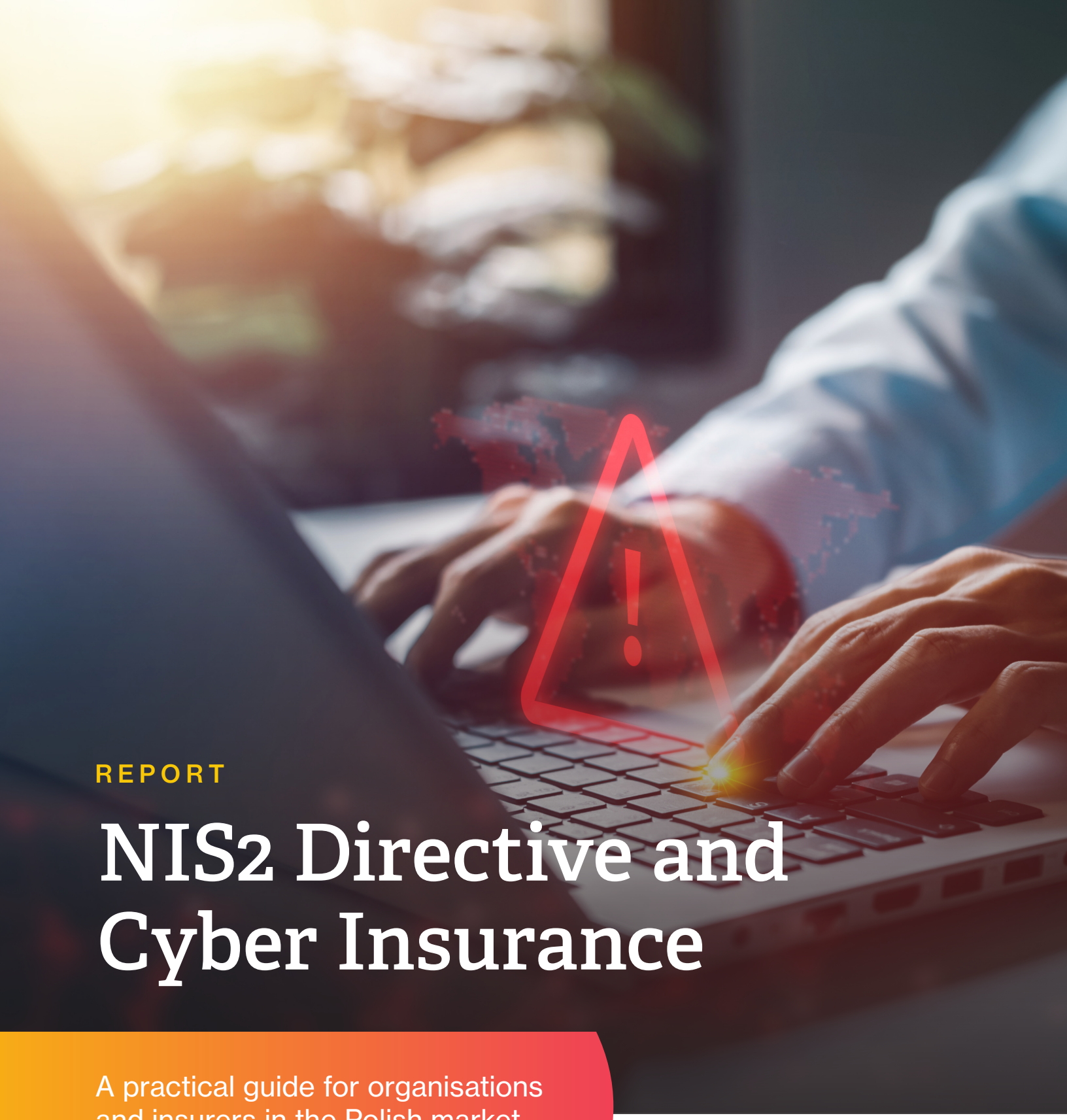

REPORT

NIS2 Directive and Cyber Insurance

A practical guide for organisations and insurers in the Polish market

Crawford®

Global Technical Services

NIS2

A New Reality for Cyber Risk Management

A New Reality

More than half of all cybersecurity incidents in Europe affect organisations classified by the NIS2 Directive as critical to the functioning of states and economies – according to the ENISA Threat Landscape 2025 report. **The growing scale of cyber threats means that cybersecurity is no longer a purely technical problem: it has become one of the central pillars of enterprise risk management.**

In response to these challenges, the European Union adopted the NIS2 Directive, substantially raising cybersecurity management requirements across organisations. These changes matter not only for entities directly covered by the regulation, but also for the insurance market, for which an organisation's cybersecurity maturity is becoming an increasingly important factor in risk assessment.

Background: From NIS to NIS2

The foundation of European cybersecurity regulation was the original NIS Directive adopted in 2016, which introduced the first common framework for the security of network and information systems across member states. Its scope was, however, relatively narrow – covering mainly operators of essential services and selected digital infrastructure organisations.

The rapid expansion of the digital economy and a rising tide of cyber incidents demonstrated that the existing framework was inadequate. In response, the EU adopted the NIS2 Directive in 2022, significantly broadening the range of sectors covered and introducing more detailed and enforceable requirements.

Implementation Across Member States

NIS2 was adopted at EU level, but – as with any directive – its provisions must be transposed into national law by each member state individually. In many countries this involves amending existing cybersecurity legislation or adopting entirely new acts. At the time of writing, a number of EU member states have not yet completed transposition of the NIS2 requirements, including France, Ireland, Luxembourg, the Netherlands and Spain.

Once transposed at national level, organisations within scope must be classified as either essential or important entities and then align their cybersecurity management systems with the new regulatory requirements. In practice, this means implementing cyber risk management measures, incident handling processes and cybersecurity governance mechanisms. Many member states have also provided transitional periods to allow organisations time to adapt.

Who Does NIS2 Cover?

The new rules divide in-scope organisations into two main categories: essential entities and important entities. The first group comprises organisations of critical importance to the functioning of the state and economy; the second covers enterprises operating in significant sectors whose activities may also affect the stability of services and infrastructure.

The catalogue of sectors covered has been substantially expanded, encompassing energy, transport, the financial sector, healthcare, water and wastewater management, public administration and food production.

A significant change is also the explicit inclusion of supply chains. Entities subject to NIS2 must manage cyber risk in their relationships with suppliers and business partners. As a result, companies outside the scope of the regulation may nonetheless be required to meet certain security standards in order to work with NIS2-covered organisations.

In practice, this means organisations must actively manage supplier risk: from verifying vendors' cybersecurity maturity, through ongoing monitoring of vulnerabilities in ICT products and services, to formal procedures for classifying high-risk suppliers. NIS2 therefore reaches far beyond directly regulated entities – it effectively extends across entire supply chains.

In the short term, this will likely trigger a significant increase in due-diligence questionnaires sent by NIS2-covered entities to their contractors, as well as changes to cooperation agreements – including audit rights clauses and detailed security requirements. The practical impact of the regulation will therefore be felt by a much wider population of organisations than the formal scope of the directive might suggest.

According to European Commission estimates, NIS2 may directly affect around 110,000 medium and large entities across the EU, though some legal analyses suggest the figure could reach approximately 300,000 institutions – particularly when supply-chain obligations and the extension of scope to public-sector bodies are taken into account.

The catalogue of sectors covered has been substantially expanded, encompassing energy, transport, the financial sector, healthcare, water and wastewater management, public administration and food production.

Essential Entities

ENERGY

TRANSPORT

BANKING

FINANCIAL MARKET INFRASTRUCTURE

HEALTHCARE

DRINKING WATER & WASTEWATER

DIGITAL INFRASTRUCTURE

ICT SERVICE MANAGEMENT

PUBLIC ADMINISTRATION

SPACE

Important Entities

POSTAL & COURIER SERVICES

WASTE MANAGEMENT

CHEMICALS - MANUFACTURE

FOOD PRODUCTION AND DISTROBUTION

MANUFACTURING (BROAD SCOPE)

DIGITAL SERVICES

RESEARCH

Significant Penalties

Maximum Administrative Penalties Under NIS2

Essential Entities

up to **€10 Million** or **2% of global turnover,** whichever is higher

Important Entities

up to **€7 Million** or **1.4% of global turnover,** whichever is higher

NIS2 also introduces liability mechanisms for breaches of cybersecurity requirements. Sanctions may apply both to in-scope organisations and to the management personnel responsible for cybersecurity oversight.

The directive also emphasises management accountability for cybersecurity oversight, and member states are required to introduce appropriate supervisory and sanctioning mechanisms in national law.

In the context of these penalty levels, cyber insurance policies are not the only product gaining relevance: D&O policies and various forms of administrative fine coverage are also acquiring new significance. The prospect of personal liability for board members will almost certainly reduce organisational risk appetite in this area.

Each of these areas represents a broad competence domain in its own right – and one that increasingly requires specialised expertise. There is no single cybersecurity professional who can claim mastery of every discipline. This will intensify the already well-anticipated demand for specialists with targeted skills, and will drive greater reliance on both internal and external cybersecurity teams.

Meeting NIS2 Requirements

The new rules require organisations to implement a comprehensive cybersecurity management system. In practice, this involves a broad range of organisational and technical measures, including:

- Cyber risk management for networks and information systems
- Business continuity and disaster recovery planning (BCP/DR, backups, crisis management)
- Supply chain security management and supplier risk assessment
- Protection of information systems throughout their lifecycle, including vulnerability and patch management
- Incident monitoring and detection, event logging and threat response
- Appropriate protective measures such as encryption and multi-factor authentication
- Human resources security
- Incident response procedures and reporting to competent authorities and CSIRTs
- Cybersecurity training, including for senior management
- Management-level oversight of cybersecurity governance

NIS2 and the Insurance Market

The growing scale of cyber threats is already one of the insurance market's defining challenges. According to the IBM Cost of a Data Breach Report 2025, the average global cost of a data breach has exceeded USD 4.4 million, with a significant portion of those losses arising from operational disruption.

Cyber incidents can result in financial losses, data breaches and operational disruption – and their consequences are increasingly systemic in character. In this context, NIS2 is also significant for financial and insurance institutions, which are incorporating clients' cybersecurity maturity into their risk assessment processes with growing frequency.

The new rules may contribute to a gradual raising of cybersecurity management standards across many sectors of the economy. For insurers, organisations subject to NIS2 – which are required to adopt a systemic approach to cyber risk management – may represent better-identified risks and greater transparency regarding the security controls in place.

At the same time, NIS2 is raising board-level awareness of accountability for cybersecurity and the necessity of building organisational resilience. For the insurance market, this means growing importance is attached not only to the technological aspects of security, but also to the maturity of risk management processes, business continuity planning and incident management capabilities.

As regulatory requirements intensify, so does demand for tools enabling organisations to better identify and manage cyber risk. Cybersecurity is increasingly the subject of a structured dialogue between companies, brokers and insurers.

In Summary

The NIS2 Directive introduces a new logic for cybersecurity management across Europe – moving from reactive to systemic. It is an organisational challenge, but also an opportunity: companies that implement appropriate processes will not only satisfy regulatory requirements, but will also meaningfully increase their operational resilience. For the insurance market, it represents a more mature dialogue on cyber risk and an opportunity for better risk identification, pricing and transfer.

Cyber Insurance in the NIS2 Environment

A Practical Dimension of Risk Transfer

NIS2 formalises and systematises what the mature insurance market has long expected: a systemic approach to cybersecurity, management-level oversight and documented operational resilience. For organisations within scope, cyber insurance is ceasing to be a nice-to-have item in the policy catalogue – it is becoming a rational complement to the risk management programmeme that NIS2 already mandates.

The NIS2 Timeline

The NIS2 Directive formally entered into force on 16 January 2023. Member states were required to transpose it into national law by 17 October 2024; in practice, however, this process has proceeded unevenly across the EU. A number of countries missed this deadline, creating a meaningful divergence between the formal applicability of the regulation and its actual enforcement.

For example, in Poland, implementation is occurring through an amendment to the Act on the National Cybersecurity System (UKSC). The practical start date for the new rules is 2026, with transitional periods allowing in-scope entities time to adapt – including several months to be formally brought within the system and up to approximately one year to implement the required organisational and technical measures. Full enforcement and the realistic risk of financial sanctions will therefore build progressively through 2027–2028.

For organisations operating across the EU, it is essential not only to monitor the EU-level implementation timeline, but also – and above all – to track the national legislative schedules in each relevant jurisdiction, as these currently vary significantly and determine the actual moment at which regulatory obligations arise.

What a Cyber Policy Actually Covers in the NIS2 Context

Administrative fines

Many cyber policies available in the EU include coverage for fines imposed by supervisory authorities – including fines arising from breaches of data protection and network security regulations. In the context of the sanctions provided for by NIS2 (up to €10 million or 2% of global turnover for essential entities), this represents one of the most significant elements of insurance protection. Coverage terms and conditions vary between policies and should be reviewed carefully.

Incident Response costs

NIS2 requires the reporting of significant incidents to the relevant CSIRT within 24 hours (early warning) and 72 hours (formal notification). A cyber policy funds the immediate deployment of an IR team, forensic investigators and legal support for drafting notifications – resources that most organisations do not have available on an on-call basis.

Business Interruption (BI)

BI coverage compensates the insured for lost income during systems downtime caused by a covered cyber event.

Third-party liability

If a cyber incident at an NIS2-covered organisation causes harm to its clients or business partners, the cyber policy covers the resulting liability claims. This is particularly significant in environments where a single platform serves hundreds or thousands of dependent entities – such as ICT service providers or operators of digital services.

Supply chain risk

NIS2 transfers responsibility for supplier security to the essential or important entity itself. The insurance market is responding with increasingly broad supply chain liability clauses, covering losses arising from incidents originating with sub-suppliers over which the insured has no direct operational control.

NIS2 as a New Language for Dialogue with Insurers

NIS2 compliance has a measurable impact on insurance conditions. Underwriters are increasingly structuring their questionnaires around precisely the areas that NIS2 directly addresses: vulnerability management, multi-factor authentication (MFA), offline backups, incident response procedures, and board-level oversight of cybersecurity. An organisation that implements the directive's requirements in a documented manner gains a concrete negotiating argument – both at first application and at renewal following an incident.

Also significant is the prospect of personal liability for board members. NIS2 explicitly requires senior management engagement in cybersecurity oversight. A D&O policy provides a distinct layer of protection here – covering claims directed against individual managers for breach of supervisory duty. Both products – cyber and D&O – should be analysed in conjunction: their coverage in this area may be both complementary and overlapping, which requires careful coordination at the policy design stage.

Crawford's Role

NIS2 compliance raises the general level of cyber hygiene – but it does not eliminate the risk of an incident. Market experience consistently shows that organisations with mature security procedures are able to contain the consequences of an attack more quickly. However, it is precisely in the first hours of a crisis that decisions are made under time pressure, with incomplete information and at the risk of costly errors.

This is the moment at which Crawford plays a critical role, acting to support insurers and organisations through complex cyber incidents. Its role extends beyond coordinating the claims process to helping navigate regulatory obligations, supporting timely incident reporting, assessing potential data breach notification requirements, and documenting the course of the incident for potential administrative or legal proceedings. In fast-moving cyber events, this combination of claims expertise, technical understanding and regulatory awareness can help organisations respond effectively and manage operational disruption with greater confidence.

Key takeaway

The NIS2 environment does not change the fundamental nature of a cyber loss – but it changes its regulatory context and places new demands on all participants in the process: insureds, brokers, insurers and claims experts alike, in terms of speed of response, scope of documentation and legal awareness.

Risk transfer through a cyber policy remains one of the most effective cyber risk management instruments available, provided the insurance programme is designed around the organisation's real operational needs rather than solely around formal compliance requirements.

Please visit crawco.co.uk to learn more.

About Crawford & Company®

For over 80 years, Crawford has led the industry through a relentless focus on people and the innovative tools that empower them.

10K employees | **50K** field resources | **70** countries | **$18B** claims managed annually

Crawford® Global Technical Services®

Learn more at
www.crawco.co.uk