# FROM NIS2 TO StromVV

## What really matters in the complex field of cyber regulations

**Why cybersecurity is more important than ever**

Nothing works without electricity; it's the lifeline of our modern society, without which everything from households to essential industries such as telecommunications, healthcare, water supply, and financial systems cannot function.

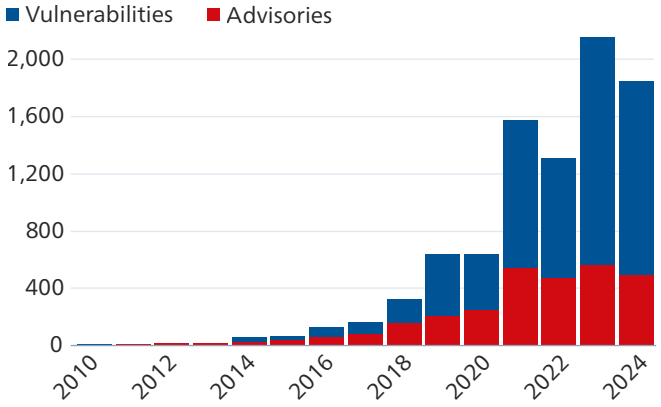
This insight isn't new but is more relevant today than ever. Daily headlines and reports from Europe's ENISA, Austria's Federal Chancellery, and Germany's BSI show that the threat of cyber attacks is growing, and energy companies, in particular, are their focus.

Digitalization has transformed the energy industry. Although new technologies open up opportunities, they also increase risks. Critical infrastructure's increasing interconnectedness with IT systems make them more vulnerable than ever.

Looking into known vulnerabilities reveals the scale of the problem: OT system manufacturers regularly publish security advisories for their products. The number of reported vulnerabilities has increased significantly in recent years – a clear sign that cyberspace threats are continuing to grow. Therefore, protecting these supply-critical businesses from cyber and physical attacks is vital.

**Recent developments in cyber security legislation**

Since its introduction in 2022, the EU's NIS2 Directive has sparked intense discussions and debates about cybersecurity. It required member states to transpose enhanced




Number of vulnerabilities and security advisories

*«The number of reported vulnerabilities has increased significantly in recent years – **a clear sign that cyberspace threats are continuing to grow.»***

## HOWEVER, THE EU ISN'T THE ONLY PART OF THE WORLD WHERE CYBER SECURITY REGULATIONS ARE PROGRESSING:

**USA**

In May 2023, the US government updated the implementation plan for its National Cybersecurity Strategy, which aims to protect critical infrastructure from cyber threats. Executive Order 14028, which mandates strengthening the supply chain's security, is a prime example of this.

**Switzerland**

The Electricity Supply Ordinance (StromVV) will make the ICT Minimum Standard mandatory on July 1, 2024. It defines basic security measures for critical infrastructure operators and other companies. Examples include mandatory vulnerability analyses and implementing network segmentation.

**Australia**

Cyber Security Strategy 2023–2030 provides a clear framework that will be specified by the Cyber Security Act 2024. This law sets new cybersecurity standards for businesses and critical infrastructure.

**Singapore**

With a cybersecurity master plan specifically designed for OT, Singapore has made protecting industrial control systems a national priority.

security requirements into national law by October 2024 – a target that 23 of the EU's 27 member states have failed to meet.

This is a remarkable lapse, especially since cybersecurity issues are nothing new. The 2016 NIS Directive already requires member states to improve their protection of critical systems. NIS2 only reinforced these requirements and extended them to more sectors of the economy, including the food industry and public transport.

The vast number of planned or implemented regulations underscore that cybersecurity in the energy industry is no longer an option but an obligation. Specific companies that have been affected by this are defined by the regulations of the respective member states. For example, NIS2 addresses all entities that provide essential or important services to the European economy or society. However, in many countries, regulations still need to be developed.

### The NIS2 directive's content

The NIS2 Directive outlines mandatory minimum cyber security measures that companies must implement. These include:

- Reporting and managing security incidents: Companies must report incidents to the appropriate authorities within a short period of time.
- Risk management: Companies are obligated to identify and assess security risks.
- Vulnerability management: Companies must identify and remediate IT and OT system vulnerabilities.

Many of these measures are based on recognized standards such as ISO 27001, BSI IT-Grundschutz, or the NIST Cybersecurity Framework. The penalties for non-compliance are severe, making compliance a business-critical task.

### Implications for businesses: Economic and security implications

Even without new legislation, investing in cybersecurity has always been advisable from a business perspective. However, the return on such investments has often been difficult to measure, as prevented disruptions or reputational damage to a business are difficult to quantify.

## RELEVANT ENERGY INDUSTRY LEGISLATION

Cybersecurity requirements play a central role in the energy industry and are regulated by numerous laws around the world. This is a selection of them:

- **Energy Industry Act (EnWG) – Germany:** This law regulates, among other things, the security requirements of the energy infrastructure. When the NIS2 Implementation Act comes into force, it will be supplemented by equivalent requirements.
- **Electricity Supply Act and Ordinance – Switzerland:** The ICT minimum standard defines binding measures for grid operators, energy producers, and service providers.
- **NIS Implementation Act – Austria:** The current NIS Act of 2018 will be replaced by an NIS2 version, which is currently under development.
- **Critical Infrastructure Cybersecurity Act – USA:** This law was designed to protect critical infrastructures, including the energy industry.
- **Critical Entities Resilience (CER) – EU:** This regulation obliges companies to take physical protection measures to secure critical infrastructures.
- **Cyber Resilience Act (CRA) – EU:** This law requires the security of digital products and their manufacturers to minimize cyber threats to product users.

These new regulations will make cybersecurity measures mandatory for all market participants. This will ensure greater security and a level playing field: companies that invest in security will no longer be at a competitive disadvantage.

As a result, investing in the latest security standards makes more sense from a business point of view—failure to comply results in the high costs associated with a successful attack and the penalty of sanctions.

At the same time, many cyber insurance policies depend on compliance with these standards. Failure to implement the necessary measures (e.g., contingency management, backup management, anti-virus protection) may result in reduced insurance coverage or none at all, which is a risk of its own.

### What should you do first?

Even before the legal requirements are finalized, preparations can be made to strengthen your company's cybersecurity posture significantly.

- **Conduct an impact assessment:** If it's unclear whether your company will be affected by NIS2 legislation, you should take advantage of a free assessment offered by national security institutions such as BSI (Germany) or the WKO Online Ratgeber (Austria).
- **Define responsibilities:** Identify and train individuals responsible for IT and OT system information security. These individuals should also become the single contact point for reporting requirements.
- **Involve senior management:** Senior management must communicate cybersecurity information to the rest of the organization.
- **Determine security status:** Use requirement catalogs such as ISO 27001 Annex A, NIST CSF, or the ICT Minimum Standard to assess your organization's security status and prioritize actions. Service providers also offer specialized cyber risk assessments for this purpose.

A complete asset inventory is the foundation for effective risk and vulnerability management, especially in OT. Following the "I can only protect what I know" principle makes creating an inventory a top priority.

External experts can help establish security processes more effectively in an earlier stage. However, the knowledge gained by a company must be sustainably integrated.

### Using NIS2 for concrete implementation

Cyber risk management is a key requirement for companies covered by NIS2 legislation. As mentioned above, the first step is identifying a cyber risk. The process consists of several steps:

1. **Identify key business processes:** What processes are critical to your business or the delivery of business-critical services?
2. **Identify the relevant IT/OT components:** Map processes to the appropriate assets, such as IT/OT assets or buildings, including responsibilities.
3. **Perform risk analysis:** Use the asset inventory to determine the magnitude of damage and the likelihood of risks occurring. Relevant standards (ISO 27005, BSI IT-Grundschutz) may or may not be used.
4. **Plan actions:** Reduce risks to an acceptable level with state-of-the-art measures. Implementing legally required measures, such as attack detection systems in Germany, should be a priority.
5. **Document comprehensively:** All specifications, plans and implementation of measures must be documented. This includes regularly monitoring the effectiveness of measures.

*«External experts can help establish security processes more effectively in an earlier stage.* ***However, the knowledge gained by a company must be sustainably integrated.»***

In accordance with the NIS2 directive, the following topics are a minimum requirement for documentation:

- Risk methodology for analysis, assessment, and treatment;
- Cybersecurity requirements for IT and OT components;
- Processes and responsibilities for handling security incidents;
- Business continuity, e.g., backup management, disaster recovery, and crisis management;
- Supply chain security and service providers relationships;
- Security from the procurement, development, and maintenance of systems, especially when dealing with vulnerabilities;
- Strategies for evaluating the effectiveness of cybersecurity measures;
- Basic cyber hygiene and training;
- Use of cryptography and encryption where appropriate;
- Personnel security, access controls, and asset management;
- The use of multi-factor authentication or other authentication methods.

These are familiar requirements from standards such as ISO 27001 or BSI IT-Grundschutz and the core of an information security management system (ISMS). However, it may be challenging for areas of OT that weren't covered by the scope of these standards. Adapting existing IT security processes to OT security requirements is useful.

### Conclusion

New cybersecurity legislation presents a significant challenge, but also an opportunity to improve business operations with long-term security. A structured approach can help you comply with regulations and establish a robust level of security that meets legal requirements while building trust with customers and partners.

## HELP FROM OMICRON

We offer comprehensive solutions that help your company meet NIS2 requirements:

### StationGuard Solution

- **Intrusion Detection System:** BSI-certified system for substations and control centers with intuitive operation and SIEM integration.
- **Asset management:** Automatic IT/OT system recordings reduce the effort to create and maintain inventories.
- **Vulnerability management:** Identifying affected OT systems makes patch management much easier.
- **Functional monitoring:** Detects misconfigurations and increases reliability.

### ADMO/Insight

- **Workflow optimization:** Improves workflows while ensuring data integrity and availability.
- **Data management:** Centralized planning and organization for engineering, testing, and maintenance tasks.

### Training and engineering services

- Conducting **security risk assessments** and audit preparation
- Support for creating and implementing **security concepts**
- Secure OT network configuration
- **24/7 support** for security incidents
- **Customized training** for IT and OT specialists

Our solutions facilitate security process automation while helping you meet standards such as ISO 27001 and NIS2 requirements. For more information, please visit:

omicroncybersecurity.com