

Cyber Security Strategy

Table of Contents

1. Introduction, Context, and Regulatory Requirements.....	3
2. Requirements and Expectations for Companies in the Scope of NIS2	3
2.1 Risk Management.....	3
2.2 Incident Reporting.....	3
2.3 Supply Chain Security	3
2.4 Oversight and Enforcement	3
3. Strategic Objectives.....	4
4. Specific Measures for Improving Cybersecurity.....	4
4.1 Applicable Regulatory Requirements for Cybersecurity.....	5
4.2 Information Asset Management System.....	5
4.3 Monitoring and Management of Information Security.....	5
5. Value and Requirements for the Identified Improvement Measures	5
5.1 Documentation Development	5
5.2 Information Asset Management System.....	7
5.3 Information Security Monitoring and Management Service	7
5.4 Additional Information on Estimated Values	9

1. Introduction, Context, and Regulatory Requirements

The Republic of Bulgaria and the European Union have recognized information protection and cybersecurity as key priorities due to the exponentially growing threats across all sectors of public and social life.

With the introduction of *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)*, Boni Holding faces additional obligations in the field of cybersecurity, particularly due to the presence of a Research Institute with six centers for research and consultancy.

Currently, the specific regulation addressing cybersecurity is the *Ordinance on Minimum Requirements for Network and Information Security*, adopted by *Decree No.186 of 26.07.2019 (published in State Gazette No. 59 of 26.07.2019)*. Its updated version is expected to apply to entities falling under the scope of *Directive (EU) 2022/2555*.

2. Requirements and Expectations for Companies in the Scope of NIS2

To comply with NIS2, Boni Holding must be prepared to demonstrate the following during audits by regulatory bodies or second parties:

2.1 Risk Management

- Regular risk assessments, including mitigation measures for identified risks. These assessments consider specific threats to the organization's assets and operations, along with known vulnerabilities. A treatment plan with concrete actions and deadlines is to be developed.
- Periodic penetration testing and security audits.

2.2 Incident Reporting

- Organizations must report significant incidents within 24 hours of occurrence. It is crucial to demonstrate the ability to detect incidents and collect digital evidence and artifacts.
- A final report must be submitted within one month, detailing the incident, affected third parties and systems, and measures taken to prevent recurrence.

2.3 Supply Chain Security

- Measures must be implemented to manage risks from suppliers and third parties, focusing on supply chain resilience.
- Evaluation of suppliers' information security and/or inclusion of specific contractual requirements.

2.4 Oversight and Enforcement

- The directive mandates stricter oversight by national authorities, including regular audits and on-site inspections, as outlined in the proposed new *Cybersecurity Act*.

- Competent authorities will have the power to request information and access documents to ensure compliance.

3. Strategic Objectives

The strategic cybersecurity goals of Boni Holding focus on ensuring the resilience and predictability of IT-dependent production processes and business operations. This includes the adoption of new technologies, cybersecurity tools, services, and documentation aligned with risk analysis.

Key objectives include:

- Implementing an effective cybersecurity management process in line with the *Ordinance on Minimum Requirements for Network and Information Security*.
- Ensuring cyber resilience through carefully selected tools and technologies.
- Reducing the risk of cybersecurity incidents through continuous monitoring and behavioral analysis of systems and users.
- Achieving readiness for incident detection, reporting, and response to minimize potential damage.
- Managing known and emerging vulnerabilities by improving or introducing new countermeasures.
- Defining roles and responsibilities for IT and cybersecurity management within the company.
- Conducting informed risk assessments followed by actionable treatment plans.
- Efficient use of public funds to support cybersecurity and IT operations.
- Outsourcing activities that cannot be internally supported due to lack of personnel.
- Documenting and updating responsibilities, activities, and processes related to IT and cybersecurity.
- Ensuring business goals are met through effective security measures supporting IT-dependent operations.
- Introducing a service management process for services provided to students, with resilience and security as key success indicators.

4. Specific Measures for Improving Cybersecurity

Following the previous section, an analysis of the current state of the IT infrastructure at Boni Holding was conducted. The conclusions from this report led to the creation of a list of short-term (urgent) goals for improving cybersecurity. This list is not exhaustive in terms of necessary reforms or technological upgrades, but it serves as a solid starting point for the future development of cybersecurity within the company.

4.1 Applicable Regulatory Requirements for Cybersecurity

An update to the current *Ordinance on Minimum Requirements for Network and Information Security* is expected. It will introduce mandatory measures for improving cybersecurity, and Boni Holding falls within its scope and audit requirements.

It is essential to prioritize compliance with this ordinance, as failure to implement the required measures and maintain accountability could not only damage the company's reputation but also result in administrative sanctions from regulatory authorities.

To this end, detailed documentation must be developed to reflect the actual state of security-related processes at Boni Holding in the context of the Ordinance. Regarding *Directive (EU) 2022/2555*, the Bulgarian legislation is still being harmonized, and the new measures are expected to complement and expand the existing *Ordinance on Minimum Requirements for Network and Information Security*.

4.2 Information Asset Management System

Implementing an information security management system requires continuous maintenance and full visibility over the assets it is meant to protect. A universally applicable measure in this area is the introduction of an IT Asset Management (ITAM) system.

Boni Holding should plan to implement such a system as the only way to control the number, condition, and current status of IT assets within its infrastructure. Since risk assessments mandated by law focus specifically on organizational assets, the implementation of this technology is considered essential.

4.3 Monitoring and Management of Information Security

The reliability and effectiveness of an information security management system are proven by its ability to monitor and respond to threats in real time. It is not sufficient to rely solely on technical controls without incorporating user actions, DNS queries, vulnerabilities, and metadata generated by various systems at Boni Holding.

Therefore, the improvement strategy includes the implementation of a SIEM (Security Information and Event Management) platform, which will provide full infrastructure visibility and enable vulnerability management. Recognizing the complexity of deploying such a platform, Boni Holding considers outsourcing it to a third party as a viable option. This approach ensures access to the necessary expertise, implementation, maintenance, and incident investigation—already a widely adopted practice among public organizations. Studies in the field also show significant cost savings with this model.

5. Value and Requirements for the Identified Improvement Measures

5.1 Documentation Development

This process has already begun, with a designated contractor and set deadlines. The finalization of the documentation depends on the specifics of the upcoming *Cybersecurity Act*, which will transpose the NIS2 requirements into Bulgarian law.

In the meantime, the first version of the Information Security Policy has been created. It will be supplemented with the following content/documents:

1.	Network and Information Security Policy
2.	Information Classification
3.	Information Classification Form
4.	Risk Management
5.	Risk Assessment
6.	Information Asset Management
7.	Information Asset Inventory
8.	Human Resource Security
9.	Confidentiality Declaration
10.	Third-Party Confidentiality Agreement
11.	Third-Party Interaction Management
12.	Change Management for Information Assets
13.	Change Plan
14.	Security in the Development and Acquisition of Information and
15.	Traffic Filtering
16.	List of Prohibited Ports for Incoming/Outgoing Traffic
17.	Unauthorized Use of Devices
18.	Cryptography
19.	Administration of Information and Communication Systems
20.	List of Administrator Accounts
21.	Network and Information Security Status Report
22.	Monitoring and Control Plan
23.	Administration Environment
24.	Connectivity Diagram
25.	Access Management
26.	Access Request/Change/Termination Form
27.	Access Matrix for Information and Communication Systems (ICS)
28.	Remote Access/Telework Protection
29.	Hardware Device Protection
30.	Software and Firmware Protection
31.	Approved Software List
32.	Malware Protection
33.	Web Server Protection
34.	Domain Name System (DNS) Protection
35.	Physical Security
36.	Monitoring
37.	Checklist
38.	System Logs
39.	Network and Information Security Incident Management
40.	Incident Register
41.	Incident Classification and Priority

42.	Incident Notification
43.	Data Backup and Archiving
44.	Data Backup and Archiving Schedule
45.	Infrastructure Component Backup
46.	Business Continuity Plans
47.	Plan Testing Program

5.2 Information Asset Management System

The implementation of an Information Asset Management System is fundamental to effective cybersecurity management. According to a specialized checklist published by the Center for Internet Security, having an asset management system is the first item in their assessment questionnaires. This approach has also been adopted by Bulgarian regulatory authorities with the same goal—to identify and manage all devices connected to an organization’s infrastructure.

We have proposed a tested product—runzero—which is quick and easy to implement and provides highly detailed statistics about what is connected to Boni Holding’s infrastructure at any given moment. The product is available for direct purchase from the manufacturer’s website.

5.3 Information Security Monitoring and Management Service

This service should include the necessary licenses for a cloud-based SIEM platform and a vulnerability management system. It should cover the entire infrastructure of Boni Holding and include costs for a set of activities and technologies that fully meet current regulatory requirements.

By implementing such a solution, Boni Holding will be able to:

- Demonstrate the ability to detect incidents,
- Collect evidence,
- Protect metadata (logs) from manipulation and deletion,
- And track administrator and user actions in the context of cybersecurity.

Service features	
1.	Monitoring and response to malware alerts based on priorities defined in the documentation.
2.	Monitoring updates of modules, signatures, and product versions, and identifying computers/assets not connected to the management console within Boni Holding’s IT environment.
3.	Management of protection user groups and their configurations.

4.	Management of security policies related to malware protection, tailored to current needs.
5.	Integration and maintenance with MS Active Directory Services.
6.	Monitoring processes initiated during the execution of a given program.
7.	Monitoring the status of recently connected critical assets.
8.	Configuration and verification of on-demand scans on endpoints and servers.
9.	Regular monthly checks of Boni Holding's public web-based applications, and upon request by the Client.
10.	Assistance and guidance to Boni Holding's web platform developers for resolving identified vulnerabilities.
11.	Rechecking and verification after vulnerabilities have been addressed.
12.	Updating and configuring scanners and their placement within Boni Holding's infrastructure.
13.	Performing authenticated scans using Selenium scripts for deeper application analysis.
14.	Analysis of the effectiveness of actions taken to eliminate vulnerabilities.
15.	Configuration and maintenance of scanning agents and inventory agents.
16.	Aggregation of metadata and log files from critical IT systems or other systems specified by the Client.
17.	Development of various automation scenarios for improving security measures.
18.	Daily monitoring and analysis of metadata from the selected platform.
19.	Correlation and processing of collected data to extract information about threats, incidents, or malicious attempts targeting Boni Holding's infrastructure.
20.	Manual review of reported incidents to determine their status (false positive, true positive) before forwarding for further processing by Boni Holding's team
21.	Preparation and scripting of log parsers for non-standard systems in Boni Holding's infrastructure.
22.	Enhancement or integration with new Boni Holding services during the contract period.
23.	The Service Provider must be able to provide information from the SIEM logs in case of incident investigation or anomaly analysis.
24.	Support for Boni Holding's team with real data for compiling and updating the risk register.
25.	Consulting Boni Holding's team on updating existing policies/procedures or internal rules related to information security.
26.	Consulting on updating diagrams, schemes, configuration sheets, architecture, or other elements depending on the organization's business model and
27.	Regular meetings with Boni Holding's team to analyze and plan actions to reduce risks from current threats to the IT infrastructure.

28.	Vulnerability analysis of Boni Holding's infrastructure, accompanied by recommendations for remediation by the responsible team or external provider.
29.	Confirmation of vulnerability elimination after verification until successful resolution.

5.4 Additional Information on Estimated Values

The planned platform for implementing the service described in section 5 is Rapid7 InsightIDR/InsightVM, covering approximately 400 assets. These assets include a combination of employee computers (both desktop and mobile), servers, and network devices.

Cameras, DVRs, printers, and specialized machines transmit their data differently to the SIEM platform and are not subject to licensing.

Version number	Approver	Periodic review date	Performed by	Next review date
1.0	Board of directors decision dated 05.06.2025			01.07.2026
2.0	Board of directors decision dated 05.06.2026			01.07.2028

