New LEGO City police station Security Policy using NIST CSF framework

Governance and Management of Cyber Security (ICS0009)

Group: 2

Elliina Gorobets, Erik Kaljumäe, Anamul Hoque Shihab, Jaan Metlitski

Table of Contents

Introduction of the Police Station

The New Lego police station is located in Lego city. The size of the building is 2000 sq meters. There are 200 police officers working in this building. This station outsources the heating of the office building for a third party company.

Employees: There are 200 police officers from which one is the head of the police station, 2 System administrators. 2 IT security experts. Both System administrators and Information IT security experts are part of the information security team.

Building infrastructure is secure-minded - all non-public areas are accessed via doors that require a key card. All non-public areas accessing doors can be unlocked remotely.

Areas and Access:

- Non-restricted / Public areas (Non-related people can access these areas)
    - Waiting room
    - 3 Servicing rooms
- Non-public areas (Police station related personnel only)
    - Holding cells
    - Changing rooms & showers
    - Interrogation rooms
- Restricted areas (Access for only personnel related to given rooms)
    - Server room
    - Evidence & sensitive items storage

Assets:

- 50 workstations
- 1 server
- 2 printers
- 5 security cameras
- 5 sensors
- Heat pump unit
- Diesel Generator

Overview of the Framework

The NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a standardised framework meant to be flexible and adaptable to an infinite amount of criteria including geographical location, organisation size and type, and specification. The framework is dependent on continuous review and improvement and includes it in every step of the process, including before its implementation and during its execution.

The core controls are defined within the five functions of identify, protect, detect, respond and recover. The majority of them refer to specific processes and policies particularly the protect function.

These policies can stem from other frameworks and are referred to throughout, in order to implement certain procedures for the entire cycle.

The implementation is performed in tiers or maturity levels in order to allow for quantitative data to measure the implementation itself.

While complete invulnerability is unachievable, the NIST CSF attempts to not only limit them, but also develop the framework and policies along with the developing technology, the company assets and abilities.

The process involves 6 (six) general steps prior to and during the implementation:

- Prioritization and scoping
- Orientation
- Creation of a Current Profile
- Creation of a Target Profile
- Analysis
- The Implementation

This document will explore the effect to which the NIST CSF has been implemented so far and its effectiveness within the police station in outsourcing heating.

Implementing the NIST CSF Framework

Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The five Framework Core Functions are: identify, protect, detect, respond, recover

This document will go through these five steps in the context of the organization in the described order. References to policies will occur to separate documentation following the templates provided by the NIST.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Identify

This function will develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Asset Management (ID.AM)

ID.AM-1: Physical devices and systems within the organization will be inventoried: Lansweeper will be utilized as a main asset management solution. The tool provides inventory of all workstations, servers, routers, switches, monitors, printers, NAS devices. Inventory specifications include: manufacturer, device type, model.

ID.AM-2: List of authorized softwares will be documented by the IT-department and a person shall be designated to be responsible for the process.

ID.AM-3: Guidelines on transferring data between all employees shall be described in Acceptable use policy, Email policy.

ID.AM-4: External information systems include:

- ➔ Personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants)
- ➔ Information systems owned or controlled by non-federal governmental organizations
- ➔ Procedure of asset management is described in Acceptable Use Policy, Access policy.

ID.AM-5: Organization's Information classification guidelines are described in Information Classification Policy

- ➔ High priority security facilities
  - ◆ Infrastructure room
- ➔ High priority security hardware
  - ◆ Heat Pump Unit (HPU)
  - ◆ Security, Alarm & Signal Systems
  - ◆ Diesel Generator
  - ◆ Fire Alarm Systems
  - ◆ Server
- ➔ High priority security software
  - ◆ Monitoring software
  - ◆ Windows 2016 Server
- ➔ High priority security personnel:
  - ◆ Head of the police station
  - ◆ Technician on duty

ID.AM-6: Cybersecurity roles and responsibilities shall be established within Information Security Policy, Vulnerability Management, IT Security Incident Response policies.

- ➔ System administrator
- ➔ IT security expert
- ➔ Technician

Business Environment (ID.BE)

The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

ID.BE-1: The police station provides public safety and security on behalf of the government.
The director is the head of this police station. System administrator and its security experts are responsible for maintaining the security of the office infrastructures,all assets owned by the police station.

Documentation of legal agreements such as contracts with vendors, leases and licensing agreements is not implemented;

ID.BE-2: Assessing overall risk to the critical functions:

- ➔ Governance Impact: Effects on Federal, State, and local governments.
- ➔ Economic Security Impact: Effects on the users and greater economy.
- ➔ Public Health and Safety Impact: Effects on human health by injuries and loss of life.
- ➔ the number of people affected, and the length of time needed to switch to alternative sources.

ID.BE-3: Planning Activities:

- ➔ Identify major strategic issues, legislative changes and budget funding, and their likely impacts on future actions.
- ➔ Ensure a comprehensive understanding of the customers of the company and the services it provides or plans to provide to them.

ID.BE-4: Secondary commercial power supply is implemented. Long-term alternate power supply provided by UPS and/or diesel generators

ID.BE-5: Critical infrastructure services concentrated in the office server room which provides continuity of daily operation for critical systems.

Governance(ID.GV):

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-1: The organization has developed Information Security Policy that defines objectives and principles of information security. The Policy also defines the roles and responsibilities of all relevant representatives involved into information security activities;

The company has an ISMS (Information Security Management System) which includes the following policies:

1. Acceptable Use Policy
2. Security Response Plan Policy
3. Email Policy
4. Remote Access Policy
5. Disaster Recovery Plan Policy
6. Access policy

7. Security alarm system policy
8. Visitors policy
9. Cryptography policy
10. IOT security policy

ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

ID.GV-3: The organization adheres to legal compliance with EU and Estonian legislation.The organization provides individuals the right to obtain a copy of their personal data. The organization does not store the client CC (credit card) numbers.

ID.GV-4: The organization did not establish a risk management process addressing cybersecurity risks.

Risk Assessment (ID.RA)

ID.RA-1: The organization has implemented policy which defines roles, responsibilities and procedures within the Vulnerability Management Process. At the moment, the organization has implemented Tenable.IO and Nessus Professional which is used for scanning staging, development, production environments and internal infrastructure. Web Application scanning.
There are approximately 60 scanned assets.

ID.RA-2: Cyber threat intelligence is not received on a regular basis. Organization receives cyber threat intelligence from the government cyber security agency.

ID.RA-3: External threats are identified and documented within Tenable.IO and Nessus Professional reports. Internal threats are not identified due to the absence of related procedures.

ID.RA-4: Due to absence of formal risk assessment process potential business impacts and likelihoods are not identified

ID.RA-5: Formal risk assessment process was not implemented.

ID.RA-6: Due to absence of formal risk assessment process risk responses are not identified.

Risk Management Strategy (ID.RM)

ID.RM-1: The organization has not developed and documented a comprehensive Risk Management Framework that would describe all steps and relevant methods required to be carried out in terms of risk assessment process, including: - Asset Identification; - Threat Identification; - Vulnerability Identification; - Control Analysis; - Likelihood Determination; - Impact Analysis; - Risk Determination; - Control Recommendations; - Results Documentation.

ID.RM-2: Due to absence risk management process risk tolerance is not determined.

ID.RM-3: Due to absence of risk tolerance it cannot be informed by its role in critical infrastructure.

Supply Chain Risk Management (ID.SC)

ID.SC-1: Cyber Supply Chain Risk Management processes are not established.

ID.SC-2: Suppliers and third party partners of information systems, components are identified within different departments. List of contractors and suppliers are documented.

ID.SC-3: Contractual agreements established with suppliers and third-party partners. Lego police station utilizes a third party company for providing and maintaining the heating of the office building.

ID.SC-4: We did not find evidence of the existence of formal policy describing procedures of assessment or evaluation of suppliers and third-party partners. Third party partners can remotely access the heating system for maintenance and monitoring.

ID.SC-5: We did not find evidence of the existence of formal procedures describing response, recovery planning and testing with suppliers and third-party providers

Protect

This Function includes: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Identity Management, Authentication and Access Control (PR.AC)

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

- There is a user identity and management through a digital identity. The ID itself, including the description of the user and his/her/its access privileges. (“Its” because an endpoint, such as a laptop or smartphone, can have its own digital identity.)

PR.AC-2: Physical access to assets is managed and protected.

- In non-public areas doors should be locked and each user have some sort of card to access it.

PR.AC-3: Remote access is managed.

- Remote access must be secure, examples for remote access are Microsoft Windows DirectAccess Remote Client Management, PuTTy or SSH.

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

- Access permissions and authorizations could be done through Access management.

  Access management refers to the processes and technologies used to control and monitor network access. Access management features, such as authentication, authorization, trust and security auditing, are part and parcel of the top ID management systems for both on-premises and cloud-based systems.

PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).

- To provide network integrity firewalls and/or VLAN must be used.

PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.

An identifier employed by the user to gain access to a network such as the user's password, public key infrastructure (PKI) certificate, or biometric information (fingerprint, iris scan).

PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction.

- Users are authenticated through multi-factor authentication (when more than just a single factor, such as a username and password, is required for authentication to a network or system) or by biometric authentication that relies upon the user's unique characteristic.

Awareness and Training (PR.AT)

PR.AT-1: All users are informed and trained.

- Define cybersecurity roles and responsibilities within Security Awareness and Training Policy.

PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.

- Users must be informed about most used cyber attacks(malware, phishing) and know how to handle them.

Data Security (PR.DS)

PR.DS-1: Data-at-rest is protected.

- Physical and cyber security of databases, data warehouses, servers, archives, off-site backups are implemented.

PR.DS-2: Data-in-transit is protected.

- For accessing internal network resources across the public network and for the transmission of confidential data across public networks, only secure connections must be used: VPN connections, SSL / HTTPS connections, and encrypted mail messages.

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.

- Integrity checking mechanism could be done by mirroring data and RAID parity.

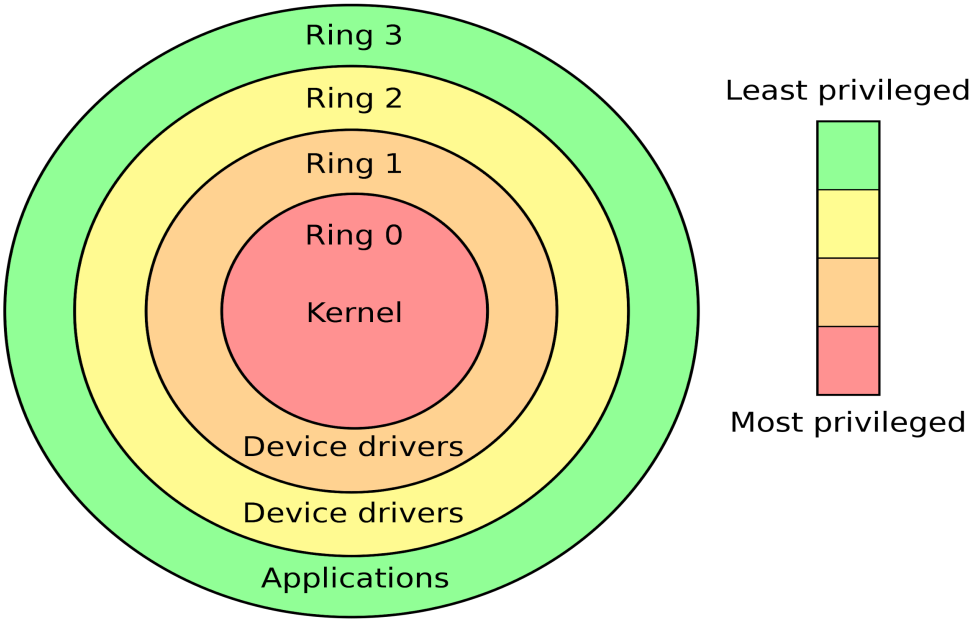
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.

- Conduct risk assessment on the importance of monitoring hardware integrity. Based on results of risk assessment, decide to what extent the organization should monitor hardware integrity.

Information Protection Processes and Procedures (PR.IP)

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).

Giving a user account or process only those privileges which are essential to perform its intended function. For example, a user account for the sole purpose of creating backups does not need to install software: hence, it has rights only to run backup and backup-related applications. Any other privileges, such as installing new software, are blocked.



PR.IP-6: Data is destroyed according to policy

- All unnecessary paper documents with confidential data must be destroyed with an approve cross blade shredder
- Retired and / or discarded from archive storage media must be destroyed physically.

PR.IP-12: A vulnerability management plan is developed and implemented

- Establish and maintain a process that allows continuous review of vulnerabilities, and defines strategies to mitigate them.
- Restrict access to privileged vulnerability data.
- Create, implement and continuously maintain Patch Management Policy. The policy must define downtime windows.
- Downtime window must be defined for each device and application system in order to apply the appropriate patches.
- All patches must be downloaded from the relevant system vendor or other trusted source.

Maintenance (PR.MA)

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

- Document and communicate procedures of maintenance and repairs. For example, to prevent data leakage check whether full disk encryption is enabled or hard drive is removed before sending the laptop to the repair service.

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

- Establish, implement and communicate formal procedures which would describe how the organization:
    - Approves and monitors nonlocal maintenance and diagnostic activities
    - Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system
    - Maintains records for nonlocal maintenance and diagnostic activities

    - Terminates session and network connections when nonlocal maintenance is completed

Protective Technology (PR.PT)

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

- Logs must be able to identify authorized and unauthorized attempts to access resources, with the exact time and place of origin.

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

- Ensure criteria used for granting access privileges is based on the principle of “least privilege” whereby authorized users will only be granted access to information system and network domains which are necessary for them to carry out the responsibilities of their company role or function.

PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

- Test redundant information systems to ensure the failover from one component to another component works as intended.
- Use redundant servers.

Detect

This function is to detect Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Anomalies and Events (DE.AE)

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed

- Implement automated mechanisms that help the organization maintain consistent baseline configurations for information systems include, for example:
    - hardware and software inventory tools
    - configuration management tools
    - network management tools

DE.AE-2: Detected events are analyzed to understand attack targets and methods

- Events should be collected and forwarded to log management solutions so that administrators can analyze suspicious events.

DE.AE-3: Event data are collected and correlated from multiple sources and sensors

- Ensure that event data is compiled and correlated across the organization system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

DE.AE-5: Incident alert thresholds are established in Priority Matrix. Each priority has expected time to resolve(e.g,, 2 hours, 1 business day, etc.)

Security Continuous Monitoring (DE.CM)

DE.CM-1: The network is monitored to detect potential cybersecurity events

- Implement correlation rules within your log management solutions to automate threat detection and log analysis. Tools like zabbix and prometheus could be used.

DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

- The physical environment is monitored with:
    - Security cameras
    - Motion Sensors

DE.CM-4: Malicious code is detected

- Consider using Antivirus software
- Use account of limited permissions

DE.CM-5: Unauthorized mobile code is detected

- Create and implement a policy which will describe how to use Mobile Code Security.

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

- Conduct ongoing security status monitoring of external service provider activity
- Detect attacks and indicators of potential attacks from external service providers

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

- Define, document and implement procedures in Access Control Policy that would describe roles and responsibilities related to physical access.

Detection Processes (DE.DP)

DE.DP-2: Detection activities comply with all applicable requirements

- Define, document, implement and communicate procedures describing configuring monitoring of services before deploying into production

DE.DP-3: Detection processes are tested

- Be sure that detection testing is executed in a timely manner
- Reviews detection testing and monitoring plans for consistency with the organizational risk strategy

DE.DP-4: Event detection information is communicated

- Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, physical access, temperature and humidity

Respond

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

RESPOND (RS) Function

RS.RP-1: The organization has adopted policies which regulate roles, responsibilities and procedures in terms of the incident management process. Policies include Incident management, IT Security Incident Response processes. Duty Team implemented separate Incident Management and Problem Management processes.Response plans is executed during or after an incident

Communications (RS.CO)

RS.CO-1: Roles described within general Incident Management Policy and IT Security Incident Response Policy. Incident Management and IT Security Incident Response policies shall be updated on a regular basis.

RS.CO-2: Formal procedure of how and where the employees can report the incident shall be described in Incident Handling Procedure.

RS.CO-3: IT Security Incident Response Policy contains a procedure that obligates Administrator to share: - name and IP of affected item. - suggested type of incident - date and time of incident - other relevant information

RS.CO-4: Coordination with stakeholders does not occur consistent with response plans

RS.CO-5: The organization’s security training and awareness program will be in place and in cooperation with CERT- EU and estonian cyber security agency.

Analysis (RS.AN)

Analysis is conducted to ensure effective response and support recovery activities
RS.AN-1: There are 3000 events collected from Symantec endpoint protection. IT Security Team started to analyze and categorize these events. The process in the initial phase.

RS.AN-2: We have found no evidence of the existence of the formal procedures describing how the impact of the incident is understood.

RS.AN-3: We did not find evidence of the existence of formal forensics procedures.

RS.AN-4: According to IT Security Incident Response Policy incidents are categorized and classified into three categories: low, high, critical.

RS.AN-5: We did not find evidence of the existence of information whether the company has a private bug bounty program on the platform.

Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
RS.MI-1: We have found procedures which might describe containment of cybersecurity incidents. Detailed description of Containment Phase is documented in Security Response Plan Policy.

RS.MI-2: We have found procedures which might describe mitigation of cybersecurity incidents.

RS.MI-3: Vulnerability Management Policy doesn't include procedures which describe how to mitigate newly vulnerability or document accepted risks.

Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities
RS.IM-1: IT Security Team conducts weekly sync-up where current improvements are discussed; Security Assessment and Penetration Tests are conducted within this control.

RS.IM-2: Response plan will be issued in May 2020 and will be kept relevant on a monthly basis.

Recover

Recovery Planning (RC.RP)

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents
RC.RP-1: There is a Disaster Recovery Plan document that describes recovery procedures of internal infrastructure. Roles are represented in tables. We have found no described responsibilities within the Plan; Disaster Recovery Plan will be executed during or after a cybersecurity incident.

Recover – Improvements (RC.IM):

Recovery planning and processes are improved by incorporating
lessons learned into future activities.
RC.IM-1: Disaster Recovery Plan plan is tested on a regular basis. Lesson learned procedures were implemented.

RC.IM-2: Recovery strategies are updated after lessons learned. Formal procedures are in place. Project plan is established, roles and responsibilities are described.

Recover - Communications (RC.CO)

Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
RC.CO-1: procedures which include following things: managing media interactions, coordinating and logging all requests for interviews, handling and ‘triaging’ phone calls and e-mail requests are documented.

RC.CO-2: : Reputation repair plan is not developed.

RC.CO-3 Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

List of Sources

https://www.nist.gov/cyberframework/framework
https://www.gsa.gov/technology/technology-products-services/it-security/nist-cybersecurity-framework-csf
https://www-west.symantec.com/content/dam/symantec/docs/solution-briefs/ccs-achieve-nist-cybersecurity-en.pdf
https://underdefense.com/wp-content/uploads/2019/05/Anonymized-NIST-CSF-Assessment-Report.pdf
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
https://www.cisecurity.org/wp-content/uploads/2019/08/NCSR-SANS-Policy-Templates.pdf