Published on *The National Law Review* https://natlawreview.com

Network Topology and Network Mapping: The NIST Cybersecurity Framework – Part 2

Article By:

Sinan Pismisoglu

A previous installment discussed the centrality of network topology to an organization's data security and outlined the legal framework and obligations incumbent upon many organizations in the U.S. The first installment can be found here. The second and final part of this series will discuss strategies for optimizing network topology and data security, focusing on the NIST Cybersecurity Framework as one of several security frameworks with broad industry recognition.

The NIST Cybersecurity Framework is a voluntary set of standards, guidelines, and best practices for improving the security and resilience of critical infrastructure sectors. It was developed by the National Institute of Standards and Technology (NIST) in collaboration with various stakeholders from the public and private sectors, and it is widely recognized as a valuable tool for enhancing data security practices across different industries and organizations. Network topology plays a pivotal role within this framework, as it is the foundational blueprint upon which the security measures are built.

Five Functions of the NIST Framework

For each of the five core functions of the NIST Cybersecurity Framework – Identify, Protect, Detect, Respond, and Recover – network topology influences the implementation and performance of the corresponding subcategories. Network topology helps organizations identify and protect their network assets and data, detect and respond to network incidents, and recover from network breaches. **Some examples are:**

- **Identify (ID) Function:** This function involves developing an organizational understanding of the systems, assets, data, and capabilities that must be protected. Network topology supports this function by helping organizations inventory their physical devices and systems (ID.AM-1), map their organizational communication and data flows (ID.AM-3), and identify their network boundaries (ID.BE-5).
- **Protect (PR) Function:** This function involves developing and implementing appropriate safeguards to ensure the delivery of critical services. Network topology helps organizations protect the integrity of their network (PR.AC-5), implement network segmentation (PR.AC-6), encrypt data in transit and at rest (PR.DS-2), and manage network access rights (PR.AC-1).
- **Detect (DE) Function:** This function involves developing and implementing appropriate activities to identify the occurrence of a cybersecurity event, with network topology supporting

the monitoring network activity (DE.AE-1), detecting anomalies and events (DE.AE-2), and implementing continuous monitoring capabilities (DE.CM-1).
- **Respond (RS) Function:** This function involves developing and implementing appropriate activities to take action regarding a detected cybersecurity event. Network topology helps organizations analyze network incidents (RS.AN-1), contain network incidents (RS.CO-1), eradicate network incidents (RS.ER-1), and communicate network incidents internally and externally (RS.CO-2).
- **Recover (RC) Function:** This function involves developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Network topology aids organizations to restore network services (RC.RP-1), improve network recovery planning (RC.IM-1), and incorporate lessons learned from network incidents (RC.IM-2).

Maintaining a secure network topology in alignment with the NIST Cybersecurity Framework can be challenging for organizations due to the complexity and diversity of network environments, the evolving nature of cyber threats, and the variability of legal standards. **In consideration of these complexities, organizations can be guided by some best practices, such as:**

- Conducting regular risk assessments to identify and prioritize network vulnerabilities and threats.
- Updating network diagrams and documentation to reflect changes in network configuration, devices, data, and legal requirements.
- Implementing industry-standard security controls, such as firewalls, antivirus software, encryption, authentication, authorization, etc., to protect network assets and data.
- Using network discovery tools, diagramming software, and monitoring systems to automate and simplify the network mapping process.
- Training employees on security awareness and best practices for using network resources.

FTC Endorsement of the NIST Framework

The Federal Trade Commission (FTC), the primary federal agency responsible for protecting consumers and promoting competition, has recognized the value and consistency of the NIST Framework with its approach to data security, acknowledging its usefulness and relevance for businesses of all sizes and sectors, without formally endorsing it. The NIST Framework is aligned with the FTC's data security guidance and enforcement actions, which are based on a case-by-case evaluation of the reasonableness of data security practices, considering factors such as the nature and size of the business, the sensitivity and volume of the data, and the availability and cost of tools to improve security and reduce vulnerabilities. The FTC has recognized the NIST Framework in various official publications, statements, and collaborative efforts with NIST. **Some examples are:**

- The FTC published a blog post explaining how the NIST Framework is consistent with the FTC's data security guidance, summarized in its "Start with Security" initiative. The blog post links other resources to help businesses implement the NIST Framework.
- The FTC's "Data Breach Response: A Guide for Business" mentions the NIST Framework as one of several sources of additional information on data security. The guide provides practical advice on effectively preparing for and responding to data breaches.
- In various congressional testimonies, the FTC chairperson has acknowledged the relevance and usefulness of the NIST Framework for improving data security. The chair also highlighted the FTC's collaboration with NIST on developing standards and guidelines for privacy and consumer protection, such as the Privacy Framework and the Consumer Privacy Bill of

Rights.

Cross-Mapping the NIST Framework with Data Security Standards

Network topology not only assists with implementing the NIST Cybersecurity Framework, it also supports compliance with various information security standards that apply to different sectors and contexts. Several of the NIST Framework's core functions, such as "Identify" and "Protect," require organizations to understand their network layout, assets and vulnerabilities. Network topology directly supports these functions by identifying and prioritizing critical assets, assessing risks, and implementing protective measures. These standards provide specific controls and guidelines directly related to network topology and mapping and help organizations achieve data security objectives such as confidentiality, integrity, availability, accountability, and resilience. These standards are:

Center for Internet Security (CIS) Controls: These universally recognized controls provide actionable guidance for enhancing an organization's cybersecurity stance. Network topology intertwines closely with CIS Control 1 (Inventory and Control of Hardware Assets) and Control 2 (Inventory and Control of Software Assets). Accurate mapping of network assets and their configurations is central to these controls, specifically aligning with CIS Control 1.1 (Active Physical Asset Inventory) and CIS Control 2.1 (Inventory of Authorized and Unauthorized Software).

COBIT 2019: The COBIT framework aids organizations in governing and managing enterprise IT, aligning IT with business objectives. Network topology is particularly relevant within the COBIT control framework, notably in Control APO12 (Managed Business Process Controls) and Control DSS02 (Manage Service Requests and Incidents). Accurate network mapping substantiates COBIT's objectives by facilitating efficient resource allocation, directly supporting Control APO12.05 (Managed Business Process Controls Monitoring and Reporting), and enhancing risk management, aligning with Control DSS02.03 (Incident and Service Request Data).

ISA Standards: The International Society of Automation has formulated standards such as ISA-95 (Enterprise-Control System Integration) and ISA-99 (Industrial Automation and Control Systems Security). In industrial contexts, network topology is pivotal for securing process control systems. Notably, ISA-99 includes standards such as ISA-99-02-01 (Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control System Security Program) and ISA-99-02-02 (Security for Industrial Automation and Control Systems: Technical Security Requirements for Industrial Automation and Control Systems), which emphasize the critical role of network topology in ensuring the security of these systems.

ISO/IEC 27001:2017: The ISO 27001 standard concerns information security management systems (ISMS). Network topology is pivotal in ISO 27001, particularly in Control A.12.1.1 (Control Objective: Control of Network Perimeter), which mandates assessing and managing network security risks. Additionally, Control A.12.1.2 (Control Objective: Management of Security in Networks) underscores the importance of secure network management, reinforcing the relevance of network topology.

NIST SP 800-53 Rev.5: This exhaustive catalog of security and privacy controls for federal information systems and organizations encompasses controls deeply rooted in network-centricity. Specifically, NIST SP 800-53 Rev.5 includes control families such as "Access Control" (AC) and "Audit and Accountability" (AU), which directly involve knowledge of network topology. Control AC-2 (Account Management) and Control AU-4 (Audit Storage Capacity) emphasize the importance of network configuration and monitoring. Additionally, Control AC-17 (Remote Access) addresses secure network access, highlighting the indispensable role of network topology knowledge. These

controls harmonize seamlessly with the NIST Cybersecurity Framework, further underlining the significance of network topology in government and private-sector cybersecurity initiatives.

Network Topology Optimization for Data Security

Optimizing network topology for data security is an ongoing process that requires constant monitoring, evaluation, and improvement as organizations work towards efficiency, scalability, reliability, and security. Here are some strategies for optimizing network topology for data security:

- **Network Segmentation:** Network segmentation involves dividing the network into smaller subnetworks or segments based on function, location, or access level criteria. This strategy reduces the network's attack surface by limiting the exposure of sensitive data and devices to unauthorized users or malicious actors. It also improves network performance by reducing congestion and latency.
- **Network Isolation:** Network isolation involves creating separate networks for different purposes or data types. This strategy enhances the security of sensitive data by preventing interaction or communication between networks that are not authorized or necessary. It also reduces the risk of network compromise by isolating potential sources of infection or intrusion.
- **Network Encryption:** Network encryption involves using cryptographic techniques to protect data in transit over the network from unauthorized access or modification. This strategy ensures the confidentiality and integrity of data by preventing eavesdropping or tampering by third parties. It also protects against man-in-the-middle attacks by verifying the identity of network endpoints.
- **Network Access Control:** Network access control involves policies and mechanisms regulating who can access what on the network. This strategy enforces the principle of least privilege by granting only the minimum level of access required for each user or device to perform their tasks. It also prevents unauthorized access by requiring authentication, authorization, and accounting for network resources.
- **Network Monitoring:** Network monitoring involves collecting and analyzing network activity and performance data. This strategy enables the detection and prevention of network anomalies and incidents by providing visibility into network traffic, devices, and configurations. It also supports network optimization by identifying and resolving network issues, bottlenecks, or inefficiencies.

Conclusion

Data security is a top concern for organizations in today's digital landscape. It protects data from unauthorized access, use, modification, or disclosure. Data security requires implementing technical, administrative, and physical measures to safeguard data from internal and external threats. Network topology and network mapping can strengthen data security strategy. They provide a comprehensive view of the organization's digital infrastructure. Network topology and mapping also can be aligned with various legal frameworks and standards that regulate data security and privacy. Organizations can develop and implement tailored security strategies that address specific vulnerabilities and risks, leveraging the information gained through network topology and mapping, guiding data security practices and meeting compliance requirements.

National Law Review, Volumess XIII, Number 339

Source URL:https://natlawreview.com/article/network-topology-and-network-mapping-nist-cybersecurity-framework-part-2