

NP-View

Cyber Hygiene, What a Culture of Compliance Looks Like & Why It Is Important



+1 (872) 245-4100

info@network-perception.com

<https://network-perception.com>

1. Introduction:

1.1 What is cyber hygiene

Cyber hygiene is the set of practices and proactive measures that organizations adopt to ensure a robust, healthy, and secure digital environment. Drawing parallels from personal hygiene, where consistent habits and routines protect against diseases and ensure wellness, cyber hygiene is designed to shield our critical infrastructure from cyber threats, to safeguard our mission-critical assets, and to foster cyber resilience.

Understanding the 'cleanliness' aspect of cyber hygiene is essential. In the physical world, cleanliness reduces the risk of diseases. In the digital realm, 'clean' systems are those free from malware, running only necessary and updated software, and configured securely with defense in depth and segmentation. A clean system is significantly less vulnerable to threats and attacks.

At its core, cyber hygiene is about being proactive rather than reactive and that it is more effective and less costly to prevent issues than to deal with the aftermath of a cyber incident. Proactive measures, like regular security assessments and penetration testing, ensure that potential vulnerabilities are identified and addressed before they can be exploited.

1.2 Why is it important

Operational Technology (OT) environments, which involve the hardware and software dedicated to detecting or causing changes in physical processes, play an unparalleled role in the functioning of modern societies. From electricity grids and water treatment facilities to traffic management systems and manufacturing plants, the smooth operation of these sectors is foundational to everyday life. As a result, ensuring their cybersecurity through robust cyber hygiene practices is not just advisable—it's imperative.

As OT environments modernize, there's an increasing trend towards integrating IT (Information Technology) and OT systems. This means that traditionally isolated systems are now connected to wider networks, opening up a host of vulnerabilities that were previously non-existent. Cyber hygiene ensures these interconnected systems are shielded from emerging threats.

The implications of a cyberattack on critical infrastructure are far-reaching. A compromise can lead to physical harm (e.g., a malfunctioning power plant), loss of essential services (e.g., disrupted water supply), and significant economic consequences. Given the stakes, maintaining impeccable cyber hygiene is paramount.

In essence, cyber hygiene is to OT and critical infrastructure what regular maintenance is to

machinery; it ensures smooth operation, longevity, and safety. In an age where the digital and physical worlds are increasingly intertwined, the necessity of robust cyber hygiene practices for critical infrastructure and OT environments can't be emphasized enough. It's not just about preventing data breaches—it's about safeguarding the very fabric of modern society.

Why is it challenging

From many aspects, OT cybersecurity presents a nearly insurmountable obstacle. OT devices often have remained unchanged for long periods of time, perhaps even decades. Due to their age, the technology of many such devices may lack or not support security controls that the industry considers “standard” today. The OT infrastructure will therefore often be wrapped in additional layers of third-party applications and hardware, each with its own unique administrative toolsets and control mechanisms.

Into this multiplicity of control points, an organization must apply limited resources. The number of qualified persons will always have limitations, but in the case of OT cybersecurity, the constraints seem even heavier. Finding a qualified resource means knowledge or expertise in not only OT and cybersecurity but also compliance frameworks. To this, an entity must then also sufficiently train the individuals on each of the additional external cybersecurity control systems (the aforementioned “wrappers”).

A second limitation comes from a lack of a well-defined cybersecurity and compliance Program. The Program defines by role the vital “who” in the who, what, when, why, and how liturgy. Any Program must function as a hierarchical body of Policies, Processes, Procedures, and Practices. At each level of this 5-P structure, an owner must be defined. The owner accepts the responsibility to manage the assets designated. The owner may assign custodians of assets to do the work, but only from their own organization, as responsibility cannot be assigned without authority. This fact alone causes many programs to stumble and shows a particularly stark relief at audit.

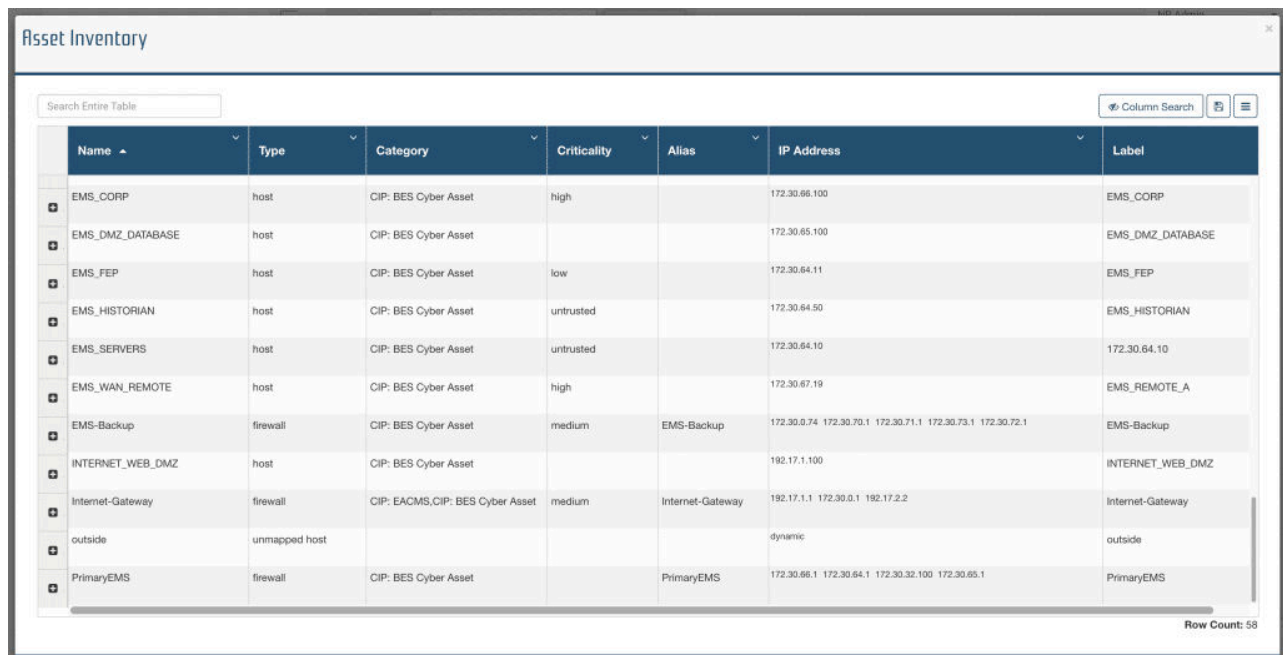
The Program structure provides the foundation for a true culture of compliance in the organization, but cannot serve alone. Leadership, from the highest level, must reinforce not only the presence of the Program but also the details. Usually, a senior leader parroting the sentiment of “follow the program” falls flat without some significant personal investment in the working elements of the constituent Policies and Processes. There must exist a uniform culture of compliance that is deeply felt throughout, from executives to the front line personnel. Any variation will be detectable and misinterpreted to mean OT cybersecurity ranks as less important than other obligations. The safety culture serves as a model for good compliance and cybersecurity reinforcement.

2. Building Blocks (Basics of cybersecurity):

Asset inventory

Asset inventory refers to a comprehensive cataloging of all hardware components, software applications, networking equipment, endpoints, controllers, and any other digital and physical components that form a part of the OT system. It's essentially a map that lists all assets, their configurations, interconnections, and attributes.

For organizations to effectively defend their systems, they first need to know what those systems are. An asset inventory provides a clear view of the entire OT infrastructure, ensuring there are no 'blind spots' that might be left unprotected.

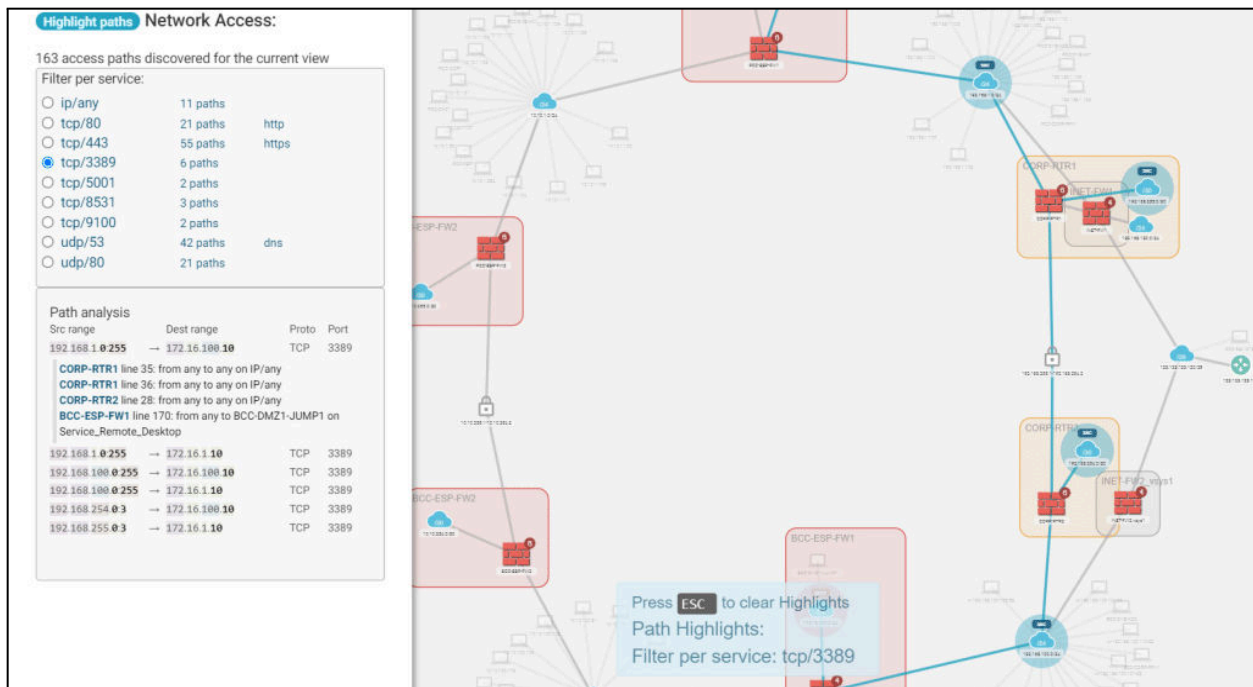


Name	Type	Category	Criticality	Alias	IP Address	Label
EMS_CORP	host	CIP: BES Cyber Asset	high		172.30.66.100	EMS_CORP
EMS_DMZ_DATABASE	host	CIP: BES Cyber Asset			172.30.65.100	EMS_DMZ_DATABASE
EMS_FEP	host	CIP: BES Cyber Asset	low		172.30.64.11	EMS_FEP
EMS_HISTORIAN	host	CIP: BES Cyber Asset	untrusted		172.30.64.50	EMS_HISTORIAN
EMS_SERVERS	host	CIP: BES Cyber Asset	untrusted		172.30.64.10	172.30.64.10
EMS_WAN_REMOTE	host	CIP: BES Cyber Asset	high		172.30.67.19	EMS_REMOTE_A
EMS-Backup	firewall	CIP: BES Cyber Asset	medium	EMS-Backup	172.30.0.74 172.30.70.1 172.30.71.1 172.30.73.1 172.30.72.1	EMS-Backup
INTERNET_WEB_DMZ	host	CIP: BES Cyber Asset			192.17.1.100	INTERNET_WEB_DMZ
Internet-Gateway	firewall	CIP: EACMS,CIP: BES Cyber Asset	medium	Internet-Gateway	192.17.1.1 172.30.0.1 192.17.2.2	Internet-Gateway
outside	unmapped host				dynamic	outside
PrimaryEMS	firewall	CIP: BES Cyber Asset		PrimaryEMS	172.30.66.1 172.30.64.1 172.30.32.100 172.30.65.1	PrimaryEMS

Asset inventory is a foundational pillar of cyber hygiene in OT environments. It is the starting point from which effective cybersecurity strategies are crafted. In a domain where the stakes are high – where OT systems might control critical utilities, manufacturing processes, or essential services – the significance of a comprehensive, up-to-date asset inventory cannot be overstated. It's not just a list; it's a strategic tool for defense in the ever-challenging world of cybersecurity.

Network mapping

A network topology diagram is a visual representation of the layout of a network, showcasing how different network devices (like switches, routers, firewalls, servers, and endpoints) are connected. It displays the structural layout, providing insights into the logical interconnections among the various devices and systems.



Before any robust cybersecurity measures can be put in place, there's a need to understand the architecture of the network. A topology diagram provides a clear, bird's-eye view, helping cybersecurity professionals and OT engineers visualize the complete network and its intricacies. The diagram offers a universally understandable representation of the network, facilitating communication between different departments—whether it's IT, OT, cybersecurity, or management. For security reasons, OT networks need segmentation to isolate critical systems from non-critical ones. A network topology diagram aids in devising effective segmentation strategies, ensuring that sensitive systems have added layers of protection.

A network topology diagram in an OT environment acts as both a map and a blueprint. It's a map because it provides a comprehensive overview of the 'terrain' – the layout of the network. It's a blueprint because it's essential for planning, strategizing, and building out cybersecurity defenses. In the realm of OT, where ensuring the seamless operation of systems can be a matter of public safety and where downtime can have significant repercussions, the role of a network topology diagram in maintaining cyber hygiene is paramount.

Data flow diagram

A Data Flow Diagram (DFD) is a graphical representation that depicts the flow of data within a network. At its core, a DFD provides a clear visualization of how data traverses within an OT system. This visibility is foundational, ensuring that there are no hidden or undocumented paths that data can take, which might introduce vulnerabilities. Knowing where data flows and is

processed allows cybersecurity professionals to place defenses—like firewalls, intrusion detection systems, or encryption mechanisms—at strategic points, ensuring maximum protection.

Highlight paths Network Access:

55 access paths discovered for the current view

Filter per service:

<input type="radio"/> ip/any	8 paths	
<input type="radio"/> tcp/22	6 paths	ssh
<input type="radio"/> tcp/443	17 paths	https
<input type="radio"/> tcp/445	2 paths	
<input checked="" type="radio"/> tcp/3389	11 paths	
<input type="radio"/> tcp/5001	2 paths	
<input type="radio"/> tcp/8531	3 paths	
<input type="radio"/> tcp/9100	2 paths	
<input type="radio"/> udp/53	2 paths	dns
<input type="radio"/> udp/80	2 paths	

In OT environments, where systems often control tangible processes or machinery and where a minor data discrepancy can lead to significant real-world consequences, understanding the flow of data is crucial. A Data Flow Diagram serves as both an illuminating guide and a strategic tool. It's not just about knowing the journey of data; it's about ensuring that this journey is safe, efficient, and secure. In the broader context of cyber hygiene, a DFD ensures that organizations are not just defending their perimeter but are also safeguarding the very lifeblood of their OT systems—the data itself.

3. Step-by-step Guidelines and Best Practices:

	Asset Inventory	Network mapping Data flow diagram
What	Comprehensive cataloging of all hardware components, software applications, networking equipment, endpoints, controllers, and any other components that form a part of the OT system.	<ul style="list-style-type: none"> • A network topology diagram. • A clear visualization of how data provides insights into the logical traversal within an OT system through interconnections among the various network devices and systems.
Why	<ul style="list-style-type: none"> • It is the starting point from which the attack surface can be understood and an effective cybersecurity strategy can be crafted. • It is the blueprint that is essential for communication among diverse groups of stakeholders to plan, strategize, and build our cybersecurity defenses. • It completes the attack surface understanding and it ensures that there are no hidden or undocumented paths that data can take, which might introduce vulnerabilities. Knowing where data flows and is processed allows cybersecurity professionals to place defenses – like firewalls, intrusion detection systems, or encryption mechanisms– at strategic points, ensuring maximum protection. 	
Who	Asset Managers Networking / Compliance Networking / Cybersecurity	
Phase 1: For organizations getting started on their Cyber Hygiene Program (crawl)		
When	Yearly	
Where	High and medium impact OT facilities	
How	<p>Excel spreadsheet with: Visio diagram or a one-line in an EMS display</p> <p>Manually develop a network segmentation matrix in Excel to have an inventory of application and services</p> <p>Needed in the OT environment:</p> <ul style="list-style-type: none"> • Name • IP address • MAC address or Serial # • Location / System • Firmware / OS • Owner / custodian 	

Phase 2: For organizations maturing their Cyber Hygiene Program (walk)		
When	Quarterly	
Where	High, medium, and low impact OT facilities	
How	Software-based verification using a manual tool such as an OT-sensitive network scanner.	Network modeling based on configuration files from network devices that are manually imported.
Phase 3: For organizations optimizing their Cyber Hygiene Program (run)		
When	Continuously	
Where	OT and IT environments	
How	Software-based generation and maintenance using an automated tool such as an OT-sensitive network probe and/or asset agents.	Network modeling enriched via asset inventory/network scanner integration and automatically refreshed via connectors. Network monitoring for live traffic visualization and automated integration with network modeling

4. Audit readiness:

A well-run cybersecurity and compliance program creates perpetual audit readiness. The program, signed by the most senior manager applicable, provides the authority. Each policy defines the goal, such as high-level password requirements, patch management, or network security. The processes create basic (without swimlanes) workflows of the work required to meet each policy. The process occupies a pivotal role, as it defines all decision branches that require compliance artifacts. The traditional diamond shape in a flowchart represents this. Each decision requires some form of documentation, which includes the date, details, and designee (i.e., the individual making the decision).

The NERC CIP Report provides specific information about your network that can be used to check compliance with NERC CIP requirements. The North American Corporation Critical Infrastructure Protection is a set of cybersecurity requirements designed to secure the assets required for operating the bulk power systems. About NERC CIP standards by visiting the [NERC Website](#).

The generated report covers the following NERC CIP requirements:

- **CIP-005 R1.1:** All applicable Cyber Assets that are connected to a network via a routable protocol, shall reside within a defined ESP.
- **CIP-005 R1.2:** All External Routable Connectivity must be through an identified Electronic Access Point (EAP).
- **CIP-005 R1.3:** Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
- **CIP-005 R2.1:** Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

A useful report requires proper categorization and segmentation of topology nodes. This categorization can be done through the topology map, or by running the Wizard. The following categories have to be set for the following nodes:

1. Categorize all EACMS's (firewalls and routers)
2. Categorize all EAP's (interfaces)
3. Categorize all BES Cyber Assets (end point nodes)

The Wizard will then guide you through:

4. Reviewing the Access Rules Table, and justifying access permissions for rules bound to your EAPs.
5. Reviewing the Connectivity Paths Table, and annotating paths as needed for inbound and outbound connectivity to and from the ESP.

NERC CIP Wizard

These artifacts are defined at the process level because each business unit or group within the organization will achieve them by different means. The procedure for changing a password will appear vastly different, for instance, on a firewall versus a Windows server. Despite that fact, a good process that engenders multiple procedures serves a forcing function to document consistently, even across disparate systems.

All of this goes to a perpetual state of audit readiness.

If an entity follows their program with due rigor, the procedures will naturally create all the documentation required. Accessing and indexing the artifacts remains the only challenge. Building the documentation repository and training personnel in the correct storage methodology closes that loop.

Finally, an internal or independent audit program proves the audit readiness of the organization. Without a consistent “friendly” audit schedule, an entity will fly blindly into the audit by their regulators, tantamount to a student who fails to study for the final exam. Organizations often have a group of qualified cybersecurity audit professionals in other business areas, such as in SOX or HIPAA compliance. A cybersecurity program may tap into these standing teams and gain fast insights into their real-world cybersecurity results. Without internal audit availability, an entity may engage outside consulting to provide mock audits and review.

5. Conclusion and next steps:

Effective cyber hygiene is more than just a set of tasks; it's a culture. A culture where security isn't an afterthought but is integrated into every action, decision, and strategy. This white paper underscores the need for consistent cyber hygiene practices, the role of every stakeholder, and the importance of preparation, not just for potential threats, but also for regulatory audits. This starts with documenting the environment to protect through three foundational pillars: asset inventory, network map, and data flow diagram. As threats evolve, so should our defenses. To this end, organizations must commit to continuous learning, periodic reviews, and a proactive approach to cybersecurity.



 +1 (872) 245-4100

 info@network-perception.com

 <https://network-perception.com>