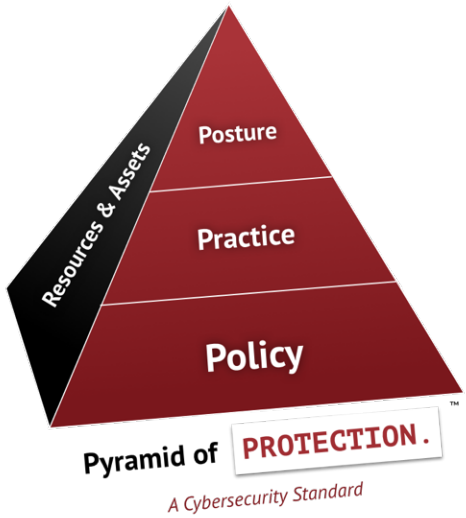
Pyramid of Protection

SHINE Systems
One Mission. One Team.

Cyber disruptions are increasing in such frequency and severity that it's no longer a matter of "if" but "when" an organization will need to respond. Adverse cyber events that lead to disruption in confidentiality, integrity, or availability may stem from malicious attacks, accidents, or natural occurrences. Cyber resilient organizations can continuously operate in the face of cyber disruptions through proactive prevention and detection, streamlined response, and rapid recovery.



Cyber resilience unifies the areas of cybersecurity, business continuity, and organizational resilience. Presidential Policy Directive PPD-21 defines resilience as the "ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions".

SHINE System's Pyramid of Protection™ helps organizations ensure cyber resilience through policy, practice, and posture across all resources and assets.

Cybersecurity policy provides a solid foundation beginning with a leadership-endorsed culture of security. To build a strong cybersecurity management program based on policy, an organization must gain a holistic understanding of an their assets, data, and risk. Asset and data classification and risk assessment guide cybersecurity policy development, while cybersecurity teams help ensure organization-wide cybersecurity awareness and continual improvement.

Cybersecurity practice aligns a solid foundation of policy with the technologies, processes, and people to implement protection and detection measures for networks, systems, and data. Cybersecurity teams build threat landscape knowledge, aggregate and share information, and collaborate with internal and external stakeholders.

Cybersecurity posture is the overall strength of an organization's defenses based on the policies, practices, and resources to protect and respond to threats. Cybersecurity posture may be assessed through defensive and offensive techniques. Defensive techniques continuously monitor networks and systems to detect and respond to events and to enforce policy adherence. Highly skilled cybersecurity experts use offensive testing techniques such as threat hunting, simulations, and vulnerability discovery to identify and remediate hidden threats. Cyber resilience is measured and assessed based on the strength of an organization's security posture.

Policy	Practice	Posture
Ensure leadership support Develop a culture of security Develop cybersecurity management program Identify and classify critical data Identify and assess risk Develop security policies Create IRP/BCP/DRP Develop cybersecurity teams Develop a cybersecurity awareness program Implement continual process improvement	Protect networks, systems, and data from cyberattacks, failures, and accidents Implement continual asset and network discovery and mapping Deploy cybersecurity technologies, processes, and people to protect systems, networks, and data Build threat landscape awareness Implement threat management program Share information and collaborate with internal and external stakeholders	Continuously monitor networks and systems Monitor and enforce policy adherence Respond to events and incidents Test IRP/BCP/DRP Perform risk assessments and simulations Identify and remediate vulnerabilities Perform threat hunting Measure and track cyber resilience

The Pyramid of Protection aligns with the NIST Cybersecurity Framework (CSF) and addresses all aspects of people, processes, and technology. The CSF has been adopted by industry, academia, and government at all levels, including internationally. It provides a common language and systematic methodology for managing cybersecurity risk and ensuring cyber resilience. The CSF Core consists of five concurrent and continuous Functions – Identify, Protect, Detect, Respond, and Recover. The Functions help organizations organize information, make decisions, address threats, and improve processes. The Pyramid of Protection integrates these functions to provide a strategic approach and operational culture of cyber resilience.

Pyramid of Protection	NIST CSF Function Area	Description
Policy	Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Practice	Protect	Develop and implement the appropriate safeguards to ensure delivery of critical services.
Posture	Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
	Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
	Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

SHINE System's Pyramid of Protection provides a framework and assessment methodology to help organizations:

- Reduce financial impact of cyber disruptions
- Meet regulatory requirements
- Improve internal processes
- Protect brand and reputation
- Strengthen customer trust

Cyber resilience goes beyond traditional checklist approaches to ensure proactive measures and dynamic testing based on current threat conditions. SHINE System's Pyramid of Protection aligns cybersecurity and business processes with people, processes, and technology to prepare for and respond to inevitable cyber disruptions.