Cybersecurity Risk Assessment - SolaraVive Helios Platform

SolaraVive is a renewable energy company headquartered in Washington, DC, operating solar and wind energy projects across the United States.

The company relies on the Helios platform, a cloud-based system used to monitor energy production, system health, and operational performance across its energy assets.

Helios aggregates real-time and historical data and is considered a critical system for operational decision-making and regulatory reporting.

Crown Jewel (Key Asset): Helios Operations Platform

Why it is critical:

- Contains operational energy data
- Used for decision-making
- Required for compliance and reporting
- High-risk classification

Key Assets:

Asset	Description
Helios platform	Main monitoring system for energy production
Operational databases	Store energy output and system data
Employee accounts	Access to dashboards and systems
Cloud infrastructure (AWS)	Hosts all systems and data

Threats

Threat Actor	Example Attack	Impact
Cybercriminals	Phishing, ransomware	Data loss, downtime
Nation-state actors	Infrastructure attacks	Energy disruption
Insiders	Misuse of access	Data leaks
Hacktivists	Data exposure	Reputation damage

Risk Table (Core GRC Element)

Asset	Threat	Risk	Control
Helios dashboard	Stolen credentials	Unauthorized access to energy data	MFA + role-based access
Cloud database	Ransomware	Data loss and downtime	Backups + endpoint protection
API connections	Vendor breach	Data exposure through third party	Vendor security review
Employee accounts	Phishing	Account takeover	Security awareness training

Connecting Domains to the Tech Stack

To ensure effective risk management, security domains must be mapped to the organization's technology stack. This approach helps identify where specific risks exist and what controls should be implemented at each technical layer.

Security Domain	Tech Stack Layer	Risk	Security Control
Insider Threat	User Interface (dashboards)	Unauthorized employee access	Role-based access control
Insider Threat	Database	Data misuse or deletion	Restricted database permissions
Third-Party Risk	APIs	Vendor compromise	API authentication and access limits
Third-Party Risk	Cloud infrastructure (AWS)	Weak vendor security	Vendor security review and compliance checks
Threat Intelligence	User logins	Suspicious login activity	Alerting on abnormal login attempts
Threat Intelligence	Operating system	Malicious processes	System activity monitoring
Privacy	Database	Exposure of sensitive operational data	Data encryption at rest
Privacy	Network connections	Data interception	Encrypted connections (HTTPS/TLS)

Domain to Tech Stack

Insider Threat

Layer	**What it Means**	**Security Control**
User Interface	Who can log into dashboards	Role-based logins using IAM
Middleware (APIs)	Who can send or receive data requests	API access control
Database	Who can read or change data	Restricted database permissions
Operating System	Who can manage servers?	Limited admin accounts
Hardware/Network	Where users connect from	Monitor unusual access locations

Third Party & Supply Chain Security

Layer	**What it Means**	**Security Control**
User Interface	Who can log into dashboards	Vendor login restrictions
Middleware (APIs)	Connections to outside systems	API access control
Database	Vendors accessing stored data	Restricted database permissions
Operating System	Who can manage servers?	Limited admin accounts
Hardware/Network	AWS cloud infrastructure	Review cloud provider security

Threat Intelligence

Layer	**What it Means**	**Security Control**
User Interface	Monitor logins	Alert for suspicious login activity
Middleware (APIs)	Monitor data requests	Alert on abnormal API usage

Database	Monitor data access patterns	Detect unusual access
Operating System	Monitor server activity	Detect abnormal activity
Hardware/Network	Monitor cloud network traffic	Detect unusual connections

Privacy

Layer	**What it Means**	**Security Control**
User Interface	Who can see sensitive reports?	Access limits for confidential data
Middleware (APIs)	How data moves between systems	Encrypted data
Database	Where data is stored	Encrypted data
Operating System	How data is stored on servers	Secure permissions
Hardware/Network	Where users connect from	Monitor unusual access locations

Conclusion:

Mapping security domains to the technology stack allows SolaraVive to implement targeted controls where risks actually exist. This structured approach supports stronger access control, improved monitoring, and better protection of the Helios platform, which represents the organization’s primary operational asset.