SDI Director of Information Security - Interview Study Guide (Role-Tailored Q&A, One Page)

Role Context At SDI

- Q: Where does the Director of Information Security sit in SDI's org and governance? A: The Director of Information Security leads the InfoSec team and program; the CFO oversees cybersecurity safeguards and risk management, and the Board/Audit Committee receive regular cyber updates.[1]

- Q: What is the security program aligned to? A: SDI states its program aligns to NIST and is integrated into enterprise risk management.[1]

What Success Looks Like (First 6-12 Months)

- Q: What are your top three outcomes in year one? A: 1) Reduce OT downtime risk with segmentation, secure remote access, and recovery playbooks. 2) Establish board-ready risk metrics tied to uptime and financial impact. 3) Harden third-party and identity controls across critical operations.

- Q: How do you balance security with production? A: Use risk-based prioritization, align changes to maintenance windows, and favor controls that improve visibility and containment without disrupting operations.

OT/IT Security Focus

- Q: How would you start an OT security program at SDI? A: Build an OT asset and criticality map, segment high-risk zones, and implement secure remote access for vendors while protecting line uptime.

- Q: What OT risks are most material in a steel manufacturer? A: Unplanned downtime, safety impacts, and loss of production control from ransomware or lateral movement into OT networks.[1]

- Q: How do you handle patching in OT environments? A: Apply compensating controls (segmentation, allowlisting, monitoring) and align patching to planned outages with plant leadership approval.

Incident Response (Plant Disruption Scenario)

- Q: Malware impacts a flat roll line network segment. What do you do first? A: Contain the segment, preserve safety and control integrity, communicate with plant leaders, and initiate IR while keeping production stable if safe.

- Q: How do you decide materiality and escalation? A: Assess potential production loss, safety impact, and financial exposure; escalate to CFO and Audit Committee if thresholds are met.

Governance And Metrics

- Q: What KPIs would you report quarterly to the Audit Committee? A: OT asset visibility %, segmentation coverage, MFA/privileged access coverage, critical vendor risk ratings, and IR readiness (tabletop

frequency, RTO/MTTR).

- Q: How would you present cyber risk in business terms? A: Translate into downtime hours avoided, safety risk reduction, and revenue protection.

Third-Party Risk

- Q: How would you manage OT vendor access? A: Tier vendors by production impact, require MFA and just-in-time access, log and monitor sessions, and enforce incident notification SLAs.

- Q: How do you avoid slowing the business with vendor controls? A: Focus on Tier 1 suppliers first, implement lightweight controls for low-risk vendors, and automate access reviews.

Financial And Business Literacy

- Q: What were SDI's FY2024 results? A: Net sales $17.54B, operating income $1.94B, net income $1.54B.[1]

- Q: What is the biggest revenue driver? A: Steel operations, which represented 69% of 2024 net sales.[1]

- Q: What operational scale do you need to protect? A: Large EAF-based steel operations, metals recycling, and steel fabrication plants with national footprint.[1]

Culture And People

- Q: How would you fit SDI's team-based culture? A: Build shared accountability with operations, align security KPIs to team performance, and emphasize training and practical workflows.

- Q: What would you do to improve security awareness? A: Continue monthly training, add OT-specific drills, and track participation and phishing results by site.[1]

Leadership And Change Management

- Q: How do you lead security across multiple plants? A: Use a hub-and-spoke model with site champions, standardize core controls, and tailor execution to each plant's constraints.

- Q: How do you handle resistance to security changes? A: Tie changes to safety and uptime, pilot in one site, and scale based on measured results.

Compensation Benchmark (For Discussion)

- Q: What is a public benchmark for a Director of Information Security? A: Salary.com lists a US median base of about $208,843, with a typical range of about $176,295 to $230,116 (national benchmark).[2]

Questions You Can Ask Them

- Q: Which plants or lines have the highest unplanned downtime risk today?
- Q: What is the current cadence and format for cyber reporting to the Audit Committee?
- Q: How do you balance plant uptime with security change windows?
- Q: Which vendors are most critical to OT operations and remote support?

Sources

1. SDI FY2024 Form 10-K (SEC): https://www.sec.gov/Archives/edgar/data/1022671/000155837025001886/stld-20241231x10k.htm
2. Salary.com benchmark: https://www.salary.com/research/salary/benchmark/information-security-director-salary