DERISK CRQ · LEVEL 3 · BOARD-GRADE · CISO

Security Posture and Remediation Priorities — October 2026

Generated by DeRISK CRQ on the DeRISK™ Intelligence Platform.

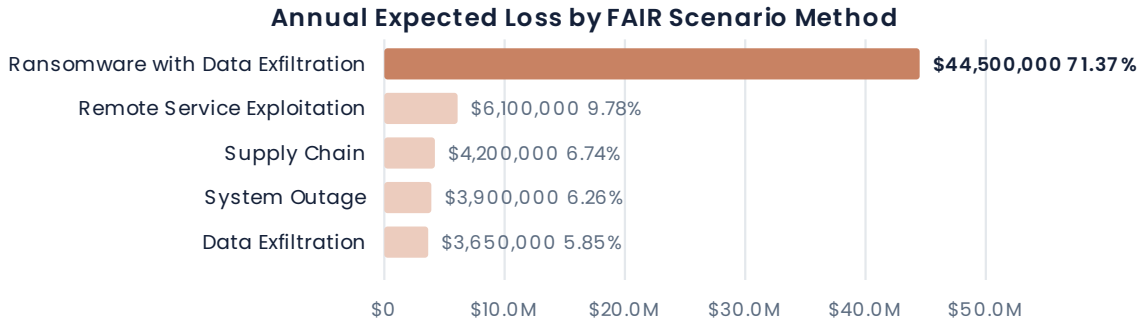
Entity: Aldermere Energy **Scope:** Company **Level:** 3 · Board-Grade **Inputs provided:** Oct 20, 2026
Report generated: Oct 27, 2026 **Cadence:** Monthly

Where the risk comes in, which controls trail peers, and which projects buy the most risk reduction per dollar.

1 · RISK POSITION SUMMARY

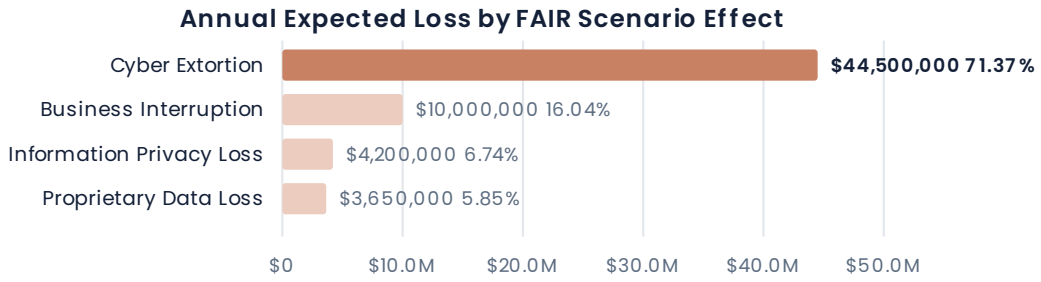
SCOPE	AEL	VAR 95TH	VAR 99TH
Company	$62,350,000	$172,000,000	$246,000,000

2 · ATTACK SURFACE PRIORITIES



The largest FAIR scenario Method exposure is **Ransomware with Data Exfiltration** at $44,500,000 — 71.37% of company Annual Expected Loss.

3 · WHERE THE LOSS LANDS



The largest FAIR scenario Effects are **Cyber Extortion** and **Business Interruption** — together 87.4% of company Annual Expected Loss.

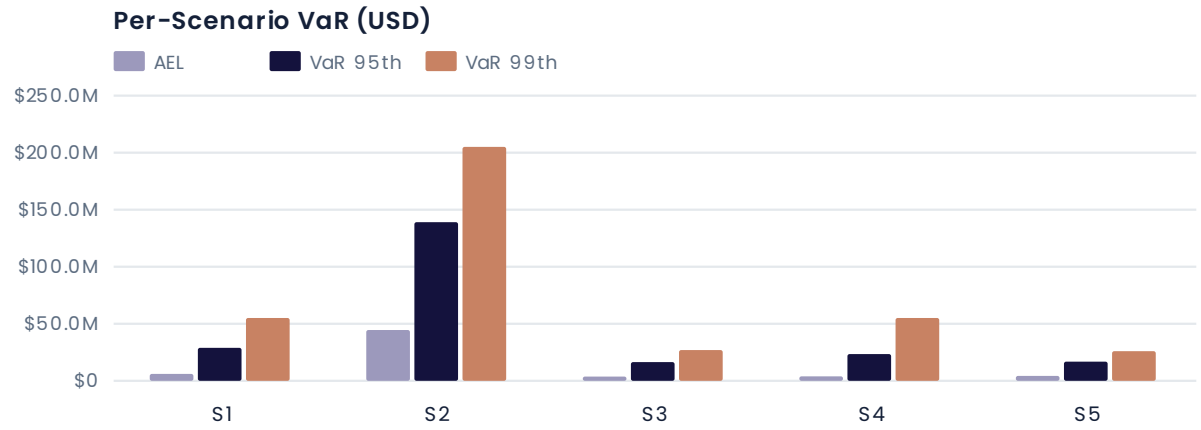
© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

4 · FAIR SCENARIO ANALYSIS

4.1 FAIR Scenario Register

ID	THREAT	ASSET	METHOD	EFFECT	RELEVANCE
S1	**Nation-State**	Business Process Impacting Third-Party Revenue	Remote Service Exploitation	Business Interruption	Nation-states target critical energy infrastructure to disrupt grid operations and impact dependent third parties. Remote exploitation of SCADA/ICS systems across the company's 70 facilities can cause cascading outages affecting regional power supply and dependent customers.
S2	**Cyber Criminals**	Business Process Generating Revenue	Ransomware with Data Exfiltration	Cyber Extortion	Ransomware operators target energy companies for dual-extortion: encrypting operational data to halt generation/distribution processes while threatening to release sensitive operational or customer data. This forces urgent payment decisions for a distributed operator managing 70 facilities.
S3	**Privileged Insider**	IP & Trade Secrets Data	Data Exfiltration	Proprietary Data Loss	Employees with access to energy generation systems, efficiency algorithms, or infrastructure designs may exfiltrate proprietary data to competitors or nation-states. A distributed operation increases insider risk surface across multiple facility locations and contractor access points.
S4	**Cyber Terrorists**	Physical Assets & Facilities	System Outage	Business Interruption	Terrorist actors may target renewable energy facilities (solar, wind) across multiple US locations via ICS/SCADA compromise to cause widespread grid instability. Command and control of distributed generation systems can create cascading power disruptions with public safety implications.
S5	**Competitor Driven Threat Actors**	Confidential Business Information	Supply Chain	Information Privacy Loss	Competitors may compromise third-party vendors, maintenance providers, or software suppliers serving the company's 70 facilities to gain access to operational details, contract terms, or infrastructure intelligence that provides competitive advantage in energy markets.

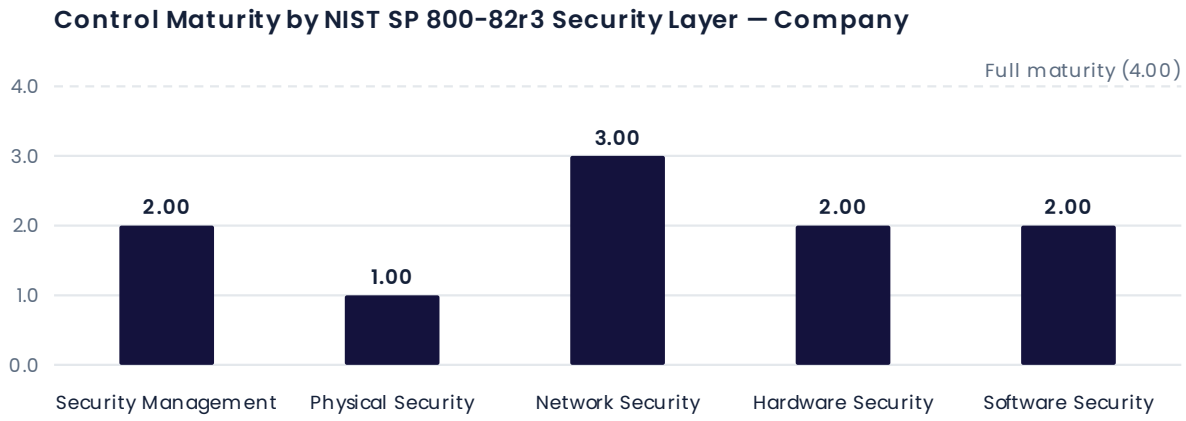
4.2 Per-Scenario VaR and Contribution



© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

SCENARIO	AEL	VAR 95TH	VAR 95TH CONTRIBUTION	VAR 99TH	VAR 99TH CONTRIBUTION
S1	$6,100,000	$28,900,000	12.87%	$55,000,000	14.95%
S2	$44,500,000	$139,000,000	61.92%	$205,000,000	55.71%
S3	$3,650,000	$16,400,000	7.30%	$27,000,000	7.34%
S4	$3,900,000	$23,500,000	10.47%	$55,000,000	14.94%
S5	$4,200,000	$16,700,000	7.44%	$26,000,000	7.06%

5 · CONTROL GAPS VS. PEERS



Overall control maturity is **2.00 of 4.00 (Developing)**. Aldermere Energy demonstrates solid network segmentation and remote-access controls (DMZ, VPN, MFA, jump host) and a strong asset inventory, but overall maturity is Developing because key gaps remain in OT-specific policy and physical security, credential and privileged-access hygiene, software integrity validation, and hardware risks such as unseparated safety systems and ~35% end-of-life equipment. Strengthening these areas, along with verifying controls across all 70 facilities, would raise the organization toward a Defined and Operational level. Comparable industry peer data are not available.

6 · METHODOLOGY AND TRANSPARENCY

6.1 Data Sufficiency and Confidence

ASPECT	ASSESSMENT
Data sufficiency	Partial. Strong financial anchors were provided (hourly downtime revenue loss, restart cost, incident-response rate, equipment replacement value) along with a detailed OT control questionnaire that informs vulnerability. However, no historical event frequencies, no scenario-specific loss history, and several low-confidence financial answers require that threat frequency and loss magnitude parameters be derived through structured assumptions.
Confidence level	Moderate. Results are directionally reliable for decision support and are grounded in company-supplied financial figures and control posture, but frequency parameters and secondary-loss ranges are assumption-driven and several key financial inputs were self-rated low confidence, so absolute VaR magnitudes carry material uncertainty.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

6.2 Threat Event Frequency (TEF)

SCENARIO	DISTRIBUTION	MINIMUM	MODE	MAXIMUM	UNIT	JUSTIFICATION
S1	PERT	0.05	0.15	0.4	events/year	Nation-state targeting of US energy ICS is credible but infrequent; questionnaire indicates remote access exists with MFA/DMZ controls, lowering but not eliminating attempt frequency.
S2	PERT	0.3	0.8	2.0	events/year	Ransomware is the most prevalent threat to energy operators; IT policy applied to OT, EoL assets (35%), and shared/default-credential weaknesses raise attempt frequency across 70 facilities.
S3	PERT	0.1	0.3	0.8	events/year	Insider exfiltration attempts are moderate; 10 shared-account holders and over-one-year privilege audits increase exposure across distributed sites.
S4	PERT	0.03	0.1	0.3	events/year	Cyber-terrorist physical-impact campaigns are rare; segmentation and BPCS/safety separation gaps modestly raise feasibility.
S5	PERT	0.2	0.5	1.2	events/year	Supply-chain and vendor-mediated information compromise is common; unknown third-party dependencies and no transient-device authorization increase attempt frequency.

6.3 Vulnerability

SCENARIO	DISTRIBUTION	MINIMUM	MODE	MAXIMUM	JUSTIFICATION
S1	PERT	0.2	0.4	0.65	Partial remote-access hardening (MFA, DMZ, jump host) reduces susceptibility, offset by EoL assets, IT/OT trust relationship, and no redundancy for critical assets.
S2	PERT	0.3	0.55	0.8	High susceptibility due to default passwords not changed, no admin/day-to-day credential separation, 35% EoL assets, and IT security policy applied to OT; EDR presence partially offsets.
S3	PERT	0.15	0.35	0.6	Shared accounts and infrequent privilege audits raise insider success likelihood; centralized password management and documented roles partially reduce it.
S4	PERT	0.15	0.35	0.6	Logical area separation and fallback processes reduce success, but unsegmented BPCS/safety systems and no redundancy enable physical-impact outcomes.
S5	PERT	0.25	0.45	0.7	Unknown third-party dependencies, no transient-device authorization, and no digital-integrity validation of software raise supply-chain susceptibility.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

6.4 Loss Event Frequency (LEF)

SCENARIO	MEAN	RANGE	UNIT
S1	0.062	0.01 to 0.26	events/year
S2	0.510	0.09 to 1.60	events/year
S3	0.123	0.015 to 0.48	events/year
S4	0.040	0.0045 to 0.18	events/year
S5	0.248	0.05 to 0.84	events/year

6.5 Primary Loss

SCENARIO	LOSS COMPONENT	MINIMUM	MODE	MAXIMUM	UNIT	JUSTIFICATION
S1	Operational downtime (lost revenue)	$52,237,440	$156,712,320	$626,849,280	USD	Downtime hours (PERT 4/12/48) multiplied by reported fleet-wide hourly revenue loss of $13,059,360.
S1	Facility restart and incident response	$575,000	$1,750,000	$5,750,000	USD	Restart cost $25,000 across affected facilities plus third-party response at $2,500/hour.
S2	Operational downtime (lost revenue)	$26,118,720	$104,474,880	$313,424,640	USD	Downtime hours (PERT 2/8/24) multiplied by reported hourly revenue loss.
S2	Extortion payment and recovery	$1,000,000	$5,000,000	$25,000,000	USD	Ransom demand plus restart and incident-response labor for a distributed 70-facility operator.
S3	Proprietary data / IP value loss	$500,000	$3,000,000	$20,000,000	USD	Estimated value of exfiltrated generation efficiency algorithms and infrastructure designs; no explicit IP valuation provided.
S4	Operational downtime (lost revenue)	$78,356,160	$235,068,480	$940,273,920	USD	Extended outage hours (PERT 6/18/72) multiplied by hourly revenue loss, reflecting cascading grid impact.
S4	Physical equipment damage	$5,000,000	$25,000,000	$150,000,000	USD	Turbine/equipment damage per questionnaire item 23; bounded well below the $16,230,000,000 total replacement value as a partial-fleet loss.
S5	Confidential business information loss	$200,000	$1,500,000	$8,000,000	USD	Competitive value of exposed contract terms and operational intelligence; no explicit valuation provided.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

6.6 Secondary Loss

SCENARIO	LOSS COMPONENT	MINIMUM	MODE	MAXIMUM	UNIT	JUSTIFICATION
S1	Regulatory, legal and reputation	$2,000,000	$8,000,000	$40,000,000	USD	Grid-disruption events trigger regulatory scrutiny (FERC/NERC), fines, and reputational harm to third-party revenue relationships.
S2	Regulatory, legal and reputation (data breach)	$3,000,000	$10,000,000	$50,000,000	USD	Dual-extortion data exposure drives notification costs, litigation, regulatory penalties, and reputational damage.
S3	Legal action and competitive erosion	$1,000,000	$4,000,000	$25,000,000	USD	Loss of competitive position and litigation costs following IP theft.
S4	Regulatory, safety liability and reputation	$3,000,000	$15,000,000	$80,000,000	USD	Public-safety implications and physical damage elevate regulatory, liability, and reputational secondary losses.
S5	Competitive disadvantage and contractual	$500,000	$2,500,000	$15,000,000	USD	Lost bids, eroded negotiating position, and contractual exposure in competitive energy markets.

6.7 Loss Magnitude

SCENARIO	MEAN PER EVENT	RANGE PER EVENT
S1	$98,000,000	$60,000,000 to $670,000,000
S2	$87,000,000	$35,000,000 to $390,000,000
S3	$7,500,000	$1,800,000 to $45,000,000
S4	$97,000,000	$90,000,000 to $1,170,000,000
S5	$4,100,000	$800,000 to $23,000,000

6.8 Assumptions Register

1. How often cyber attacks are likely to be attempted against the company's operational technology was not provided, so attack frequency had to be estimated from energy-sector experience and the company's reported security posture.
2. The financial impact of operational downtime relied on the company's own hourly loss figure, which the company rated as only moderately confident and which conflicted with other downtime figures it provided.
3. The value of proprietary technology, trade secrets, and confidential business information was not provided, so these losses had to be estimated.
4. The likely costs of regulatory penalties, legal action, and reputational damage following an incident were not provided and were estimated from comparable energy-sector events.
5. The effectiveness of the company's existing security controls was taken from a self-assessment questionnaire that was largely marked as low confidence, so control strength had to be interpreted.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

6.9 Limitations

- The results provide a reliable directional view of where the company's largest cyber losses would come from, but the specific dollar figures depend heavily on assumed information; providing verified downtime economics and historical incident records would significantly sharpen the estimates.
- Because the value of the company's intellectual property and confidential information was not available, the losses estimated for data-theft and competitor-driven scenarios are indicative only and would benefit from an internal valuation of these assets.
- The security-control information underlying the likelihood estimates was largely self-rated as low confidence by the company, so independent validation of the actual state of operational technology controls would increase trust in the likelihood of the modeled events.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.