DERISK CRQ · LEVEL 4 · EVIDENCE-GRADE · CFO

Cyber Risk Financial Exposure and Capital Allocation — Q4 2026

Generated by DeRISK CRQ on the DeRISK™ Intelligence Platform.

Entity: Aldermere Energy **Facility:** Example Facility 1 **Scope:** Facility **Level:** 4 · Evidence-Grade
Inputs provided: Oct 27, 2026 **Report generated:** Oct 27, 2026 **Cadence:** Quarterly + budget cycle

Expected and tail exposure in financial terms, and whether proposed CapEx clears the return hurdle.

1 · EXPOSURE STATEMENT

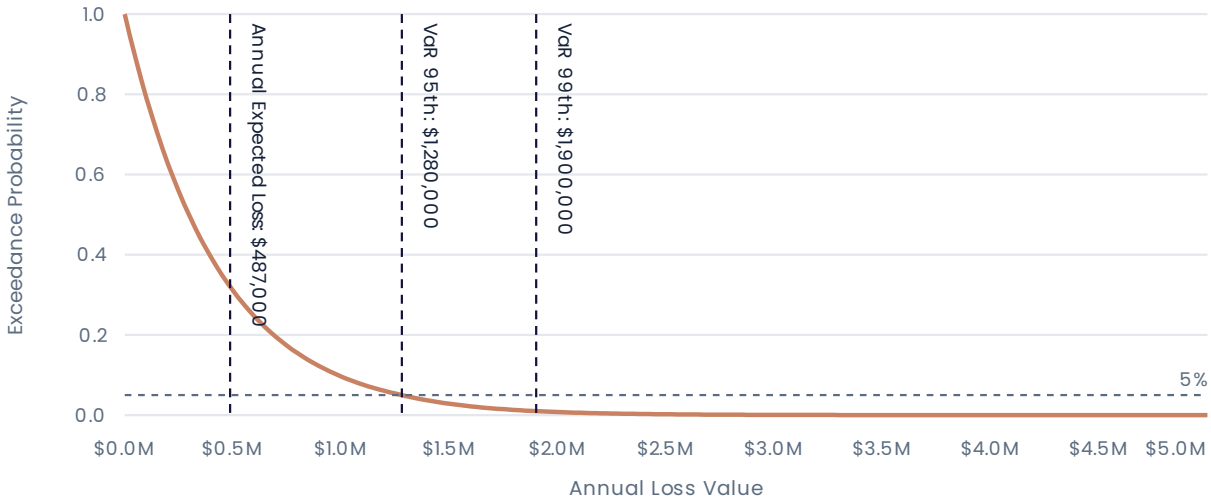
Anchored to facility revenue of **$15.42M**:

METRIC	LOSS	DAYS OF REVENUE
Annual Expected Loss	**$487,000**	**11.53**
Rare scenario — 1 in 20 years (VaR 95th)	$1,280,000	30.29
Extreme scenario — 1 in 100 years (VaR 99th)	$1,900,000	44.97

2 · TAIL RISK — LOSS EXCEEDANCE

There is a 5% annual probability that losses exceed approximately **$1.28M**, and a 1% annual probability that they exceed approximately **$1.9M**.

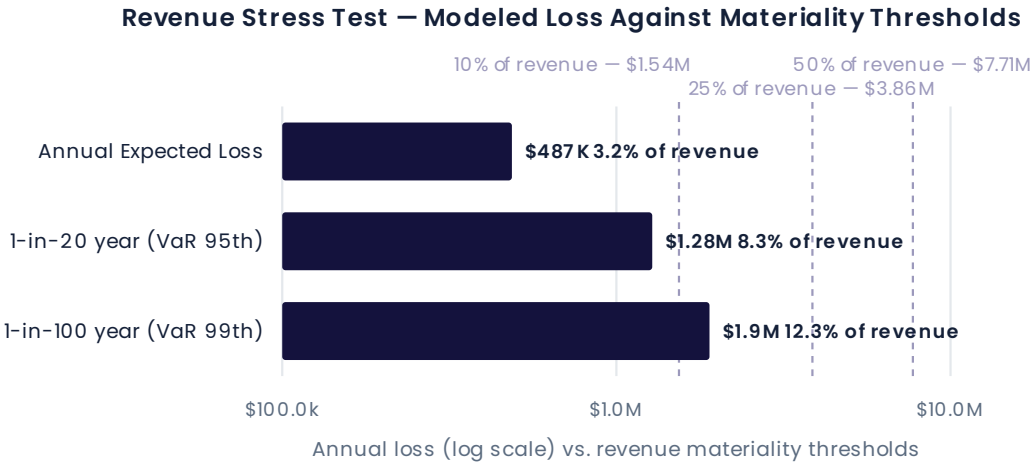
Facility Annual Loss Exceedance Curve



Exact by definition: 5% annual probability of exceeding VaR 95th ($1.28M); 1% of exceeding VaR 99th ($1.9M). Curve shape between and beyond these anchors is illustrative.

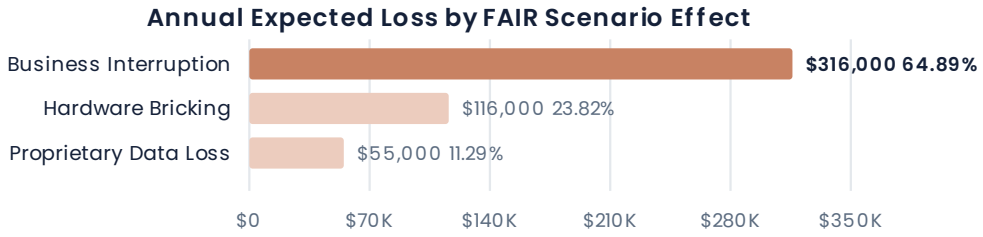
© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

3 · REVENUE STRESS TEST



One or more displayed modeled loss measures **reach or exceed** the lowest revenue materiality threshold, set at 10% of annual facility revenue. The 1-in-100-year loss reaches **12.32%** of annual facility revenue. The thresholds are a configurable input in DeRISK: set them to the materiality levels Finance uses for internal assessment or disclosure.

4 · COST OF LOSS STRUCTURE



The largest FAIR scenario Effects are **Business Interruption** and **Hardware Bricking** — together 88.7% of facility Annual Expected Loss.

5 · FAIR SCENARIO ANALYSIS

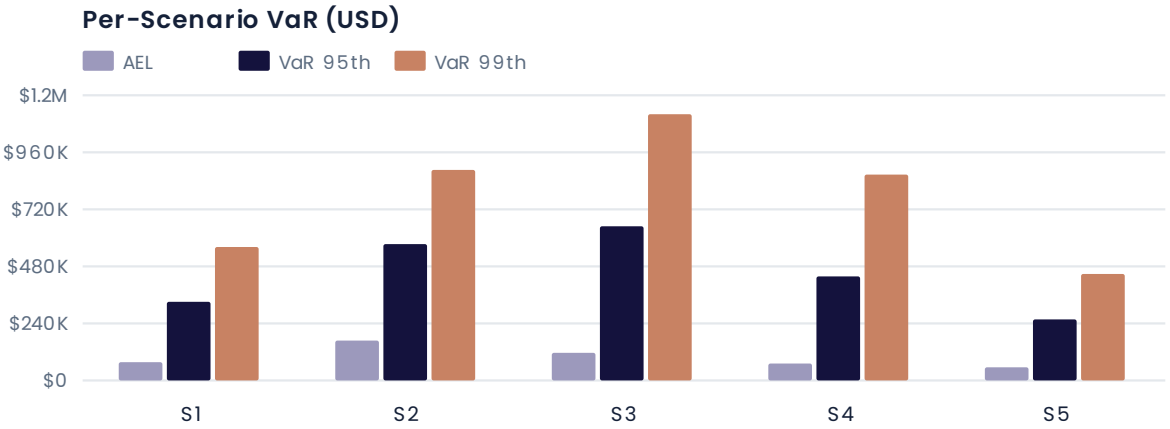
5.1 FAIR Scenario Register

ID	THREAT	ASSET	METHOD	EFFECT	RELEVANCE
S1	**Nation-State**	Business Process Generating Revenue	Remote Service Exploitation	Business Interruption	Unpatched critical vulnerabilities on GE DCS controllers, reachable from an enterprise management server via a flat IT/OT network, give nation-state actors a viable path to disrupt physical process control.
S2	**Cyber Criminals**	Business Process Generating Revenue	Ransomware without Data Exfiltration	Business Interruption	Actively exploited vulnerabilities on IT-facing servers and an end-of-life Windows workstation, with no effective IT/OT segmentation, let ransomware groups propagate from corporate systems into OT and halt industrial operations.
S3	**Privileged Insider**	Physical Assets & Facilities	Privileged Abuse	Hardware Bricking	A privileged insider with access to the enterprise management server can use legitimate admin protocols to traverse an unsegmented OT network and deliver destructive payloads to GE DCS controllers, causing prolonged physical downtime.

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

ID	THREAT	ASSET	METHOD	EFFECT	RELEVANCE
S4	Cyber Terrorists	Physical Assets & Facilities	Malware	Business Interruption	Field-level OT devices connect directly to an RTU with an unpatched remote-code-execution vulnerability, creating a path for destructive malware to reach DCS controllers and cause total loss of process visibility and control.
S5	Competitor Driven Threat Actors	IP & Trade Secrets Data	Data Exfiltration	Proprietary Data Loss	Exploitable vulnerabilities on IT-facing management servers, combined with direct connectivity to OT workstations and RTUs storing proprietary process data, expose the facility to stealthy, long-term industrial IP theft.

5.2 Per-Scenario VaR and Contribution



SCENARIO	AEL	VAR 95TH	VAR 95TH CONTRIBUTION	VAR 99TH	VAR 99TH CONTRIBUTION
S1	$77,000	$331,000	14.72%	$562,000	14.48%
S2	$168,000	$574,000	25.52%	$886,000	22.82%
S3	$116,000	$649,000	28.86%	$1,120,000	28.85%
S4	$71,000	$438,000	19.47%	$866,000	22.31%
S5	$55,000	$257,000	11.43%	$448,000	11.54%

6 · METHODOLOGY AND TRANSPARENCY

6.1 Financial and Contextual Inputs

INPUT	VALUE
Company name	Aldermere Energy
Industry	Energy
Geography	Several locations in the US
Number of facilities	70
Average cost per hour of Cybersec Forensic Services during a loss event	$500
Estimated Revenue loss per hour during a downtime event	$2,000
Total cost of equipment that could be damaged in a loss event	$255,000,000
Annual facility revenue	$15,422,000

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

INPUT	VALUE
Annual company revenue	$1,429,000,000
Critical assets in the facility topology	0
Target assets of the exploitable attack paths	3
Highly feasible exploitable attack paths analyzed	24
Applicable MITRE ATT&CK techniques in the exploitable paths (inferred from the topology)	5
Potentially applicable CVEs in the exploitable paths (inferred from the topology)	5

6.2 Primary Loss

SCENARIO	LOSS COMPONENT	MINIMUM	MODE	MAXIMUM	UNIT	JUSTIFICATION
S1	Business interruption downtime	180,000	420,000	840,000	USD	Downtime of 72-336 hours across dual DCS disruption valued at 2,500 USD/hour (revenue loss plus forensic services).
S1	Incident recovery/restoration	50,000	150,000	500,000	USD	Rebuild and re-commissioning of compromised management servers and controllers.
S2	Business interruption downtime	120,000	300,000	660,000	USD	48-264 hours of halted operations at 2,500 USD/hour pending restoration from ransomware.
S2	Recovery and ransom-related cost	100,000	250,000	750,000	USD	System restoration, negotiation, and potential ransom outlay for OT/IT recovery.
S3	Equipment replacement (bricked DCS)	500,000	2,000,000	8,000,000	USD	Permanent destruction of GE DCS controllers; bounded well below total equipment value of 255,000,000 USD.
S3	Extended downtime	840,000	1,800,000	3,600,000	USD	336-1440 hours (weeks to months) for procurement and re-commissioning at 2,500 USD/hour.
S4	Equipment damage	200,000	1,000,000	5,000,000	USD	Destructive ICS malware damaging controllers and field devices, partial equipment loss.
S4	Business interruption downtime	300,000	840,000	1,800,000	USD	120-720 hours of emergency shutdown and recovery at 2,500 USD/hour.
S5	Proprietary data/IP loss	100,000	400,000	1,500,000	USD	Estimated competitive value of exfiltrated process configurations and trade secrets.

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

6.3 Secondary Loss

SCENARIO	LOSS COMPONENT	MINIMUM	MODE	MAXIMUM	UNIT	JUSTIFICATION
S1	Regulatory and reputation	100,000	300,000	1,000,000	USD	Critical-infrastructure incident likely triggers regulatory scrutiny and stakeholder response costs.
S2	Reputation and third-party	150,000	400,000	1,200,000	USD	Public ransomware disclosure, customer impact, and notification costs.
S3	Investigation and legal	50,000	150,000	500,000	USD	Insider investigation, legal action, and HR/forensic response.
S4	Regulatory, safety and reputation	100,000	300,000	1,500,000	USD	Safety-event response, regulatory penalties, and public confidence impact.
S5	Legal and forensic	50,000	200,000	800,000	USD	Investigation, legal pursuit, and remediation after IP theft.

6.4 Loss Magnitude

SCENARIO	MEAN PER EVENT	RANGE PER EVENT
S1	1,200,000 USD	430,000 - 2,340,000 USD
S2	955,000 USD	370,000 - 2,610,000 USD
S3	3,230,000 USD	1,440,000 - 12,600,000 USD
S4	1,860,000 USD	600,000 - 8,300,000 USD
S5	545,000 USD	150,000 - 2,300,000 USD

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