CASE STUDY — CYBER INCIDENTS & BUSINESS INTERRUPTION

Quantifying Loss From a Cyber Incident at an Industrial Operator

Matter type	First-party insurance coverage dispute over business interruption and contingent loss following a cyber incident
Retained by	Counsel for the policyholder
Issue	The quantum of loss attributable to the incident, and whether the operator's controls and recovery planning met the standard the policy and industry practice assumed
Role	Testifying expert — quantitative cyber risk and loss modeling

Background

A cyber incident disrupted operational and business systems at an industrial operator, halting production for a period and degrading throughput for a longer one. The carrier disputed both the period of restoration and the causal attribution of losses in the degraded-operations period, and raised the adequacy of the insured's controls and continuity planning.

Scope of work

- Reconstruction of the incident and recovery timeline from system, network and operational records.
- Separation of the loss into the outage period and the degraded-operations period, with causal attribution modeled rather than assumed.
- Counterfactual production modeling to establish the throughput that would have obtained absent the incident, accounting for scheduled maintenance, demand and seasonal variation.
- Loss distribution modeling and Monte Carlo simulation to produce a loss estimate with a stated confidence interval rather than a single point figure.
- Assessment of control effectiveness against the NIST Cybersecurity Framework, and of continuity and recovery planning against the restoration period actually achieved.
- Sensitivity analysis identifying which assumptions the loss estimate was actually driven by.

Findings

Modeling the counterfactual production case rather than assuming it materially changed the attributable loss, and located the disagreement between the parties in two specific assumptions rather than across the whole claim. The degraded-operations period was shown to be causally connected to the incident through a mechanism the carrier's expert had not modeled. Sensitivity analysis demonstrated that the estimate was insensitive to most contested inputs and sensitive to two, which focused the remaining dispute. On controls, the operator's posture was consistent with framework expectations in the relevant areas, and the restoration period achieved was within the range the continuity plan contemplated.

Deliverables and use in the case

- Loss quantification presented as a distribution with a stated confidence interval, not a single figure — the form the underlying methods actually support.
- Counterfactual production model delivered in reproducible form.
- Sensitivity analysis isolating the two assumptions that drove the disagreement, which narrowed the scope of the dispute before mediation.
- Control effectiveness assessment against the NIST framework.
- Rebuttal of the carrier expert's attribution analysis; the matter resolved at mediation.

WORKING WITH FORWARD THINKING

How We Support Counsel

Early case assessment	A candid technical read before you commit to a theory. If the engineering does not support the claim or defense, we say so early, while that information is still useful and inexpensive.
Data preservation	Log files, condition monitoring archives and control system records overwrite on a schedule and are frequently lost before anyone asks for them. We identify what must be preserved, and how, in the first days of a matter.
Defensible methodology	Our methods are published and peer-reviewed rather than developed for the case. Models are delivered in reproducible form, with assumptions and uncertainty stated — the standard Rule 702 actually asks about.
Clear communication	Quantitative results are translated into terms a judge and jury can follow, without losing the precision that has to survive cross-examination. Uncertainty is stated plainly rather than hidden in a point estimate.
Rebuttal work	We are frequently retained solely to evaluate an opposing expert's risk, reliability or causation analysis, and to identify where the conclusions outrun what the model and the data actually support.
Conflict checking	Prompt conflict clearance and a written engagement scope before substantive work begins.

Practice areas

Energy, power and utility infrastructure · Industrial equipment failure and maintenance adequacy · Marine, offshore and autonomous systems · Cyber incidents and business interruption · Root cause and complex system accident analysis

Discuss a matter

Initial consultations to determine whether a matter is within our expertise are without charge. Contact us with the case posture, the technical question at issue and your key deadlines.

Tara Parhizkar, Ph.D., P.E. · 310.408.6750 · expertwitness@forwardthinkingsolution.com · www.forwardthinkingsolution.com

This case study is an illustrative composite prepared for informational purposes. Party names, locations, dates and identifying details have been omitted or altered. Nothing herein constitutes an opinion on any pending matter, creates an expert–client relationship, or discloses confidential information from any engagement.