From ATT&CK to AEL

The OT Cyber Impact-to-Loss Reference

How industrial cyber-attacks become financial loss — and how to model the bridge

---

Prepared by DeNexus

OT Cyber Risk Quantification & Underwriting Intelligence

PART 1 Why Threat Frameworks Stop at Impact

MITRE ATT&CK is the most widely adopted catalog of adversary behavior in cybersecurity. It is rigorous, comprehensive, and updated continuously by a global community of contributors. It is also, by deliberate design, silent on financial consequence.

ATT&CK describes what attackers do. It does not describe what the attack costs the victim. The framework ends at Impact — the final tactic in both the Enterprise and ICS matrices — and stops there. Whether a successful Impact event produces a few hours of inconvenience or a hundred million dollars of equipment damage and regulatory exposure is, from the framework's perspective, a question for someone else to answer.

This gap is the right design choice for a threat behavior catalog. The variables that determine financial consequence — facility revenue, equipment replacement value, downtime cost per hour, regulatory jurisdiction, insurance coverage, the affected population — live entirely outside what threat researchers observe and document. Pushing financial modeling into the framework itself would compromise its precision as a description of adversary behavior.

But the gap creates a practical problem for everyone downstream of the threat researcher. The CISO defending a budget, the underwriter pricing OT cyber coverage, the operations leader prioritizing remediation work, the board member assessing material cyber risk — every one of these audiences needs to translate "what happened" into "what it cost." That translation is its own discipline, and it has its own framework.

What This Document Is

This reference is the DeNexus framework for translating MITRE ATT&CK impacts into financial loss. It covers the five Impact Tactics that sit to the right of Command and Control in the Enterprise and ICS matrices, the eleven Impact Groups that those tactics aggregate into, five categories of Primary Loss that industrial operators actually absorb when an attack succeeds, and four categories of Secondary Loss that cascade from there.

It is the technical foundation of the DeRISK Platform's financial modeling — published as a reference so that the people who need to use, evaluate, or extend the model can do so with full transparency on the methodology.

Who This Document Is For

Three audiences benefit most:

- **OT cybersecurity professionals** responsible for building or defending a risk-based security program who need to express that program's value in financial terms.

- **Insurance underwriters** developing or refining their approach to industrial cyber risk who need a defensible methodology for translating technical findings into expected loss.
- **Risk and finance leaders** evaluating cyber risk quantification methodologies who need to understand how attack chains become AEL and VaR figures, and where the model's assumptions sit.

Familiarity with MITRE ATT&CK helps but is not required. The companion article on the DeNexus /learn/ section provides the framework background; this document picks up where the article ends.

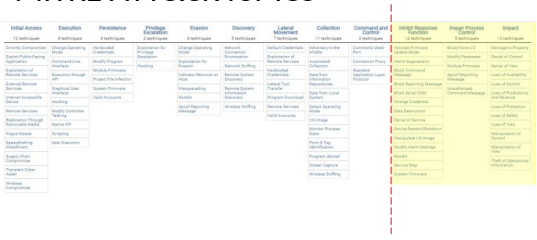
PART 2 The 5 Impact Tactics

The MITRE ATT&CK framework organizes adversary behavior into tactics that describe the adversary's tactical goal at each phase of the campaign. Most tactics describe how the adversary moves through the environment — gaining access, establishing persistence, moving laterally, evading detection. The tactics on the right side of the matrix, to the right of Command and Control, describe what happens when the adversary acts on their objective.

These are the impact tactics. Five matter for industrial environments — two from Enterprise, three from ICS.

MITRE ATT&CK for Enterprise

MITRE ATT&CK for ICS



MITRE ATT&CK Enterprise and ICS matrices — impact tactics highlighted in yellow

Exfiltration (Enterprise, TA0010)

The data leaves the environment. This is the moment a "data breach" actually becomes a breach: information moves from inside the perimeter to outside it, by whatever channel the adversary has established. Common techniques include exfiltration over command-and-control channels, over alternative protocols, over web services, and through physical media.

Collection (Enterprise, TA0009) is sometimes treated as the breach moment, but the regulatory exposure that follows a breach — notification requirements, regulatory penalty, compensation per affected person — is triggered when data leaves the premises. Collection alone, without exfiltration, is a precursor.

Impact (Enterprise, TA0040)

IT-side consequences executed against the corporate network: data destruction, ransomware encryption, service stop, system shutdown, account access removal, resource hijacking. This is where Enterprise-domain attacks produce measurable disruption — encrypted file servers, shut-down domain controllers, wiped endpoints.

Although Enterprise Impact targets IT systems, the consequence reaches OT regularly. Colonial Pipeline in 2021 was an Enterprise-matrix event end to end, and the operational shutdown — 5,500 miles of pipeline halted for five days — came from the operator's decision that they could not safely operate OT systems while IT systems were compromised. Norsk Hydro in 2019

followed the same pattern. Enterprise Impact is sufficient to produce significant OT consequence without any ICS-specific technique entering the attack chain.

Inhibit Response Function (ICS, TA0107)

Disables or disrupts safety and protective functions in the industrial environment. Techniques include alarm suppression, modify alarm settings, block command message, block reporting message, denial of service against safety systems, and direct manipulation of safety instrumented system logic.

Inhibit Response is what removes the operator's ability to react. A process that would normally be caught by an alarm and addressed through operator intervention becomes a process that proceeds unchecked. Combined with Impair Process Control, it is the signature of attacks designed for physical impact rather than disruption. TRITON was designed specifically to disable Schneider Triconex safety controllers — the last engineering layer between a process upset and a physical catastrophe.

Impair Process Control (ICS, TA0106)

Manipulates the physical process directly through modified setpoints, modified control logic, brute-forced I/O, modified parameters, spoofed reporting messages, or unauthorized command messages. This is the tactic that executes the physical attack — the adversary's hand on the steering wheel of the control system.

Stuxnet operated in this tactic when it varied centrifuge rotation speeds beyond safe operating thresholds. The same techniques used to drive a centrifuge out of spec can be applied to any controlled process: a turbine generator, a chemical reaction, a high-voltage substation, a water treatment dosing system.

Impact (ICS, TA0105)

The final physical outcome: loss of safety, loss of control, loss of view, loss of availability, loss of productivity and revenue, damage to property, denial of control, denial of view, manipulation of control, manipulation of view, theft of operational information.

ICS Impact is where the consequence becomes physical and the financial loss becomes measurable in industrial terms. Unlike Enterprise Impact, which is bounded by what can be done to digital systems, ICS Impact can include equipment destruction, injury, and loss of life. The ceiling of consequence is higher.

> **The key takeaway**
>
> These five tactics are where attacks produce physical and financial loss. Everything earlier in the campaign — initial access, lateral movement, persistence, discovery — creates the capability for loss. The impact tactics turn that capability into a measurable event.

For loss modeling purposes, the question is not whether an attack is sophisticated or which threat group is responsible. The question is which impact tactics the attack reaches, and what each of those impact tactics costs when it does.

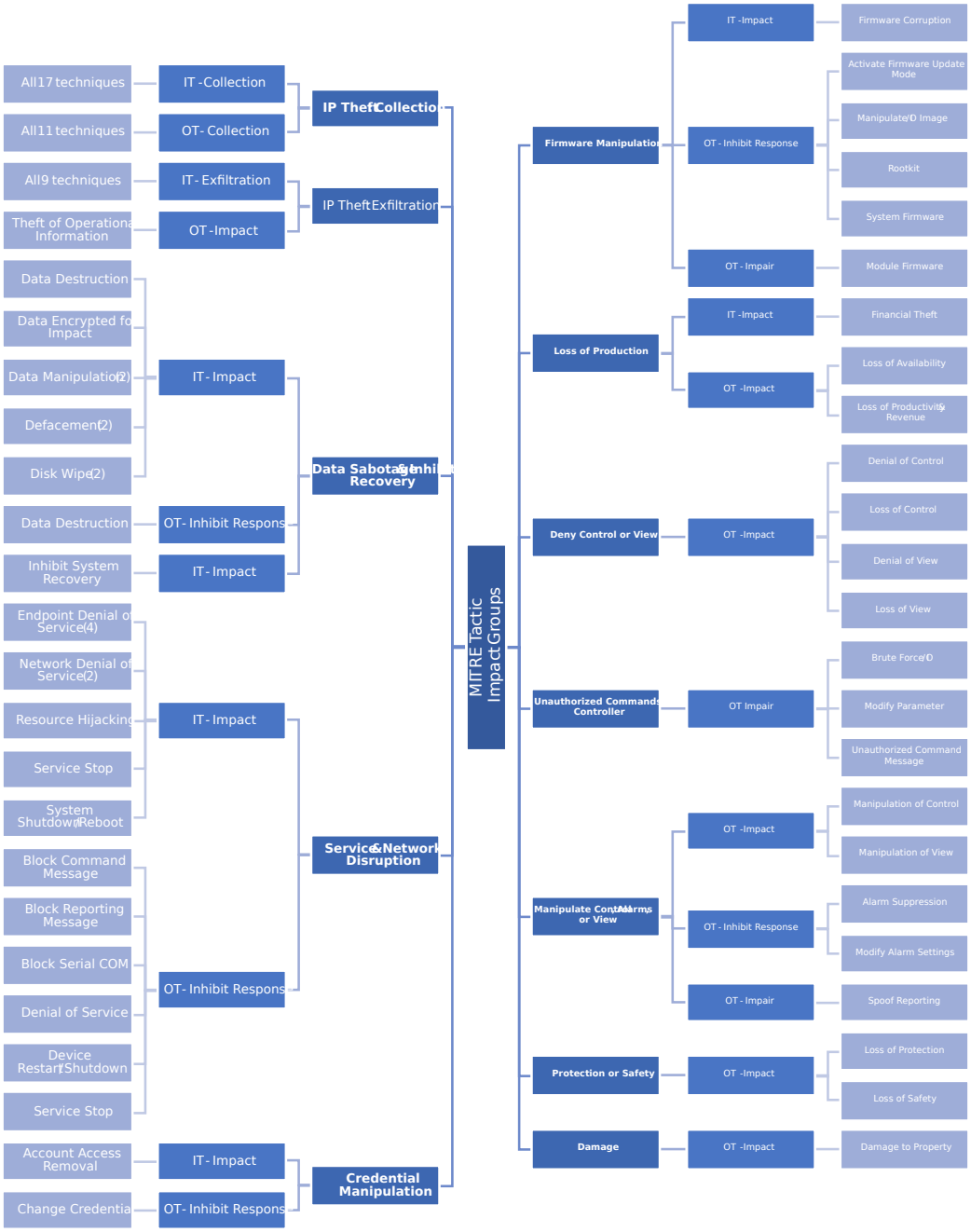
PART 3 Impact Groups — The Technique Taxonomy

Beneath the tactic layer, individual techniques aggregate into Impact Groups — clusters of techniques that produce similar types of consequence. The Impact Groups are the analytical bridge between the tactic-level abstraction ("Impact") and the loss-level specificity ("equipment damage of $4M").

Eleven Impact Groups span the Enterprise and ICS impact tactics:

Impact Group	What It Aggregates
IP Theft	Collection and exfiltration of intellectual property, operational data, or trade secrets
Data Sabotage & Inhibit Recovery	Data destruction, encryption for ransom, wiping, removal of recovery options
Service & Network Disruption	Denial of service, system shutdown, network blocking — IT-side disruption
Credential Manipulation	Account removal, credential changes that lock out legitimate users
Firmware Manipulation	Modification or corruption of device firmware in industrial systems
Loss of Production	Reduced output, full or partial production stoppage on industrial assets
Deny Control or View	Operators lose ability to see process state or to command the process
Unauthorized Commands to Controller	Direct sending of process commands that bypass operator intent
Manipulate Control, Alarms, or View	Subtle manipulation that operators may or may not detect
Protection or Safety	Compromise of safety systems, alarms, or protective functions
Damage	Direct physical damage to property, equipment, or infrastructure

The Impact Groups are where the technique-level catalog (hundreds of individual techniques across both matrices) becomes manageable for risk analysis. Modeling at the technique level produces too many variables to calibrate against real loss data. Modeling at the tactic level (just "Impact") loses the specificity that determines what kind of loss results. Impact Groups sit at the right level of abstraction: specific enough to drive loss differentiation, general enough to calibrate against the available data.



MITRE technique-to-Impact-Group taxonomy — how techniques across IT and OT aggregate into impact categories

The diagram above shows how techniques from both matrices roll up. Each Impact Group connects to multiple ATT&CK technique entries, drawn from both Enterprise and ICS. The IT and OT split visible in the middle column shows where a given Impact Group is realized through Enterprise techniques, ICS techniques, or both.

PART 4 Primary Losses — The Cyber-to-Physical Bridge

Primary losses are the direct, measurable consequence of a successful cyber impact. They are what the operator's finance team will see on a P&L statement, what an insurance claim will be filed against, and what an underwriter will be asked to indemnify. DeRISK starts by modelling five categories of primary loss.

Downtime

Full business disruption — 100% capacity loss. The facility, the production line, or the affected operational segment is offline. Revenue stops for the duration. Downtime is calibrated in the model by the facility's revenue rate (hourly or daily depending on the operation), the duration of the outage in hours or days, and any contractual minimum delivery obligations that convert downtime into immediate penalty rather than deferred revenue.

Downtime is the primary loss most directly associated with Service & Network Disruption (Enterprise) and ICS Impact techniques like Loss of Availability, Denial of Control, and System Shutdown. It is also the most common loss category in ransomware-driven incidents, where IT encryption forces operators to safely shut down OT systems they cannot confidently operate without IT support.

Loss of Productivity

Partial capacity loss between 1% and 99%. The facility continues to operate but at reduced output, reduced quality, or reduced efficiency. This category captures the realistic outcome of many ICS attacks where the operator can keep running with degraded automation, manual operation, or limited monitoring — but at a cost.

Loss of Productivity is calibrated by the percentage capacity reduction, the duration, and the marginal revenue contribution at affected capacity. It is the primary loss most associated with Impair Process Control attacks where the process can continue but with reduced confidence in setpoints, sensor readings, or control loop integrity. The Loss of Production Impact Group maps directly to this loss category.

Equipment Damage

Physical damage to industrial assets — turbines, motors, transformers, reactors, pipes, instrumentation. Equipment Damage is what makes ICS attacks fundamentally different from IT attacks: the consequence isn't bounded by digital systems. A pressure vessel that fails due to manipulated control logic must be replaced, not just patched.

Equipment Damage is calibrated by the replacement value of affected assets, the lead time to procure and install replacements (which often drives downtime longer than the cyber event itself), and the cascading effects on adjacent equipment. It is the primary loss most associated

with Manipulate Control/Alarms/View combined with Inhibit Response Function — the pattern where process limits are violated and safety systems are prevented from intervening.

Human Damage

Injury, illness, or loss of life resulting from cyber-induced process failures. Human Damage is the highest-consequence primary loss category, and the one most resistant to quantification because of the moral and regulatory weight involved. DeRISK models it for industrial processes where physical safety consequences are a credible result of the attack chain — transformers, generators, large moving equipment, robots, etc.

Human Damage is calibrated by historical incident benchmarks (industrial accidents with cyber or non-cyber causes producing similar physical consequences), facility population, and the protective layers between cyber-induced upset and physical injury. It triggers compensation per person as a secondary loss, sometimes also regulatory penalty. It is associated almost exclusively with the Protection or Safety and Damage Impact Groups in the ICS matrix.

Extortion

Ransom paid to attackers to recover encrypted systems, prevent disclosure of exfiltrated data, or restore operations. Extortion is distinct from other primary losses because it represents a deliberate operator decision — the payment is voluntary even when the underlying coercion is not. The model treats it as a primary loss because, on the balance sheet, the dollars leave the company in a directly attributable cyber event.

Extortion is calibrated by historical ransom data for comparable victims (sector, revenue, threat group), regulatory and policy constraints (some jurisdictions prohibit ransom payments to sanctioned entities or specific actors), and the operator's own stated position on payment. It is most directly associated with Data Sabotage & Inhibit Recovery (encryption ransomware) and IP Theft (extortion based on exfiltrated data).

PART 5 Secondary Losses — Cascading Consequences

Secondary losses are the cascading consequences that follow from a primary loss event. They are not the direct result of the cyber impact itself but of the operator's response to it, the regulatory environment around it, and the market and stakeholder reaction that follows. DeRISK starts by modelling multiple categories of secondary loss.

Incident Response Costs

External and internal costs of responding to and recovering from the incident. External costs typically include digital forensics firms, OT-specialized incident responders, legal counsel, crisis communications support, and any specialized engineering services required to restore operations.

Incident Response is the most universal secondary loss — almost every primary loss event triggers some level of response cost, even if no other secondary categories apply. The model calibrates it by the severity of the primary loss, the duration of the response window, and the typical hourly rates of the specialized services involved.

Reputational Loss

Financial consequence of damaged customer, partner, and market trust. Reputational Loss is the most difficult secondary category to quantify because the mechanisms are diffuse: lost customer renewals, longer sales cycles, lower contract values, supplier hesitation, talent retention costs, and equity valuation impact (for public companies). Despite the diffusion, the loss is real and material — independent studies routinely document multi-quarter revenue impact following publicly disclosed cyber events.

DeRISK models Reputational Loss as a percentage adjustment to expected revenue over a defined recovery window, calibrated to sector-specific patterns from comparable publicly disclosed incidents and a focus on the public relations costs to prevent excessive reputation loss.

Regulatory Penalty

Fines, sanctions, or remediation orders imposed by regulators in response to the incident. Regulatory Penalty varies enormously by jurisdiction and sector. The same incident in different jurisdictions can produce orders of magnitude different penalty exposure. Environmental regulators for releases and sector-specific industrial accident reporting regimes all have distinct penalty structures.

The model calibrates Regulatory Penalty by the jurisdictional footprint of the facility, the regulatory category triggered by the specific primary loss, and historical penalty patterns for comparable violations. For multinational operators, this often becomes the most uncertain secondary loss category because penalty regimes overlap and interact in non-additive ways.

Compensation per Person

Direct compensation payments to individuals affected by the incident — employees harmed in safety incidents directly associated with the Human Damage primary loss.

How Secondary Losses Stack

Secondary losses do not all apply to every primary loss event. The mapping is specific: a ransomware encryption that produces Downtime and Extortion as primary losses typically triggers Incident Response and Reputational Loss as secondary, sometimes Regulatory Penalty depending on jurisdiction, but does not typically trigger Compensation per Person. A safety system compromise producing Human Damage typically triggers all four secondary categories at significant magnitude.

The mapping is what makes the model defensible. Treating every secondary loss as additive to every primary loss would overstate total exposure. Treating any individual loss in isolation would understate it. The mapping in the next section is how the model preserves both rigor and realism.

PART 6 Mapping It Together

The full DeRISK impact-to-loss mapping links every Impact Group to its applicable primary loss categories, and every primary loss to its applicable secondary categories. The diagram below shows the complete map.

Full DeRISK impact-to-loss mapping — MITRE Impact Groups to Primary Losses to Secondary Losses

Reading the Diagram

The mind map diagram flows from the center outward. Impact Groups near the center aggregate the techniques that produced the attack outcome. The next green column shows which primary losses each group can produce, and excluded paths labeled "Not Realistic" or "Not Viable" for those deemed immaterial for modelling at this time. The outside columns show which secondary losses follow from each primary loss path.

Three patterns are worth attention.

Not every primary loss is viable for every Impact Group

The diagram explicitly excludes implausible paths. A Credential Manipulation event in an IT environment does not credibly produce Equipment Damage or Human Damage — those outcomes require physical-process techniques. Similarly, a Data Sabotage event does not credibly produce direct safety consequence on its own. The exclusions are as important to the model as the inclusions: they prevent the analysis from inflating expected loss with consequence paths that don't actually exist.

Some Impact Groups produce only one primary loss category

Damage and Protection or Safety produce focused loss patterns — Equipment Damage and Human Damage respectively, with corresponding secondary consequences. Other Impact Groups, particularly Manipulate Control/Alarms/View and Unauthorized Commands to Controller, produce broader loss distributions because the consequence depends heavily on what the attacker chose to manipulate. The breadth of possible consequence is itself an attribute of the Impact Group.

Secondary losses are not symmetric across primary losses

The diagram shows Equipment Damage paths leading to Human Damage and Compensation per Person in some Impact Group contexts (Protection or Safety, Damage) but not in others (Manipulate Control/Alarms/View). This asymmetry reflects how cascade chains actually work: equipment damage in a context where human safety is high risk produces different secondary consequences than equipment damage in a context where it is very low risk.

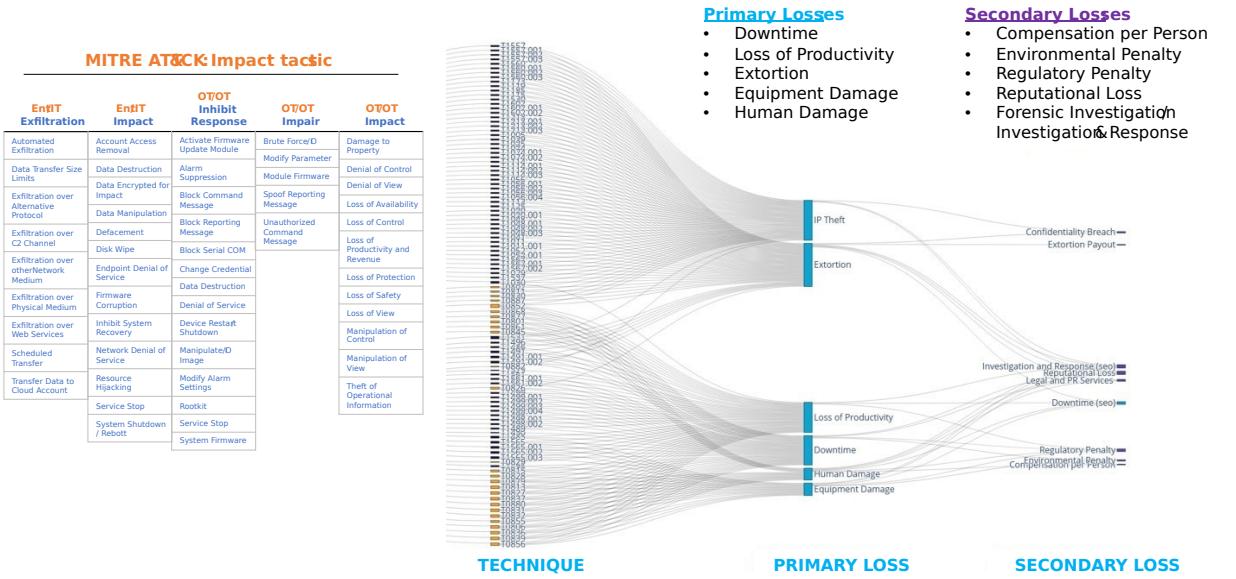
The diagram is the model

The mapping shown above is an illustraion of DeRISK's logic. Many of the relationships in the diagram are used for calculating expected loss for a given attack chain.

Customers, partners, and reviewers can inspect the mapping directly, challenge specific paths, and propose refinements with full visibility into how the model would respond.

PART 7 The Technical Deep View

The mapping shown in Part 6 operates at the Impact Group level. Beneath it, every ATT&CK technique in the Enterprise and ICS impact tactics is mapped to its Impact Group, and through the Impact Group to its primary and secondary loss categories. The flow diagram below shows the full technique-level view.



Full technique-level Sankey: every Enterprise and ICS impact-tactic technique mapped through Impact Groups to Primary and Secondary Losses

The flow diagram is the most complete view of the mapping. Each line on the left represents a specific ATT&CK technique drawn from the five impact tactics. The flows traverse through Impact Groups in the center, into Primary Losses, and on to Secondary Losses on the right. The visual density reflects the actual technique inventory — Enterprise techniques contribute more lines to IP Theft and Data Sabotage flows; ICS techniques dominate the Loss of Productivity and Damage flows.

For practitioners building or evaluating quantitative cyber risk models, this view answers the question "can I see how a specific technique contributes to expected loss?" The answer is yes — every technique in scope has a documented path from the threat catalog to the financial output. There are no black boxes between the ATT&CK identifier and the dollar figure.

PART 8 Worked Example

Scenario: Ransomware Pivot into a $300M Manufacturing Facility

A discrete manufacturing operator runs a single facility producing specialty industrial components. Annual revenue is approximately $300M. Hourly production revenue at full capacity is approximately $34,000/hr. Engineering workstations can change OT, HMIs operate the production floor PLCs; the historian sits on a DMZ between the corporate network and the OT zone.

The attack chain follows the cross-matrix pattern described in the companion article: phishing-based initial access to IT, lateral movement through the historian to engineering workstations, collection of PLC configurations, pre-staged ladder logic modification, and synchronized ransomware encryption combined with PLC modification activation.

Impact Tactics Reached

The attack reaches four of the five impact tactics:

- Enterprise Impact (TA0040) — ransomware encryption of IT infrastructure including domain controllers, file servers, engineering workstations, and the historian
- ICS Impair Process Control (TA0106) — pre-staged PLC modifications activated to corrupt production line controllers
- ICS Inhibit Response Function (TA0107) — alarm suppression on the affected production lines (limited; the operator detected the attack within hours)
- ICS Impact (TA0105) — loss of availability on two of four production lines

Impact Groups Triggered

Mapping the impact tactics to Impact Groups:

- Data Sabotage & Inhibit Recovery — ransomware encryption
- Unauthorized Commands to Controller — PLC ladder logic modification
- Manipulate Control, Alarms, or View — partial alarm suppression
- Loss of Production — production line shutdown

Primary Losses (Illustrative)

The numbers below are illustrative ranges, not a forecast for any specific operator. Real model outputs are calibrated to the facility's specific revenue, asset values, and operational profile.

Primary Loss	Illustrative Magnitude
Downtime	Two production lines offline for 8 days. Hourly production revenue on

Primary Loss	Illustrative Magnitude
	affected lines: ~$17K. Total downtime exposure: $3.2M–$3.8M.
Loss of Productivity	Remaining two lines operate at reduced capacity (manual configuration management) for 14 days. Estimated productivity loss: $400K–$800K.
Equipment Damage	Limited — PLC modifications were reversible. Two robots experienced damage while moving out of safe range. Estimated: $40K–$80K.
Human Damage	None in this scenario — manufacturing line, no safety-critical process upset.
Extortion	Ransom demanded: $5M. Operator decided not to pay; full restoration achieved through backups and OEM support. Counterfactual range had payment occurred: $3M–$5M.

Secondary Losses (Illustrative)

Secondary Loss	Illustrative Magnitude
Incident Response	External forensics and OT IR support, legal, crisis communications, OEM engineering support for PLC restoration: $1.2M–$1.8M.
Reputational Loss	Public relations firm hired to help manage and limit customer churn: $400K.
Regulatory Penalty	No direct data breach; jurisdictional reporting requirements met without penalty. Net regulatory exposure in this scenario: $0.
Compensation per Person	Not triggered in this scenario — no individuals harmed.

Total Illustrative Exposure

Summing the ranges: approximately $5.3M to $8.5M in total exposure from this single attack chain. The model output is not a point estimate but a probability distribution over the range, weighted by the likelihood of the attack chain reaching each impact tactic given the operator's specific security controls.

Two things to notice. First, the financial exposure is materially larger than the ransom demanded — $5M ransom versus $5–8M total exposure even after refusing payment. The financial argument for resilience is rarely the ransom itself; it is the downstream consequence the attacker uses ransom as a proxy for. Second, the exposure varies by a factor of 1.5x across the modeled range. That uncertainty is the model being honest about what is and is not knowable in advance.

PART 9 How DeRISK Models This

The DeRISK Platform uses MITRE ATT&CK as the core of its attack path modeling — not as a reference document, but as the operational threat structure that drives the financial model. The architecture has four components.

Initial Access Vectors From Both Matrices

The model considers every plausible entry point into the customer's environment — phishing, exposed services, vendor remote access, supply chain compromise, removable media, wireless reach, physical access. Each vector is drawn from the appropriate ATT&CK matrix (Enterprise for IT-side entry, ICS for direct OT-side entry where applicable) and assigned a base probability calibrated to industry threat intelligence data, sector-specific incident history, and observed adversary preferences for the customer's industry vertical.

Lateral Movement Across Network Architecture

Lateral movement is modeled across the customer's actual network architecture, with the Purdue model layers and identified pivot points determining which paths exist between initial access and target assets. The model evaluates feasibility against vulnerabilities, devices, and communication patterns, or firewall rules present in the customer's environment.

Maturity as Inhibitor

The maturity of the customer's cyber program is modeled as an inhibitor to attack progression — not as a binary control-in-place / control-absent flag. Strong segmentation lowers the probability that lateral movement succeeds. Mature monitoring lowers the probability that an attack proceeds undetected long enough to reach impact. Patch management, access control, incident response readiness, and the other security program elements assessed in the customer's submission all contribute to the inhibitor model. The result: two facilities with identical attack surfaces but different program maturities produce different expected loss values, because their probability of reaching successful impact differs.

Probability-Weighted Financial Output

The output is probability-weighted financial loss across the full set of modeled attack paths. The Impact-to-Loss mapping described in Parts 4 through 6 is the final transformation: each successful attack path is mapped through its Impact Group to applicable primary and secondary loss categories, with magnitudes calibrated to the customer's specific facility profile.

Three output formats are typical:

- **Annual Expected Loss (AEL)** — the probability-weighted average loss across all modeled attack paths over a one-year horizon. Useful for budget benchmarking and insurance pricing.

- **Value at Risk (VaR)** — the loss magnitude at a specified percentile (typically 95th or 99th). Useful for catastrophic-event planning and capital reserve sizing.
- **Attack-path-ranked prioritization** — specific remediation actions ordered by expected loss reduction per dollar of investment. Useful for capital allocation and program planning.

What This Approach Differs From

Most cyber risk quantification approaches use one of two simpler methodologies. The first applies a control-maturity score to a generic loss curve from industry benchmark data — useful for board-level reporting but disconnected from any specific threat path. The second uses Monte Carlo simulation over loss distributions parameterized from breach surveys — accurate in aggregate but unable to support "which remediation reduces this specific exposure?" conversations because no specific attack paths are modeled.

DeRISK's path-based modeling produces a financial output that is traceable back to a specific chain of ATT&CK tactics and techniques and the safeguard maturity that inhibits attacker success. That modelling approach is what makes the output more defensible in an underwriting conversation, a board review, or an internal budget allocation discussion. The mapping shown in this document is the audit trail.

Where the discussion goes from here

If you are evaluating the DeRISK approach — as an asset owner considering CRQ, as an underwriter assessing OT cyber submissions, or as a partner exploring integration — the next step is a walkthrough of the model output against a representative facility profile.

Reach out at denexus.io to schedule a technical discussion.

Closing

Threat frameworks describe adversary behavior. Loss frameworks describe financial consequence. The discipline that connects them — translating one into the other with sufficient rigor that the output is defensible in front of finance, in front of regulators, and in front of underwriters — is its own field, separate from threat intelligence and separate from actuarial science.

This document is the DeNexus contribution to that discipline. The mapping shown here — five impact tactics, eleven Impact Groups, primary losses, secondary losses, with explicit exclusions where consequence paths are not credible — is the foundation of DeRISK's financial output. It is published openly so that the people who use the output, evaluate the output, or extend the model can do so with full visibility into the methodology.

ATT&CK gave the industry a shared vocabulary for adversary behavior. The work continues on the loss side.

denexus.io

Learn more at denexus.io/derisk-platform