

Original Research Article

Monte Carlo Quantification of Financial Loss from Ransomware-Induced Service Disruptions in Urban Water Treatment and Distribution Systems

Adebiyi Adisa^{1*}, Olajide Dare², Isidore Ugochukwu Opara³, Ekundayo Peter Buremoh⁴, Stephen Sobulo⁵¹Civil Engineering and Construction Management, Heriot-Watt University, Edinburgh, United Kingdom²Department of Computer Science and Engineering, University of Fairfax, Salem, Virginia, USA³Department of Business Analytics, University of Fairfax, Salem, Virginia, USA⁴Department of Computer Science and Engineering, University of Fairfax, Salem, Virginia, USA⁵Department of Computer Science and Engineering, University of Fairfax, Salem, Virginia, USA**Article History**

Received: 13.11.2024

Accepted: 20.12.2024

Published: 24.12.2024

Journal homepage:<https://www.easpublisher.com>**Quick Response Code**

Abstract: We developed a Monte Carlo cyber-risk quantification model that translates ransomware disruption of urban water treatment and distribution systems into service, cash-flow, and tail-loss outcomes. Unlike attack-detection studies, the analysis began after compromise and examined how attack locus, outage duration, treatment or pumping capacity loss, water-storage buffer, infrastructure redundancy, network segmentation, backup maturity, manual operating capability, privileged-access maturity, and incident-response readiness interact. The synthetic experiment comprised 15,000 scenarios across six attack loci: enterprise information technology, SCADA/HMI, historian and telemetry, pump stations, treatment controls, and enterprise-wide compromise. Direct operator loss combined incident response, emergency water supply, overtime, energy inefficiency, revenue loss, public communication, regulatory response, asset restoration, and data restoration. A separate societal layer represented business interruption and expected public-health consequence. Mean direct operator loss was \$1.49 million, median loss was \$1.09 million, 95% value at risk was \$3.81 million, and 95% conditional value at risk was \$5.71 million. Enterprise-wide scenarios produced the largest median and tail losses. Attack duration explained most modeled loss variance, followed by capacity loss, daily demand, backup maturity, and population served. An integrated resilience portfolio combining segmentation, offline backup, manual continuity, incident-response capability, and privileged-access improvement reduced mean modeled loss by 40.6% and CVaR95 by approximately 40%. The study provides a transparent framework for engineering, cybersecurity, finance, and executive teams to compare mitigation investments using service continuity and loss distributions rather than qualitative risk ratings alone.

Keywords: Ransomware, Water Infrastructure, Cyber Risk Quantification, Monte Carlo Simulation, Service Continuity, Value At Risk, Conditional Value At Risk, Operational Technology, Financial Resilience.

Copyright © 2024 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

I. INTRODUCTION

Ransomware has evolved from file encryption on office computers into an organizational disruption mechanism that can affect identity systems, enterprise resource planning, work-order platforms, historians, human-machine interfaces, engineering workstations, and operational technology. In a water utility, the most important consequence is not the ransom demand itself. It is the possibility that treatment, pumping, storage, monitoring, billing, laboratory, and emergency-response

functions become unavailable or untrusted at the same time. The resulting loss combines cyber recovery with physical service interruption and financial stress [2-23].

Water treatment and distribution are particularly suitable for cyber-physical loss modeling because service continuity depends on interacting buffers. Reservoirs and tanks can maintain delivery after control impairment; redundant pumps and treatment trains can absorb partial failure; manual operating

*Corresponding Author: Adebiyi Adisa

Civil Engineering and Construction Management, Heriot-Watt University, Edinburgh, United Kingdom

procedures can sustain critical functions; and network segmentation or offline backups can shorten recovery. The same utility may therefore experience very different consequences from attacks with similar technical severity. A corporate IT event may disrupt billing and work orders but leave hydraulic service intact, while compromise of pump stations or treatment controls can reduce capacity and create immediate operational risk [8-27].

Traditional cyber-risk registers often score likelihood and impact on ordinal scales. These scores support prioritization but cannot show the probability that an event exceeds a utility's liquidity, insurance retention, emergency-procurement authority, or outage tolerance. Cyber value-at-risk methods translate uncertainty into loss distributions, while resilience engineering represents the depth and duration of degraded service. Combining the two allows a utility to ask decision-relevant questions: What is the 95th-percentile direct loss? Which control reduces expected loss and tail loss? How much storage is economically equivalent to a faster cyber recovery? When does an integrated mitigation portfolio become preferable to isolated controls? [32-36].

We addressed these questions through a completed simulation-based study of ransomware-induced water-service disruption. The model did not estimate the frequency of real ransomware attacks and did not use confidential utility or insurance data. Instead, it created a transparent scenario library in which engineering and cyber-control variables generated service-loss trajectories and financial consequences. All results are conditional on the parameter ranges and loss functions reported in the manuscript.

The study contributes five elements. First, it defines six ransomware attack loci with different physical consequences. Second, it links outage duration and capacity loss to storage, redundancy, manual operation, and recovery maturity. Third, it decomposes direct and societal losses instead of reporting one unexplained total. Fourth, it reports mean, median, value at risk, and conditional value at risk. Fifth, it compares mitigation portfolios through changes in both central tendency and tail loss.

II. RANSOMWARE AND WATER-SECTOR OPERATIONAL RISK

- A. Attack pathways and attack loci.
- B. Service continuity as the impact boundary.
- C. Financial quantification and tail risk

Ransomware incidents usually involve more than encryption. Attackers may exploit remote access, credentials, unpatched services, phishing, third parties,

exposed interfaces, or privileged accounts; then move laterally, exfiltrate data, disable backups, and disrupt recovery. Operational-technology environments add legacy protocols, long asset lives, safety and availability constraints, and specialized vendor access. NIST, CISA, EPA, and AWWA guidance therefore emphasizes asset inventory, network architecture, access control, backups, incident response, manual operations, and coordinated recovery [4-28].

We distinguished six attack loci. Enterprise IT compromise affects finance, billing, identity, and work management but may leave direct process control available. Historian and telemetry compromise reduces situational awareness and confidence in data. SCADA/HMI compromise impairs supervisory control. Pumpstation compromise reduces conveyance and pressure. Treatment-control compromise reduces safe production capacity. Enterprisewide compromise combines multiple failures and creates the greatest recovery coordination burden. This taxonomy is intentionally operational; it describes the function lost rather than a particular malware family.

Service continuity was modeled as the fraction of daily demand that could be safely delivered. Storage delayed the onset of customer impact. Redundancy reduced effective capacity loss. Manual capability reduced dependence on digital control, and incident-response or backup maturity shortened recovery. The resulting resilience curve represented degradation, sustained reduced service, and restoration. This approach follows resilience research that treats both loss depth and recovery time as important [16-37].

Financial consequence was separated into direct operator loss and broader societal loss. Direct operator loss included incident-response services, emergency water, overtime, inefficient energy use, lost revenue, communications, regulatory response, physical restoration, and data restoration. Societal loss added interruption to households and businesses and an expected public-health component. These categories are not accounting estimates for a particular utility; they are modeled cost functions used to compare scenarios.

Value at risk at confidence q is the q -quantile of the loss distribution. Conditional value at risk is the expected loss beyond that quantile. CVaR is useful for critical infrastructure because decision makers may care more about catastrophic but plausible events than about the average. Cyber risk quantification research has adapted these financial concepts to security investment and risk transfer, while emphasizing the sensitivity of outputs to model assumptions and data quality [20-35].

$$VaR_q(L) = \inf\{l : P(L \leq l) \geq q\} \quad (1)$$

$$CVaR_q(L) = E[L \mid L \geq VaR_q(L)] \quad (2)$$

Table 1: Ransomware attack loci used in the scenario model

Attack locus	Primary impaired functions	Expected service effect	Dominant financial consequences
Enterprise IT	Identity, billing, finance, work orders, email	Low direct hydraulic effect; coordination delays	Incident response, data restoration, revenue and productivity loss
Historian/telemetry	Monitoring, trends, alarms, operational confidence	Reduced observability; conservative operation	Forensics, manual monitoring, overtime, delayed decisions
SCADA/HMI	Supervisory control and operator interface	Moderate capacity and control loss	Response, manual operations, service degradation
Pump stations	Conveyance, pressure, zone transfer	High localized or system-wide delivery deficit	Emergency water, energy inefficiency, asset recovery
Treatment controls	Chemical dosing, process trains, safe production	High production and water-quality constraint	Emergency supply, testing, communication, regulatory response
Enterprise-wide	Combined IT and OT compromise	Deepest and longest service reduction	All categories; high tail loss and coordination burden

III. RESEARCH QUESTIONS AND HYPOTHESES

The study asked four questions. First, how do attack locus, duration, and capacity loss change direct and societal loss distributions? Second, which infrastructure and cyber-control variables dominate loss? Third, how do utility size and storage buffer alter cash-flow stress? Fourth, how much do alternative mitigation portfolios reduce mean loss and CVaR95?

H1 proposed that attack duration would be the dominant loss driver because it affects recovery labor, emergency supply, revenue, and service interruption simultaneously. H2 proposed that enterprise-wide, treatment-control, and pump-station attacks would generate larger tail losses than enterprise IT or historian events. H3 proposed that storage and redundancy would primarily reduce service loss, while segmentation, backups, privileged access controls, and incident-response maturity would primarily reduce duration and recovery cost. H4 proposed that an integrated resilience portfolio would reduce both expected loss and CVaR more than any isolated control family.

IV. SYSTEM BOUNDARY AND SERVICE DISRUPTION MODEL

- Utility and demand model.
- Cyber-control maturity variables.
- Service-loss function.
- Recovery trajectory.

The Monte Carlo library represented utilities serving approximately 40,000 to 750,000 people. Daily demand was generated from population with variability in per-capita use. Utilities differed in usable storage hours, infrastructure redundancy, segmentation, offline backup maturity, manual operating capability, incident-response maturity, privileged access and multifactor-

authentication maturity, and exposure of operational interfaces.

Control maturity variables were bounded between zero and one. They are comparative parameters rather than audit scores. Segmentation reduced lateral movement and the probability that an enterprise event affected operational control. Backup maturity reduced restoration time and data-reconstruction cost. Manual capability reduced capacity loss during control outages. Incident response maturity reduced containment and recovery duration. Privileged-access maturity reduced the effect of compromised credentials. Internet-exposed OT increased modeled duration and spread.

Attack duration was generated from a lognormal base distribution and modified by attack locus and controls. Capacity loss was assigned by attack locus and reduced by redundancy and manual capability. Storage delayed the point at which reduced production or pumping became unmet demand. The service-loss fraction increased nonlinearly after the storage buffer was exhausted, reflecting the transition from internal buffering to customer impact.

Recovery was not modeled as an instantaneous return. Service capacity fell after attack onset, remained degraded during containment, and recovered through restoration of systems, validation of data, and return of automated control. Representative trajectories demonstrate that shorter, narrower events can be absorbed, whereas enterprise-wide events create prolonged loss even after initial systems are restored.

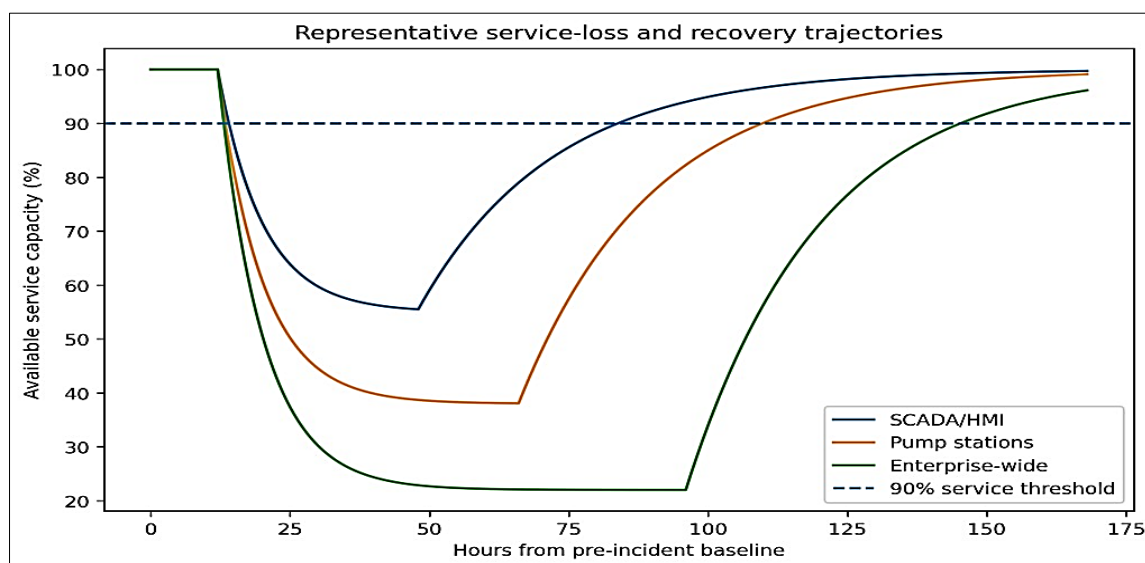
$$D_r = D_0 \cdot m_a \cdot (1.38 - 0.34S - 0.35B - 0.25I + 0.25E) \quad (3)$$

$$C_{loss} = C_a \cdot (1.15 - 0.35R - 0.22M) + \varepsilon_c \quad (4)$$

$$U = Q_d \cdot 1000 \cdot (D_r/24) \cdot C_{loss} \cdot [1 - \exp(-\max(0, D_{rH_s}/18))] \quad (5)$$

Table 2: Principal simulation variables

Variable	Interpretation	Modeled range or role
Population served	Utility service population	40,000-750,000
Daily demand	Average water demand	Population-derived with $\pm 15\%$ variation
Usable storage	Buffer before external service loss	5-24 hours
Redundancy	Alternative pump/treatment capacity	0-1 maturity index
Segmentation	IT/OT isolation and containment	0-1 maturity index
Backup maturity	Offline, tested restoration capability	0-1 maturity index
Manual operations	Ability to sustain safe operation without normal control	0-1 maturity index
Incident response	Containment, forensics, and restoration readiness	0-1 maturity index
PAM/MFA maturity	Protection of privileged and remote access	0-1 maturity index
Attack duration	Time before operational containment/restoration	1-240 hours

**Fig. 1: Representative service-loss and recovery trajectories for three ransomware attack loci**

V. FINANCIAL LOSS MODEL

- A. Direct operator losses
- B. Societal consequences
- C. Monte Carlo and risk measures
- D. Counterfactual mitigation portfolios

Incident-response cost combined a fixed mobilization component, population-related coordination cost, recovery hours, and lognormal professional-service variability. Emergency-water cost was proportional to unmet demand and the difficulty of replacement. Overtime depended on attack and recovery duration. Energy inefficiency reflected suboptimal pump and treatment operation during degraded control. Revenue loss followed unmet billed volume. Communication and regulatory costs increased with boil-notice duration and service population. Asset and data restoration depended on capacity damage and backup maturity.

The direct operator loss boundary was chosen because it can be compared with reserves, insurance retention, emergency authority, and mitigation budgets. The societal boundary added business interruption and expected public-health consequences. These broader

values are more uncertain, so they were reported separately. A utility should not combine direct and societal losses without explaining the decision purpose and valuation method.

We generated 15,000 independent scenarios using a fixed random seed. The model reported the mean, median, 75th percentile, VaR95, CVaR95, VaR99, and CVaR99. Attack-locus distributions were compared to determine whether the same mitigation policy was appropriate for IT, monitoring, control, pumping, and treatment events. A random-forest surrogate was used only for global importance ranking of the generated loss function; it was not the primary risk model.

Five mitigation portfolios were applied counterfactually to the same underlying scenario distributions: baseline; cyber hygiene; segmentation plus offline backup; manual continuity plus response retainer; and an integrated resilience portfolio. Each portfolio increased selected maturity variables. We compared annualized program cost with expected loss reduction and changes in VaR95 and CVaR95. Benefit-cost ratios were interpreted as annual loss avoidance per annualized

dollar in this conditional scenario set, not as a full investment appraisal or event-frequency estimate.

$$L_{direct} = L_{IR} + L_{water} + L_{overtime} + L_{energy} + L_{revenue} + L_{communications} + L_{regulatory} + L_{assets} + L_{data} \quad (6)$$

$$L_{societal} = L_{direct} + L_{business_interruption} + L_{expected_health} \quad (7)$$

Table 3: Direct loss components and model drivers

Loss component	Primary drivers	Interpretation
Incident response	Population, recovery hours, IR maturity	Containment, forensics, legal/technical coordination
Emergency water	Unmet demand, redundancy	Tankers, interconnections, bottled or temporary supply
Overtime	Attack and recovery duration	Operator, engineering, IT, communications, and management labor
Energy inefficiency	Capacity loss, duration, demand	Suboptimal pump and treatment schedules
Revenue loss	Unmet billed volume	Reduced or delayed utility collections
Communication/regulatory	Boil-notice duration, population	Public notification, testing, reporting, compliance
Asset restoration	Capacity impact	Equipment inspection, replacement, recommissioning
Data restoration	Backup maturity	Rebuild, validation, and recovery of systems and records

VI. RESULTS

- A. Overall loss distribution
- B. Attack-locus comparison
- C. Cost composition
- D. Loss drivers and utility size
- E. Mitigation portfolios

Across 15,000 scenarios, mean direct operator loss was \$1.49 million, median loss was \$1.09 million,

VaR95 was \$3.81 million, and CVaR95 was \$5.71 million. The distribution was rightskewed: VaR99 reached \$6.78 million, and the mean of the worst 1% of scenarios reached \$9.01 million. Mean societal loss was \$2.51 million, while societal CVaR95 was \$13.61 million. The difference between direct and societal tails shows why outage consequences can exceed the accounting loss borne by the utility.

Table 4: Overall direct and societal loss statistics

Loss boundary	Mean	Median	75th percentile	VaR9 5	CVaR9 5	VaR9 9	CVaR9 9
Direct operator	\$1.49 million	\$1.09 million	\$1.73 million	\$3.81 million	\$5.71 million	\$6.78 million	\$9.01 million
Total societal	\$2.51 million	\$1.39 million	\$2.76 million	\$8.31 million	\$13.61 million	\$16.31 million	\$23.67 million

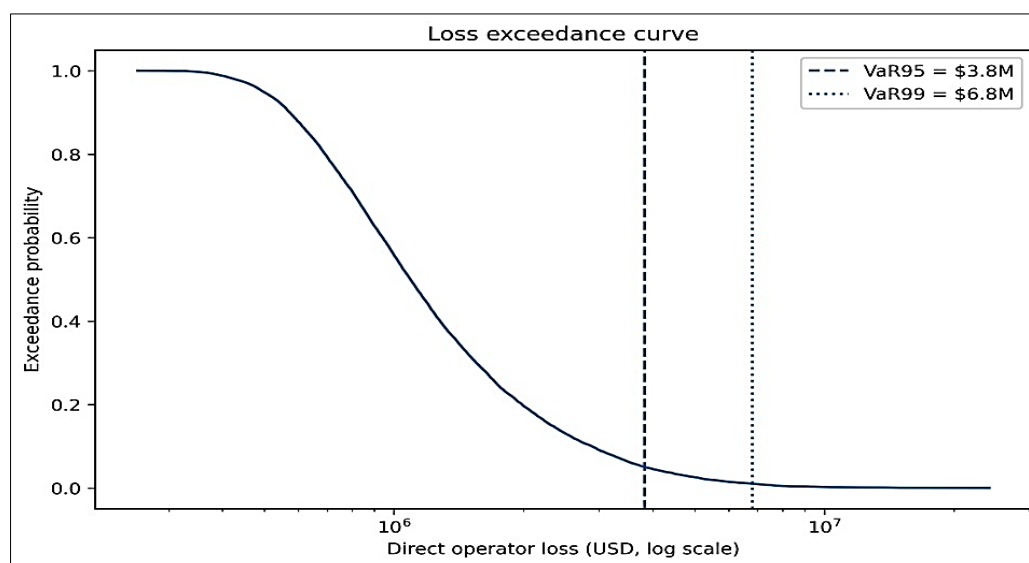


Fig. 2: Direct-operator loss exceedance curve with VaR95 and VaR99

Enterprise-wide attacks generated the greatest median and tail loss. Treatment-control and pump-station scenarios followed, reflecting their direct effect on safe production and delivery. SCADA/HMI compromise produced intermediate loss, while historian/telemetry and enterprise IT scenarios generally

retained more physical service. The ordering supports H2 but should not be interpreted as universal. A poorly segmented utility can experience operational consequences from enterprise IT, and a strong manual operating capability can reduce control-system impact.

Table 5: Direct loss and service consequence by ransomware attack locus

Attack locus	Median duration (h)	Median service loss	Median unmet demand (m ³)	Mean loss	Median loss	VaR9 5	CVaR 95
enterprise-wide	32.6	44.6%	45,981	\$2.33 million	\$1.73 million	\$5.86 million	\$8.42 million
treatment controls	28.1	31.4%	27,561	\$1.79 million	\$1.36 million	\$4.45 million	\$6.13 million
pump stations	26.0	25.6%	20,584	\$1.62 million	\$1.24 million	\$3.95 million	\$5.58 million
SCADA/HMI	22.9	15.2%	11,092	\$1.27 million	\$1.02 million	\$2.87 million	\$4.09 million
historian/telemetry	19.2	5.1%	3,060	\$961 thousand	\$805 thousand	\$2.01 million	\$2.65 million
enterprise IT	16.9	1.1%	532	\$843 thousand	\$731 thousand	\$1.67 million	\$2.19 million

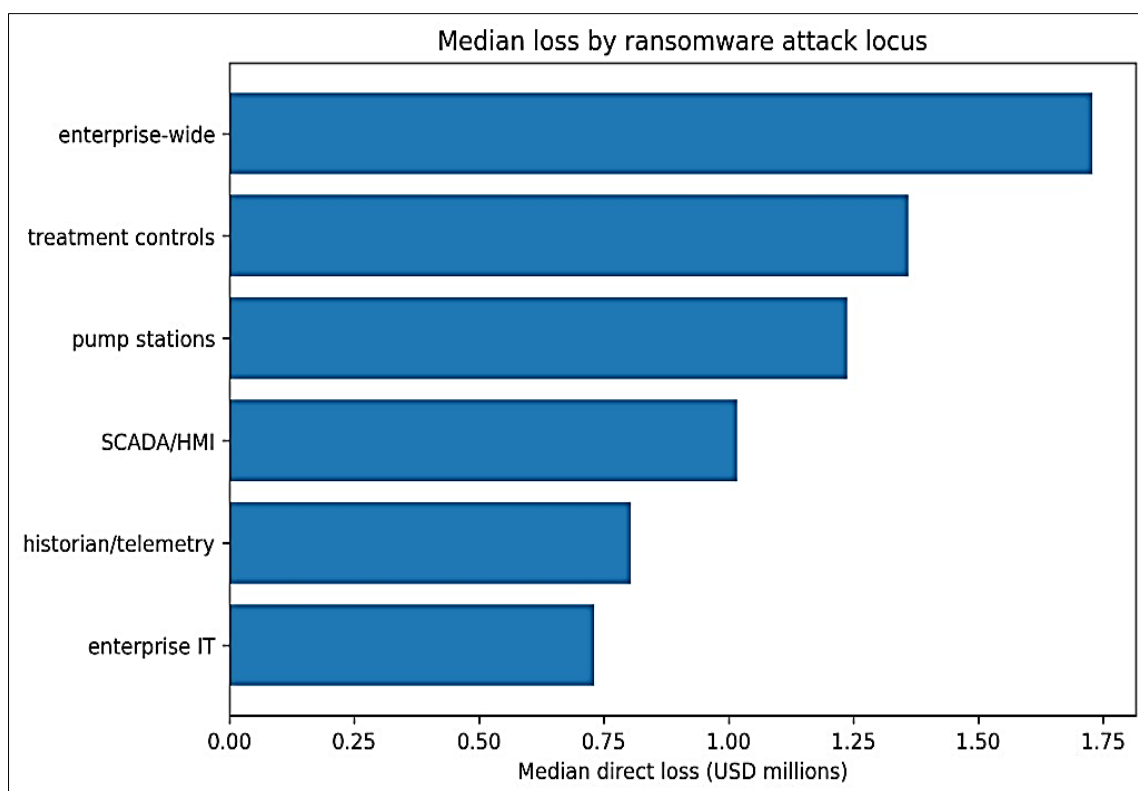


Fig. 3: Median direct operator loss by ransomware attack locus

Cost composition changed by attack locus. Enterprise IT and historian events concentrated loss in incident response and data restoration. Pump and treatment scenarios shifted the distribution toward emergency water, overtime, energy inefficiency, communication, and asset restoration. Enterprise-wide

scenarios combined both patterns. This decomposition matters because controls influence different loss terms: backup investment reduces data recovery, whereas storage, redundancy, and manual operation reduce unmet demand and emergency supply.

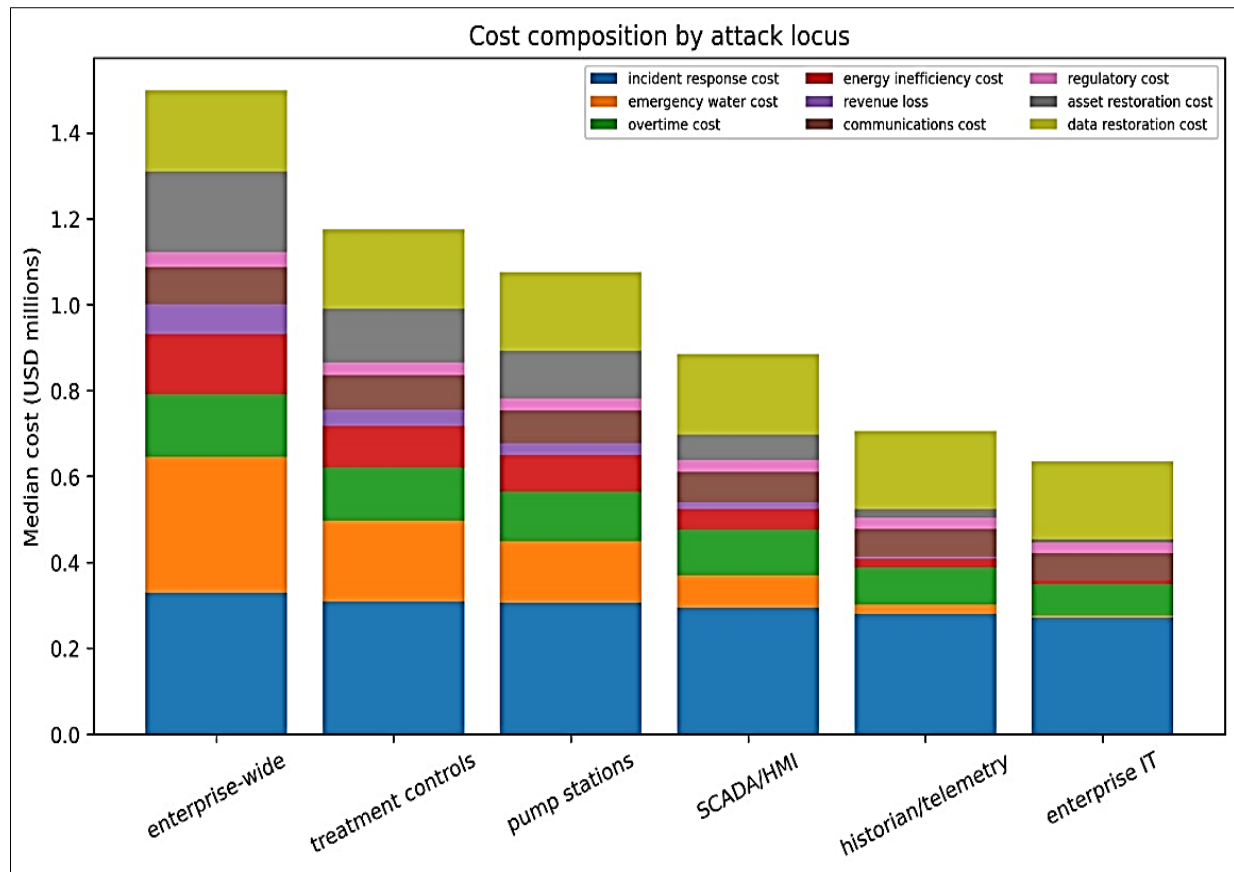


Fig. 4: Median direct-cost composition by attack locus

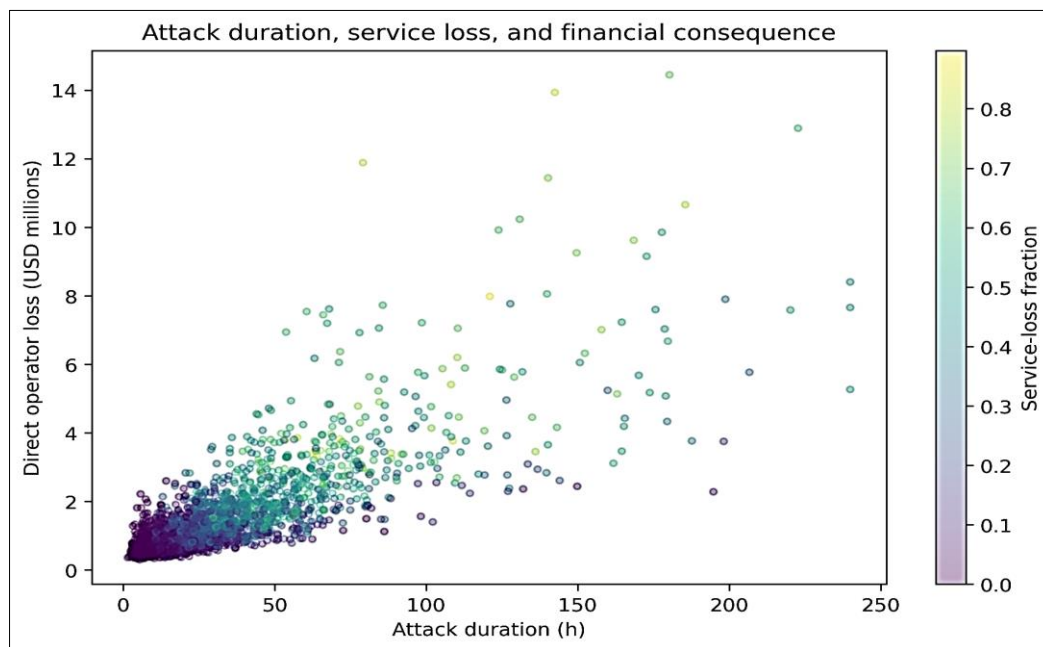


Fig. 5: Relationship among attack duration, service-loss fraction, and direct operator loss

Global importance analysis supported H1. Attack duration accounted for 69.0% of the surrogate model's importance, followed by capacity loss at 12.7%, daily demand at 5.4%, backup maturity at 5.0%, and population served at 4.1%. The dominance of duration is

structurally plausible because time multiplies response labor, water replacement, energy inefficiency, revenue, and service loss. It also implies that recovery controls may have greater financial leverage than controls that reduce only one cost component.

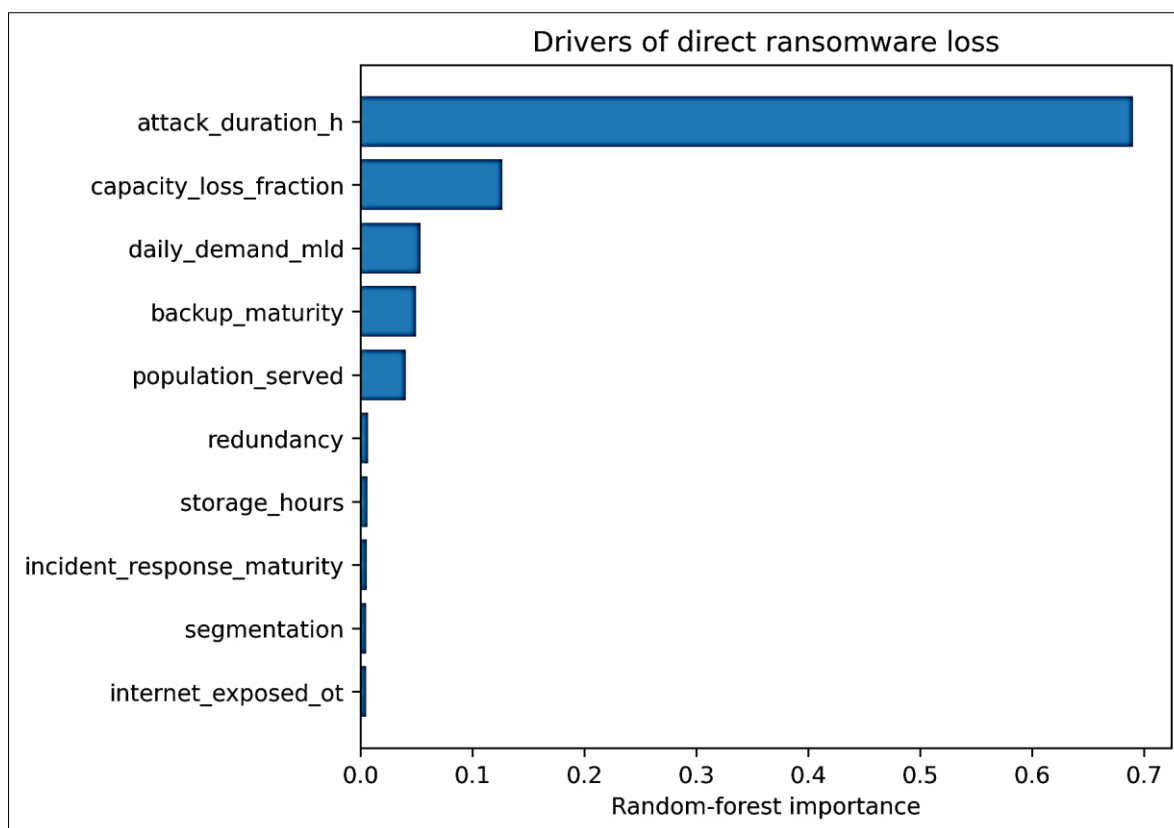


Fig. 6: Global importance ranking for direct ransomware loss

Table 6: Highest-ranked loss drivers

Rank	Variable	Importance	Decision interpretation
1	attack duration h	0.6901	Containment and restoration time compounds multiple costs
2	capacity loss fraction	0.1270	Determines depth of physical service impairment
3	daily demand mld	0.0538	Scales unmet demand and emergency supply
4	backup maturity	0.0499	Reduces restoration time and data-recovery cost
5	population served	0.0405	Scales communication, response, and societal exposure
6	redundancy	0.0069	Provides alternate treatment and pumping capacity
7	storage hours	0.0064	Delays customer-visible service loss
8	incident response maturity	0.0060	Shortens containment and coordination
9	segmentation	0.0051	Limits propagation across IT and OT zones
10	internet exposed ot	0.0050	Increases spread and recovery complexity

Utility size changed absolute cash-flow stress. Median direct loss increased from approximately \$0.90 million in the small category to \$1.37 million in the large category; the 95th percentile increased from \$2.68 million to \$5.66 million. Smaller utilities nevertheless

may face greater relative stress because they have lower revenue, fewer specialized staff, and less borrowing capacity. Absolute loss should therefore be paired with ratios to revenue, unrestricted cash, insurance limits, and emergency reserves during field validation.

Table 7: Direct-loss distribution by utility size

Utility size	Median direct loss	95th percentile
small	\$895 thousand	\$2.68 million
medium	\$1.08 million	\$3.59 million
large	\$1.37 million	\$5.66 million

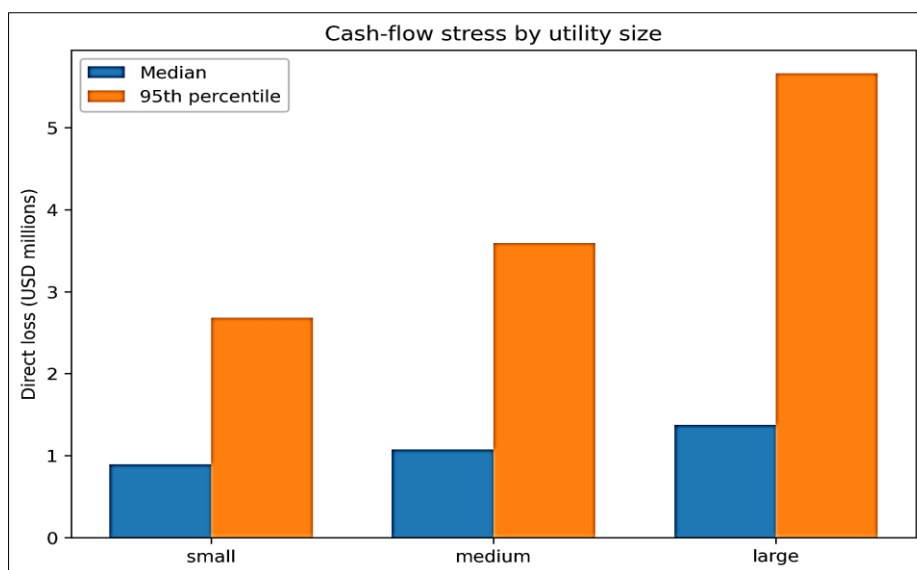


Fig. 7: Direct-loss cash-flow stress by utility size.

All mitigation portfolios reduced modeled loss. Cyber hygiene reduced mean loss by 12.6%. Segmentation plus offline backup reduced mean loss by 31.7% and CVaR95 by 29.0%. Manual continuity plus a

response retainer reduced mean loss by 20.8%. The integrated portfolio produced the largest reduction: 40.6% in mean loss and about 40% in CVaR95, supporting H4.

Table 8: Modeled mitigation-portfolio performance

Portfolio	Annualized cost	Mean loss	VaR 95	CVaR 95	Mean reduction	CVaR95 reduction	Benefit/cost ratio
Baseline	\$0	\$1.49 million	\$3.81 million	\$5.71 million	0.0%	0.0%	0.00
Cyber hygiene	\$480 thousand	\$1.31 million	\$3.38 million	\$5.01 million	12.6%	12.2%	0.39
Segmentation + offline backup	\$1.25 million	\$1.02 million	\$2.69 million	\$4.05 million	31.7%	29.0%	0.38
Manual continuity + response retainer	\$850 thousand	\$1.18 million	\$2.97 million	\$4.43 million	20.8%	22.4%	0.37
Integrated resilience portfolio	\$2.15 million	\$0.888 million	\$2.19 million	\$3.40 million	40.6%	40.3%	0.28

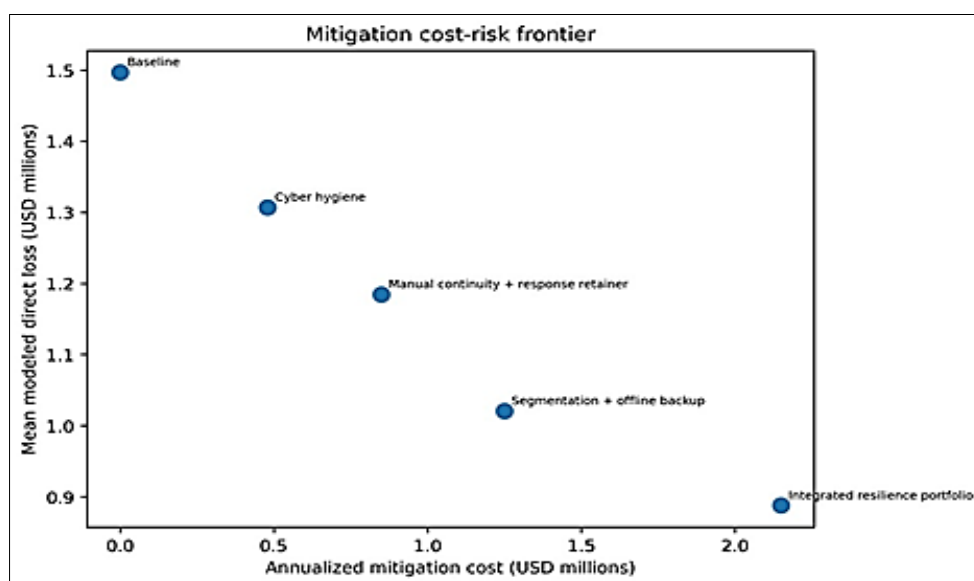


Fig. 8: Annualized mitigation cost versus mean modeled direct loss

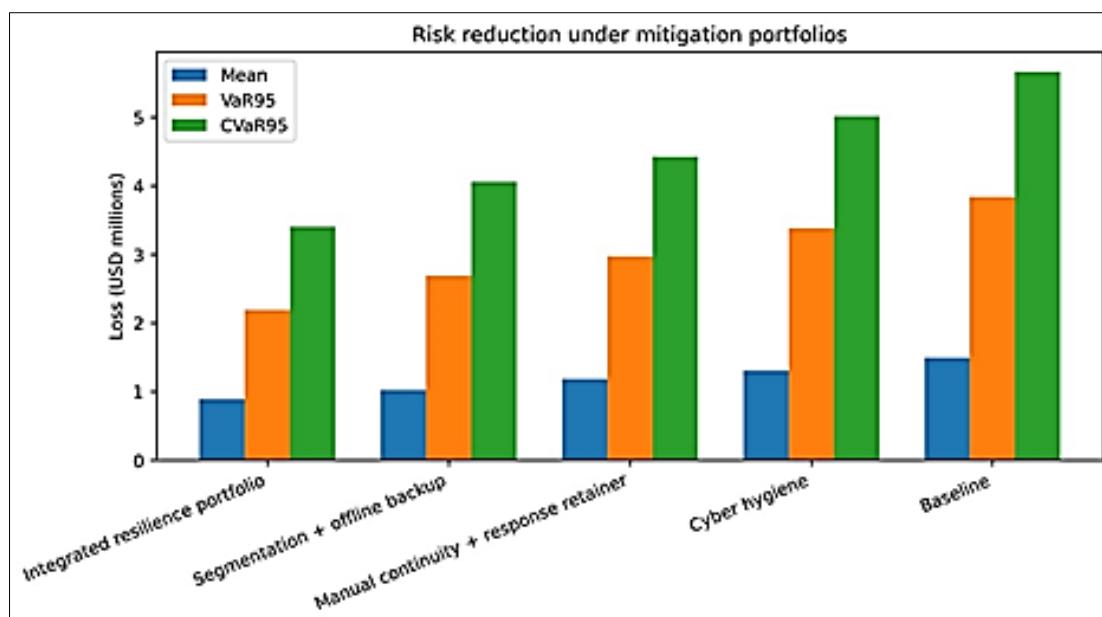


Fig. 9: Mean, VaR95, and CVaR95 under alternative mitigation portfolios

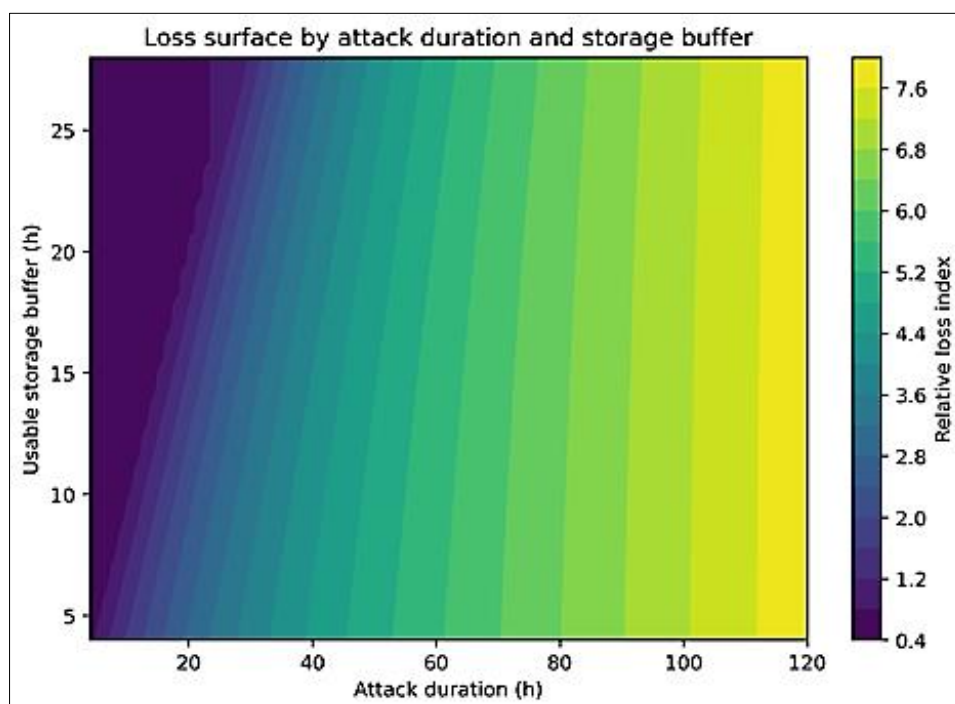


Fig. 10: Relative loss surface defined by attack duration and usable storage buffer

VII. FINANCIAL RESILIENCE AND FINTECH DECISION SUPPORT

- A. Liquidity and reserve planning
- B. Cyber insurance and risk transfer
- C. Investment prioritization

The loss distribution can support treasury and emergency finance planning. VaR95 is a candidate stress-testing amount, while CVaR95 estimates the average requirement if the 95th percentile is exceeded. A utility can compare these values with cash reserves, lines of credit, mutual-aid agreements, emergency procurement authority, and insurance. The result is more

actionable than an impact rating because it connects cyber and infrastructure assumptions to a financial tolerance.

Risk transfer should not be treated as a substitute for operational resilience. Insurance may reimburse portions of incident response, data restoration, business interruption, or liability, but coverage terms, exclusions, waiting periods, sub limits, deductibles, and infrastructure-specific consequences vary. The modeled loss components should be mapped to actual policy language. Tail scenarios involving treatment and public

health consequences may exceed conventional cyber-policy boundaries.

FinTech-enabled decision support can combine asset inventories, work orders, payment data, insurance terms, reserve balances, and cyber-control evidence. A dashboard should present the full distribution, not only expected loss. It should also allow decision makers to test control portfolios, storage projects, interconnections, and manual continuity. The financial model must retain traceability to engineering and security assumptions so that apparent precision does not conceal weak inputs.

Benefit-cost ratios in Table 8 are less than one because the simulation did not estimate annual event frequency; it modeled loss conditional on an event. A complete investment case would multiply conditional loss reduction by event frequency, add avoided regulatory and reputational effects, account for cobenefits, discount multiyear cash flows, and compare alternatives. The present values are therefore risk-reduction indicators, not recommendations to accept or reject a project.

Table 9: Financial decision uses of the modeled risk distribution

Decision	Relevant metric	Required additional data
Emergency reserve	VaR95 or chosen tolerance percentile	Cash balances, revenue, borrowing, response contracts
Tail-risk reserve	CVaR95/ CVaR99	Risk appetite, regulatory expectations, critical customer exposure
Insurance design	Loss components and exceedance curve	Policy wording, retention, limits, sublimits, exclusions
Mitigation selection	Expected and tail-loss reduction	Control cost, implementation time, cobenefits, event frequency
Continuity investment	Unmet demand and recovery trajectory	Storage, interconnections, mobile treatment, manual procedures
Executive reporting	Scenario range and assumptions	Validation status, uncertainty, ownership, review cycle

VIII. OPERATIONAL IMPLEMENTATION AND VALIDATION

- A. Data required from a utility
- B. Validation sequence
- C. Governance and model risk

Field implementation begins with a joint asset and process inventory. Engineering data include treatment capacity, pressure zones, pump and storage configuration, critical customers, interconnections, manual operating limits, and recovery dependencies. Cybersecurity data include network zones, identities, remote access, backups, incident-response contracts, recovery objectives, and known single points of failure. Financial data include labor rates, emergency-water agreements, energy tariffs, revenue structure, insurance, and reserve capacity.

Validation should proceed in stages. First, subject-matter experts validate equations and parameter ranges. Second, historical non-malicious outages test whether the service model reproduces known resilience behavior. Third, tabletop and cyberrange exercises test attack and recovery assumptions. Fourth, the model

operates in shadow mode during planning exercises. Fifth, assumptions and distributions are updated with real restoration, procurement, and payment records. No single synthetic estimate should be used for regulatory disclosure or insurance placement without this process.

Model risk governance should identify an accountable owner, approval authority, version control, input lineage, sensitivity analysis, and independent review. Scenario distributions should be reviewed at least annually and after major architecture, treatment, storage, tariff, or insurance changes. Decision makers should see ranges and confidence levels. NIST enterprise-risk and cybersecurity guidance supports integrating cyber risk into organizational governance rather than isolating it within technical teams [28-30].

Operational exercises should explicitly test manual water quality controls, alternative communications, isolated authentication, restoration from offline backups, and reconciliation of trustworthy and untrustworthy telemetry. The goal is not merely to restore computers; it is to restore safe, verified water service.

Table 10: Minimum data fields for productizing the model

Domain	Minimum fields	Validation owner
Civil/water engineering	Demand, capacity, storage, redundancy, pressure zones, critical customers, manual limits	Operations and engineering
Cybersecurity	Zones, remote access, privileged identities, backups, recovery objectives, incident response	CISO/OT security
Finance/FinTech	Labor, energy, emergency procurement, revenue, liquidity, insurance terms	Finance, treasury, risk

Domain	Minimum fields	Validation owner
Emergency management	Mutual aid, public communication, alternative water, regulatory contacts	Emergency management
Model governance	Parameter source, version, reviewer, uncertainty, approval date	Enterprise risk/internal audit

E. Literature Synthesis and Cross-Domain Positioning

Water cyber-physical research provides the technical basis for linking attacks to service consequence. SWaT offers a controlled water-treatment testbed, while EPANET and WNTR support simulation of hydraulic and resilience outcomes [22-38]. BATADAL and later studies demonstrate how process data can be used to identify and localize cyberattacks in distribution networks [1-39]. Model-based and hydraulic-attack research further shows that adversarial control can alter pressure, flow, storage, and service while attempting to remain stealthy [3-17].

Ransomware research emphasizes multistage compromise, backup impairment, lateral movement, data loss, and operational downtime [2-23]. Official guidance translates these threat characteristics into controls: NIST's ransomware profile, incident response guidance, OT security guidance, cyber-resilience engineering, CSF 2.0, and Zero Trust architecture; CISA's Stop Ransomware guidance; and water-sector guidance from EPA and AWWA [4-40].

Economic cyber-risk research shows that incident costs are heterogeneous and right-skewed. Romanosky [36], documents variation in observed cyber-incident costs; Eling and Schnell [10], examine the challenges of cyber risk and insurance; Gordon *et al.*, [15], discuss security investment; and Woods *et al.*, [43], infer loss distributions from insurance pricing. The World Bank (2024) reviews broader evidence on cyber-incident costs, while the World Economic Forum (2024) highlights organizational and systemic cyber risk. These sources support the use of distributions rather than a single deterministic loss estimate.

Cyber value-at-risk and Open FAIR approaches provide a bridge from security scenarios to financial decision making [31, 32]. Kucukkaya *et al.*, [20], extend value-at-risk thinking to IoT cyber risk. We add a civil-engineering layer by making service capacity, demand, storage, redundancy, and manual operation explicit. The resulting loss is therefore conditional not only on attack and control maturity but also on physical buffering.

Digital-twin, edge-intelligence, IoT-security, and simulation research demonstrates how cyber-physical state and decision support can be coupled [3-12]. Our Monte Carlo model is not a real-time digital twin, but it is designed so that utility-specific hydraulic and financial inputs can replace the synthetic parameter distributions. Scikit-learn was used for the surrogate importance model and reproducible analytics [33].

F. Dependence, Uncertainty, and Scenario Stress Testing

Monte Carlo results depend on both marginal distributions and dependence among variables. In practice, longer attacks may coincide with weaker backups, poor segmentation, limited staffing, or high OT exposure; extreme weather may increase demand while reducing access to replacement equipment; and a regional incident may increase emergency-water and contractor prices. Assuming independence can understate tail loss. The present model embeds selected structural relationships but does not estimate a full empirical dependence model.

A field implementation should test alternative correlations and tail assumptions. At minimum, analysts should compare independent sampling, positive dependence among weak controls, common-cause utility stress, and regional price escalation. Copulas or Bayesian networks can be used when data support them, but transparent stress scenarios remain valuable when historical samples are sparse. Decision makers should receive a range of VaR and CVaR values across plausible dependence structures.

Parameter uncertainty differs from scenario variability. Scenario variability describes which attack and operating state occurs. Parameter uncertainty describes whether the cost per unit, recovery multiplier, service-loss relationship, or control effect is correctly specified. The two should be separated. A practical approach is nested simulation: draw uncertain model parameters in an outer loop and event scenarios in an inner loop, then report confidence intervals around the risk metrics.

Model validation should include back-testing against non malicious outages and actual cyber incidents where data are available. Recovery duration, labor, emergency procurement, water demand, and communication costs can be calibrated from internal records even when ransomware examples are limited. Tabletop and cyber-range exercises can calibrate control-effect assumptions. Insurance claims and external benchmarks may improve cost distributions, but confidentiality, selection bias, and coverage definitions must be documented.

Stress testing should include low-probability combinations that historical data may not contain: enterprise-wide compromise during peak demand; unusable backups; depleted storage; simultaneous telecom failure; unavailable specialist vendors; and compromised identity systems that delay restoration.

These cases are not forecasts. They test whether liquidity, manual operations, and governance remain adequate when several defenses fail together.

Table 11: Uncertainty and stress-testing dimensions

Dimension	Baseline treatment	Alternative stress test	Decision use
Attack duration	Lognormal, control-adjusted	Heavier tail or prolonged extortion/validation delay	Test reserves and response contracts
Control dependence	Partially structural	Weak segmentation, backups, PAM, and IR occur together	Test systemic governance weakness
Emergency prices	Scenario-specific unit costs	Regional scarcity multiplier for tankers, labor, and equipment	Test procurement authority and liquidity
Demand	Population-derived with variation	Peak demand, heat event, critical-customer concentration	Test storage and continuity
Recovery capacity	Maturity-index effect	Vendor unavailability, telecom failure, identity outage	Test manual and mutual-aid plans
Public-health consequence	Expected value proportional to service/notice	Low-frequency severe consequence range	Separate societal tail from operator accounting loss

D. Reserve, Insurance, and Liquidity Stress Example

To illustrate use of the distribution, consider a medium utility that selects direct-loss VaR95 as an operational reserve benchmark and CVaR95 as a tail-planning benchmark. In the synthetic library, medium utilities had a median direct loss of approximately \$1.08 million and a 95th percentile near \$3.59 million. An organization with a \$1 million cyber retention and \$1.5 million of unrestricted emergency cash would remain exposed to a large liquidity gap in a 95th-percentile event unless insurance, credit, mutual aid, or emergency financing responded quickly.

The gap should be analyzed by timing as well as amount. Incident-response retainers, overtime, emergency water, and public communication require cash early. Insurance reimbursement may occur later and may require documentation. Revenue loss and regulatory costs may emerge over weeks or months. A cash-flow

model should therefore map each loss category to expected payment timing and recovery source.

Insurance stress testing should map modeled components to actual coverage. Forensic response and data restoration may be covered; physical asset damage, pollution, public-health liability, utility revenue, regulatory penalties, and infrastructure failure may be excluded or sublimited. Waiting periods can leave short but costly outages uninsured. The model should show gross loss, insured loss, retention, coinsurance, uncovered categories, and timing of recovery.

FinTech systems can support rapid, controlled response through pre-approved emergency vendors, digitally verified bank accounts, segregated approval, spending limits, real-time liquidity views, and auditable payment trails. These controls reduce response friction without abandoning fraud prevention. They also create evidence for later insurance and regulatory review.

Table 12: Illustrative liquidity bridge for a medium utility

Funding source or need	Illustrative amount	Timing	Key condition
Immediate response and overtime need	\$0.75 million	Days 0-7	Retainer, payroll, emergency authority
Emergency water and communication	\$0.85 million	Days 1-21	Vendor capacity and verified payment details
Restoration and data recovery	\$1.20 million	Weeks 1-8	Scope, procurement, specialist availability
Unrestricted emergency cash	\$1.50 million	Immediate	Board/management authority and minimum operating cash
Cyber insurance retention	\$1.00 million	Before recovery	Covered event and documented claim
Illustrative gross VaR95	\$3.59 million	Full event horizon	Scenario-specific, not a forecast
Potential bridge gap	\$1.09 million	Before insurance reimbursement	Credit, mutual aid, reserve, or public financing

E. Risk Appetite and Portfolio Governance

Risk appetite should be expressed in multiple dimensions: maximum safe service degradation, maximum outage duration, maximum probability of

exceeding liquidity, maximum uninsured loss, and maximum acceptable public-health consequence. A single dollar threshold can obscure an unacceptable

service outcome, while a purely engineering threshold can ignore financial insolvency or delayed recovery.

Portfolio governance should require a named owner for every modeled control effect. Segmentation is owned jointly by network architecture and OT operations; backups by technology and application owners; manual continuity by operations; emergency water and mutual aid by engineering and emergency management; reserves and insurance by finance; and model assumptions by enterprise risk. Evidence of tested performance should replace maturity self-ratings over time.

Investment selection should compare marginal risk reduction. For example, utilities with strong backups but limited storage may gain more from physical continuity, while utilities with extensive storage but flat networks may gain more from segmentation and

privileged-access controls. The model can identify these interactions only after local calibration.

An annual governance cycle should review incidents, exercises, architecture changes, treatment capacity, demand, storage, suppliers, policy terms, and financial reserves. Material changes should trigger a model update. Board and executive reporting should show assumptions, validation status, central and tail risk, and unresolved uncertainty rather than presenting the output as an actuarial fact.

Appendix A. Utility Calibration Workbook

The calibration workbook below identifies the evidence needed to replace synthetic parameters with local values. Utilities can begin with ranges and progressively narrow them through records, exercises, and validated models. Each parameter should record source, owner, date, confidence, and next review.

Table A1: Utility-specific calibration workbook

Parameter	Preferred evidence	Fallback evidence	Validation test
Daily demand and critical load	SCADA/historian and billing demand by zone	Design demand and seasonal summaries	Compare simulated and observed daily profiles
Usable storage hours	Tank curves, operating rules, minimum pressure constraints	Nominal volume divided by average demand	Replay pump or power outage
Redundancy	Asset topology, capacity, failure modes, interconnections	Engineering judgment and design documents	N-1 and common-cause simulation
Manual operating capability	Written procedure, staffing, local controls, exercise results	Self-assessed maturity	Timed exercise under loss of normal HMI/identity
Backup maturity	Immutable/offline backup inventory and restore tests	Policy and backup job reports	Restore representative systems in isolated environment
Incident response duration	Historical incidents, exercises, retainer service levels	Expert ranges	Tabletop/cyberrange timing
Direct cost rates	Payroll, contracts, tariffs, vendor schedules, insurance claims	External benchmarks adjusted to utility	Reconcile prior outages and incidents
Insurance recovery	Policy wording, endorsements, limits, retention, waiting periods	Broker summary	Coverage counsel and scenario walkthrough

Calibration should preserve physical and financial units. Maturity scores can be useful for initial comparison, but they should be translated into tested effects such as hours to restore identity, percentage of capacity available manually, or probability that a compromise crosses a network boundary.

Appendix B: Control-to-Model Mapping and Reproducibility

Reproducibility requires a traceable link from control evidence to scenario parameters and from scenario parameters to loss outputs. The mapping below provides a minimum structure for versioned implementation.

Table B1: Control-to-model mapping

Control or capability	Model variable affected	Evidence of effectiveness	Failure-mode test
Network segmentation	Attack duration and attack-locus spread	Architecture, firewall rules, monitored pathways	Attempt controlled lateral movement in a test environment
PAM/MFA and remote access	Compromise duration and spread	Account inventory, session recording, MFA coverage	Simulate stolen credential and emergency access
Offline/immutable backups	Recovery hours and data-restoration cost	Restore tests, isolation, recovery objectives	Ransomware recovery exercise
Manual operations	Capacity-loss fraction and continuity	Procedures, local control, staffing, water-quality checks	Operate critical process without normal SCADA/HMI

Control or capability	Model variable affected	Evidence of effectiveness	Failure-mode test
Storage/interconnections	Service-loss onset and unmet demand	Hydraulic model, tank rules, agreements	Extended pump/treatment outage simulation
Incident-response retainer	Containment/recovery duration and response cost	Contract scope, response times, exercise performance	After-hours activation test
Emergency procurement/FinTech controls	Emergency cost, timing, fraud/control risk	Prequalified vendors, verified accounts, approval workflow	Rapid purchase and payment drill
Insurance/risk transfer	Net loss and liquidity timing	Policy, sublimits, exclusions, claims process	Scenariospecific coverage review

The simulation seed, raw scenario table, loss-component outputs, attack-locus summaries, mitigation counterfactuals, and figure data are supplied in machine-readable form. A field study should store an immutable model package containing code version, parameter file, random seed, software environment, reviewer approval, and checksum for every published result.

D. Digital-Twin Integration and Secure Data Exchange

A productized implementation can be connected to a utility digital twin, but the financial-risk model should remain logically separate from real-time control. The digital twin supplies validated asset state, demand, storage, topology, and recovery dependencies. The risk engine converts scenario outputs into loss distributions. A decision layer compares those distributions with reserves, insurance, service tolerances, and mitigation costs. This separation prevents a finance-oriented model from issuing operational commands and allows each component to be independently validated.

Data exchange should use stable identifiers for facilities, treatment trains, pumps, tanks, pressure zones, applications, identities, vendors, policies, and financial accounts. Time-series data should retain sampling

interval, quality flags, source, calibration status, and clock accuracy. Scenario results should retain input version, model version, random seed, loss boundary, confidence level, and reviewer. Without these fields, a later update can change a risk number without explaining why.

Security architecture is especially important because the risk platform aggregates sensitive operational and financial information. Read-only data feeds, network separation, service identities, encryption, least privilege, immutable audit logs, and controlled export should be implemented. The platform should not require inbound connectivity to operational control networks. Where feasible, data should be replicated through a broker or historian boundary into an analytics zone.

A digital twin also supports exercise learning. After a tabletop, non-malicious outage, or actual incident, observed restoration time and cost can be compared with the scenario distribution. Deviations should update specific parameters rather than be absorbed into an unexplained adjustment factor. This creates a cumulative evidence base for improving both engineering and financial resilience.

Table 13: Secure integration between utility data, digital twin, and financial-risk engine

Layer	Inputs	Outputs	Security boundary
Operational source	Historian, asset state, demand, storage, work status	Validated time series and events	No model writeback to control devices
Engineering twin	Topology, capacity, hydraulics, dependencies, recovery constraints	Service-loss trajectories and unmet demand	Versioned model and quality assurance
Cyber scenario engine	Attack locus, duration, spread, control maturity	Compromise and restoration scenarios	Restricted threat and architecture data
Financial-risk engine	Service trajectories, labor, tariffs, contracts, insurance, reserves	Loss distribution, VaR, CVaR, liquidity gap	Finance and risk access controls
Decision/governance	Risk appetite, service tolerance, mitigation portfolio	Approved actions and investment decisions	Human authorization and audit trail

Appendix C: Monte Carlo Scenario Dictionary

The scenario dictionary identifies the main machine-readable fields supplied with the study. It distinguishes exogenous context, cyber controls,

physical consequences, financial components, and derived risk metrics. A field implementation should preserve these categories and add data-source confidence.

Table C1: Condensed Monte Carlo scenario dictionary

Category	Representative fields	Unit/scale	Use
Utility context	population_served, daily_demand_mld, storage_hours	People, MLD, hours	Scales service and cash-flow exposure
Physical resilience	redundancy, manual_operations	0-1 maturity	Reduces capacity loss and customer impact
Cyber resilience	segmentation, backup_maturity, incident_response_maturity, pam_mfa_maturity	0-1 maturity	Changes attack spread, duration, and restoration
Threat context	attack_type, internet_exposed_ot	Category, 0-1	Defines attack locus and exposure
Disruption	attack_duration_h, capacity_loss_fraction, service_loss_fraction	Hours, proportion	Connects compromise to physical consequence
Service outcome	unmet_demand_m3, boil_notice_h, recovery_h	m ³ , hours	Drives emergency and societal consequences
Direct costs	incident_response_cost, emergency_water_cost, overtime_cost, energy_inefficiency_cost, revenue_loss	USD	Operator accounting boundary
Additional costs	communications_cost, regulatory_cost, asset_restoration_cost, data_restoration_cost	USD	Completes direct loss model
Societal costs	societal_business_loss, health_expected_loss	USD expected value	Broader consequence reported separately
Risk outputs	direct_operator_loss, total_societal_loss, VaR, CVaR	USD	Decision and portfolio comparison

Scenario records should not be interpreted as independent real incidents. They are draws from the modeled parameter distributions. When field data are added, each record should include origin values such as synthetic, historical outage, exercise, actual cyber incident, or expert-elicited scenario so that validation can be stratified by evidence type.

IX. DISCUSSION

The principal finding is that ransomware impact in water infrastructure is governed by time and physical buffering. Attack duration dominated the model because it simultaneously extends service loss, response labor, emergency procurement, communication, and restoration. Storage and redundancy convert some cyber events into manageable operational disturbances, while weak recovery converts moderate compromise into sustained financial loss. Cybersecurity and civil resilience are therefore economic complements.

The attack-locus comparison also demonstrates why generic ransomware cost factors are insufficient. Enterprise IT compromise can be expensive without materially reducing water output; treatment and pump compromise create direct service costs; enterprise-wide compromise combines both. A credible loss model must identify which functions are unavailable and how operators continue service.

The integrated portfolio achieved the greatest loss reduction, but it also had the highest annualized cost and the lowest conditional benefit-cost ratio among active portfolios. This illustrates a common risk-decision tension. Tail-risk reduction may justify an integrated portfolio even when annual expected loss alone does not.

Decision makers should compare portfolios against risk appetite, regulatory obligations, critical-customer consequence, co-benefits, and event frequency.

The framework also clarifies roles. Cybersecurity teams define attack pathways and recovery controls. Civil and water engineers define service dependencies, storage, redundancy, manual limits, and safe operating states. Finance and FinTech specialists define loss boundaries, payment and liquidity effects, risk metrics, and insurance. Executive management sets tolerance and approves investment. Removing any one perspective produces an incomplete decision model.

The results should not be interpreted as a forecast for a named utility. They are evidence that the selected variables and loss categories can be integrated coherently and that tail metrics reveal information hidden by average loss. External calibration is the decisive next step.

X. LIMITATIONS

The study is simulation based. Parameter distributions were designed to be technically plausible but were not fitted to confidential utility, ransomware, insurance, or public-health loss data. The results are conditional loss estimates, not annualized risk estimates, because event frequency was not modeled.

The hydraulic component is a service-level surrogate rather than a calibrated EPANET model of a specific network. It does not represent detailed pressure, water age, chlorine residual, contamination transport, or asset-specific failure. Productization should connect the

scenario engine to a validated digital hydraulic model such as EPANET or WNTR and to product-specific operating constraints.

Loss functions simplify legal, regulatory, public-health, reputational, and macroeconomic consequences. Societal values are especially uncertain. They were reported separately to avoid false equivalence with audited operator costs. Insurance recoveries, ransom payments, litigation, tax effects, and long-term capital-market consequences were not modeled.

Control maturity indices summarize complex capabilities. A high backup score does not guarantee usable restoration, and manual operation may be limited by staffing, safety, telemetry, or chemical-control constraints. Field exercises and evidence of tested performance should replace self-assessment wherever possible.

The random-forest importance ranking reflects the generated model and correlated variables; it is not causal. Sensitivity analysis should be repeated with alternative distributions, dependence structures, and extreme-event assumptions before decisions are made.

XI. CONCLUSION

We completed a Monte Carlo ransomware-loss study that linked cyber compromise to water-service continuity and financial consequence. Across 15,000 synthetic scenarios, mean direct operator loss was \$1.49 million, VaR95 was \$3.81 million, and CVaR95 was \$5.71 million. Enterprise-wide, treatment-control, and pump-station attacks produced the largest tail losses. Attack duration was the dominant model driver, followed by physical capacity loss, demand, backup maturity, and population served. The integrated resilience portfolio reduced mean and tail loss by approximately 40%. The framework provides a transparent basis for utilities to connect cybersecurity, engineering continuity, reserves, insurance, and investment decisions, provided that synthetic assumptions are replaced with validated local data before operational use.

XII. DECLARATIONS

Data Availability Statement: The findings are based on synthetic Monte Carlo scenarios generated from the model documented in this manuscript. The scenario table, parameter dictionary, equations, risk calculations, and figure-generation code should be deposited in a public repository before final publication. No confidential utility, insurance, customer, employee, or incident data were used.

Study Transparency Statement: This manuscript reports a simulation-based cyber-physical and financial-risk study. Monetary values are conditional model outputs under stated assumptions and are not forecasts, actuarial estimates, audited losses, or valuations for any identified water utility.

Ethics Statement: No human participants, patient data, customer-identifiable data, live operational systems, or active cyber intrusions were involved; human-subject approval was not required. Field validation must comply with utility security, critical-infrastructure, privacy, and incident-disclosure requirements.

Conflict of Interest: The authors declare no conflict of interest.

Funding: No external funding was received for this study.

Author Contributions: Adebiyi Adisa led ransomware taxonomy, cybersecurity-control modeling, and cyber-risk governance. Olajide Dare led water-infrastructure service modeling, operational continuity, and civil-engineering interpretation. Isdore Ugochukwu Opara led financial-loss architecture, tail-risk metrics, mitigation economics, and forensic-control interpretation. Ekundayo Peter Buremoh contributed ransomware threat modeling, cybersecurity analytics, attack-path interpretation, and critical revision. Stephen Sobulo contributed human-factors framing, cognitive-resilience interpretation, socio-technical risk analysis, and critical revision. All authors contributed to conceptualization, methodology, interpretation, writing, critical revision, and approval.

Cyber-loss estimation benefits from a broader cyber-physical and digital-transformation perspective. Distributed IoT security and edge-intelligence research highlights the dependence of modern physical services on networked sensing and distributed decision systems [44, 45]. Studies in data intensive quality assessment, healthcare cloud adoption, digital-twin risk management, and wireless integrity monitoring illustrate complementary approaches for translating digital-system behavior into operational or economic risk signals [46-49]. These cross-domain examples support the modeling principle used here: cyber disruption should be translated into measurable service, control, and financial consequences rather than reported only as a technical incident.

REFERENCES

1. Abokifa, A. A., Haddad, K., Lo, C. S., & Biswas, P., "Detection Of Cyber Physical Attacks On Water Distribution Systems Via Principal Component Analysis And Artificial Neural Networks," In *World Environmental And Water Resources Congress 2019* (Pp. 676-691). American Society of Civil Engineers. <https://doi.org/10.1061/9780784482360.061>, 2019.
2. Al-Rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M., "Ransomware Threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions," *Computers & Security*, Vol. 74, Pp.

- 144-166.
<https://doi.org/10.1016/J.Cose.2018.01.001>, 2018.
3. Zhan, Z., Xu, M., & Xu, S. (2013). Characterizing honeypot-captured cyber attacks: Statistical framework and case study. *IEEE Transactions on Information Forensics and Security*, 8(11), 1775-1789.
4. Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K., "Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions," *Computers & Security*, Vol. 111, Art. 102490.
<https://doi.org/10.1016/J.Cose.2021.102490>, 2021.
5. Brentan, B. M., Campbell, E., Goulart, T., Manzi, D., Ayala-Cabrera, D., Herrera, M., Montalvo, I., & Izquierdo, J., "Social Network Community Detection And Hybrid Machine Learning For Cyber-Attack Detection In Water Distribution Systems," *Water*, Vol. 13, No. 6, Pp. 795.
<https://doi.org/10.3390/W13060795>, 2021.
6. Cybersecurity and Infrastructure Security Agency, "#Stopransomware Guide," U.S. Department of Homeland Security, 2023.
7. Cybersecurity and Infrastructure Security Agency, Environmental Protection Agency, Federal Bureau of Investigation, & Multi-State Information Sharing and Analysis Center, "Internet-Exposed Hmis Pose Cybersecurity Risks To Water and Wastewater Systems," U.S. Government, 2024.
8. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, & U.S. Environmental Protection Agency, "Incident Response Guide: Water and Wastewater Sector," U.S. Government, 2024.
9. Eling, M., & Schnell, W., "What Do We Know About Cyber Risk And Cyber Risk Insurance? *Journal of Risk Finance*, 17(5), 474-491,"
<https://doi.org/10.1108/Jrf-09-2016-0122>, 2016.
10. Falayi, A., Ayeni, A., Adebayo, B., & Abdullahi, A., "Towards Digitalization of Fruits and Vegetables Supply Chain: Digital Twins and Internet of Things Approach," *Global Journal of Researches in Engineering: G Industrial Engineering*, Vol. 24, No. 1, Pp. 10-20, 2024.
11. Falayi, A., Wang, Q., Liao, W., & Yu, W., "Survey Of Distributed And Decentralized Iot Securities: Approaches Using Deep Learning And Blockchain Technology," *Future Internet*, Vol. 15, No. 5, Pp. 178.
<https://doi.org/10.3390/Fi15050178>, 2023.
12. Zhan, Z., Xu, M., & Xu, S. (2015). Predicting cyber attack rates with extreme values. *IEEE Transactions on Information Forensics and Security*, 10(8), 1666-1677..
13. Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyber attacks rates. *EURASIP Journal on Information security*, 2019(1), 5..
14. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L., "Increasing Cybersecurity Investments In Private Sector Firms," *Journal of Cybersecurity*, Vol. 6, No. 1, Pp. Tyaa005.
<https://doi.org/10.1093/Cybsec/Tyaa005>, 2020.
15. Henry, D., & Ramirez-Marquez, J. E., "Generic Metrics and Quantitative Approaches for System Resilience as A Function of Time," *Reliability Engineering & System Safety*, Vol. 99, Pp. 114-122.
<https://doi.org/10.1016/J.Ress.2011.09.002>, 2012.
16. Housh, M., & Ohar, Z., "Model-Based Approach for Cyber-Physical Attack Detection in Water Distribution Systems," *Water Research*, Vol. 139, Pp. 132-143.
<https://doi.org/10.1016/J.Watres.2018.03.061>, 2018.
17. Klise, K. A., Hart, D. B., Moriarty, D., Bynum, M. L., Murray, R., Burkhardt, J., & Haxton, T., "Water Network Tool for Resilience (Wntr) User Manual," Sandia National Laboratories and U.S. Environmental Protection Agency, 2017.
18. Klise, K. A., Murray, R., & Haxton, T., "An Overview of the Water Network Tool for Resilience (Wntr)," *Environmental Modelling & Software*, Vol. 95, Pp. 420-431.
<https://doi.org/10.1016/J.Envsoft.2017.06.039>, 2017.
19. Kotenko, I., Saenko, I., Lauta, O., & Kribel, A. (2022). Ensuring the survivability of embedded computer networks based on early detection of cyber attacks by integrating fractal analysis and statistical methods. *Microprocessors and Microsystems*, 90, 104459.
20. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M., & Thiel-Clemen, T., "Changing The Resilience Paradigm," *Nature Climate Change*, Vol. 4, Pp. 407-409.
<https://doi.org/10.1038/Nclimate2227>, 2014.
21. Mathur, A. P., & Tippenhauer, N. O., "Swat: A Water Treatment Testbed for Research and Training on Ics Security," In 2016 International Workshop on Cyber-Physical Systems for Smart Water Networks (Pp. 31-36). Ieee.
<https://doi.org/10.1109/Cyswater.2016.7469060>, 2016.
22. McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P., "Ransomware Mitigation In The Modern Era: A Comprehensive Review, Research Challenges, And Future Directions," *Acm Computing Surveys*, Vol. 54, No. 9, Pp. Article 197.
<https://doi.org/10.1145/3479393>, 2021.
23. National Institute Of Standards and Technology, "Zero Trust Architecture (Special Publication 800-207)," U.S. Department of Commerce.
<https://doi.org/10.6028/Nist.Sp.800-207>, 2020.
24. National Institute Of Standards and Technology, "Developing CyberResilient Systems: A Systems Security Engineering Approach (Special Publication 800-160, Volume 2, Revision 1)," U.S. Department Of Commerce.

25. National Institute Of Standards and Technology, "Ransomware Risk Management: A Cybersecurity Framework Profile (Interagency Report 8374)," U.S. Department Of Commerce. <https://Doi.Org/10.6028/Nist.Sp.800-160v2r1>, 2021.
26. National Institute Of Standards and Technology, "Guide to Operational Technology Security (Special Publication 800-82, Revision 3)," U.S. Department of Commerce. <https://Doi.Org/10.6028/Nist.Sp.800-82r3>, 2023.
27. National Institute Of Standards and Technology. (2024a). The Nist Cybersecurity Framework (Csf) 2.0. U.S. Department of Commerce. <https://Doi.Org/10.6028/Nist.Cswp.29>.
28. Sun, Z., Xu, M., Schweitzer, K. M., Bateman, R. M., Kott, A., & Xu, S. (2023, July). Cyber attacks against enterprise networks: characterization, modeling and forecasting. In *International Conference on Science of Cyber Security* (pp. 60-81). Cham: Springer Nature Switzerland.
29. National Institute of Standards and Technology, "Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile (Interagency Report 8374, Revision 1)," U.S. Department Of Commerce, 2024.
30. Open Group, "Open Fair Body of Knowledge: Risk Analysis Standard," The Open Group, 2022.
31. Orlando, A, "Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk," Risks, Vol. 9, No. 10, Pp. 184. <https://Doi.Org/10.3390/Risks9100184>, 2021.
32. Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, E, "Scikit-Learn: Machine Learning In Python," Journal Of Machine Learning Research, Vol. 12, Pp. 2825-2830, 2011.
33. Ramotsoela, D. T., Hancke, G. P., & Abu-Mahfouz, A. M, "Attack Detection In Water Distribution Systems Using Machine Learning," Human-Centric Computing And Information Sciences, 9, 13. <https://Doi.Org/10.1186/S13673-019-0175-8>, 2019.
34. Rockafellar, R. T., & Uryasev, S, "Optimization of Conditional ValueAt-Risk," Journal of Risk, Vol. 2, No. 3, Pp. 21-42. <https://Doi.Org/10.21314/Jor.2000.038>, 2000.
35. Romanosky, S, "Examining The Costs And Causes Of Cyber Incidents," Journal of Cybersecurity, Vol. 2, No. 2, Pp. 121-135. <https://Doi.Org/10.1093/Cybsec/Tyw001>, 2016.
36. Rose, A, "Defining and Measuring Economic Resilience from A Societal, Environmental and Security Perspective," Springer, 2017.
37. Rossman, L. A., Woo, H., Tryby, M., Shang, F., Janke, R., & Haxton, T, "Epanet 2.2 User Manual," U.S. Environmental Protection Agency, 2020.
38. Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A, "Battle Of The Attack Detection Algorithms: Disclosing Cyber Attacks On Water Distribution Networks," Journal Of Water Resources Planning And Management, Vol. 144, No. 8, Pp. 04018048. [https://Doi.Org/10.1061/\(Asce\)Wr.1943-5452.0000969](https://Doi.Org/10.1061/(Asce)Wr.1943-5452.0000969), 2018.
39. U.S. Environmental Protection Agency, "Cybersecurity for the Water Sector," Epa, 2024.
40. World Bank, "A Review of the Economic Costs of Cyber Incidents," World Bank Group, 2024.
41. World Economic Forum, "Global Cybersecurity Outlook 2024," World Economic Forum, 2024.
42. Woods, D. W., Moore, T., & Simpson, A. C, "The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices," Digital Threats: Research and Practice, Vol. 2, No. 2, Pp. Article 14. <https://Doi.Org/10.1145/3436667>, 2021.

Cite This Article: Adebiyi Adisa, Olajide Dare, Isdore Ugochukwu Opara, Ekundayo Peter Buremoh, Stephen Sobulo (2024). Monte Carlo Quantification of Financial Loss from Ransomware-Induced Service Disruptions in Urban Water Treatment and Distribution Systems. *East African Scholars J Eng Comput Sci*, 7(9), 147-165.