International Journal of Scientific Research and Modern Education (IJSRME)
Impact Factor: 7.137, ISSN (Online): 2455 - 5630
(www.rdmodernresearch.com) Volume 6, Issue 2, 2021

CYBER INSURANCE EXCLUSIONS AND CORPORATE RECOVERY AFTER SUPPLY CHAIN ATTACKS

Kannan Vishwanath* & Lloyd Zulu**
* Fellow, Albert Schweitzer International Foundation, Karl-Löwe-Gasse 22/12, A-1120 Wien, Vienna, Austria
** World Christian University, Lusaka, Zambia

Cite This Article: Kannan Vishwanath & Lloyd Zulu, "Cyber Insurance Exclusions and Corporate Recovery After Supply Chain Attacks", International Journal of Scientific Research and Modern Education, Volume 6, Issue 2, Page Number 41-51, 2021.

Copy Right: © IJSRME, 2021 (All Rights Reserved). This is an Open Access Article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract:

This analysis examines how insurance protection and exclusion disputes intersect with corporate recovery after a global software supply chain attack. A descriptive comparative design combines 26 documentary evidence records across six multinational corporations affected by NotPetya, covering reporting periods from 2017 to 2020, with accounting reconciliation and claim chronology analysis. Operational restoration coexisted with continuing financial losses and incomplete reimbursement. Merck's recognized insurance recovery represented 13.6 percent of its identified gross expense component, while its adverse sales effect persisted into the following year. FedEx restored critical systems despite lacking applicable insurance. Mondelēz's complaint documented changes in coverage decisions without receipt of a promised advance. These contrasts distinguish contractual eligibility, claim administration and realized financial relief as separate dimensions of protection. The analysis refines risk transfer reasoning by separating operational restoration from financial loss persistence and insurance realization, without attributing causal effects to exclusions. The framework supports multinational risk management through separate monitoring of restoration milestones, residual losses and insurance receipts, alongside clearer disclosure of disputed and realized protection.

Key Words: Cyber Insurance; Supply Chain Attacks; Corporate Recovery; Insurance Exclusions; Comparative Case Analysis

1. Introduction:

A corporation can restore its information systems while continuing to absorb commercial losses and pursue disputed insurance claims. This separation matters after supply chain cyber attacks because technical disruption, business interruption and contractual indemnification concern different outcomes. Shared software dependencies can expose several organizations to the same attack, while insurance arrangements determine which financial consequences may transfer to insurers. Biener et al. (2015) identify interrelated losses, information asymmetries and limited data as obstacles to cyber risk insurability. These conditions make policy ownership an incomplete indicator of financial protection and operational restoration an incomplete indicator of corporate recovery.

Supply chain attacks sharpen this distinction by connecting technological dependence with financial exposure. Microsoft's account of NotPetya identifies malicious execution through the legitimate M.E.Doc software update process. The compromised distribution mechanism allowed trusted software infrastructure to become an attack channel. Its significance extends beyond individual organizations because firms can experience related disruption despite differences in their operations and insurance arrangements. This analysis uses that shared attack setting to examine how reported recovery outcomes differ across affected corporations, without assuming that every firm experienced an identical entry route or level of damage (Microsoft, 2017).

Cyber insurance research explains why transferring risk does not eliminate the need to manage it. Marotta et al. (2017) synthesize the contractual, technological and market conditions shaping cyber insurance. The Organisation for Economic Co-operation and Development (2017) identifies financial protection and incident response support as potential contributions of insurance while distinguishing them from security investment. The relevant theoretical expectation is therefore conditional: insurance can transfer eligible financial consequences when the incident falls within the contract and reimbursement becomes available. This expectation does not imply that insured firms necessarily restore operations faster or experience smaller total losses.

The closest empirical research establishes important elements of this problem but examines different objects. Romanosky et al. (2019) analyze insurance contracts, including coverage, exclusions, application questionnaires and pricing schedules. Their findings clarify how insurers define and assess protection. Eling and Wirfs (2019) examine actual cyber loss events and distinguish patterns relevant to estimating financial risk. These approaches illuminate contractual design and loss magnitude, respectively. However, the reviewed evidence does not establish how policy protection, documented claim decisions, restoration milestones and continuing business losses align within the same corporate incident. The gap addressed here concerns the

connection between these documentary measures rather than the existence of insurance contracts or cyber losses themselves.

Measurement determines whether that connection can be interpreted. Corporate disclosures may report lost sales, remediation expenditure, operating income effects, recognized insurance recoveries or claim amounts. These categories differ in accounting meaning and observation period. A claim threshold is not an exact realized loss, a promised advance is not a received payment, and a restoration milestone does not establish the end of commercial disruption. Romanosky (2016) documents the incomplete and heterogeneous nature of publicly available cyber incident cost information. This analysis addresses that measurement problem by preserving source classifications, reporting periods and accounting boundaries rather than combining unlike amounts into an aggregate recovery score.

This study aims to examine how documented insurance arrangements and exclusion decisions relate descriptively to corporate recovery after supply chain cyber attacks. The central research question asks what becomes visible when coverage, claim handling, operational restoration and financial consequences are examined together. Three objectives guide the analysis: identify reported coverage arrangements and insurance recoveries, examine the documented sequence of exclusion decisions, and compare restoration evidence with continuing expenses and business losses. These objectives support descriptive research questions rather than directional hypotheses requiring comparable outcomes and independent observations.

The empirical analysis draws on 26 evidence records across six multinational corporations affected by NotPetya: Maersk, FedEx through TNT Express, Merck, Mondelēz, Nuance and Saint Gobain. The records concern reporting periods from 2017 to 2020 and are supported by sources published through December 31, 2020. Corporate filings, announcements and claim documentation provide the evidence for case comparison and accounting reconciliation. The corporation and incident define the case; individual records represent distinct measures within that case. This design enables comparison of documented recovery dimensions while retaining the dependence created by a shared attack.

The findings contribute by distinguishing three outcomes that require separate interpretation: operational restoration, persistence of financial losses and realization of insurance reimbursement. FedEx reports restoration despite having no applicable insurance. Merck records partial reimbursement alongside continuing sales disruption. The Mondelēz claim documentation distinguishes changes in coverage decisions from payment availability. Together, these observations refine the application of risk transfer logic: contractual protection and realized financial relief must be evaluated separately, and neither can substitute for direct evidence of operational recovery.

The contribution is relevant to international corporate risk management because the cases involve multinational operations exposed to a common technological disruption. Its transferable insight concerns measurement and interpretation rather than an estimated difference between countries. Corporate decision makers can use the distinction to track restoration milestones, residual business losses and insurance receipts separately. Researchers can use it to specify which dimension of recovery an insurance measure is expected to explain. The analysis provides a bounded empirical basis for that distinction without attributing recovery outcomes causally to insurance exclusions.

2. Theory, Conceptual Framework and Research Question Development:

This analysis combines risk transfer logic with supply chain interdependence to examine insurance restrictions and corporate recovery after cyber attacks. Firms depend on external software and service providers whose security they cannot fully control. A compromised supplier can transmit disruption across otherwise separate organizations. Boyens et al. (2015) explain how limited visibility into technology development and distribution creates supply chain exposure. This mechanism establishes the setting for comparing insurance arrangements and recovery outcomes across affected firms.

Insurance transfers a defined portion of financial exposure to an insurer. Its contribution depends on whether the contract covers the incident, which losses qualify and whether reimbursement occurs. Corporate recovery includes restoring operations, managing remediation expenditure and reducing continuing business losses. Technical restoration and financial recovery remain distinct outcomes. Bartock et al. (2016) identify recovery planning, resource prioritization and restoration metrics as components of organizational resilience. Accordingly, this analysis examines operational restoration separately from financial consequences.

Coverage scope provides the first analytical dimension. Applicable insurance creates a contractual route to reimbursement, while policy limits and deductibles determine the boundaries of financial protection. The theoretical expectation is that applicable coverage can reduce the financial burden retained by the insured firm. However, coverage does not establish that reimbursement occurred or that operations recovered faster. The Organisation for Economic Co-operation and Development (2017) identifies insurance as a mechanism for financing cyber losses and supporting incident response. This analysis therefore compares documented coverage arrangements with recognized insurance recoveries without treating policy limits as payments.

- RQ1: What coverage arrangements and insurance recoveries are documented among the affected firms?

Exclusion invocation provides the second analytical dimension. An insurer may acknowledge an existing policy while disputing whether it covers a particular event. This separates the purchase of insurance from access to indemnification. An invoked war exclusion records a coverage position rather than a judicial determination that the exclusion applies. The Organisation for Economic Co-operation and Development (2020) identifies unclear coverage boundaries as a challenge in cyber insurance. This analysis examines documented exclusion decisions and their procedural sequence, including denial, withdrawal and renewed denial where recorded.

- RQ2: How are exclusion invocation and changes in coverage decisions documented within the available claim records?

Recovery outcomes provide the third analytical dimension. Remediation expenses represent resources committed to restoring systems and processes, whereas residual revenue and operating income losses capture continuing business consequences. Higher expenditure may reflect greater damage, a more extensive restoration effort or both. Its magnitude alone therefore does not establish recovery effectiveness. Dreyer et al. (2018) distinguish financial exposures and emphasize uncertainty and variation in cyber cost estimation. This analysis preserves the original measurement categories, currencies and reporting periods rather than combining unlike amounts into a single recovery score.

- RQ3: What patterns of operational restoration, remediation expenditure and continuing business losses appear in the available corporate disclosures?

The conceptual framework organizes the evidence around coverage arrangements, exclusion invocation and claim handling alongside five recovery measures: operational restoration time, residual revenue losses, remediation expenses, operating income losses and insurance recoveries. These are observed documentary measures rather than latent constructs or composite indices. The connection between insurance arrangements and recovery represents a theoretical expectation examined through descriptive case comparison. The research questions guide that comparison without imposing a directional relationship that the available records cannot establish.

3. Data:

This analysis uses corporate disclosures and claim documentation to examine insurance coverage, exclusion disputes and recovery after supply chain cyber attacks. Source identifiers, reporting periods, measurement units and evidence classifications provide a traceable basis for descriptive comparison.

3.1 Data Sources, Population and Sample Construction:

The target population comprises corporations affected by supply chain cyber attacks during 2010 to 2020. The accessible sampling frame consists of the organizations represented in the assembled documentary workbook. Selection follows the availability of identifiable disclosures concerning incident losses, insurance arrangements, claim decisions or operational restoration. The sample is purposive and does not represent a census of affected corporations.

The source corpus includes annual reports, quarterly filings, corporate announcements, technical analysis and an insurance complaint. Corporate filings provide financial and operational disclosures, while the complaint documents the policyholder's allegations concerning coverage decisions. Microsoft's technical account establishes the compromised software update mechanism associated with NotPetya at the attack level, without establishing an identical entry route for every affected firm.

The analytical sample contains six corporate cases associated with NotPetya: Maersk, FedEx through TNT Express, Merck, Mondelēz, Nuance and Saint Gobain. Maersk reports an estimated business impact range. FedEx provides financial impact estimates and restoration milestones. Merck reports adverse sales effects, remediation expenses and recognized insurance recoveries. Mondelēz provides recovery expenditure and claim documentation. Nuance reports expense components and subsequent reimbursements. Saint Gobain provides sales and operating income effects alongside a restoration date.

The workbook initially contains 34 evidence records across seven organizations. Applying a source publication cutoff of December 31, 2020, retains 27 records. One retained SolarWinds record concerns potential installations of vulnerable software rather than corporate loss or recovery. It remains contextual evidence and is excluded from the core recovery comparison. The resulting analytical sample contains 26 evidence records across six corporations. FedEx Corporation (2018), Merck & Co., Inc. (2019), Mondelēz International, Inc. (2018a), Nuance Communications, Inc. (2020), and Saint Gobain (2017) provide the principal corporate disclosures.

Table 1: Sample construction

Stage	Corporate Units	Evidence Records	Selection Rule
Assembled workbook	7	34	All documented evidence records
Records published by December 31, 2020	7	27	Exclude seven records supported by publications outside the cutoff

Stage	Corporate Units	Evidence Records	Selection Rule
Contextual SolarWinds evidence	1	1	Retain separately as exposure context
Core recovery comparison	6	26	Include financial, insurance, claim and restoration evidence
Unique identifiers in the core sample	6	26	No repeated evidence identifiers or identical complete records

The corporate incident is the case unit, while each evidence record represents a distinct reported measure. Multiple records from one corporation are not independent incidents. The data form a documentary case dataset with irregular reporting intervals rather than a balanced panel. Sixteen records relate to 2017, eight to 2018, one to 2019 and one to 2020. Calendar and fiscal reporting labels remain as disclosed.

Source access relies on public corporate websites, the United States Securities and Exchange Commission archive and a publicly hosted copy of the insurance complaint. Source identifiers connect each record to its URL and document location. Public accessibility does not imply an unrestricted reuse licence. Compilation metadata remain separate from the historical observation and publication periods.

3.2 Data Integration, Cleaning and Quality Assurance:

Integration uses standardized corporation names, attack names, evidence identifiers and source identifiers. The source identifier links multiple evidence records to their documentary reference. Corporation and attack identifiers group records into cases. Reporting periods and metric definitions distinguish repeated disclosures from separate observations.

The integration preserves the source hierarchy and evidential status. Corporate accounting disclosures remain distinct from management estimates and plaintiff allegations. The Mondelēz complaint supplies a claim threshold and a sequence of coverage decisions; these statements are classified as allegations rather than adjudicated findings. Technical reporting supplies attack context rather than corporate financial measurements. This distinction follows the different evidential functions of the complaint and Microsoft's technical analysis, as documented by Mondelēz International, Inc. (2018b) and Microsoft (2017).

Overlapping amounts remain separate and are not added. FedEx's initial quarterly estimate forms part of its subsequent first half estimate. Maersk's lower and upper estimates define one uncertainty interval rather than two losses. Saint Gobain's sales and operating income effects measure different consequences. Merck's expenses reported net of insurance are not reduced by the same recovery a second time.

Fiscal periods remain attached to their original labels. FedEx's fiscal 2018 observations include activity occurring during calendar 2017. Nuance's observations follow its fiscal reporting years. No annual interpolation or calendar conversion is applied. Monetary amounts remain in nominal USD millions or EUR millions, without currency conversion or inflation adjustment.

Unavailable information remains coded NR. An explicit statement that no insurance covers an incident receives zero for applicable coverage. Silence about an exclusion does not receive zero for exclusion invocation. The statement that incident costs were immaterial remains qualitative. Promised payments remain separate from recognized or received reimbursements.

The identifier check confirms 26 unique evidence identifiers and no identical complete records in the core sample. Large reported amounts remain unchanged because the sources describe material corporate disruptions. No trimming, winsorization, imputation or synthetic completion is applied.

3.3 Variable Measurement, Construction and Validation:

Insurance arrangements are represented through observed coverage statements, policy descriptions and documented claim decisions. Corporate recovery is represented through restoration evidence, residual revenue effects, remediation expenses, operating income effects and insurance recoveries. These measures remain separate rather than forming an aggregate recovery index.

Table 2: Variable dictionary

Variable or Indicator	Analytical Role	Definition and Construction	Source Identifier	Unit and Reporting Basis	Interpretation and Missingness
Applicable insurance coverage	Insurance descriptor	Explicit coverage statement or documented recovery attributable to the incident	S02, S04, S08, S09, S10	Binary or documentary statement	Zero requires explicit absence; otherwise NR when unreported
Policy type	Insurance descriptor	Reported category of insurance associated with the claim	S08	Categorical	Describes contractual form without assuming complete coverage
Exclusion invocation	Claim descriptor	Documented allegation that an insurer invoked a war exclusion	S08	Documentary indicator	Invocation does not establish legal applicability
Coverage decision	Claim process	Reported denial, withdrawal and renewed denial	S08	Dated events	Events remain within the same claim

Variable or Indicator	Analytical Role	Definition and Construction	Source Identifier	Unit and Reporting Basis	Interpretation and Missingness
sequence					
Operational restoration	Recovery outcome	Disclosed restoration milestone or return to normal operations	S03, S07, S11	Milestone or calendar days	Exact duration is calculated only from disclosed dates
Residual revenue loss	Recovery outcome	Reported adverse sales amount or revenue growth effect	S04, S05, S07, S11	USD millions, EUR millions or percentage points	Higher values indicate greater reported disruption; units remain separate
Remediation expenditure	Recovery outcome	Reported restoration costs, professional fees and related expense components	S04, S07, S09	USD millions by reporting period	Gross and net accounting bases remain identified
Operating income effect	Recovery outcome	Reported adverse effect on operating income	S11	EUR millions for the first half	Not added to sales losses
Insurance recovery	Recovery outcome	Recognized recovery, cash receipt or reimbursement	S04, S09, S10	USD millions by reporting period	Higher values indicate greater disclosed reimbursement
Claim loss threshold	Claim context	Reported losses exceeding a stated amount	S08	USD millions	A lower threshold is not treated as an exact loss
Equipment damage	Incident context	Reported numbers of affected servers and laptops	S08	Approximate equipment counts	Classified as plaintiff allegations
Estimated business impact	Incident context	Reported financial impact estimate or interval	S01, S02, S03	USD millions	Overlapping estimates and interval bounds are not aggregated

Derived calculations retain a narrow accounting interpretation. Merck's disclosed gross expense component equals USD 285 million of net expenses plus USD 45 million of insurance recoveries, producing USD 330 million. Dividing the recovery by that expense component gives 13.6 percent. This calculation excludes lost sales and does not represent a final claim settlement ratio.

Nuance's disclosed expense components total USD 26.1 million across the reported professional services, asset write down and restoration categories. Its reported reimbursements total USD 0.8 million across 2019 and 2020. These totals summarize the identified components rather than complete incident losses or lifetime insurance receipts.

Saint Gobain's disclosed dates yield 13 elapsed calendar days between June 27 and July 10, 2017. Maersk's estimated impact interval extends from USD 250 million to USD 300 million, with a width of USD 50 million. These constructions use disclosed inputs and retain their original measurement meaning.

Validation consists of checking identifiers, units, reporting periods, accounting bases and arithmetic consistency. No latent construct, reliability coefficient or factor structure is estimated. Pooled means across different loss categories would combine unlike measures and are therefore not reported.

Coverage is uneven across indicators. Within the six core cases, applicable insurance status is identifiable for four corporations and remains NR for two. Exclusion invocation is documented within the retained evidence for one corporation. Exact elapsed restoration time is available for one corporation. Positive insurance recoveries are reported for two corporations across three reporting periods. These counts describe documentary availability rather than the prevalence of coverage, exclusions or successful recovery.

3.4 Analytical Framework, Identification and Reproducibility:

The analysis uses descriptive case comparison to answer three questions: which insurance arrangements and recoveries are documented, how exclusion decisions develop within available claim records, and which operational and financial recovery patterns appear in corporate disclosures. The procedure compares measures only when their definitions, units and reporting periods permit interpretation.

No regression specification, causal estimator or statistical significance test is implemented. All six core corporations share the same attack family, so their experiences represent related exposures rather than independent cyber attack realizations. Differences in reported losses may reflect corporate scale, operational exposure, accounting treatment and disclosure practices. The analysis does not attribute these differences to insurance arrangements alone.

Claim process evidence and corporate recovery evidence remain analytically distinct. A disputed claim establishes a contractual disagreement but does not establish that the disagreement delayed system restoration. Similarly, an insurance receipt establishes reimbursement without proving that it financed a particular restoration activity. This separation follows the distinction between financial protection and operational resilience discussed by the Organisation for Economic Co-operation and Development (2017).

Reproducibility rests on the workbook's evidence identifiers, source identifiers, URLs, passage locations, reporting years, units and interpretation notes. The analytical selection applies two explicit rules: source publication must fall within the historical cutoff, and the core record must concern corporate financial consequences, insurance or restoration. Contextual exposure evidence remains separate.

The resulting framework supports transparent comparison of documented events and amounts. It preserves the distinction between observed values, estimates, allegations and calculated summaries, while avoiding unsupported aggregation or causal interpretation.

4. Methods:

4.1 Research Design and Analytical Scope:

This analysis uses a descriptive comparative case design to examine documented insurance protection, claim decisions and corporate recovery following NotPetya. The corporation and incident define the case, while individual evidence records represent reported financial amounts, contractual statements or restoration milestones. The design addresses three questions: what protection and reimbursement are documented, how exclusion decisions develop within available claim records, and how operational restoration compares with continuing financial consequences. Case comparison is appropriate for examining these related processes within their organizational settings, consistent with the methodological rationale described by Crowe et al. (2011).

The analytical sample comprises six corporations and 26 evidence records concerning reporting periods from 2017 to 2020. Table 1 documents selection, and Table 2 defines the measures. All retained sources were published by December 31, 2020. The sample permits comparison across documented experiences of a shared attack, but the common exposure does not make corporations equivalent in incident severity, resources or operational dependence. Differences are therefore interpreted as case characteristics rather than effects attributable to insurance arrangements.

The analytical target is the documented relationship between contractual protection, claim status, restoration and financial consequences. No treatment effect, predictive model or population parameter is estimated. Corporate scale, accounting practices and disclosure incentives remain competing explanations for differences in reported amounts. The interpretation consequently concerns the selected cases and their available records, without treating evidence records as independent incidents.

4.2 Documentary Classification and Comparative Procedure:

The procedure organizes evidence around the research questions using the measurement categories in Table 2. Each record retains its corporation, attack, observation period, metric, value, unit, source identifier, passage location and evidential status. Classification distinguishes corporate disclosures, management estimates, plaintiff allegations and calculated summaries. This separation preserves the purpose and status of each document. Dalglish et al. (2020) explain the importance of systematic extraction and contextual interpretation in document analysis; this analysis applies those principles through its structured evidence fields and source references.

Analysis proceeds within cases before comparison across cases. Within each corporation, records are arranged by the period or event date explicitly reported. Financial statements establish the accounting scope of amounts, while claim documentation supplies the reported sequence of coverage decisions. Dates describing different events remain distinct: incident occurrence, restoration, reporting and reimbursement are not treated as interchangeable.

The comparison then examines whether operational restoration, continuing losses and insurance realization appear together or at different reporting points. Contrasting cases are retained where they qualify a simple interpretation. Restoration without applicable insurance is considered separately from restoration accompanied by recognized reimbursement. A disputed claim is examined as a contractual process rather than evidence that the dispute caused operational delay.

Claim allegations remain attributed to the policyholder. Denial, withdrawal and renewed denial are recorded as separate events within the same claim, without converting their sequence into a judicial finding. A promised advance is not classified as received reimbursement. No independent coding agreement statistic is reported because the analysis did not implement a multiple coder assessment.

4.3 Accounting Reconciliation and Derived Measures:

Calculations are restricted to disclosed inputs with identifiable accounting relationships. Monetary amounts remain in nominal USD millions or EUR millions. Fiscal and calendar reporting periods retain their original labels. No currency conversion, inflation adjustment or annual interpolation is applied. For the Merck expense reconciliation, gross expenses and the recognized recovery share are calculated using Equation 1:

$$G = N + R, \qquad S = 100 \times \frac{R}{G}$$

Here, G denotes the disclosed gross expense component, N denotes expenses reported net of insurance, R denotes recognized insurance recovery, and S denotes that recovery as a percentage of the gross expense component. All monetary inputs share the same currency, reporting period and expense scope. The denominator excludes lost sales, so the result is neither a comprehensive loss recovery ratio nor a final settlement ratio. The reduction in Merck's annual adverse sales effect is calculated using Equation 2:

$$D = 100 \times \frac{L_{2017} - L_{2018}}{L_{2017}}$$

Here, D denotes the percentage reduction in the reported adverse sales effect, and L_{2017} and L_{2018} denote the corresponding disclosed amounts for the two calendar years. The calculation describes a change in reported disruption rather than total sales growth or an insurance effect. Elapsed restoration time is calculated only where both relevant dates are disclosed, using Equation 3:

$$T = d_{normal} - d_{attack}$$

Here, T denotes elapsed calendar days, d_{normal} denotes the reported date of return to normal operations, and d_{attack} denotes the attack date. Date subtraction excludes the starting day. This calculation is applied to Saint Gobain; milestone statements for other corporations are not converted into estimated durations.

Nuance's identified expense components and reimbursements are summed separately across their specified reporting periods. These totals retain the scope of the disclosed components and do not represent complete lifetime losses or payments. Maersk's lower and upper estimates remain the bounds of one interval. FedEx's initial quarterly impact is not added to the subsequent first half estimate because the periods overlap. Sales losses, operating income effects and remediation expenses are not combined into a single total.

4.4 Verification, Interpretation and Reproducibility:

Verification checks evidence identifiers, complete record duplication, units, reporting periods, source classifications and arithmetic consistency. The retained analytical records contain unique evidence identifiers and no identical complete rows. These checks establish internal consistency without implying that every source estimate is independently verified.

Unavailable information remains coded NR. Zero is used only where a source explicitly states the absence of applicable insurance. Silence about an exclusion does not establish that no exclusion existed. Qualitative statements of immaterial costs remain textual, and claim thresholds remain bounds rather than exact losses. No imputation, interpolation, trimming or winsorization is applied.

The numerical workflow uses Python 3.12.14 and lxml 6.1.1 to inspect workbook records, apply the publication cutoff, verify identifiers and calculate descriptive reconciliations. Excel formulas retain the workbook's supporting calculations. No stochastic procedure, optimization routine or random seed is required. Interpretation rests on documentary comparison and arithmetic, so standard errors, significance tests and regression diagnostics are not produced.

The publication cutoff and separation of contextual exposure evidence from recovery records define the final analytical sample. These restrictions were applied during manuscript development and are not presented as preregistered decisions. No alternative sample analysis or sensitivity estimate is claimed. Findings are assessed through consistency with the retained records, attention to contrasting cases and preservation of differences in measurement scope.

The workbook provides the evidence identifiers, source URLs, passage locations, definitions and calculation inputs needed to trace the reported comparisons. The method supports replication of the classifications and arithmetic, while access to original documents remains subject to their providers' terms. Its contribution is the transparent application of documentary comparison and accounting reconciliation to distinguish contractual protection, operational restoration and realized financial relief.

5. Findings:

This analysis examines documented insurance protection, exclusion decisions and corporate recovery across six firms affected by NotPetya. The findings distinguish operational restoration, continuing financial losses and insurance reimbursement. The evidence answers three descriptive research questions through case comparison and accounting reconciliation.

The analytical sample comprises 26 evidence records supported by sources published through December 31, 2020. Sixteen records concern 2017, eight concern 2018, and one each concern 2019 and 2020. These records represent different measures within six corporate cases rather than 26 independent incidents. Monetary values retain their original currencies and reporting periods. Estimates, recognized expenses, reimbursements and plaintiff allegations remain separate.

Table 3: Corporate evidence and measurement coverage

Corporate Case	Evidence Records	Principal Financial Measures	Insurance and Recovery Evidence
Maersk	2	Estimated business impact of USD 250 million to USD 300 million	Impact interval includes revenue loss, restoration and operational costs
FedEx through TNT Express	4	Estimated first half impact of USD 400 million in fiscal 2018	Explicit absence of applicable insurance; critical systems restored by fiscal second quarter
Merck	5	Adverse sales effects of USD 260 million in 2017 and USD 150 million in 2018	USD 45 million recognized insurance recovery; USD 285 million expenses net of recovery
Mondelēz	7	USD 84 million recovery expenses;	Main systems restored; disputed property

Corporate Case	Evidence Records	Principal Financial Measures	Insurance and Recovery Evidence
		adverse revenue growth effect of 0.4 percentage points	insurance claim
Nuance	5	USD 26.1 million across disclosed expense components	Reimbursements of USD 0.5 million in 2019 and USD 0.3 million in 2020
Saint Gobain	3	First half sales impact of EUR 220 million and operating income impact of EUR 65 million	Normal operations reported 13 elapsed calendar days after the attack

Applicable insurance status is identifiable for four firms. Three have documented coverage or incident related recoveries, while FedEx explicitly reports that no cyber or other insurance covered the attack. Coverage remains unreported in the retained evidence for two firms. An exclusion dispute is documented for one firm, and exact elapsed restoration time is available for one firm. These differences establish the limits of comparison: absence of disclosure cannot be interpreted as absence of insurance, exclusions or recovery.

The first finding concerns the distinction between insurance protection and realized financial relief. Merck recognized USD 45 million in insurance recoveries against manufacturing and remediation expenses reported at USD 285 million net of those recoveries. Adding the recovery back produces a disclosed gross expense component of USD 330 million. The recognized recovery therefore represents 13.6 percent of that component. This is an accounting reconciliation rather than a final settlement ratio, and it excludes the separate sales effect. Merck & Co., Inc. (2018) thus provides evidence of partial financial relief alongside a remaining expense burden.

Nuance records a different reimbursement pattern. Disclosed professional services expenses of USD 18.1 million and asset and inventory write downs of USD 4 million in fiscal 2017, together with USD 4 million in restoration expenses in fiscal 2018, total USD 26.1 million. The retained disclosures identify USD 0.5 million in insurance receipts during 2019 and USD 0.3 million in reimbursements during 2020. These observations establish that reimbursement continued into reporting periods beyond the initial disruption. They do not establish the date of the first payment or the complete insurance recovery. Nuance Communications, Inc. (2019, 2020) therefore supports a distinction between the reporting periods of restoration costs and subsequent reimbursements.

Table 4: Reconciled financial measures

Measure	Calculation	Result	Interpretation
Merck gross expense component in 2017	USD 285 million net expenses plus USD 45 million recoveries	USD 330 million	Disclosed expense component before recognized insurance recovery
Merck recognized recovery share	USD 45 million divided by USD 330 million	13.6 percent	Recovery relative to the identified expense component
Merck reduction in annual adverse sales effect	Difference between USD 260 million and USD 150 million, divided by USD 260 million	42.3 percent	Smaller reported sales disruption in 2018
Nuance disclosed expense components	USD 18.1 million plus USD 4 million plus USD 4 million	USD 26.1 million	Sum of identified components across fiscal 2017 and fiscal 2018
Nuance disclosed reimbursements	USD 0.5 million plus USD 0.3 million	USD 0.8 million	Reimbursements identified across fiscal 2019 and fiscal 2020
Saint Gobain elapsed restoration interval	July 10 less June 27, 2017	13 calendar days	Time to reported return to normal operations

FedEx provides a contrasting case. The corporation explicitly disclosed that no applicable insurance covered the attack. Nevertheless, its annual report states that all critical TNT Express operational systems had been restored by the second quarter of fiscal 2018. The estimated first half financial impact remained USD 400 million, principally reflecting reduced shipments and restoration costs. Operational restoration therefore occurred despite the absence of applicable insurance, while substantial financial consequences remained. This case prevents interpreting insurance coverage as a necessary condition for technical recovery, without establishing how coverage would have changed the outcome (FedEx Corporation, 2017, 2018).

The second finding concerns the difference between policy existence and payment availability. Mondelēz's complaint describes an existing property policy and alleges that Zurich denied coverage on June 1, 2018, withdrew that denial on July 18, and reasserted it on October 9. The complaint also describes a promised USD 10 million advance that had not been paid as alleged when proceedings commenced. The advance is therefore excluded from received insurance recoveries. The documentary finding is a sequence of contested

coverage decisions, rather than a determination that the exclusion legally applied or that the denial was wrongful (Mondelēz International, Inc., 2018b).

This sequence identifies claim adjustment as a separate observable process. Withdrawal of a denial did not, according to the complaint, translate into payment of the promised advance. Policy existence, a change in the insurer's stated position and cash receipt consequently represent different events. The evidence supports examining them separately when assessing the financial role of insurance.

The third finding concerns the separation of operational restoration from continuing business losses. Saint Gobain reported normal operations by July 10 following the June 27 attack, producing an elapsed interval of 13 calendar days. Its disclosure nevertheless identified adverse first half effects of EUR 220 million on sales and EUR 65 million on operating income. A short-reported restoration interval therefore coexisted with material financial damage. Sales and operating income effects remain separate because adding them would combine revenue disruption with a profit consequence (Saint Gobain, 2017).

Merck demonstrates persistence across annual reporting periods. Its adverse sales effect declined from USD 260 million in 2017 to USD 150 million in 2018, a reduction of USD 110 million, or 42.3 percent. However, the remaining USD 150 million reflected a residual order backlog. The company also characterized incident costs in 2018 as immaterial. The contrast shows that lower remediation expenses did not coincide with the disappearance of commercial disruption. The calculated reduction describes the change in the reported sales effect; it does not measure the contribution of insurance to recovery (Merck & Co., Inc., 2019).

Mondelēz reported restoration of its main operating systems alongside USD 84 million in incremental recovery expenses and an adverse revenue growth effect of 0.4 percentage points. Maersk reported a broader estimated impact of USD 250 million to USD 300 million, combining revenue loss, restoration and extraordinary operational costs. These disclosures reinforce the need to retain accounting scope when comparing firms. A larger reported amount may reflect broader measurement coverage rather than a slower or less effective recovery process (A.P. Møller - Mærsk A/S, 2018; Mondelēz International, Inc., 2018a).

Taken together, the cases establish three distinct documentary outcomes: insurance can provide partial financial relief, coverage decisions can remain contested, and operational restoration can coexist with continuing business losses. This distinction is consistent with the Organisation for Economic Co-operation and Development (2017), which treats insurance as one component of cyber risk management rather than a substitute for operational resilience. It also accords with Bartock et al. (2016), whose recovery guidance emphasizes restoration activities and functional recovery metrics.

The evidence answers the research questions through documented variation rather than estimated causal effects. Coverage and reimbursements differ across cases; the Mondelēz record identifies a contested sequence of coverage decisions; and the corporate disclosures distinguish restoration milestones from expense and revenue consequences. The central empirical contribution is the separation of technical restoration, financial loss persistence and insurance realization within the same comparative framework. The records support that distinction but do not identify whether insurance exclusions change recovery speed or total losses.

6. Discussion:

Restoring digital operations does not restore a firm's financial position. Tables 3 and 4 show that operational restoration, continuing business losses and insurance reimbursement follow distinct paths. FedEx restored critical systems despite having no applicable insurance, while Merck recorded partial reimbursement alongside residual sales disruption. These contrasting cases refine risk transfer logic by separating the capacity to resume operations from the contractual allocation of financial consequences. Marotta et al. (2017) examine insurance as a response to residual cyber risk; this analysis adds a comparative account of how restoration milestones and financial relief can diverge within the same incident. Its contribution is this documented distinction, rather than an estimated relationship between insurance and recovery speed

The Mondelēz evidence identifies claim adjustment as a process between policy ownership and payment realization. Table 3 distinguishes an existing insurance contract from a contested claim, while the documented sequence separates denial, withdrawal and renewed denial. According to the complaint, withdrawal of the initial denial did not produce the promised advance. This sequence makes the contractual process visible without establishing a causal mediation pathway. Romanosky et al. (2019) identify variation in exclusions across insurance policies. The present analysis extends that contractual perspective by showing why a change in the insurer's stated coverage position must be distinguished from actual reimbursement. Policy wording and claim administration therefore represent related but separate elements of financial protection.

The accounting reconciliation in Table 4 further distinguishes financial relief from comprehensive loss absorption. Merck's recognized recovery represents 13.6 percent of its identified gross expense component, while the separate sales effect remains outside that denominator. This proportion measures the scope of disclosed reimbursement against a defined expense category; it cannot identify the contribution of insurance to total recovery. Nuance's expense components and subsequent reimbursements likewise describe different reporting periods rather than a complete settlement account. Eling and Wirfs (2019) demonstrate the importance of distinguishing ordinary and extreme cyber losses when estimating risk. This analysis adds that even within a

single corporate case, interpretation depends on whether the measure captures expenses, revenue disruption or reimbursement. The theoretical implication is that risk transfer must be assessed against an explicit loss boundary.

The differences across Table 3 also reveal a constraint on evaluating insurance governance: documentary availability varies by outcome. Exact restoration time appears for one firm, whereas recognized reimbursements and exclusion decisions are available for different subsets. These records describe different aspects of recovery and cannot be combined into a common performance score. Woods and Moore (2020) examine how market dynamics constrain the governance role of cyber insurance. The corporate evidence adds a measurement implication: evaluating that role requires distinguishing contractual protection, operational response and realized financial relief. Treating policy ownership as an indicator of recovery effectiveness would obscure these differences and could attribute to insurance outcomes that the records do not connect to it.

The international relevance lies in the common attack affecting corporations with different operations and financial reporting practices, rather than in an estimated difference between national economies. Tables 3 and 4 show why comparisons require consistent definitions before differences in reported amounts can be interpreted. Romanosky et al. (2019) investigate insurance contracts filed in the United States, whereas this analysis follows documented corporate consequences across multinational organizations. The comparison shifts attention from the availability of contractual protection to its realization alongside operational recovery. Decision makers should therefore track restoration milestones, continuing revenue effects and insurance receipts separately, and record changes in claim status without counting promised advances as available funds. Future comparative research can build on this framework by linking dated restoration and payment records to consistent loss categories.

7. Conclusion and Implications:

A global cyber attack can end operationally while its financial consequences remain unsettled. This analysis shows that contractual protection, claim decisions and reimbursement must be interpreted alongside restoration and continuing business losses. Their coexistence across corporate cases reveals why neither system recovery nor policy ownership establishes financial recovery. The contribution is a comparative framework that separates these outcomes while preserving their accounting and documentary boundaries. This distinction refines risk transfer reasoning by treating protection as a contractual arrangement whose financial realization requires separate evidence. For managers, the findings support maintaining restoration plans and liquidity arrangements without assuming that disputed or promised payments will become available when expenditure occurs. Finance and technology teams should reconcile incident expenses, residual commercial disruption and recognized reimbursements through a shared reporting process. Insurance purchasers should examine exclusion wording and document claim decisions separately from payment receipts. For policymakers, the evidence supports clearer disclosure categories that distinguish coverage, disputed amounts and realized indemnification, enabling more interpretable comparisons across organizations. These practices could improve accountability and help firms plan continuity expenditure during disruption. The international significance lies in a transferable method for assessing recovery across interconnected businesses, while recognizing that the cases establish documentary patterns rather than causal effects.

The purposive sample and shared attack setting create opportunities for broader comparative testing. Future research should assemble linked policy, payment and restoration records across multiple attack families and jurisdictions. Consistent reporting periods and loss definitions would permit more reliable comparison of financial consequences. Dated claims and payment histories could establish the timing of reimbursement relative to restoration expenditure. Longitudinal designs could examine whether contractual restrictions predict recovery outcomes after accounting for incident severity, organizational resources and operational exposure. Such extensions would test the framework's applicability across institutional settings and distinguish contractual effects from differences in damage and response capacity.

References:

1. A.P. Møller - Mærsk A/S. (2018). Annual report 2017. https://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf
2. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). Guide for cybersecurity event recovery (NIST Special Publication 800-184). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184
3. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance, Issues and Practice, 40(1), 131-158. https://doi.org/10.1057/gpp.2014.19
4. Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015). Supply chain risk management practices for federal information systems and organizations (NIST Special Publication 800-161). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161

5. Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. BMC Medical Research Methodology, 11, Article 100. https://doi.org/10.1186/1471-2288-11-100
6. Dalglish, S. L., Khalid, H., & McMahon, S. A. (2020). Document analysis in health policy research: The READ approach. Health Policy and Planning, 35(10), 1424-1431. https://doi.org/10.1093/heapol/czaa064
7. Dreyer, P., Jones, T. M., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). Estimating the global cost of cyber risk: Methodology and examples (Research Report RR-2299-WFHF). RAND Corporation. https://doi.org/10.7249/RR2299
8. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3), 1109-1119. https://doi.org/10.1016/j.ejor.2018.07.021
9. FedEx Corporation. (2017). Quarterly report for the quarter ended August 31, 2017. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1048911/000156459017018835/fdx-10q_20170831.htm
10. FedEx Corporation. (2018). Annual report for the year ended May 31, 2018. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1048911/000156459018016877/fdx-10k_20180531.htm
11. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. Computer Science Review, 24, 35-61. https://doi.org/10.1016/j.cosrev.2017.01.001
12. Merck & Co., Inc. (2018). Annual report for the year ended December 31, 2017. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/310158/000031015818000005/mrk1231201710k.htm
13. Merck & Co., Inc. (2019). Annual report for the year ended December 31, 2018. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/310158/000031015819000014/mrk1231201810k.htm
14. Microsoft. (2017, June 27). New ransomware, old techniques: Petya adds worm capabilities. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
15. Mondelēz International, Inc. (2018a). Annual report for the year ended December 31, 2017. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1103982/000119312518037332/d466496d10k.htm
16. Mondelēz International, Inc. (2018b, October 10). Complaint, Mondelēz International, Inc. v. Zurich American Insurance Company, No. 2018L011008. Circuit Court of Cook County, Illinois. https://regmedia.co.uk/2022/11/02/pacer_mondelez_zurich_complaint.pdf
17. Nuance Communications, Inc. (2019). Annual report for the year ended September 30, 2019. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1002517/000100251719000039/nuan0930201910-k.htm
18. Nuance Communications, Inc. (2020). Annual report for the year ended September 30, 2020. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1002517/000100251720000058/nuan0930202010-k.htm
19. Organisation for Economic Co-operation and Development. (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing. https://doi.org/10.1787/9789264282148-en
20. Organisation for Economic Co-operation and Development. (2020). Encouraging clarity in cyber insurance coverage. OECD Publishing. https://doi.org/10.1787/40beab07-en
21. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135. https://doi.org/10.1093/cybsec/tyw001
22. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? Journal of Cybersecurity, 5(1), Article tyz002. https://doi.org/10.1093/cybsec/tyz002
23. Saint-Gobain. (2017, July 27). Saint-Gobain: H1-2017 results. PR Newswire. https://www.prnewswire.com/news-releases/saint-gobain-h1-2017-results-636988613.html
24. Woods, D. W., & Moore, T. (2020). Does insurance have a future in governing cyber security? IEEE Security & Privacy, 18(1), 21-27. https://doi.org/10.1109/MSEC.2019.2935702