DAAS LABS

SCIKIQ
contextualizing data

CYBER INSURANCE

Contents

Know about Author

Gaurav Shinh is a passionate and accomplished data engineering professional with a remarkable 25-year career in the world of data. Gaurav's journey has been fuelled by his insatiable curiosity and profound understanding of the transformative power of data.

As a true thought leader and hands-on practitioner, Gaurav's unwavering commitment to data-driven transformations and extensive expertise have propelled organizations towards unparalleled success.

As the founder of **DaasLabs (https://daaslabs.ai/)**, Gaurav has built an exceptional services organization renowned for its expertise in solving complex data challenges using cutting-edge technologies such as Data Technologies, AI, NLP, and Computer Vision.

DaasLabs has established a strong global presence, catering to esteemed clients across various industries, including renowned financial institutions, insurance providers, and multinational corporations such as Barclays, American Express, Saxo Bank, PCBB Bank, Guardian Insurance, ZS Associates, GE Power, Nykaa, and ECU Worldwide, among others.

By simplifying and transforming the data journey, DaasLabs empowers organizations to make informed decisions, optimize operations, identify new revenue streams, enhance customer experiences, and foster innovation. Gaurav's true passion lies in unlocking the full potential of businesses' data.

His pioneering creation, **SCIKIQ (https://scikiq.com/),** a ground-breaking, first-generation, no-code business data platform, revolutionizes data utilization for medium to large organizations. SCIKIQ empowers business teams to access and utilize real-time data without the need for complex technical expertise, enabling operational efficiency, revenue generation, and a competitive advantage while retaining full control over invaluable data assets.

With a remarkable track record and a solid pedigree, including an **Engineering** (Honors) degree and an **MBA** from the prestigious Rotman School of Management, Gaurav is a true techno-commercial professional. His commitment to data-driven transformations and innovative solutions positions him as a thought leader in the industry.

Connect with Gaurav Shinh on **LinkedIn** at **https://www.linkedin.com/in/gauravshinh/** to learn more about his extraordinary contributions to the data management industry.

Introduction

In today's digital landscape, the need for robust cyber insurance capabilities has never been greater. This document serves as a comprehensive guide, drawing from the collective experiences of data practitioners who have tackled complex data challenges across the globe. By providing valuable insights and recommendations, we aim to empower organizations in building a strong foundation for their cyber insurance endeavors.

Executive Summary

The world of cyber insurance is evolving rapidly, presenting both opportunities and challenges for organizations. This document offers a holistic overview of the essential components required to establish a successful cyber insurance capability. From understanding the market size and underwriting frameworks to exploring data views, high-level data models, and data domain views, organizations can gain valuable insights into effectively managing and analyzing data in the cyber insurance domain.

Additionally, we delve into the role of SCIKIQ, a cutting-edge no-code data fabric platform, in streamlining the implementation process. With its unique capabilities, SCIKIQ empowers organizations to overcome the traditional barriers associated with building a cyber insurance capability, enabling rapid time-to-value and efficient data management.

By leveraging the expertise and practitioner-oriented perspectives shared in this document, organizations can navigate the complexities of the cyber insurance landscape, enhance their decision-making processes, and unlock new opportunities for growth and resilience.

Key Takeaways

1. **Cyber Insurance Market Size:** The document delves into the size of the cyber insurance market, highlighting its significance and potential for growth. Understanding the market size provides organizations with insights into the opportunities and challenges associated with offering cyber insurance products.

2. **Framework for Underwriting Cyber Insurance:** A framework for underwriting cyber insurance is discussed, providing an overview of the key factors, guidelines, rules, and adjustments involved in assessing risk and determining policy terms. This framework forms the basis for effective underwriting processes in the cyber insurance domain.

3. **Data View for Cyber Insurance**: The document explores the data view specific to cyber insurance, identifying the essential data entities and attributes necessary for capturing and managing information related to insured entities, policies, channels, KYC, underwriting factors, guidelines, rules, models, claims, payments, and more. This data view aids in effective data management and analysis in the context of cyber insurance.

4. **High-Level Data Model for Cyber Insurance Company:** A high-level data model is presented, showcasing the relationships and dependencies among various data entities in a cyber insurance company. This model provides a conceptual framework for organizing and structuring data, enabling efficient data management, and facilitating business processes.

5. **Data Domain View**: The document outlines the data domain view, focusing on the specific data domains and tables necessary for capturing and aligning data to business processes in the cyber insurance domain. The data domains include insured entities, products, policies, channels, KYC, underwriting factors, guidelines, rules, models, claims, payments, coverage, audits, agents, and more. This view helps organizations understand the data attributes and entities involved in cyber insurance operations.

6. **SCIKIQ's Role in Cyber Insurance Implementation:** The document highlights how SCIKIQ, a no-code data fabric platform, can support organizations in building their cyber insurance capabilities. It emphasizes SCIKIQ's advantages, such as its no-code approach, native support for data domain and data vault models, simplified Medallion architecture creation, comprehensive end-to-end solution, and rapid time-to-value. By leveraging SCIKIQ, organizations can streamline their implementation process and effectively manage their cyber insurance operations.

Note: This document is intended for informational purposes only and does not constitute professional advice. The information presented in this document is based on industry research, practitioner experiences, and public sources. Organizations should conduct their own analysis and consult with professionals to determine the most suitable data strategy for their specific business needs.

What is Cyber Insurance?

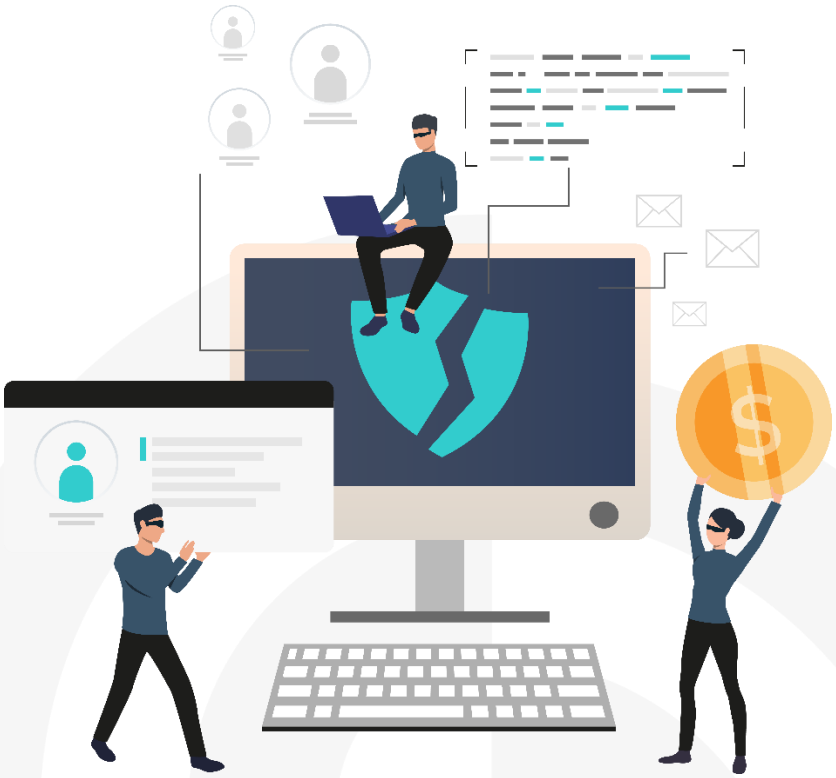
Cyber insurance, also known as cyber liability insurance or cyber risk insurance, is a type of insurance coverage designed to protect businesses and individuals against the financial losses and liabilities associated with cyber threats and incidents. It provides coverage for various risks related to cyber-attacks, data breaches, and other cyber-related incidents.

Cyber losses can vary significantly depending on the nature and scale of the incidents. According to a report by the research firm Cybersecurity Ventures, cybercrime was projected to cost the world **$6 trillion annually in 2021.** This figure includes direct damage costs, such as financial losses and the cost of remediation, as well as indirect costs, such as reputational damage and loss of customer trust.

Cyber insurance policies typically offer a range of coverages, which may include:

1. **Data Breach Response:** This coverage helps cover the costs associated with responding to a data breach, including forensic investigations, notifying affected individuals, credit monitoring services, and public relations efforts.
2. **Data Loss and Restoration**: This coverage helps cover the costs of recovering lost or damaged data, restoring systems and networks, and mitigating the impact of data loss.
3. **Business Interruption:** This coverage provides compensation for financial losses resulting from a cyber attack that disrupts business operations, leading to revenue loss or increased expenses.
4. **Cyber Extortion:** This coverage helps protect against losses resulting from extortion attempts, such as ransomware attacks, where hackers demand a payment to release encrypted data or prevent a cyber attack.
5. **Third-Party Liability:** This coverage helps protect against legal liabilities arising from a cyber incident, including claims for privacy violations, intellectual property infringement, defamation, or negligence.
6. **Regulatory Compliance:** This coverage assists in covering the costs of fines, penalties, or legal expenses resulting from non-compliance with data protection and privacy regulations.

What is the size of Cyber Insurance Market?



The cyber insurance market has been growing rapidly in response to the increasing threat landscape. Research and consulting firms have provided estimates of its size, but these figures may vary depending on the methodology and scope of the analysis.

1. According to a report by **Market Research Future**, the global cyber insurance market was projected to reach a value of $16.85 billion by 2023, growing at a compound annual growth rate (CAGR) of 24.38% during the forecast period from 2018 to 2023. This indicates a significant growth opportunity for the cyber insurance industry in the coming years (Source: Market Research Future).

2. A study by **Allied Market Research** estimated that the global cyber insurance market would reach $22.84 billion by 2026, with a compound annual growth rate (CAGR) of 27.7% from 2019 to 2026. This forecast suggests a substantial increase in the adoption of cyber insurance policies as businesses recognize the importance of protecting themselves against cyber risks (Source: Allied Market Research).

It's worth noting that these figures represent global estimates and the market size may vary across regions and countries.

Underwriting Framework for Cyber Insurance

Investing in data management and analytics empowers organizations to navigate the insurance industry effectively. Historical data provides a foundation for analysis, while future estimates shape business strategies. Industry outlooks offer insights into specific markets, and monitoring dark web activities detects potential risks. Staying updated with trends helps adapt to changes. By adopting a comprehensive approach, organizations make informed decisions, mitigate risks, and capitalize on opportunities in insurance.

To effectively underwrite cyber insurance, organizations should follow a structured approach:

1. **Data Sources**: Obtain historical data on cyber incidents and company-specific data to assess risks accurately.
    a. **Historical Data**: Obtain historical data on cyber incidents from reputable breach databases, industry reports, cybersecurity vendors, and incident response organizations.
    b. **Company-Specific Data**: Collect detailed information about the potential insured company's cybersecurity posture, including security controls, incident response plans, employee training, and any past incidents or claims.

2. **Data Pipeline**: Establish a data collection process that captures relevant data periodically, ensuring accuracy and timeliness.
    a. **Data Collection**: Implement a data collection process that periodically captures and updates relevant data from trusted sources. Automate the collection process where possible to ensure timeliness and accuracy.
    b. **Data Cleaning and Validation:** Develop procedures to clean and validate the collected data, ensuring consistency and eliminating outliers or erroneous entries.

c. **Data Storage and Management**: Establish a secure and centralized data storage system with appropriate access controls to store and manage the collected data effectively.

3. **Risk Modeling:** Develop actuarial models specific to cyber risks, considering key factors and estimating potential losses.
    a. **Actuarial Models**: Develop actuarial models specific to cyber risks, incorporating statistical techniques, machine learning algorithms, and relevant actuarial methods.
    b. **Model Inputs**: Identify and include key factors in the risk model, such as industry type, company size, revenue, geographical location, cybersecurity controls maturity, employee training effectiveness, and incident response capabilities.
    c. **Loss Estimation**: Utilize the risk model to estimate potential cyber losses by simulating various cyber event scenarios, considering factors such as data breach costs, business interruption expenses, incident response costs, legal and regulatory fines, reputational damage, and public relations expenses.

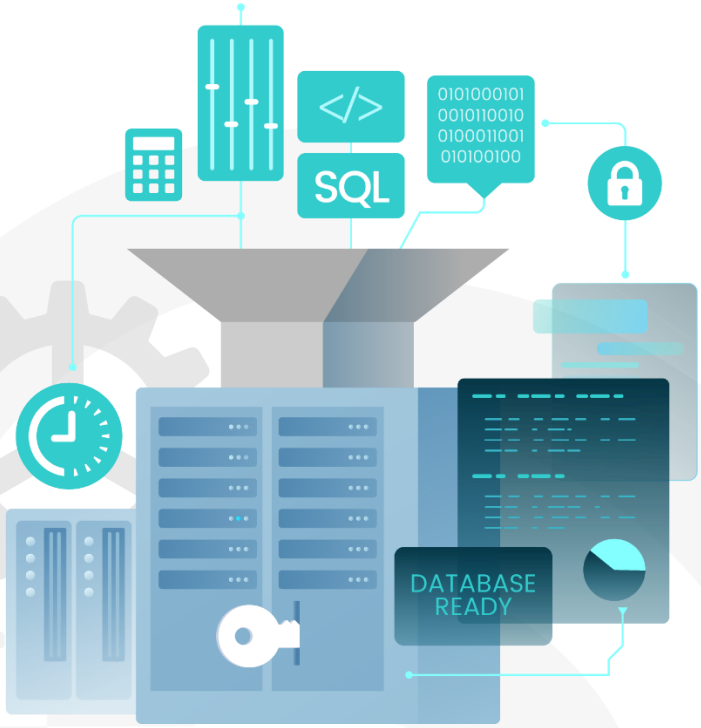
4. **Factors for Forward Look**: Stay updated on emerging threats, regulatory changes, and technological trends to assess future risks.
    a. **Emerging Threat Intelligence**: Stay updated on emerging cybersecurity threats by leveraging threat intelligence feeds, cybersecurity research organizations, and information sharing platforms.
    b. **Regulatory Landscape:** Monitor changes in cybersecurity regulations, compliance requirements, and legal frameworks to assess their impact on insured companies' risk exposure and potential claim costs.
    c. **Technology Trends**: Stay informed about technological advancements, such as cloud computing, IoT, AI, and their associated risks, to evaluate their implications on cyber insurance underwriting.

5. **Quantitative Factors for Adjustments:** Use risk assessment questionnaires, loss control recommendations, and external risk scoring to adjust premiums and coverage.
    a. **Risk Assessment Questionnaires:** Develop comprehensive risk assessment questionnaires tailored to different industries to gather detailed information about potential insured companies' risk profiles.
    b. **Loss Control Recommendations:** Provide insured companies with risk mitigation recommendations based on their risk assessment results to improve their cybersecurity posture. Adjust premiums or coverage based on the implementation of recommended measures.
    c. **External Risk Scoring:** Utilize external risk scoring services or industry benchmarks to assess the insured company's risk exposure compared to peers in the same industry. Adjust premiums based on the relative risk level.

6. **Continual Improvement:** Customize the framework to meet organizational needs, monitor the evolving risk landscape, update models, and refine underwriting processes.

By following this framework and adapting it to their specific circumstances, organizations can enhance their underwriting accuracy and responsiveness in the dynamic field of cyber insurance.

Building a Data-Centric Framework for Cyber Insurance



Investing in data management and analytics, can enhance an organization's ability to effectively manage cyber insurance risks. The below data led approach can be adapted to the cyber insurance domain to assess and quantify potential losses associated with cyber risks.

1. **Historical Data:**

    a. **Purpose**: Historical data sources store information on past cyber incidents, claims, losses, and other relevant factors to support analysis and modeling for calculations in cyber insurance.
    b. **Approach**: Internal systems, incident databases, claims management systems, and historical records are used to gather cyber-related data. Data extraction, transformation, and loading processes are employed to consolidate and organize the data for analysis.
    c. **Methodology**: The methodology involves assessing historical data to estimate potential credit losses associated with cyber risks. This includes analyzing past cyber incidents, claim amounts, claim frequencies, and other relevant factors to determine loss estimates for future periods.

2. **Future Estimates:**

    a. **Purpose**: Future estimates sources provide insights into projected cyber risks, claim frequencies, severity, and potential losses based on predictive modeling and forecasting.
    b. **Approach**: Predictive models, machine learning algorithms, and actuarial methods are utilized to generate future estimates in the context of cyber insurance. These models consider historical data, emerging cyber threats, evolving technology, and market trends.

c. **Methodology**: Future estimates are developed by analyzing historical data and incorporating external factors such as industry trends, regulatory changes, and technological advancements. The approach helps forecast potential losses based on the projected cyber risk landscape.

3. Industry and Segment Outlook:

a. **Purpose**: Industry and segment outlook sources provide data and insights on emerging cyber threats, industry-specific risks, and regulatory developments relevant to cyber insurance.
b. **Approach**: External sources, market research reports, industry publications, and collaborations with cybersecurity experts are employed to gather industry and segment-specific data.
c. **Methodology**: Market research methodologies, surveys, data analysis, and expert opinions are utilized to collect, analyze, and interpret industry-specific data. This information is integrated into the approach to enhance risk assessments and loss projections.

4. Dark Web Activities:

a. **Purpose**: Monitoring dark web activities helps identify potential cyber risks, data breaches, and emerging threats relevant to cyber insurance.
b. **Approach**: Specialized tools, threat intelligence platforms, and dark web monitoring services are employed to scan and analyze dark web marketplaces and forums.
c. **Methodology**: Dark web monitoring involves automated processes, data scraping, and artificial intelligence algorithms to detect mentions of relevant keywords, compromised data, or illegal activities related to cyber risks. This information is used to enhance the approach by incorporating the evolving threat landscape.

5. **Trends**:

a. **Purpose**: Monitoring trends in the cybersecurity landscape helps identify emerging risks, evolving attack vectors, and technological advancements relevant to cyber insurance.
b. **Approach**: Tracking industry news, cybersecurity reports, threat intelligence feeds, and research publications helps identify emerging trends and developments.
c. **Methodology**: Trend analysis involves data collection, data mining, statistical analysis, and pattern recognition techniques to identify evolving cyber threats, changing attack patterns, and technological advancements. This information is used to enhance the approach by incorporating the latest trends and developments.

By adopting the approach and leveraging data management and analytics practices, organizations can enhance their ability to assess and manage cyber insurance risks effectively. Utilizing historical data, future estimates, industry and segment outlooks, dark web monitoring, and trend analysis within the framework enables organizations to make informed decisions, allocate appropriate reserves, and mitigate potential losses associated with cyber risks.

Designing a High-Level Data Model for a Cyber Insurance Company

We will leverage data vault approach to enable the capture and alignment of cyber and process data to the business process. The data vault approach offers several advantages for identifying business entities in the modeling process of cyber insurance:

1. **Scalability**: The data vault model allows for easy scalability as new business entities or data sources can be incorporated without disrupting the existing structure. This flexibility is crucial in the ever-evolving landscape of cyber insurance, where new risks and entities constantly emerge.
2. **Traceability**: The data vault approach emphasizes traceability, providing a clear lineage of data from its source to the final analysis. This traceability enables better governance and auditing capabilities, ensuring transparency and accountability in the modeling process.
3. **Business Agility**: With its hub and satellite structure, the data vault approach allows for agile modeling and analysis. Business entities can be easily modified or added, facilitating quick adaptations to changing business needs and requirements in the cyber insurance domain.
4. **Data Consistency**: The data vault model ensures data consistency by separating business entities into hubs and capturing relationships through link tables. This structure prevents data redundancy and anomalies, enhancing data quality and accuracy for modeling purposes.
5. **Future Proofing**: By organizing data based on business entities, the data vault approach future-proofs the modeling process. As new data sources, regulations, or industry standards emerge, the existing data vault structure can adapt and accommodate these changes seamlessly.

The table below outlines a comprehensive list of hub and satellite tables for storing various types of information in a data management system. These tables cover a wide range of areas, including product, channel, KYC, underwriting guidelines and rules, predictive models, policy-related data, claims, payments, coverage, audits, agents, and more. The tables are designed to capture specific data attributes and facilitate efficient data management and analysis in the insurance domain.

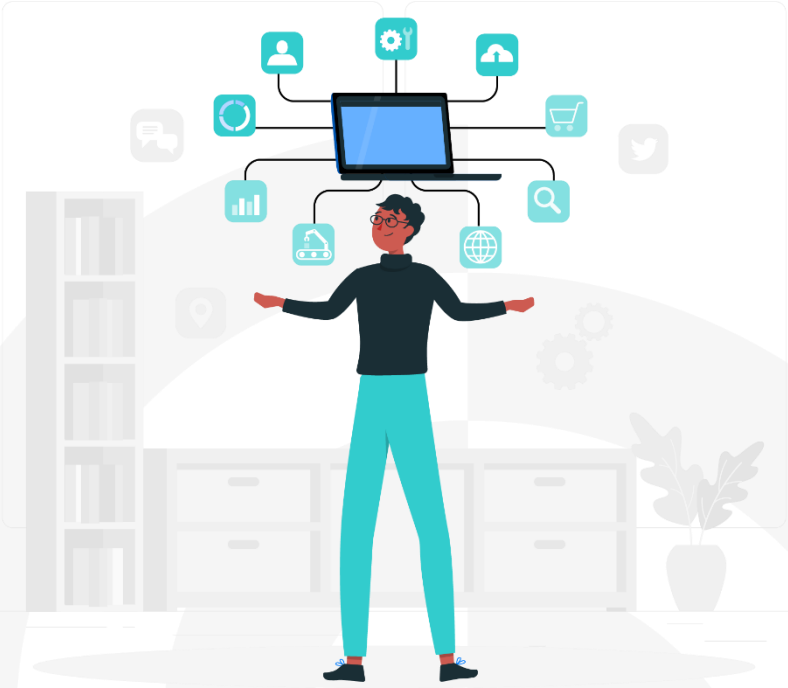
Hub/Satellite/Link Name	Description	Data Attributes
ProductHub	Table for storing product information	ProductID (Surrogate Key), ProductName, ProductType, ...
ChannelHub	Table for storing channel information	ChannelID (Surrogate Key), ChannelName, ChannelType, ...
KYCHub	Table for storing KYC information	KYCID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), KYCDate, ...
GuidelinesHub	Table for storing underwriting guidelines	GuidelinesID (Surrogate Key), GuidelinesDescription, ...
RuleHub	Table for storing underwriting rules	RuleID (Surrogate Key), RuleName, RuleDescription, ...
FactorHub	Table for storing underwriting factors	FactorID (Surrogate Key), FactorName, FactorType, ...
ModelHub	Table for storing predictive models	ModelID (Surrogate Key), ModelName, ModelType, ...
ModelOutputSatellite	Satellite table for storing model output	OutputID (Surrogate Key), ModelID (Foreign Key to Model), OutputName, OutputValue, ...
ApplicationHub	Table for storing application information	ApplicationID (Surrogate Key), PolicyID (Foreign Key to Policy), ApplicationDate, ...
PolicyIssuanceHub	Table for storing policy issuance information	PolicyIssuanceID (Surrogate Key), PolicyID (Foreign Key to Policy), IssuanceDate, ...
EndorsementHub	Table for storing policy endorsement information	EndorsementID (Surrogate Key), PolicyID (Foreign Key to Policy), EndorsementDate, ...
RenewalHub	Table for storing policy renewal information	RenewalID (Surrogate Key), PolicyID (Foreign Key to Policy), RenewalDate, RenewalStatus, ...
ClaimHub	Table for storing claim information	ClaimID (Surrogate Key), PolicyID (Foreign Key to Policy), ClaimNumber, ClaimDate, ...
LossLink	Link table for connecting loss information to other entities	LossID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), AssetID (Foreign Key to Asset), EventID (Foreign Key to Event), LossAmount, LossDate, ...

AdjustmentLink	Link table for connecting adjustment information to other entities	AdjustmentID (Surrogate Key), LossID (Foreign Key to Loss), AdjustmentFactor, AdjustmentType, ...
PremiumLink	Link table for connecting premium information to other entities	PremiumID (Surrogate Key), PolicyID (Foreign Key to Policy), PremiumAmount, PremiumDate, ...
ClaimLossLink	Link table for connecting claim and loss information	ClaimLossID (Surrogate Key), ClaimID (Foreign Key to Claim), LossID (Foreign Key to Loss), ClaimLossAmount, ...
InvoiceHub	Table for storing invoice information	InvoiceID (Surrogate Key), PolicyID (Foreign Key to Policy), InvoiceNumber, InvoiceDate, ...
PaymentHub	Table for storing payment information	PaymentID (Surrogate Key), InvoiceID (Foreign Key to Invoice), PaymentAmount, PaymentDate, ...
CoverageHub	Table for storing coverage information	CoverageID (Surrogate Key), CoverageName, CoverageType, ...
ClaimDetailsHub	Table for storing claim details information	ClaimDetailsID (Surrogate Key), ClaimID (Foreign Key to Claim), PolicyID (Foreign Key to Policy), ...
AuditHub	Table for storing audit information	AuditID (Surrogate Key), TableName, RecordID, FieldName, OldValue, NewValue, ModifiedBy, ...
AgentHub	Table for storing agent information	AgentID (Surrogate Key), AgentName, AgentType, ...
UnderwritingHub	Table for storing underwriting information	UnderwritingID (Surrogate Key), PolicyID (Foreign Key to Policy), UnderwriterID, UnderwritingDate, UnderwritingDecision, ...
BillingHub	Table for storing billing information	BillingID (Surrogate Key), PolicyID (Foreign Key to Policy), BillingAmount, BillingDate, ...
DisputeHub	Table for storing dispute information	DisputeID (Surrogate Key), ClaimID (Foreign Key to Claim), PolicyID (Foreign Key to Policy), DisputeType, DisputeStatus, ...
ScenarioHub	Table for storing scenario information	ScenarioID (Surrogate Key), ScenarioName, ScenarioDescription, ...
MethodologyHub	Table for storing methodology information	MethodologyID (Surrogate Key), MethodologyName, MethodologyDescription, ...
VaRHub	Table for storing Value at Risk (VaR) information	VaRID (Surrogate Key), PolicyID (Foreign Key to Policy), VaRValue, VaRDate, ...

AuditHub	Table for storing audit information	AuditID (Surrogate Key), PolicyID (Foreign Key to Policy), AuditDate, ...
UnderwritingHub	Table for storing underwriting information	UnderwritingID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
PolicyIssuanceHub	Table for storing policy issuance information	IssuanceID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
PolicyServicingHub	Table for storing policy servicing information	ServicingID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
BillingHub	Table for storing billing information	BillingID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
DisputeHub	Table for storing dispute information	DisputeID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
ScenarioTable	Table for storing scenario details	ScenarioID (Surrogate Key), ScenarioName, ScenarioDescription, ...
MethodologyTable	Table for storing methodology details	MethodologyID (Surrogate Key), MethodologyName, MethodologyDescription, ...
VaRTable	Table for storing Value at Risk (VaR) information	VaRID (Surrogate Key), PolicyID (Foreign Key to Policy), VaRValue, VaRDate, ...
ForwardLookTable	Table for storing forward-looking information	ForwardLookID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
EstimatesTable	Table for storing estimate information	EstimateID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
VulnerabilityTable	Table for storing vulnerability information	VulnerabilityID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
EventTable	Table for storing event information	EventID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
AttackTable	Table for storing attack information	AttackID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
IndustryDataTable	Table for storing industry-specific data	DataID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
SegmentDataTable	Table for storing segment-specific data	DataID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
OutlookTable	Table for storing outlook information	OutlookID (Surrogate Key), PolicyID (Foreign Key to Policy), ...

TestingTable	Table for storing testing-related information	TestingID (Surrogate Key), PolicyID (Foreign Key to Policy), ...
CustomerHub	Table for storing customer information	CustomerID (Surrogate Key), CustomerName, CustomerType, ...
AddressHub	Table for storing customer addresses	AddressID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
ContactHub	Table for storing customer contact information	ContactID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
CommunicationHub	Table for storing customer communication details	CommunicationID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
PaymentMethodHub	Table for storing customer payment methods	PaymentMethodID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
PolicyholderHub	Table for storing policyholder information	PolicyholderID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
BeneficiaryHub	Table for storing beneficiary information	BeneficiaryID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
RelationshipHub	Table for storing customer relationship information	RelationshipID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
PreferenceHub	Table for storing customer preferences	PreferenceID (Surrogate Key), CustomerID (Foreign Key to Customer), ...
HistoryHub	Table for storing customer interaction history	HistoryID (Surrogate Key), CustomerID (Foreign Key to Customer), ...

Uncovering Data Domains in the Cyber Insurance Landscape



Data Domain models, like the provided table, offer benefits such as standardized data organization and efficient integration, enabling organizations to build a robust cyber insurance capability by ensuring data consistency, facilitating data analysis, and supporting holistic insights into the insurance process.

The table provided represents a data domain model that can help an organization build its cyber insurance capability. Here are the benefits of using this table and data domain model:

1. **Entity Identification**: The table clearly identifies various entities involved in the cyber insurance process, such as Insured Entity, Product, Policy, Channel, KYC, Underwriting Factors, Adjustments, Guidelines, Rules, Model, and more. This identification helps in understanding the different components and relationships within the cyber insurance domain.
2. **Data Organization**: The table organizes data into hubs and satellites, providing a structured approach for storing and managing information. This organization ensures data consistency, eliminates redundancy, and facilitates efficient data retrieval and analysis.
3. **Data Integration:** The table enables the integration of data from different sources and systems. By establishing relationships between entities using foreign keys, it allows for a holistic view of the data across the cyber insurance process, enhancing decision-making and analysis.
4. **Flexibility and Scalability:** The data domain model offers flexibility and scalability as new entities or attributes can be easily added without disrupting the existing structure. This adaptability is crucial in the dynamic and evolving field of cyber insurance, where new data requirements may emerge over time.
5. **Process Understanding:** The table provides insights into the end-to-end process of cyber insurance, starting from customer onboarding to policy issuance, endorsements, renewals, claims, billing, and payments. This understanding helps in mapping and analyzing the entire lifecycle, identifying areas for improvement and optimization.

6. **Analytical Capabilities:** By capturing data attributes relevant to each entity, the table enables comprehensive analysis and reporting. It supports the evaluation of underwriting factors, adjustments, models, coverage, claim details, and other critical elements for assessing risks, making informed decisions, and improving overall cyber insurance capabilities.
7. **Data Governance:** The data domain model facilitates data governance by establishing clear ownership and accountability for each entity. It ensures data traceability and lineage, enabling compliance with regulatory requirements and maintaining data quality standards.

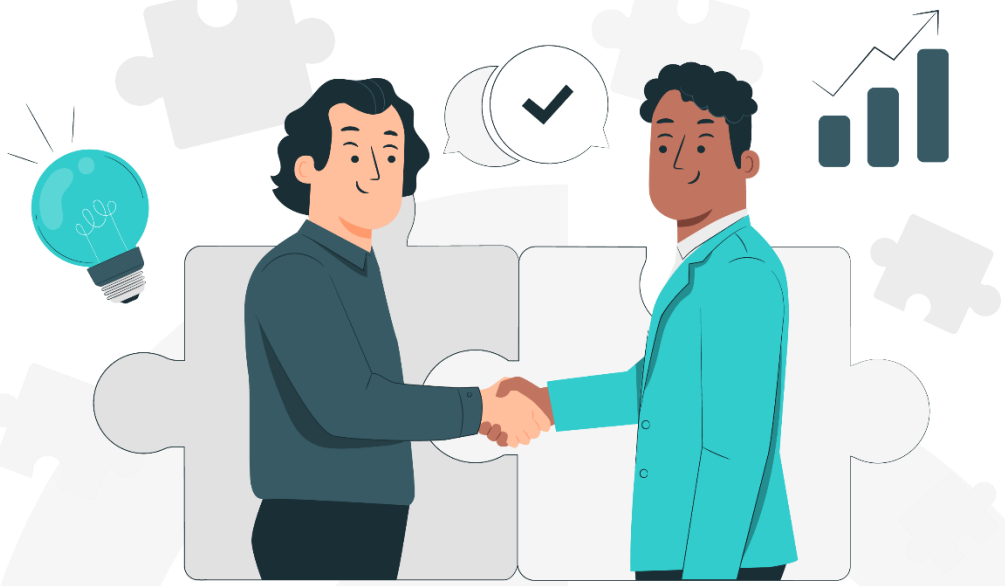
Overall, the provided table and data domain model are valuable resources for organizations looking to build their cyber insurance capability. It enhances data management, integration, and analysis while providing a comprehensive view of the entities and processes involved in cyber insurance.

Journey Type	Data Domain	Table Name	Attributes
Customer Journey	Onboarding	InsuredEntityHub	InsuredEntityID (Surrogate Key), InsuredEntityName, InsuredEntityType, ...
Product	Product	ProductHub	ProductID (Surrogate Key), ProductName, ProductType, ...
Policy	Policy	PolicyHub	PolicyID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), PolicyNumber, ...
Channel	Entity	ChannelHub	ChannelID (Surrogate Key), ChannelName, ChannelType, ...
KYC	KYC	KYCHub	KYCID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), KYCDate, ...
Qualification	Underwriting Factors	Factor	FactorHub
Underwriting Adjustments	Adjustments	AdjustmentHub	AdjustmentID (Surrogate Key), AdjustmentFactor, AdjustmentType, ...
Underwriting Guidelines	Guidelines	GuidelinesHub	GuidelinesID (Surrogate Key), GuidelinesDescription, ...
Underwriting Rules	Rules	RuleHub	RuleID (Surrogate Key), RuleName, RuleDescription, ...
Underwriting	Underwriting Decision	DecisionHub	DecisionID (Surrogate Key), DecisionType, DecisionDescription, ...
Underwriting Factors	Factors	FactorHub	FactorID (Surrogate Key), FactorName, FactorType, ...
Underwriting Adjustments	Adjustments	AdjustmentHub	AdjustmentID (Surrogate Key), AdjustmentFactor, AdjustmentType, ...
Model	Model	ModelHub	ModelID (Surrogate Key), ModelName, ModelType, ...
Model Output	Model	ModelOutputSatellite	OutputID (Surrogate Key), ModelID (Foreign Key to Model), OutputName, OutputValue, ...

Eligibility	Underwriting Factors	FactorHub	FactorID (Surrogate Key), FactorName, FactorType, ...
Underwriting Adjustments	Adjustments	AdjustmentHub	AdjustmentID (Surrogate Key), AdjustmentFactor, AdjustmentType, ...
Lead Generation	Insured Entity	InsuredEntityHub	InsuredEntityID (Surrogate Key), InsuredEntityName, InsuredEntityType, ...
Sales	Policy	PolicyHub	PolicyID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), PolicyNumber, ...
Customer Acquisition	Policy	PolicyHub	PolicyID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), PolicyNumber, ...
Retention	Policy	PolicyHub	PolicyID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), PolicyNumber, ...
Win Back	Policy	PolicyHub	PolicyID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), PolicyNumber, ...
Underwriting Factors	Factors	AdjustmentHub	FactorID (Surrogate Key), FactorName, FactorType, ...
Underwriting Adjustments	Adjustments	ApplicationHub	ApplicationID (Surrogate Key), PolicyID (Foreign Key to Policy), ApplicationDate, ...
Application	Application	ApplicationHub	ApplicationID (Surrogate Key), PolicyID (Foreign Key to Policy), ApplicationDate, ...
Policy Issuance	Policy Issuance	PolicyIssuanceHub	PolicyIssuanceID (Surrogate Key), PolicyID (Foreign Key to Policy), IssuanceDate, ...
Endorsement	Endorsement	EndorsementHub	EndorsementID (Surrogate Key), PolicyID (Foreign Key to Policy), EndorsementDate, ...
Renewal	Renewal	RenewalHub	RenewalID (Surrogate Key), PolicyID (Foreign Key to Policy), RenewalDate, RenewalStatus, ...
Claim	Claim	ClaimHub	ClaimID (Surrogate Key), PolicyID (Foreign Key to Policy), ClaimNumber, ClaimDate, ...
Adjustment	Adjustment	AdjustmentLink	AdjustmentID (Surrogate Key), LossID (Foreign Key to Loss), AdjustmentFactor, AdjustmentType, ...
Premium	Premium	PremiumLink	PremiumID (Surrogate Key), PolicyID (Foreign Key to Policy), PremiumAmount, PremiumDate, ...
Claim Loss	Claim Loss	ClaimLossLink	ClaimLossID (Surrogate Key), ClaimID (Foreign Key to Claim), LossID (Foreign Key to Loss), ClaimLossAmount, ...

Billing	Policy	PolicyHub	PolicyID (Surrogate Key), InsuredEntityID (Foreign Key to Insured Entity), PolicyNumber, ...
Invoice	Invoice	InvoiceHub	InvoiceID (Surrogate Key), PolicyID (Foreign Key to Policy), InvoiceNumber, InvoiceDate, ...
Payment	Payment	PaymentHub	PaymentID (Surrogate Key), InvoiceID (Foreign Key to Invoice), PaymentAmount, PaymentDate, ...
Coverage	Coverage	CoverageHub	CoverageID (Surrogate Key), CoverageName, CoverageType, ...

How SCIKIQ can help?



ScikIQ can significantly help achieve the above cyber insurance underwriting process by providing a unified and efficient data management and analysis solution. Here's how ScikIQ can support each step:

1. **Asset Classification:**
    a. ScikIQ can serve as a central repository to store and manage insured entities' asset inventory data.
    b. It allows for easy categorization and tagging of assets based on various risk factors and classification criteria.
    c. The platform enables seamless collaboration and data sharing among underwriters and risk assessors to ensure accurate asset classification.
2. **Loss Calculation for Events:**
    a. ScikIQ's data integration capabilities can gather and consolidate historical cyber attack data from various sources.
    b. It provides advanced analytics tools and libraries that enable the modeling and estimation of event probabilities and potential financial losses.
    c. The platform's data visualization capabilities help in understanding the impact of different events on asset portfolios.
3. **Loss Estimation and Adjustments:**
    a. ScikIQ supports statistical modeling and analysis, allowing underwriters to develop and refine loss estimation models.
    b. It enables the integration of historical claims data, Q-factors, and forward-looking information into the modeling process.
    c. The platform facilitates the application of adjustments to loss estimates based on qualitative and quantitative factors.
4. **Value at Risk (VaR) Analysis:**
    a. ScikIQ's data processing capabilities and computational power enable efficient VaR calculations using methodologies like WARM or Loss Method.
    b. It allows for the assignment of weights to events based on probabilities and potential losses.

c. The platform provides comprehensive analytics and reporting features to present VaR results at different confidence levels.

5. **Sensitivity Analysis and Stress Testing:**
    a. ScikIQ's data exploration and visualization tools enable underwriters to perform sensitivity analysis on input parameters and conduct stress testing.
    b. It supports the manipulation of parameters and running simulations to assess the portfolio's resilience against severe cyber attack scenarios.
6. **Risk Management and Mitigation:**
    a. ScikIQ facilitates continuous monitoring of the cyber threat landscape by integrating threat intelligence feeds and industry reports.
    b. It allows for the real-time updating of event probabilities and loss estimates based on the latest information.
    c. The platform supports risk management strategies by providing a holistic view of the portfolio's risk exposure and recommended risk mitigation actions.
7. **Documentation and Reporting:**
    a. ScikIQ's reporting and documentation features enable the creation of comprehensive reports on underwriting models, assumptions, calculations, and results.
    b. It provides customizable templates and dashboards to present VaR, risk exposure, and other key metrics to stakeholders in a clear and actionable manner.
8. **Production Implementation:**
    a. ScikIQ serves as a centralized data fabric platform, providing secure and scalable data infrastructure for underwriting data storage and processing.
    b. Its data integration and pipeline capabilities streamline the ingestion and transformation of data from various internal and external sources.
    c. ScikIQ's integration capabilities allow for seamless integration with existing underwriting systems, enabling automated workflows and data exchange.
    d. The platform provides role-based access control and guidelines to ensure proper data input, processing, and decision-making by underwriters.

SCIKIQ is a no-code data fabric platform that offers a differentiated solution for building a cyber insurance capability without a steep learning curve. It provides the following key advantages:

1. **No-Code Data Fabric**: SCIKIQ's no-code approach enables business users and domain experts to design and implement the cyber insurance data infrastructure without extensive technical skills or reliance on IT teams. This results in faster implementation, increased agility, and reduced costs.

2. **Native Support for Data Domain and Data Vault**: SCIKIQ supports both Data Domain and Data Vault modeling approaches, allowing organizations to capture and align data to business processes effectively. It ensures compatibility with industry-standard methodologies and leverages the scalability and flexibility of Data Vault while adhering to best practices.

3. **Simplified Medallion Architecture:** SCIKIQ simplifies the creation of a Medallion architecture using its intuitive visual interface. Users can define and manage relationships, hierarchies, and business rules easily, enabling the creation of a flexible and adaptive architecture that evolves with the organization's needs.

4. **Comprehensive End-to-End Solution:** SCIKIQ offers a complete solution for building a cyber insurance capability. It covers the entire data lifecycle, from data capture and management to analysis and reporting. Organizations can eliminate the need for multiple tools or systems, streamlining their processes and reducing complexity.

5. **Faster Time-to-Value:** With SCIKIQ's no-code approach and pre-built templates, organizations can rapidly implement their cyber insurance capability. This accelerated time-to-value allows businesses to quickly gain insights, make informed decisions, and stay ahead in the dynamic cyber insurance market.

By combining the benefits of a no-code data fabric platform, support for Data Domain and Data Vault models, and simplified Medallion architecture creation, SCIKIQ offers a differentiated solution. It empowers organizations to efficiently build and adapt their cyber insurance capabilities, reducing complexity and technical dependencies while accelerating the implementation process.

CONTACT

ADDRESS:

1st Floor, Tower-A, Millennium Plaza,
Sushant Lok Phase I, Sector 27,
Gurugram, Haryana 122001

Website:

www.daaslabs.ai

Email:

sales@daaslabs.ai

enquiry@scikiq.com