Cyber Decisions. Financially Quantified.

CloudComms Inc.

Kovrr CRQ Insurance Report

Based on Kovrr's Cyber Risk Quantification for CloudComms Inc.

August 2022

Generated for CloudComms Inc.

Table Of Content

Abstract

The aim of this report is to provide an in-depth understanding of the cyber risks and exposures to CloudComms Inc. through insights and results from Kovrr's statistical modelling of cyber event scenarios that may impact the company for the purposes of insurance. The modelling methodology makes use of the entire firmographic profile of the group that encompasses their operational footprint through operating locations, technologies, service providers in order to create an accurate representation of the hazards and vulnerabilities that the company has exposure to; enabling the quantification and estimation of losses via a simulation of 10,000 years of events that could affect the company.

The Cyber Profile of CloudComms Inc.

Basic Overview of the Company Profile

CloudComms Inc. is a communications service provider with a multinational operations profile. Kovrr was able to identify 39 different technologies and 9 different 3rd party service providers used by CloudComms Inc., which form the basis of their hazard profile (See Appendix 2 for full list). In addition to the list of hazards, the company is also described by the following inputs that each provide additional data to better understand the risk profile of the company:

Data Point	Input Provided
Name	CloudComms Inc.
Countries of Operation	Australia, China, India, Russian Federation, United Arab Emirates, United States.
Annual Revenue	USD 680,000,000
Number of Data Records on Premises	40,000 Total: (20,000 PCI, 20,000 PII)
Number of Data Records on Cloud	30,000 Total: (30,000 PII)
Employees Endpoint Productivity Reliance	100%
Employees Endpoint Income Reliance	100%
On Premise Infrastructure Productivity Reliance	100%
On Premise Infrastructure Income Reliance	100%

The set of countries of operation allow Kovrr to leverage its extensive datasets to determine an accurate view of the frequency and severity of attacks that may affect the company through its operational bases and their individual exposures.

The number of data records stored on premises and in the cloud provide the basis for all losses that can arise from data-related events.

The Annual Revenue and Productivity and Income reliance modifiers are key in determining the potential losses that can arise from operational events.

Current Cyber Posture

The Kovrr model uses the company's cyber posture to determine the likelihood of a cyber event. In order to understand the company's cyber posture we use the input from the Company Sphere. The high-detail breakdown of asset groups and asset categories allows us to understand the structure of the company's network and technical stack at a more granular level for higher accuracy modelling.

We also look at the cyber security maturity of the company based on the standard security control frameworks such as NIST and CIS to determine the likelihood and severity of the simulated events for the company.

The modelling results have been using the following set of CIS control levels:

CIS Control #	Description	Current Posture
1	Inventory and Control of Hardware Assets	**IG2**
2	Inventory and Control of Software Assets	**IG1**
3	Continuous Vulnerability Management	**IG2**
4	Controlled Use of Administrative Privileges	**IG3**
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	**IG2**
6	Maintenance, Monitoring and Analysis of Audit Logs	**IG1**
7	Email and Web Browser Protections	**IG2**
8	Malware Defenses	**IG1**
9	Limitation and Control of Network Ports, Protocols, and Services	**IG1**
10	Data Recovery Capabilities	**IG2**
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	**IG2**
12	Boundary Defense	**IG2**
13	Data Protection	**IG2**
14	Controlled Access Based on the Need to Know	**IG1**

15	Wireless Access Control	**IG1**
16	Account Monitoring and Control	**IG2**
17	Implement a Security Awareness and Training Program	**IG2**
18	Application Software Security	**IG1**
19	Incident Response and Management	**IG3**
20	Penetration Tests and Red Team Exercises	**IG2**

Cyber Posture Recommendations

Presented here is a list of the top 10 CIS controls, ordered from greatest effect descending, which by upgrading their implementation group will decrease the severity of events which therefore will also decrease the exposure business impact loss.

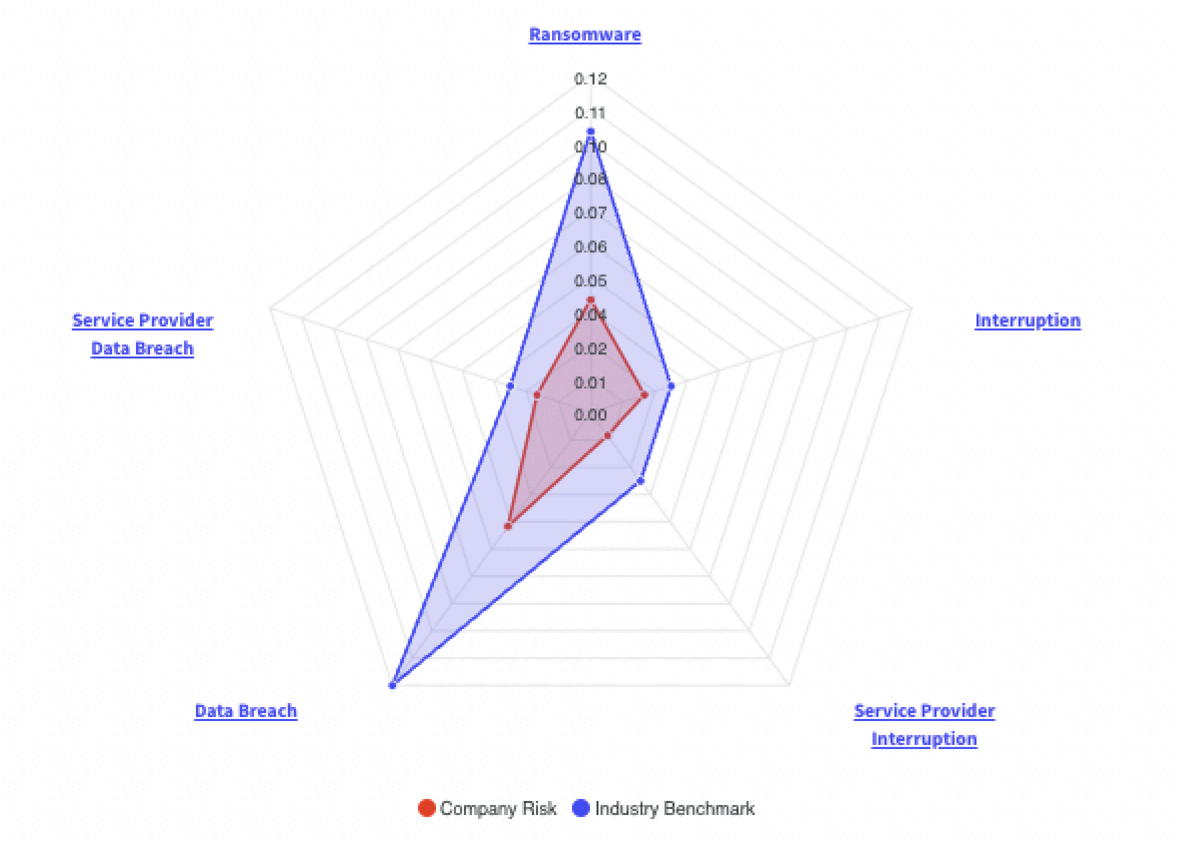
CIS Control	Recommended Action	Average Effect	Highest Effect	Main Impact Scenario Affected
#6 - Maintenance, Monitoring and Analysis of Audit Logs	**IG1 → IG2**	- $12,336 (1.63 % ↓)	- $16,015 (0.12 % ↓)	Business Interruption
#8 - Malware Defenses	**IG1 → IG2**	- $11,388 (1.50 % ↓)	- $14,702 (0.11 % ↓)	Business Interruption
#10 - Data Recovery Capabilities	**IG2 → IG3**	- $7,072 (0.93 % ↓)	- $9,030 (0.07 % ↓)	Business Interruption
#14 - Controlled Access based on the need to know	**IG1 → IG2**	- $5,521 (0.73 % ↓)	- $6,244 (0.05 % ↓)	Data Theft & Privacy
#13 - Data Protection	**IG2 → IG3**	- $4,223 (0.56 % ↓)	- $5,454 (0.04 % ↓)	Business Interruption
#3 - Continuous Vulnerability Management	**IG2 → IG3**	- $3,732 (0.49 % ↓)	- $4,542 (0.04 % ↓)	Business Interruption
#5 - Secure Configuration	**IG2 → IG3**	- $3,731 (0.49 % ↓)	- $4,436 (0.03 % ↓)	Business

for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers				Interruption
#20 - Penetration Tests and Red Team Exercises	**IG2 → IG3**	- $3,368 (0.44 % ↓)	- $4,287 (0.03 % ↓)	Business Interruption
#7 - Email and Web Browser Protections.	**IG2 → IG3**	- $3,041 (0.40 % ↓)	- $4,038 (0.03 % ↓)	Business Interruption
#11 - Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	**IG2 → IG3**	- $2,694 (0.36 % ↓)	- $2,694 (0.03 % ↓)	Business Interruption

Frequency Benchmarking

The radar graph below represents the frequencies (likelihoods) of the 5 types of events that are modeled in Kovrr's methodology.

The shaded blue radar graph, which represents the industry benchmark, has higher frequencies in all events than the modeled company, meaning CloudComms Inc. performs better than the benchmark across all of our event types.



Insurance Policy Recommendations

Model Output

The model output can be split into two sets of three coverages, one representing the operational losses, and the other representing the data-related losses. ***For CloudComms Inc. the operational losses greatly outweigh the data-related ones due to the large revenue and the reliance on network uptime for productivity and income, and the relatively small number of data records that CloudComms Inc. maintai*****ns.**

Operational Losses Breakdown

	Business Interruption (USD)	3rd Party Service Provider Failure (USD)	Ransomware and Extortion (USD)
1% Loss	10,963,700	185,200	2,006,800
Annual Average Loss (AAL)	545,000	63,700	73,700
50% Loss	35,600	12,000	12,400
75% Loss	29,000	9,900	10,100
90% Loss	22,700	7,600	8,100
95% Loss	18,200	6,600	6,800
99% Loss	8,800	3,800	3,900
Sum of 1% Loss	**USD 13,155,700**		
Sum of AAL	**USD 682,400**		

Data-Related Losses Breakdown

	Data Theft & Privacy (USD)	3rd Party Liability (USD)	Regulation & Compliance (USD)
1% Loss	361,700	171,600	53,000
Annual Average Loss (AAL)	38,600	22,300	14,800
50% Loss	12,800	12,600	12,500
75% Loss	10,100	10,000	10,100
90% Loss	7,700	8,000	8,200
95% Loss	5,800	6,800	7,100
99% Loss	1,600	4,300	5,100
Sum of 1% Loss	**USD 586,300**		
Sum of AAL	**USD 75,700**		

High-Level Policy Structure Performance

Kovrr has been provided with the policy details as per below, but for the purposes of analysis of the policy performance have had to make an assumption on the premium pricing and coverages.

	Provided Value (USD)	Kovrr's Assumption (USD)
Policy Attachment Point	-	-
Policy Deductible	350,000	-
Policy Limit	2,000,000	-
Policy Premium	-	200,000

Based on expert opinion from industry sources, Kovrr will assume a premium of USD 200K for the given policy conditions. ***Therefore, for a given year of losses the breakeven loss of exercising the insurance contract would be a loss of USD 550K (350K deductible + 200K premium), which we estimate to have an exceedance probability of 13.48%.***

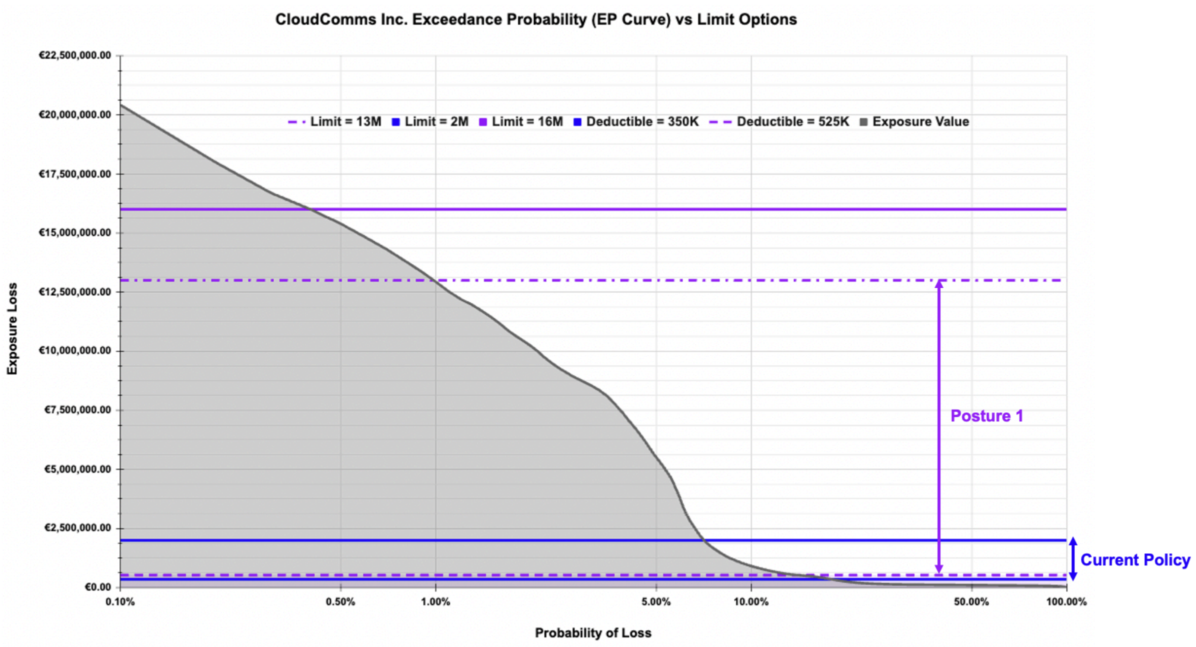
	Business Interruption (USD)	3rd Party Service Provider Failure (USD)	Ransomware and Extortion (USD)	Data Theft & Privacy (USD)	3rd Party Liability (USD)	Regulation & Compliance (USD)
1:250 Year Loss	13,361,600	6,744,400	2,833,900	450,800	191,400	62,300
1:100 Year Loss	10,963,700	185,200	2,006,800	361,700	171,600	53,000
Annual Average Loss (AAL)	545,000	63,700	73,700	38,600	22,300	14,800

At the moment, CloudComm Inc.'s insurance does not provide adequate cover for our 1:100 year modeled losses; with the current policy limit aligning approximately to our modeled losses that relate to a 1:14 year loss scenario. The sum of average annual losses across all coverages (AAL) is USD 758.1K and the total 1% loss (1:100 Years) is USD 12.873M, with the 0.04% (1:250 Years) loss being USD 15.597M

Policy Structure Performance Scenarios

Given the limited information on the insurance coverage, Kovrr has tried to estimate the premium costs for a set of different insurance postures that could potentially be negotiated with the insurer. The key consideration is for CloudComms Inc. to assess the potential policy structures against their own risk appetite, and determine which provides the greatest benefit/cost within the context of their budget and view of risk.

There is also the limitation, especially given the hardened state of the cyber insurance market at the current time, as to whether an insurer would accept a given lower deductible or higher limit due to risk and capacity restraints.



The above plot shows the Exposure Loss plotted against the logarithmically scaled Probability of the loss that allows us to get a better visualization of how different limit options compare against the probability of losses/return periods.

Posture 1: Increase Limit to 1:100 total loss estimate and Increase Deductible closer to AAL estimate

This posture would be an increase of the 350K deductible to 700K, but with an increase of the policy limit from 2M to 13M to cover the total modeled loss at the 1:100 return period rate - We estimate this would be accompanied by a ~13% increase in premium for this added coverage.

Posture 1		
	Provided Value (USD)	**Kovrr's Assumption (USD)**
Policy Attachment Point	-	-
Policy Deductible	700,000 (100% Increase)	-
Policy Limit	-	13,000,000 (650% increase)
Policy Premium	-	525,000 (262.5% increase)

Posture 2: Increase Limit to 1:250 total loss estimate and Increase Deductible closer to AAL estimate

[redacted]

Posture 2		
	Provided Value (USD)	Kovrr's Assumption (USD)
Policy Attachment Point	-	-
Policy Deductible	[redacted]	-
Policy Limit	-	[redacted]
Policy Premium	-	[redacted]

Posture 3: Increase Deductible closer to AAL estimate

[redacted]

Posture 3		
	Provided Value (USD)	Kovrr's Assumption (USD)
Policy Attachment Point	-	-

Policy Deductible	-	[redacted]
Policy Limit	[redacted]	-
Policy Premium	-	[redacted]

Posture 4: Increase Deductible closer to AAL and Increase Limit to 1:150 total loss estimate

[redacted]

Posture 4		
	Provided Value (USD)	**Kovrr's Assumption (USD)**
Policy Attachment Point	-	-
Policy Deductible	-	[redacted]
Policy Limit	-	[redacted]
Policy Premium	-	[redacted]

Coverages Structure Performance

Beyond the policy level optimisations and posturings in the previous section, there is also the opportunity to further optimize in relation to specific coverages or sub-limits through insights from the modelling output.

The coverages are split into two sections - operational and data-related, which can then also be further segmented into the cost-components that make up each coverage.

As the main loss driver for CloudComms Inc. is Business Interruption, the waiting period for operational loss coverage is a key parameter. Mostly, optimal waiting periods are established by the median of the duration which Kovrr's simulation has at 30 hours. The industry average waiting periods vary within the range between 8 to 72 hours depending on the particular company.

	Availability Duration Breakdown (Hours)	Data Records Breached
Minimum	2.3	4% of Total
Median	93.4	41% of Total
Average	101.8	43% of Total
Maximum	705.9	93% of Total

Coverage split by damage types ratios

Going a level deeper into the coverages, we split the losses into the respective damage types that make up each total. From this more granular level, you are able to directly see the key expense items for each coverage, and are able to compare these to any sub-limits in an existing policy; also able to use them to optimize the cost to coverage by focusing on particular vulnerabilities.

	#1: Business Interruption (BI)			
	Lost Income	BI Recovery Expenses	BI Forensics	Public Relations Repairment
Split	12.7%	43.2%	29.5%	14.6%
AAL (USD)	69,200	235,400	160,800	79,600
Total (USD)	545,000			

	#2: 3rd Party Service Provider Failure		
	Lost Income	BI Recovery Expenses	Public Relations Repairment
Split	[redacted]	[redacted]	[redacted]
AAL (USD)	[redacted]	[redacted]	[redacted]
Total (USD)	[redacted]		

	#3: Ransomware and Extortion	
	Extortion Recovery Expenses	Extortion Payment
Split	[redacted]	[redacted]
AAL (USD)	[redacted]	[redacted]
Total (USD)	[redacted]	

	#4: 3rd Party Liability	
	Settlements	Legal Defense

Split	[redacted]	[redacted]
AAL (USD)	[redacted]	[redacted]
Total (USD)	[redacted]	

	#5: Data Theft & Privacy				
	Data Recovery	Forensics	Public Relations Repairment	Monitoring Services	Notifications
Split	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
AAL (USD)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total (USD)	[redacted]		[redacted]		[redacted]

	#6: Regulation & Compliance	
	Regulatory Fines	Regulatory Legal Defense
Split	[redacted]	[redacted]

AAL (USD)	[redacted]	[redacted]
Total (USD)	[redacted]	

Top 12 Cyber Indicators

Based upon expert opinion of indicators for cyber risk concerns from the underwriting point of view, we have a list of 10:

Top 5		
Article Number	**Description**	**Current Posture**
1	Multi-factor Authentication	Not Implemented (CIS 11 is currently IG2)
2	Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and 24/7 Network Monitoring and Security Operations Center (SOC)	N/A
3	[redacted]	[redacted]
4	[redacted]	[redacted]

5	[illegible]	[illegible]
6	[illegible]	[illegible]
7	[illegible]	[illegible]
8	[illegible]	[illegible]
9	[illegible]	[illegible]
10	[illegible]	[illegible]
11	[illegible]	[illegible]
12	[illegible]	[illegible]

Appendix

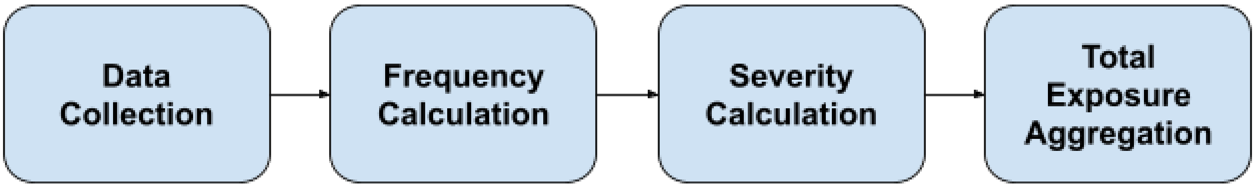
Appendix 1: Cyber Risk Quantification by Kovrr

Methodology

Kovrr’s cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures.

The purpose of this section is to describe and reflect a quick overview of the methodology and process Kovrr conducts to financially quantify the cyber risk of a company. The result of this process is a reflection of the potential damages that the company can suffer from in the following year. The input of this process is data of two types - company data and threat intelligence data.

The process can be reflected with the following flow:



The assessment process is composed of 4 steps - Data collection, Frequency calculation, Severity Calculation, and Total exposure aggregation.

1. Data collection - in the data collection step Kovrr collects two types of data - Company data and threat intelligence, which are used as the input of the model
2. Frequency calculation - in the frequency calculation step Kovrr determines the probability of a cyber event impacting the company
3. Severity calculation - in the severity calculation step Kovrr determines the financial impact that a cyber event will have on the company, in the case the company will be affected by the event.
4. Total Exposure aggregation - in the final step, the total exposure of the company is calculated based on the frequency and severity calculation, resulting in a final reflection of the total exposure of the company to cyber events.

Appendix 2: CloudComms Inc. Group Cyber Risk Quantification Input

Quantification Input

Attached below is the quantification input about the company and risk provided by the end-user

Data Point	Input Provided
Name	CloudComms Inc.
Domain	cloudcomms.com, cloudcomms.io
Annual Revenue and Currency	USD 680,000,000
Number of Employees	500-1,000
Countries of Operation	Australia, China, India, Russian Federation, United Arab Emirates, United States.
US States of Operation	California, Minnesota, Texas
Industries of Operation	Communications
Complied Regulations	US Federal Level Regulation, US State Level Regulation
Cyber Insurance Premium	N/A
Number of Employees Endpoints	750 Total
Number of Data Records on Premises	40,000 Total: (20,000 PCI, 20,000 PII)
Number of Data Records on Cloud	30,000 Total: (30,000 PII)
Employees Endpoint Productivity Reliance	100%
Employees Endpoint Income Reliance	100%
On Premise Infrastructure Productivity Reliance	100%

On Premise Infrastructure Income Reliance	100%
Obtained Security Certificates	ISO, PCI DSS
Outage Duration with Material Impact (in Hours)	1 Hour
How long does it typically take to restore your critical business operations following a network interruption?	12 Hours

Cyber Posture

Attached here is the cyber posture provided in the CIS controls framework provided by the end-user. Each control maturity level is elaborated by the "Implementation Group", and decided by the steps adopted for each.

CIS Control #	Description	Current Posture
1	Inventory and Control of Hardware Assets	**IG2**
2	Inventory and Control of Software Assets	**IG1**
3	Continuous Vulnerability Management	**IG2**
4	Controlled Use of Administrative Privileges	**IG3**
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	**IG2**
6	Maintenance, Monitoring and Analysis of Audit Logs	**IG1**
7	Email and Web Browser Protections	**IG2**
8	Malware Defenses	**IG1**
9	Limitation and Control of Network Ports, Protocols, and Services	**IG1**
10	Data Recovery Capabilities	**IG2**
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	**IG2**
12	Boundary Defense	**IG2**
13	Data Protection	**IG2**
14	Controlled Access Based on the Need to Know	**IG1**
15	Wireless Access Control	**IG1**
16	Account Monitoring and Control	**IG2**
17	Implement a Security Awareness and Training Program	**IG2**
18	Application Software Security	**IG1**

19	Incident Response and Management	**IG3**
20	Penetration Tests and Red Team Exercises	**IG2**

Past Events

Attached below are past events the company has suffered as provided by the end-user.

Event Description	Loss Description
N/A	N/A

Technological Footprint

Kovrr's 360 Sonar technology has identified the technological footprint of the company automatically through scan and the results have been verified by the end-user. The attached below is the list of technologies and 3rd party service providers that are being used within the company:

Technologies		
Type	**Vendor**	**Product**
CMS	Adobe	Adobe Experience Manager
CMS	Drupal	Drupal
CMS	Joomla	Joomla
CMS	Liferay	Liferay
CMS	Microsoft	ASP.NET
Database	Cloudera	Cloudera
Database	IBM	IBM Db2
Database	MongoDB	MongoDB
Database	Neo4J	Neo4J
Database	Oracle	MySQL
Database	PostgreSQL	PostgreSQL

Database	Teradata	Teradata
DNS	PowerDNS	PowerDNS
Infrastructure	Bootstrap Core Team	Bootstrap
Infrastructure	Citrix	Citrix
Infrastructure	The jQuery Team	jQuery
Infrastructure	Lew Cirne's	New Relic
Infrastructure	Microsoft	ASP.NET Ajax
Infrastructure	Node.js	Node.js
Infrastructure	PHP	PHP
Mail	Microsoft	Microsoft Exchange
Network App	Fortinet	FortiGate
OS	CentOS	CentOS
OS	Linux	Linux
OS	Microsoft	Windows
OS	Microsoft	Windows Server
OS	Ubuntu	Ubuntu
Remote Access	OpenSSH	OpenSSH
Web	Apache	Apache HTTP Server
Web	Apache	Hbase
Web	Apache	Hive
Web	Apache	Tomcat
Web	Font Awesome Team	Font Awesome
Web	Google	Google Font API
Web	Google	Google Tag Manager

Web	Microsoft	IIS
Web	Nginx	Nginx
Web	OpenResty	OpenResty
Web	Varnish	Tomcat

3rd Party Service Providers		
Type	**Vendor**	**Product**
CDN	Fastly	Fastly CDN
CMS	Q4web	Q4web
CRM	Salesforce	Salesforce
Email Vendor	123 Reg	123 Reg Email
Email Vendor	Dmarc	Dmarc
Email Vendor	Microsoft	Microsoft 365
PaaS	Appnexus	Appnexus
PaaS	Fastly	Fastly CDN
PaaS	Rackspace	Rackspace Hosting

Insurance Policy Input

Policy	Current Policy	Future Policy
Policy Limit	USD 2,000,000	N/A
Policy Attachment Point	N/A	N/A
Policy Deductible	USD 350,000	N/A
Policy Premium	USD 170,000	N/A

	Current Policy	Future Policy

Losses	Business Interruption	3rd Party Service Provider Failure	Ransomware and Extortion	Business Interruption	3rd Party Service Provider Failure	Ransomware and Extortion
Coverage Sub-Limit	N/A	N/A	N/A	N/A	N/A	N/A
Coverage Deductible	N/A	N/A	N/A	N/A	N/A	N/A
Coverage Waiting Period	N/A	N/A	N/A	N/A	N/A	N/A
Coverage Exclusions	N/A	N/A	N/A	N/A	N/A	N/A

	Current Policy			Future Policy		
Data-Related Losses	Data Theft & Privacy	3rd Party Liability	Regulation & Compliance	Data Theft & Privacy	3rd Party Liability	Regulation & Compliance
Coverage Sub-Limit	N/A	N/A	N/A	N/A	N/A	N/A
Coverage Deductible	N/A	N/A	N/A	N/A	N/A	N/A
Coverage Exclusions	N/A	N/A	N/A	N/A	N/A	N/A

Legal Disclaimer

THE REPORT IS PROVIDED ON AN "AS IS" BASIS AND WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, ANY IMPLIED CONDITIONS OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY AND FITNESS FOR A PARTICULAR PURPOSE) . YOU ACKNOWLEDGE THAT THE QUALITY AND ACCURACY OF THIS REPORT IS BASED AND DEPENDENT UPON THE ACCURACY, COMPLETENESS, QUALITY AND SUITABILITY OF THE DATA PROVIDED BY YOU OR ANY THIRD PARTY ON YOUR BEHALF. KOVRR DOES NOT WARRANT OR MAKE ANY REPRESENTATION REGARDING: (I) THE VERACITY OF THE REPORT OR THAT THE REPORT IS COMPLETE OR ERROR-FREE; AND/OR (II) THE EFFECTIVENESS, USEFULNESS, RELIABILITY, TIMELINESS, COMPLETENESS, OR QUALITY OF THE REPORT. YOUR USE OF AND RELIANCE UPON THIS REPORT IS ENTIRELY AT YOUR SOLE DISCRETION AND RISK, AND KOVRR, ITS AFFILIATES AND THIRD-PARTY PROVIDERS, SHALL HAVE NO RESPONSIBILITY OR LIABILITY WHATSOEVER TO YOU OR ANY THIRD PARTY IN CONNECTION WITH THE REPORT. THE REPORT DO NOT CONSTITUTE LEGAL ADVICE, AND YOU UNDERSTAND THAT YOU MUST DETERMINE FOR YOURSELF THE NEED TO OBTAIN YOUR OWN INDEPENDENT LEGAL ADVICE REGARDING THE SUBJECT MATTER OF THE REPORT.