Cyber OverVue™ User Guide

August 2018

Advisen
Transforming • Insurance™

TABLE *of* CONTENTS

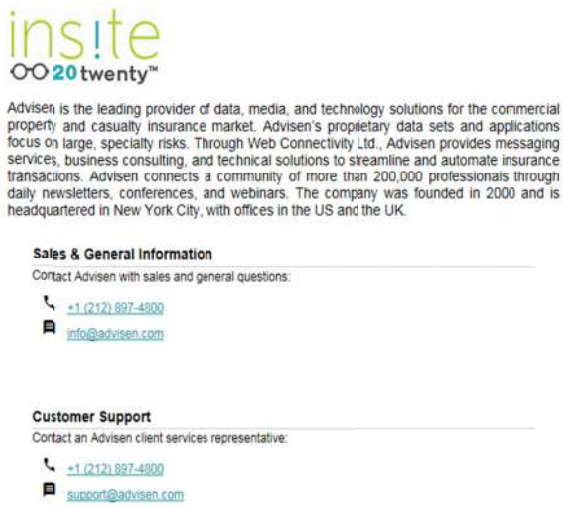
Introduction to Cyber OverVue™

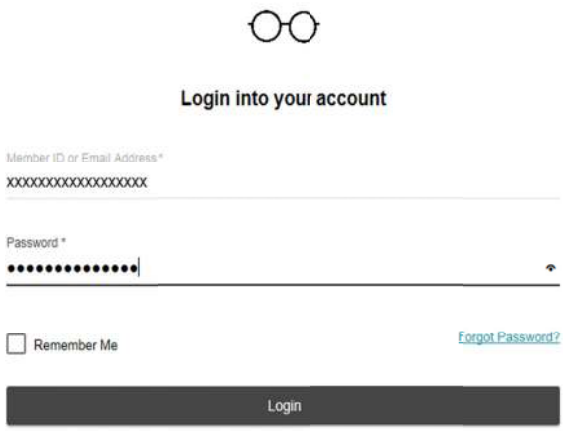
Cyber OverVue is a web-based, SaaS application that enables more efficient real-time decision-making based on the quantification of known losses. Cyber OverVue generates on-demand scores and analyses that provide users with detailed insights into an organization's cyber loss profile, which can be used as a basis for assessing its potential risks. The development of Cyber OverVue was a collaborative process with industry leaders to address a market-driven need for an analytics product based on the quantification of known losses. It not only enables more informed underwriting decisions, but also justification of coverage recommendations based on the historical loss experience of an organization.

Getting Started

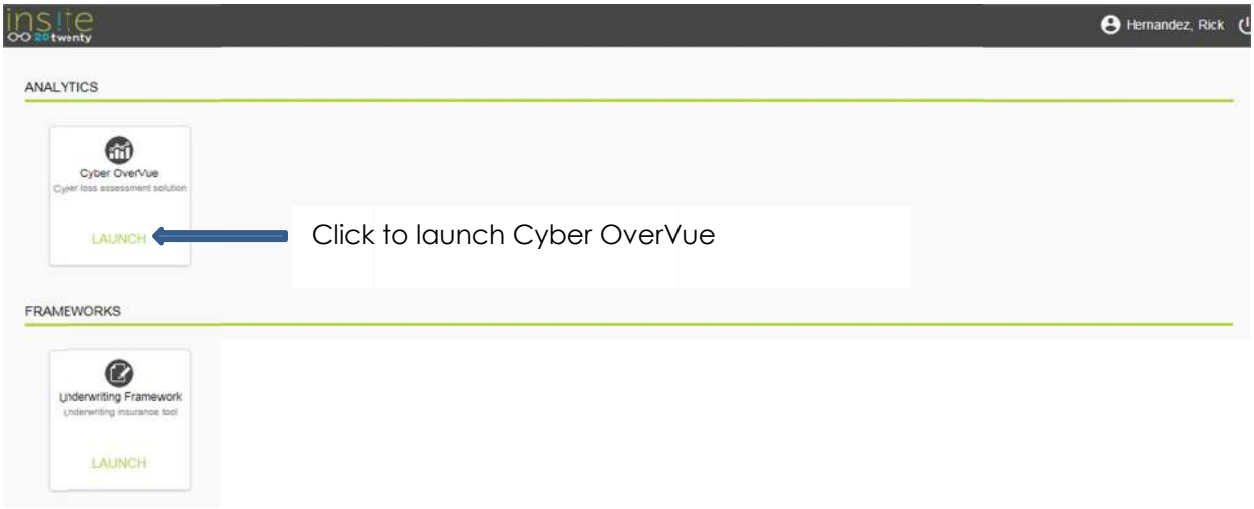
Log in to insite20twenty with credentials provided during the onboarding process with the Client Experience team.

- Insite20twenty serves as the online portal to Advisen's product portfolio.
- Login credentials will be provided during the onboarding process with the Client Experience team.





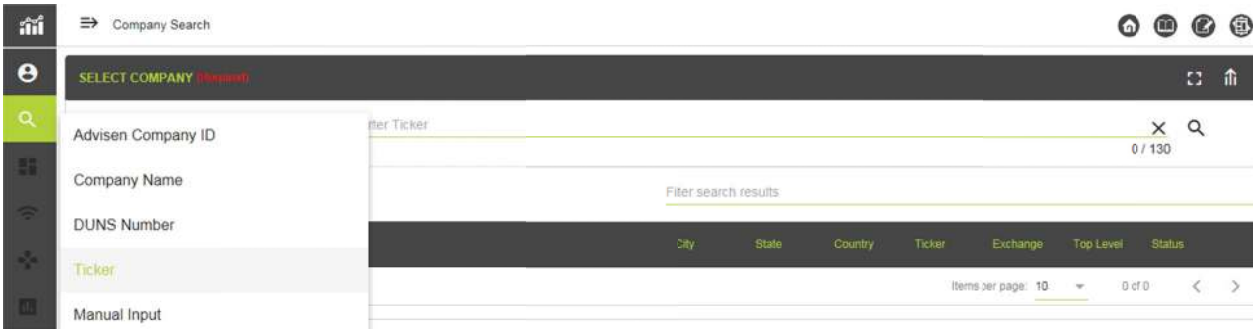
Upon logging in, the user will be brought to the product selection screen. Cyber OverVue will be part of the Analytics section, as the initial offering of the OverVue product family. Click on the Launch button to access Cyber OverVue.



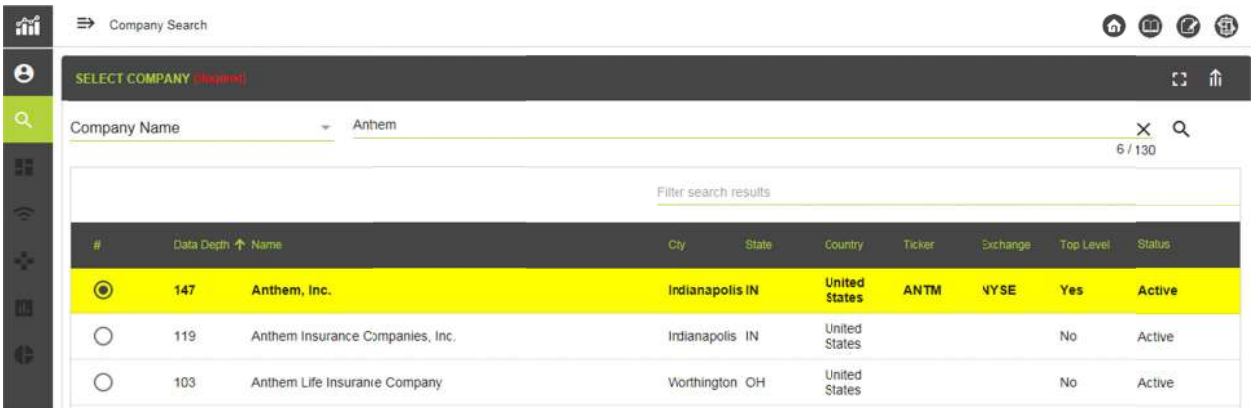
The user will be brought to the Company Search page upon launching Cyber OverVue.

Five search options are available for identifying and selecting a company:

- **Advisen Company ID:** Unique identifier for a company in the Advisen database.
- **Company Name:** Enter the actual name of the company; the search process will return the exact match or up to twenty options similar to the name entered.
- **DUNS Number:** A unique nine-digit identifier provided by Dun & Bradstreet for the identification of a business. It is used to establish a business credit file, which is often referenced by lenders and potential business partners to help predict the reliability and/or financial stability of the company in question.
- **Ticker:** Stock symbol for publicly traded companies.
- **Manual:** Enables a user to manually enter company information for new companies or to generate a peer group profile.

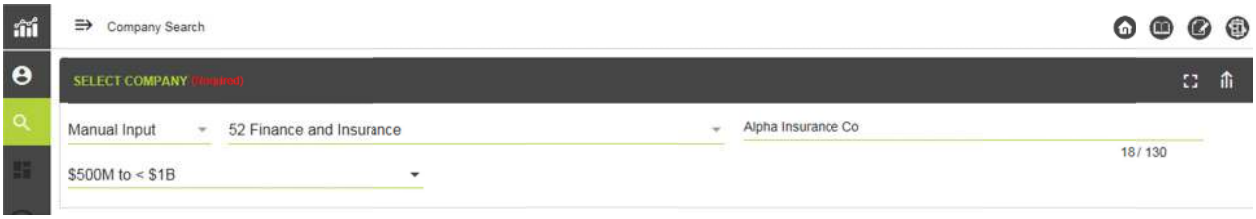


Select the search criteria and enter the appropriate company information to initiate a company search. The search will return either an exact match or a list of companies to select from which closely matches the search criteria entered.

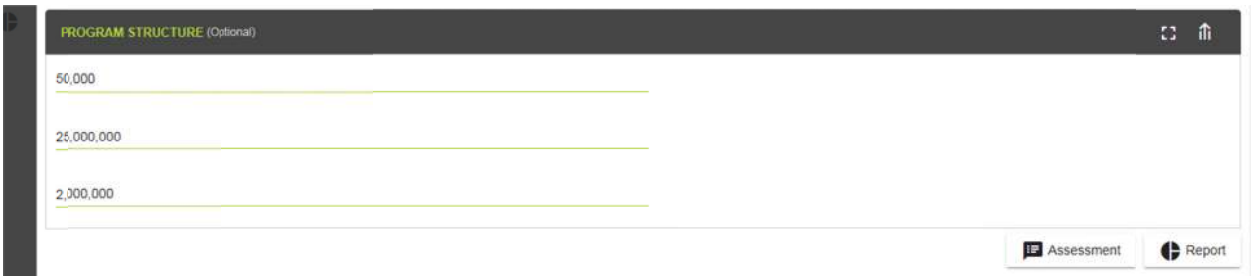


If using the Manual Input search option, additional details will be required to perform a risk assessment:

- Select the appropriate Industry.
- Enter the Company Name.
- Select the appropriate Revenue Range.



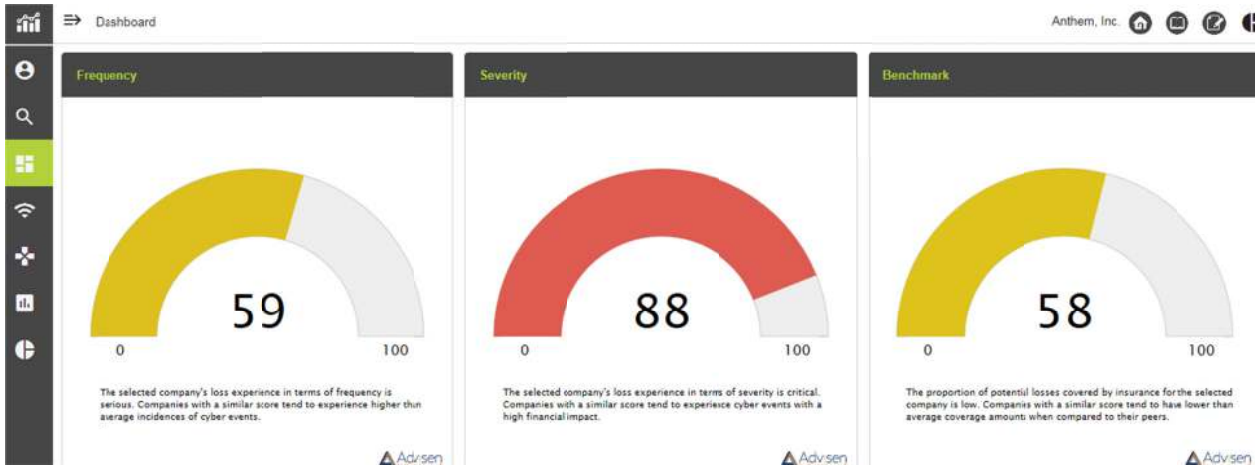
Enter the Insurance Program details to generate a Benchmark Analysis. These fields are optional; a user will still be able to perform a Risk Assessment, though it will not include a benchmark score.



Dashboard

The Dashboard provides a series of scores that assess the loss profile for the company with respect to the frequency and severity of occurrences, as well as a benchmark analysis of an existing insurance program for the company.

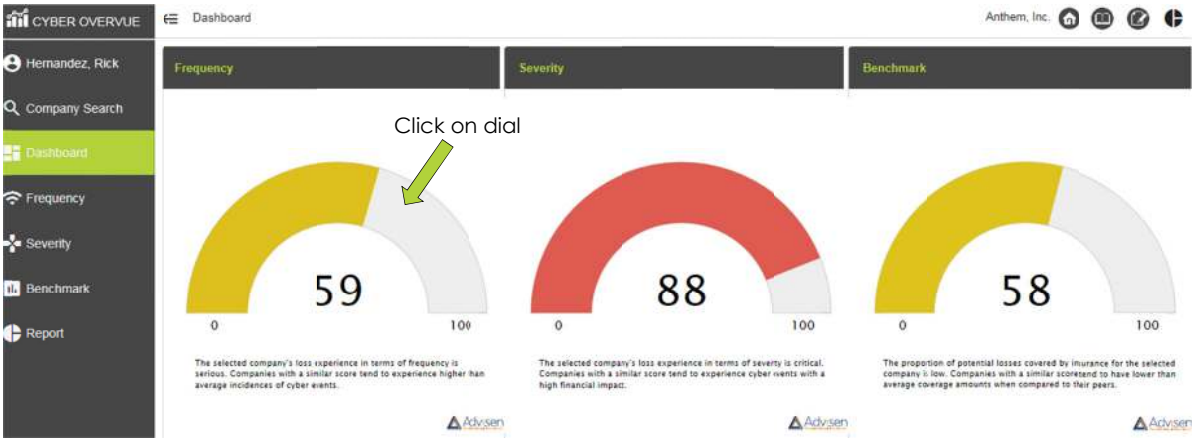
The Assessment Score ranges from 0 – 100. The greater the score the more significant the loss exposure is in terms of the frequency and severity of historical loss events for a company.



Screen Navigation

A user can easily navigate the tool to uncover additional details of the Risk Assessment by clicking on the relevant sections (i.e.: click on the frequency dial to get more information on the frequency loss exposures).

A traditional left menu of options may also be used for navigation. Note that the Reports section is only accessible through the left menu.



Frequency Analysis

The Frequency Analysis provides four views on the propensity of a cyber event:

- Industry Overview
- Trend Analysis
- Type of Incident
- Type of Loss

Industry Overview

This analysis shows the trend of losses across different company size ranges (revenue range), comparing all the peer groups within a selected industry.

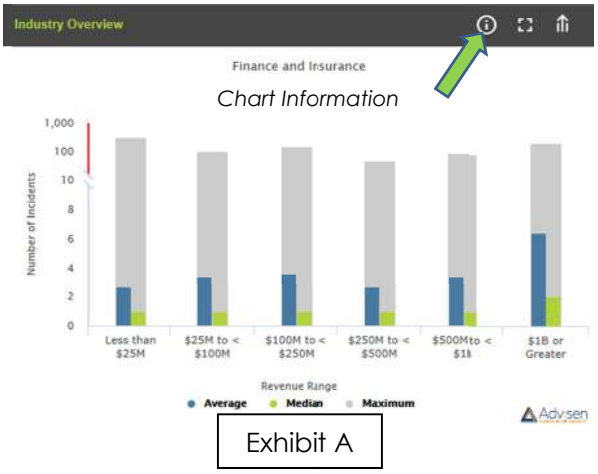


Exhibit A

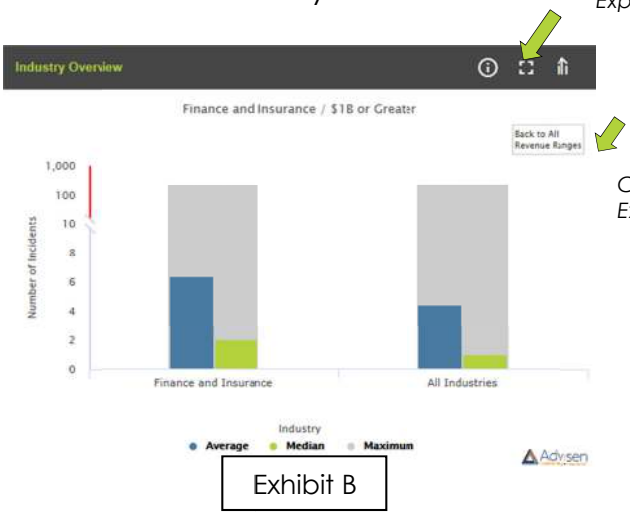
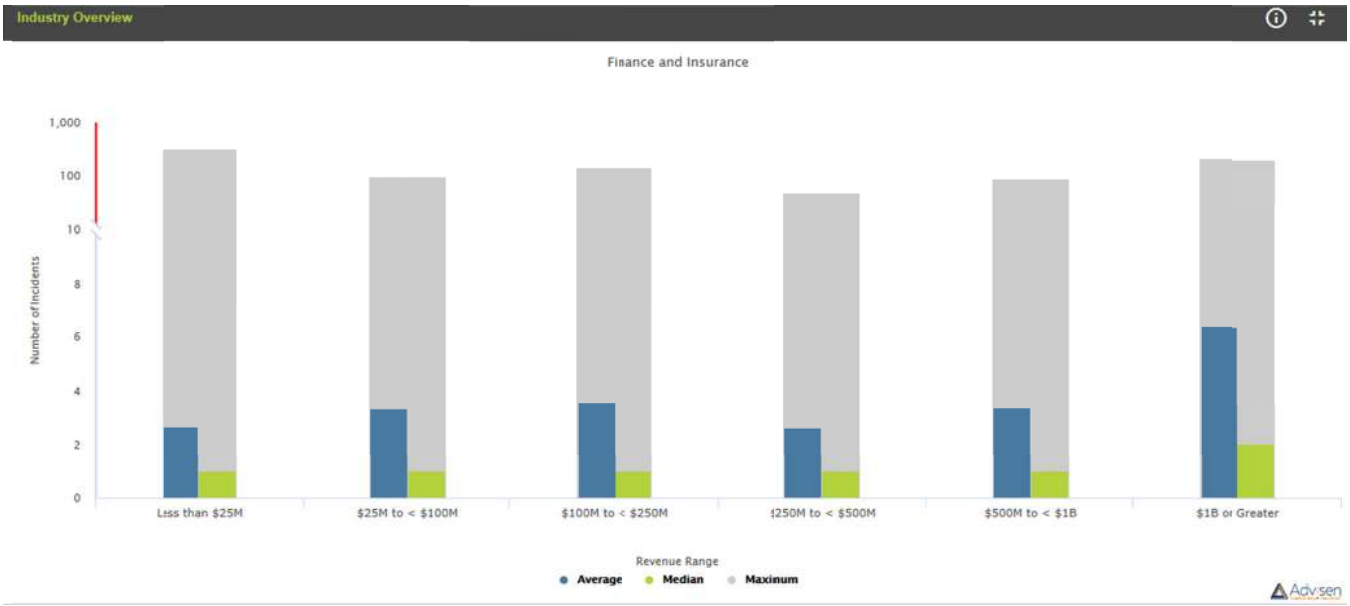


Exhibit B

The blue vertical bar represents the average loss experience for a peer group within the selected industry; green represents the median loss experience for a peer group within the selected industry; the gray vertical bar represents the tail end (maximum) loss experience for each peer group within the industry. (Exhibit A)

Click on the vertical bars to focus on a specific revenue band and view how the loss experience of the selected peer group compares to an aggregation across all industries. (Exhibit B)

Click on the expansion icon to enlarge the image to full-page view; all charts are expandable where this icon is present.



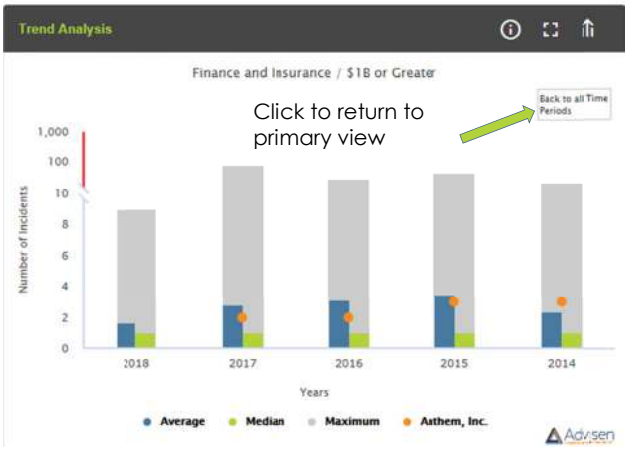
Trend Analysis

This analysis looks at the trend of losses across a time continuum. The blue vertical bar represents the average loss experience for the peer group specified; the green vertical bar represents the median loss experience for the peer group specified; the gray vertical bar represents the maximum experience for the peer group specified.

The orange circle represents the loss experience for the selected company.

Click on the vertical bars to look at the loss experience by individual years.

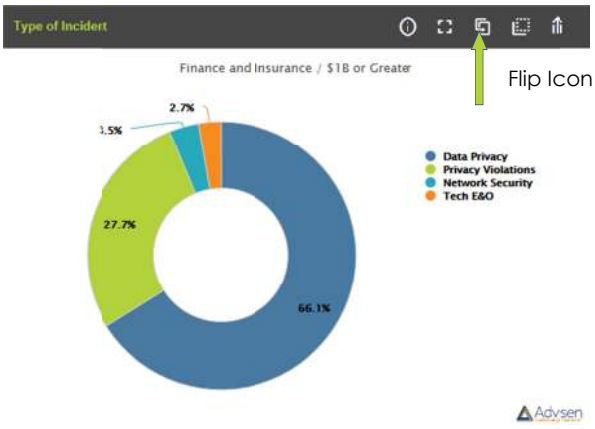
Click on "Back to All Time Periods" to return to the primary view.



Type of Incident

This analysis looks at the trend of losses by the type of incident. The blue vertical bar represents the average loss experience for the peer group specified; the green vertical bar represents the median loss experience for the peer group specified; the gray vertical bar represents the maximum experience for the peer group specified.

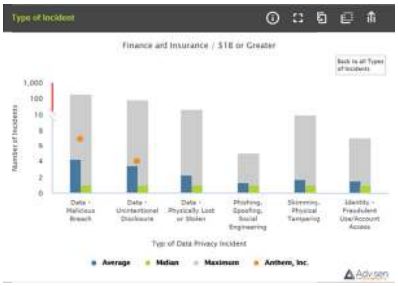
The orange circle represents the loss experience for the selected company.

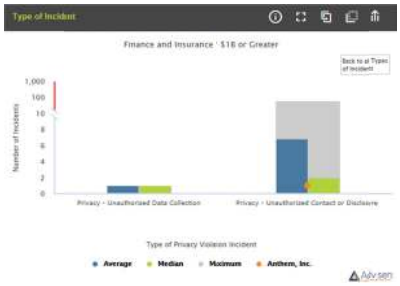


Click on the vertical bars to get a more granular look at the various types of incidents that make up the main grouping. These groupings consist of types with similar attributes:

1. **Data Privacy**
    a. Data malicious breach
    b. Data unintentional disclosure
    c. Data – Physically lost or stolen
    d. Phishing, Spoofing, Social Engineering
    e. Skimming, Physical Tampering
    f. Identity – Fraudulent User / Account Access
2. **Network Security**
    a. Network / Website Disruption
    b. Cyber Extortion
    c. Industrial Controls
3. **Technology Errors & Omissions**
    a. IT Configuration / Implementation Errors
    b. IT Processing Errors
4. **Privacy Violations**
    a. Privacy – Unauthorized Data Collection
    b. Privacy – Unauthorized Contact or Disclosure

Click on "Back to All Type of Incidents" to return to the primary view.



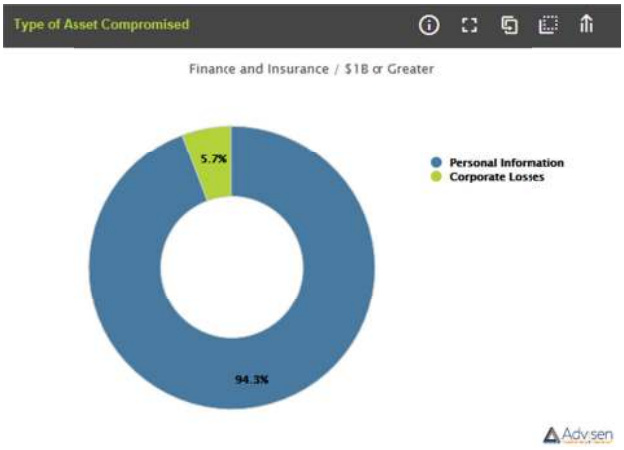


Each chart is accompanied with demographic details of the attributes within the chart and can be accessed by clicking on the Flip icon where available. Click on "Back to All Type of Incidents" to return to the primary view.

Type of Asset Compromised

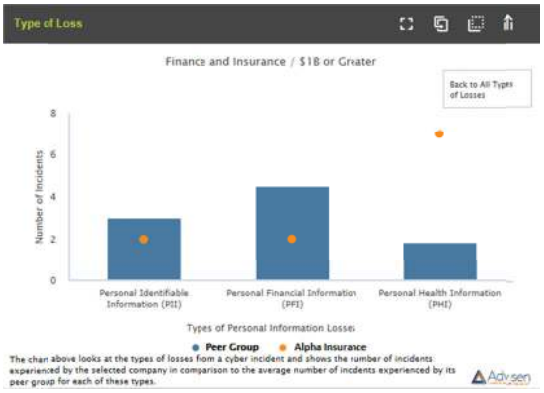
This analysis looks at the trend of losses by the type of asset compromised during a cyber incident. The blue vertical bar represents the average loss experience for the peer group specified; the green vertical bar represents the median loss experience for the peer group specified; the gray vertical bar represents the maximum experience for the peer group specified.

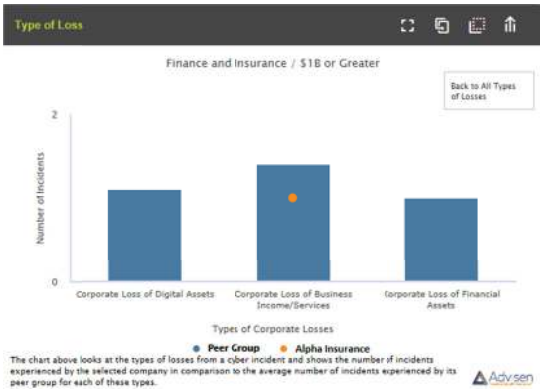
The orange circle represents the loss experience for the selected company.



Click on the vertical bars to get a more granular look at the various types of incidents that make up the main grouping. These groupings consist of types with similar attributes:

1. **Personal Information**
    a. Personal Identifiable Information (PII)
    b. Personal Financial Information (PFI)
    c. Personal health Information (PHI)
2. **Corporate Information**
    a. Corporate Loss of Digital Assets
    b. Corporate Loss of Business Income / Services
    c. Corporate Loss of Financial Assets





Most Recent Peer Group Losses

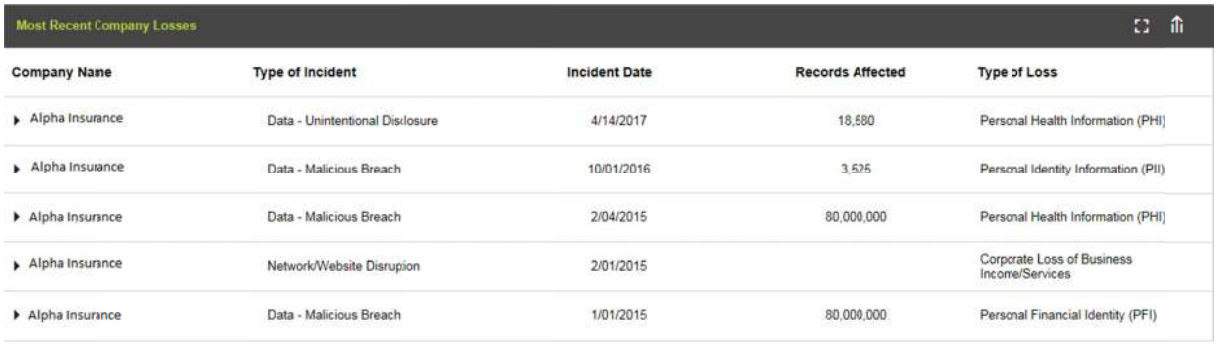
Most Recent Peer Group Losses displays the five most recent events experienced by the peer group of the selected company. Click on the individual line items for a more detailed description of the event.

Most Recent Peer Group Losses

Company Name	Type of Incident	Incident Date	Records Affected	Type of Loss
Company 1	Data - Malicious Breach	12/26/2017	1,843	Personal Identity Information (PII)
Company 2	Data - Malicious Breach	12/21/2017	1,380	Personal Identity Information (PII)
Company 3	Skimming, Physical Tampering	12/01/2017		Personal Financial Identity (PFI)
Company 4	Data - Unintentional Disclosure	11/09/2017		Personal Financial Identity (PFI)
Company 5	Data - Physically Lost or Stolen	11/01/2017	1,600	Personal Identity Information (PII)

Most Recent Company Losses

Most Recent Company Losses lists the five most recent events impacting the company under assessment. Click on the individual line items for a more detailed description of the event.

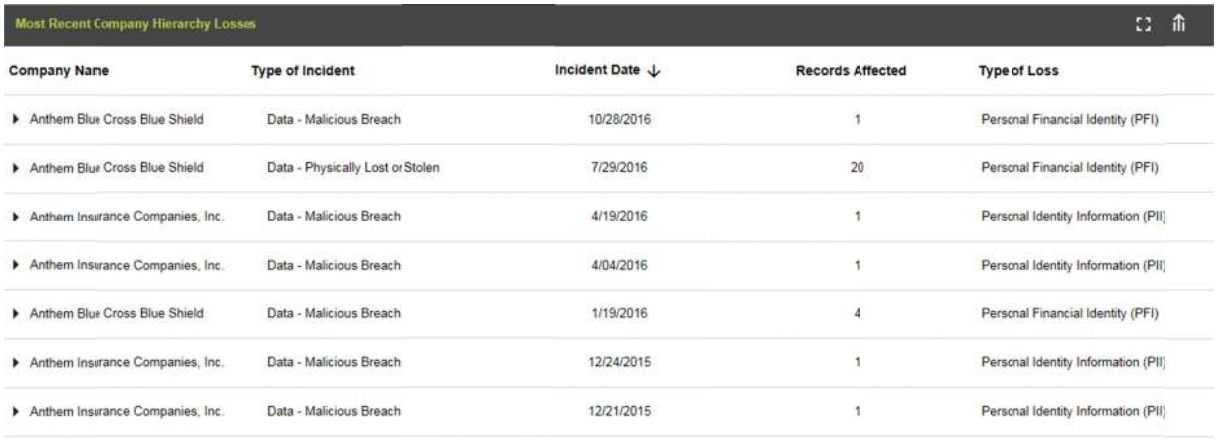


Most Recent Company Losses

Company Name	Type of Incident	Incident Date	Records Affected	Type of Loss
Alpha Insurance	Data - Unintentional Disclosure	4/14/2017	18,580	Personal Health Information (PHI)
Alpha Insurance	Data - Malicious Breach	10/01/2016	3,525	Personal Identity Information (PII)
Alpha Insurance	Data - Malicious Breach	2/04/2015	80,000,000	Personal Health Information (PHI)
Alpha Insurance	Network/Website Disruption	2/01/2015		Corporate Loss of Business Income/Services
Alpha Insurance	Data - Malicious Breach	1/01/2015	80,000,000	Personal Financial Identity (PFI)

Most Recent Company Hierarchy Losses

Most Recent Company Losses lists up to ten of the most recent events impacting the affiliates of the company under assessment. Click on the individual line items for a more detailed description of the event.



Most Recent Company Hierarchy Losses

Company Name	Type of Incident	Incident Date ↓	Records Affected	Type of Loss
Anthem Blue Cross Blue Shield	Data - Malicious Breach	10/28/2016	1	Personal Financial Identity (PFI)
Anthem Blue Cross Blue Shield	Data - Physically Lost or Stolen	7/29/2016	20	Personal Financial Identity (PFI)
Anthem Insurance Companies, Inc.	Data - Malicious Breach	4/19/2016	1	Personal Identity Information (PII)
Anthem Insurance Companies, Inc.	Data - Malicious Breach	4/04/2016	1	Personal Identity Information (PII)
Anthem Blue Cross Blue Shield	Data - Malicious Breach	1/19/2016	4	Personal Financial Identity (PFI)
Anthem Insurance Companies, Inc.	Data - Malicious Breach	12/24/2015	1	Personal Identity Information (PII)
Anthem Insurance Companies, Inc.	Data - Malicious Breach	12/21/2015	1	Personal Identity Information (PII)

Severity Analysis

The Severity analysis provides four views on the impact of a cyber event occurrence by looking at the amount and type of data records affected.

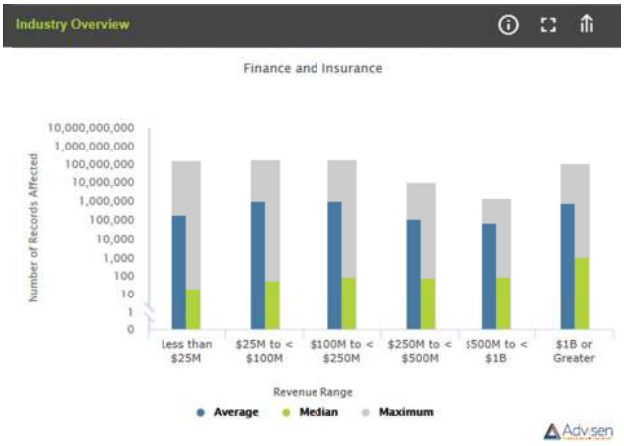
- Industry Overview
- Trend Analysis
- Type of Incident
- Type of Loss

Industry Overview

This analysis shows the trend of losses across different company size ranges (revenue range), comparing the selected industry to all industries.

The blue vertical bar represents the average loss experience for the peer group within the selected industry; green represents the median loss experience for the peer group within the selected industry; the gray vertical bar represents the tail end (maximum) loss experience for each peer group within the industry.

Click on the expansion icon to enlarge the image to full-page view; *all charts are expandable where this icon is present.*



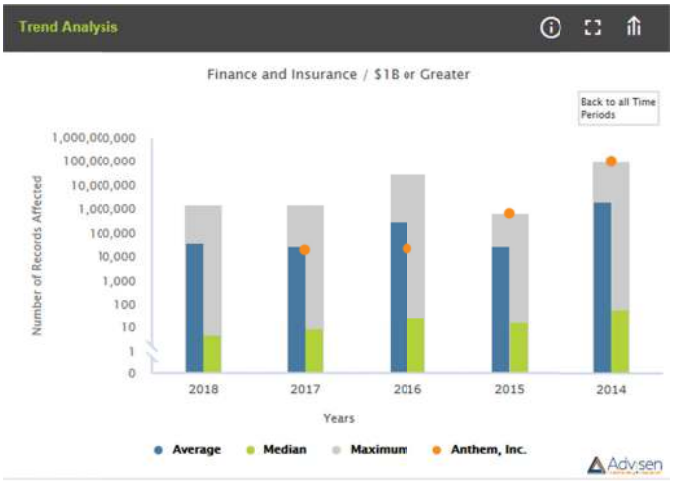
Trend Analysis

This analysis looks at the trend of losses experienced across a time continuum. The blue vertical bar represents the average loss experience for the peer group specified; the green vertical bar represents the median loss experience for the peer group specified; the gray vertical bar represents the maximum experience for the peer group specified.

The orange circle represents the loss experience for the selected company.

Click on the vertical bars to look at the loss experience by individual years

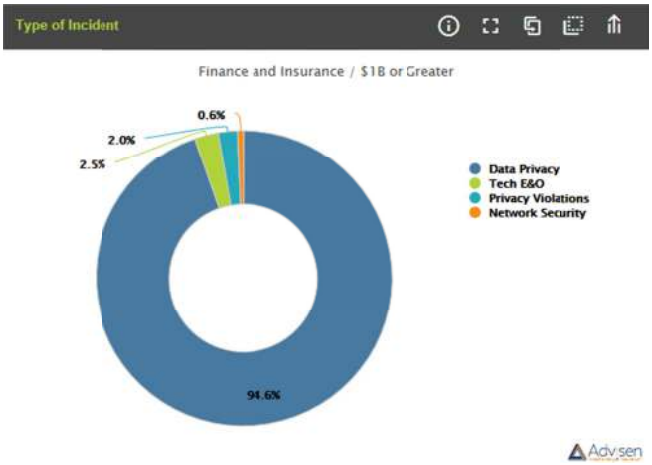
Click on "Back to All Time Periods" to return to the primary view.



Type of Incident

This analysis looks at the trend of losses by the type of incident. The blue vertical bar represents the average loss experience for the peer group specified; the green vertical bar represents the median loss experience for the peer group specified; the gray vertical bar represents the maximum experience for the peer group specified.

The orange circle represents the loss experience for the selected company.



Click on the vertical bars to get a more granular look at the various types of incidents that make up the main grouping. These groupings consist of types with similar attributes:

1. **Data Privacy**
    a. Data malicious breach
    b. Data unintentional disclosure
    c. Data – Physically lost or stolen
    d. Phishing, Spoofing, Social Engineering
    e. Skimming, Physical Tampering
    f. Identity – Fraudulent User / Account Access
2. **Network Security**
    a. Network / Website Disruption
    b. Cyber Extortion
    c. Industrial Controls
3. **Technology Errors & Omissions**
    a. IT Configuration / Implementation Errors
    b. IT Processing Errors
4. **Privacy Violations**
    a. Privacy – Unauthorized Data Collection
    b. Privacy – Unauthorized Contact or Disclosure

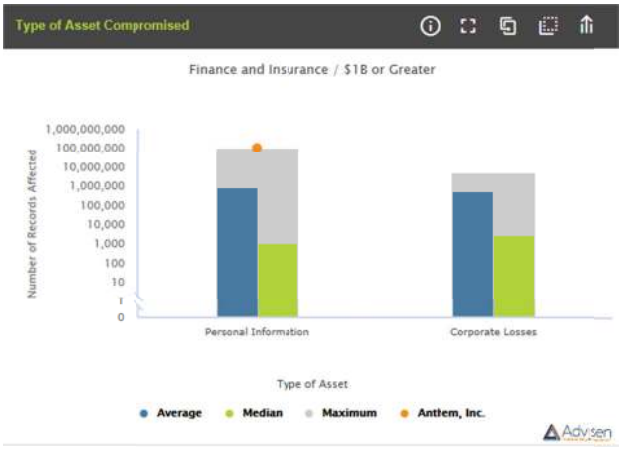
Click on "Back to All Type of Incidents" to return to primary view.

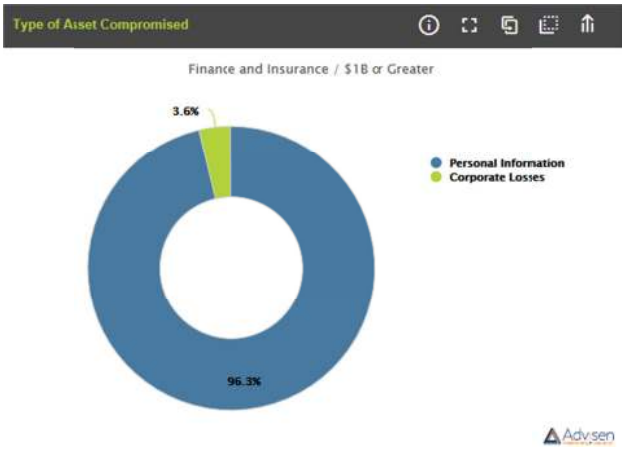
Each chart is accompanied with demographic details of the attributes within the chart and can be accessed by clicking on the Flip icon where available. Click on "Back to All Type of Incidents" to return to the primary view.

Type of Asset Compromised

This analysis looks at the trend of losses by the type of asset compromised during a cyber incident. The blue vertical bar represents the average loss experience for the peer group specified; the green vertical bar represents the median loss experience for the peer group specified; the gray vertical bar represents the maximum experience for the peer group specified.

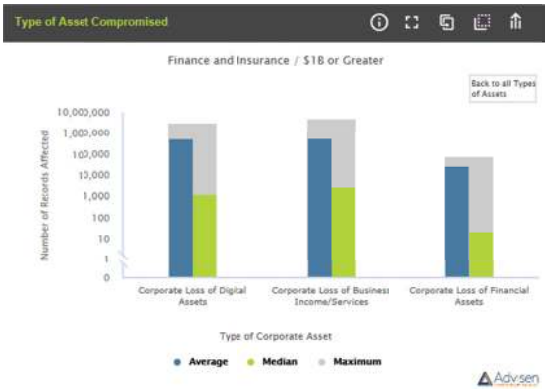
The orange circle represents the loss experience for the selected company.





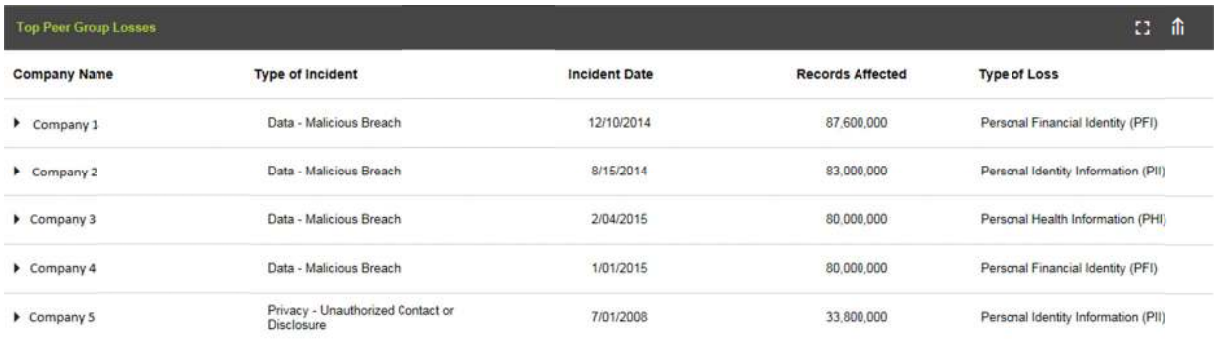
Click on the vertical bars to get a more granular look at the various types of incidents that make up the main grouping. These groupings consist of types with similar attributes:

1. **Personal Information**
    a. Personal Identifiable Information (PII)
    b. Personal Financial Information (PFI)
    c. Personal Health Information (PHI)
2. **Corporate Information**
    a. Corporate Loss of Digital Assets
    b. Corporate Loss of Business Income / Services
    c. Corporate Loss of Financial Assets



Top Peer Group Losses

Top Peer Group Losses shows events experienced by the peer group of the selected company based on the number of records affected. Click on the individual line items for a more detailed description of the events.



Top Peer Group Losses

Company Name	Type of Incident	Incident Date	Records Affected	Type of Loss
Company 1	Data - Malicious Breach	12/10/2014	87,600,000	Personal Financial Identity (PFI)
Company 2	Data - Malicious Breach	8/15/2014	83,000,000	Personal Identity Information (PII)
Company 3	Data - Malicious Breach	2/04/2015	80,000,000	Personal Health Information (PHI)
Company 4	Data - Malicious Breach	1/01/2015	80,000,000	Personal Financial Identity (PFI)
Company 5	Privacy - Unauthorized Contact or Disclosure	7/01/2008	33,800,000	Personal Identity Information (PII)

Top Company Losses

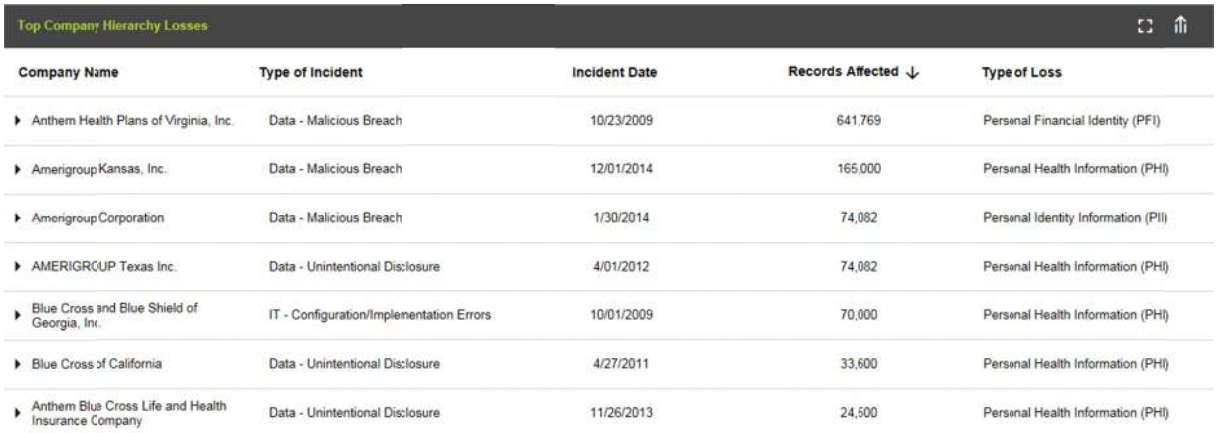
Top Company Losses displays the events impacting the company under assessment based on the number of records affected. Click on the individual line items for a more detailed description of the event.

Top Company Losses

Company Name	Type of Incident	Incident Date	Records Affected	Type of Loss
Alpha Insurance	Data - Malicious Breach	12/10/2014	87,600,000	Personal Financial Identity (PFI)
Alpha Insurance	Data - Malicious Breach	2/04/2015	80,000,000	Personal Health Information (PHI)
Alpha Insurance	Data - Malicious Breach	1/01/2015	80,000,000	Personal Financial Identity (PFI)
Alpha Insurance	Data - Malicious Breach	11/12/2014	15,000,000	Personal Health Information (PHI)
Alpha Insurance	IT - Configuration/Implementation Errors	10/23/2009	612,402	Personal Health Information (PHI)

Top Company Hierarchy Losses

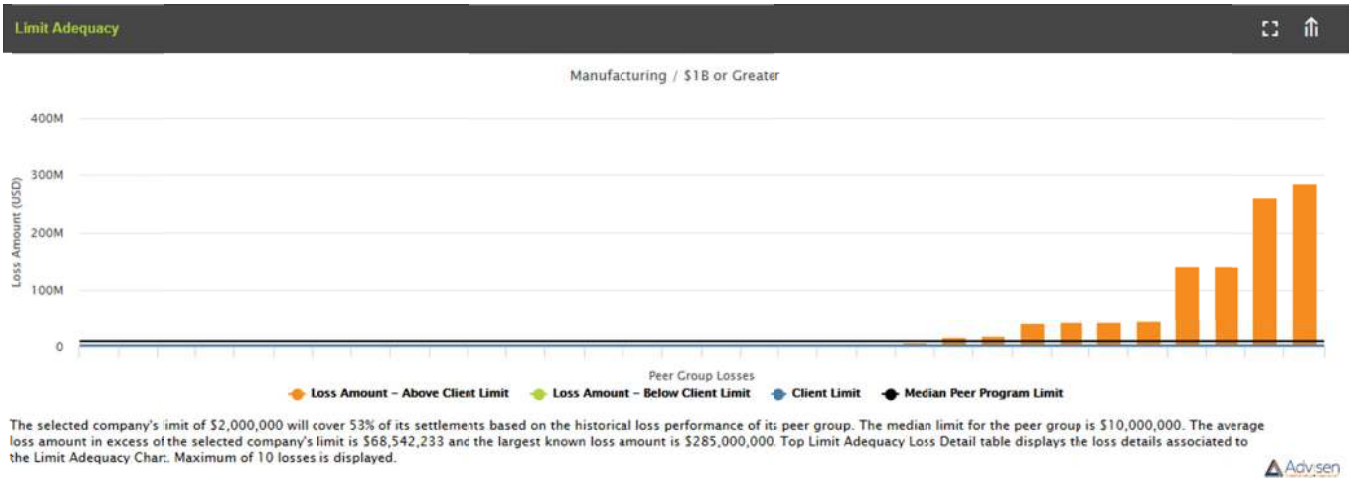
Top Company Hierarchy Losses lists up to ten of the top events impacting the affiliates of the company under assessment. Click on the individual line items for a more detailed description of the event



Top Company Hierarchy Losses

Company Name	Type of Incident	Incident Date	Records Affected ↓	Type of Loss
Anthem Health Plans of Virginia, Inc.	Data - Malicious Breach	10/23/2009	641,769	Personal Financial Identity (PFI)
Amerigroup Kansas, Inc.	Data - Malicious Breach	12/01/2014	165,000	Personal Health Information (PHI)
Amerigroup Corporation	Data - Malicious Breach	1/30/2014	74,082	Personal Identity Information (PII)
AMERIGROUP Texas Inc.	Data - Unintentional Disclosure	4/01/2012	74,082	Personal Health Information (PHI)
Blue Cross and Blue Shield of Georgia, Inc.	IT - Configuration/Implementation Errors	10/01/2009	70,000	Personal Health Information (PHI)
Blue Cross of California	Data - Unintentional Disclosure	4/27/2011	33,600	Personal Health Information (PHI)
Anthem Blue Cross Life and Health Insurance Company	Data - Unintentional Disclosure	11/26/2013	24,500	Personal Health Information (PHI)

Benchmark Analysis



The Limit Adequacy analysis compares the proposed limit to the known losses experienced by the selected peer group. Additional data points including the median limit purchased by the peer group help provide insight on the appropriate limits to purchase.

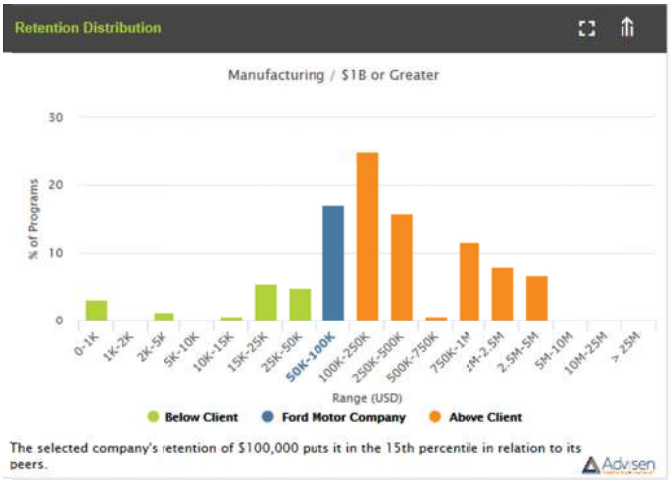
The Limit Adequacy chart is also accompanied by a table directly underneath that provides details on the top losses (up to 10) shown in the chart.

Top Limit Adequacy Loss Details

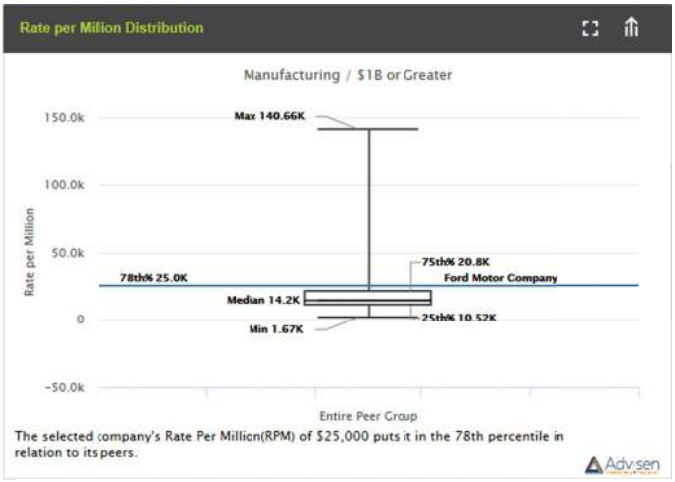
Company Name	Type of Incident	Incident Date	Records Affected	Case Status	Loss Amount	Type of Loss
Merck Sharp & Dohme Corp.	Network/Website Disruption	06/27/2017		Response Costs	285,000,000	Corporate Loss of Business Income/Services
Merck Sharp & Dohme Corp.	Network/Website Disruption	06/27/2017		Estimate	260,000,000	Corporate Loss of Business Income/Services
Reckitt Benckiser Group plc	Network/Website Disruption	06/27/2017		Estimate	142,000,000	Corporate Loss of Business Income/Services
Sony Corporation	Data - Malicious Breach	04/16/2011	100,000,000	Response Costs	142,000,000	Personal Financial Identity (PFI)
Leoni AG, Nuernberg	Phishing, Spoofing, Social Engineering	08/12/2016		Estimate	44,600,000	Corporate Loss of Financial Assets
Seagate US LLC	Phishing, Spoofing, Social Engineering	02/29/2016	8,292	Settled	42,003,500	Personal Financial Identity (PFI)
Seagate US LLC	Phishing, Spoofing, Social Engineering	02/29/2016	8,292	Estimate	42,000,000	Personal Financial Identity (PFI)

The Premium Distribution analysis benchmarks the premium of the proposed insurance program to the premiums paid by the selected peer group.

The Limit Distribution analysis benchmarks the limit of the proposed insurance program to the limits purchased by the selected peer group.



The Retention Distribution analysis benchmarks the retention of the proposed insurance program to the retention of similar companies.



The Rate per Million (RPM) Distribution analysis benchmarks the RPM of the proposed insurance program to the RPM of similar companies.

Report Generation

Users have the ability to generate a customizeable PDF document that includes any of the features previously described.

The Report function is available from the left menu option and will direct the user to the Report Selection screen.

By default, all sections will be selected when user arrives on the Report page. Users can de-select either an entire section (i.e. Frequency) or individual analyses within a section (i.e. Industry Overview).

The dashboard is a required component of the report and cannot be de-selected.

Glossary of Terms

A	
Accident Date	Date on which the incident occurred or began.
Affected Count	Refers to the number of individuals or systems affected. These could be based on the number of identities breached or stolen, social security numbers revealed, devices compromised, etc., depending on type of incident.
B	
Benchmarking Analysis	Analyses that give insight on how an organization's program compares to its peers.
C	
Case Type	The type of cyber incident based on a number of characteristics. Advisen captures 13 different case types, which are defined below.
Case Type Families	Groupings of multiple case types that share similar characteristics. These include:
Data Privacy	A grouping of case types that deal with situations where there has been an unauthorized breach or disclosure of personal information of some sort. These case types are as follows:
Data – Malicious Breach	Situations where personal confidential information or digital assets either has been or may have been exposed or stolen, by unauthorized internal or external actors whose intent appears to have been the acquisition of such information.
Data – Unintentional Disclosure	Situations where personal confidential information or digital assets have either been exposed, or may have been exposed, to unauthorized viewers due to an unintentional or inadvertent accident or error.
Data Physically Lost or Stolen	Situations where personal confidential information or digital assets have been included, or may have been included, with computer or peripheral equipment which has been lost, stolen, or improperly disposed of; the confidential information is incidentally included but unlikely to be the primary focus.
Phishing, Spoofing, Social Engineering	Attempts to get individuals to voluntarily provide information which could then be used illicitly, e.g. phishing or spoofing a legitimate website with a close replica to obtain account information.
Skimming Physical Tampering	Use of physical devices to illegally capture electronic information such as bank account or credit card

	numbers for individual transactions.
Identity - Fraudulent Use / Account Access	Actual identity theft or the fraudulent use of confidential personal information or account access.
Network Security	A grouping of case types that deal with situations involving the disruption or interference of corporate operations. These case types are as follows:
Network / Website Disruptions	Unauthorized use of or access to a computer or network, or interference with the operation of same, including virus, worm, malware, digital denial of service (DDOS), etc.
Cyber Extortion	Threats to fraudulently transfer funds, destroy data, interfere with the operation of a system/network/site, or disclose confidential digital information such as identities of customers/employees, unless payments are made
Industrial Controls & Operations	Losses involving disruption or attempted disruption to "connected" physical assets such as factories, automobiles, power plants, electrical grids, etc. (including "the internet of things")
Privacy Violations	A grouping of case types that deal with situations involving individual or corporate privacy, and frequently involves the violation of various laws and regulations dealing with the collection and disclosure of information to a third party, or contacting an individual or company without their permission. These case types are as follows:
Privacy – Unauthorized Data Collection	Cases where information about the users of electronic services, such as social media, cellphones, websites, etc. is captured and stored without their knowledge or consent
Privacy – Unauthorized Contact or Disclosure	Cases when personal information is used in an unauthorized manner to contact or publicize information regarding an individual or an organization without their explicit permission
Tech E&O	A grouping of case types that deal with situations involving the failure of corporate operations resulting from errors or oversights in the development, implementation, and/or maintenance of the organizations' IT environment. These case types are as follows:
IT – Processing Errors	Losses resulting from internal errors in electronically processing orders, purchases, registrations, etc.,

		usually due to a security or authorization inadequacy, software bug, hardware malfunction, or user error.
	IT – Configuration / Implementation Errors	Losses resulting from errors or mistakes which are made in maintaining, upgrading, replacing, or operating the hardware and software IT infrastructure of an organization, typically resulting in system, network, or web outages or disruptions
F	**Frequency Analysis**	Analyses based on the number of cyber incidents experienced over a given time period. In general, the analyses seek to compare the loss experience of a company against the average, median, and maximum loss experience of its peer group.
L	**Loss Profile**	Based off of the historical loss experience, the loss profile gives an indication of a company or peer group's loss propensity
	Company Loss Profile	The historical loss experience for the selected company. In general, this is indicated by the orange dots in the various charts.
	Peer Group Loss Profile	The historical loss experience for the peer group of the selected company. In general, this is indicated by the blue bars in the various charts.
P	**Peer Group**	A grouping of companies that share the same industry grouping (2 digit NAICS) and revenue range as the selected company.
R	**Revenue Bands**	Company revenue in USD. The following bands have been identified and are consistently applied across all industries: • Less than $25M • $25M to < $100M • $100M to < $250M • $250M to < $500M • $500M to < $1B • $1B to Greater
S	**Severity Analysis**	Analyses based on the number of records affected as a result of cyber incidents over a given time period. In general, the analyses seek to compare the loss experience of a company against the average,

	median, and maximum loss experience of its peer group.
Standard Deviation	The standard deviation quantifies the variation of a set of observations. A lower standard deviation indicates that observations tend to be closer to the mean, while a higher standard deviation indicates that observations are spread over a wider range of values in relation to the mean.
Type of Loss	The type of data, asset, or information that was compromised during a cyber incident. The two main groups are as follows:
Corporate Losses	A grouping of types of loss that relate to the compromise of corporate data or assets. These include:
Loss of Business Income / Services	Any interruption of normal business activities as a result of a cyber incident. These could be a consequence of Distributed Denial of Service (DDoS) attacks or reputational damage.
Loss of Digital Assets	Business and customer data, trade secrets, proprietary software and other confidential corporate data.
Loss of Financial Assets	Money, securities and other financial property, including digital currency such as Bitcoins that belong to either the company or its clients.
Personal Information	A grouping of types of loss that relate to the compromise of personal information. These include:
Personal Identifiable Information	Data containing identifying information, including name, address, e-mail, date of birth, gender etc.
Personal Health Information	Data specifically protected under health information laws and regulations (such as HIPAA), including medical records and health information
Personal Financial Information	Credit/debit card details, social security numbers, banking financial records (account numbers, routing numbers, etc.)