

Cyence Risk Analytics

A risk assessment tool for cyber underwriters

The Cyence Risk Analytics dashboard for Nordstrom, Inc. provides a comprehensive overview of the company's cyber risk profile. Key metrics include:

- Industry:** Retail Trade, Sub-Industry: Department Stores
- Annual revenue:** \$50-\$70B
- Estimated record count:** 315.2M + PCI 100%
- Employee count:** 10,000+
- Location:** San Mateo, California, USA

The dashboard is divided into several sections:

- Exposure Signals:** Overall risk grade is C (54), Percentile: 41st. Top exposure signals include Spam activity (Detected), Foreign hacker activity (Detected), and Network complexity (High).
- Probability of Incident:** Overall probability of incident is 15.4%, Percentile: 14th. Breakdown includes Data breach probability (10.4%) and Ransomware probability (8.2%).
- Loss Analysis:** Average Annual Loss (AAL) is \$8.8M, Percentile: 94th. Ground up AAL is \$8,842,106.

Additional features include a peer comparison section showing 39 peers filtered, and a sidebar for adding to a portfolio or viewing the Cyence Risk Report.

© 2015-2021 Cyence LLC
Privacy Policy | Terms of Use | Cyence Support



About Cyence Risk Analytics

Cyence for cyber is a risk analytics tools used by underwriters to evaluate a risk of a business with online presence.

The underwriters than use this information to make underwriting and pricing decision.

It helps them to underwrite a risk with appropriate premium for insuring an online / digital business.

Persona

Cyber Underwriters

⚠ Problems:

- I don't have enough information to determine a business risk.
- Risk evaluation is a time taking process due to administrative tasks.
- I struggle with gathering information about possible next action based on identified risk.

❑ Needs:

- I need to understand a company's risk faster and efficiently.
- I need actionable items to make effective underwriting decisions.

James
Cyber Underwriter

Age: 32
Employer: Insurer focusing on profitable cyber risks
Location: North America

Industry experience

Data analysis & technical skills

Time spent using Guidewire products

I interact with:

Internal:
Underwriting Manager
Underwriting Assistants
Pricing Actuary

External:
Agents
Carrier/Insured company

Tools I use:

- Guidewire Cyence for Cyber
- Google Search
- Office Suite (Excel, PowerPoint, Word)
- Outlook or other email service
- Policy admin systems (like PolicyCenter)

"I identify, understand, measure, and evaluate highly complex risk and provide applicable terms and conditions to make profitable decisions for my company."



I instantly gain differentiating insights to identify emerging risks.

I obtain necessary data points to write a company and determine pricing efficiently.

I am able to quantify risk based on experience history and forecasting methods.



MY RESPONSIBILITIES AND DECISIONS...

Solicit new and renewal submissions:

- What information do I need to collect to complete the submission?

Determine appropriate pricing of complex risks:

- How should the company be priced? How do I justify the risk I write?

Analyze highly complex risks underwritten:

- How do I evaluate the quality, quantity, and profitability of risks I write?

Interact with Agents:

- How can I engage them around why information is needed?

I'M FRUSTRATED WHEN...



- I don't have enough information to determine a business' risk.
- I'm unable to locate and document risk evaluation data.
- Valuable time is spent on administrative tasks.
- I can't keep up with trends in the quickly evolving marketplace.
- It's hard to differentiate from competition based on pricing and offerings.

MY SUCCESS IS MEASURED BY...



- The number of profitable businesses written.
- Growth of the company portfolio.
- Quality of interactions with Agents and colleagues.
- Timeliness and accuracy.
- Compliance with guidelines.

DESIGNING FOR JAMES:

I need clear guidance on how to use the tool and I want to understand how it can improve my work efficiency. It's important that I be able to effectively integrate it within my risk evaluation process.

I want to leverage the power of the tool to understand a company's risk thoroughly. Standardized metrics with easy-to-understand visualizations can be very helpful.

Design Process

The design process is broken down in 2 stages

Pre-production

 User Research

 Ideation & Design

 Usability Testing

 Reiterate Design

 Deliver & Develop

Post-production

 Onboarding Design

 Release

 In-App UI Feedback

 Track Usage

 Design Backlog



User Research

Research Insights:

- # of customer involved: 7
- # of users: 10 (Underwriters and Underwriter leadership)
- Research set up: 1hr online zoom calls

Research Goals:

- To understand the reason behind identified usage patterns.
- To understand how the users are currently using all the information within application.
- To identify problems and friction points users are facing while using our risk analytics tool.



4 key identified problems...



Hard to understand the correlation between data



Hard to find impactful and most concerning information



Don't know what to do with certain information

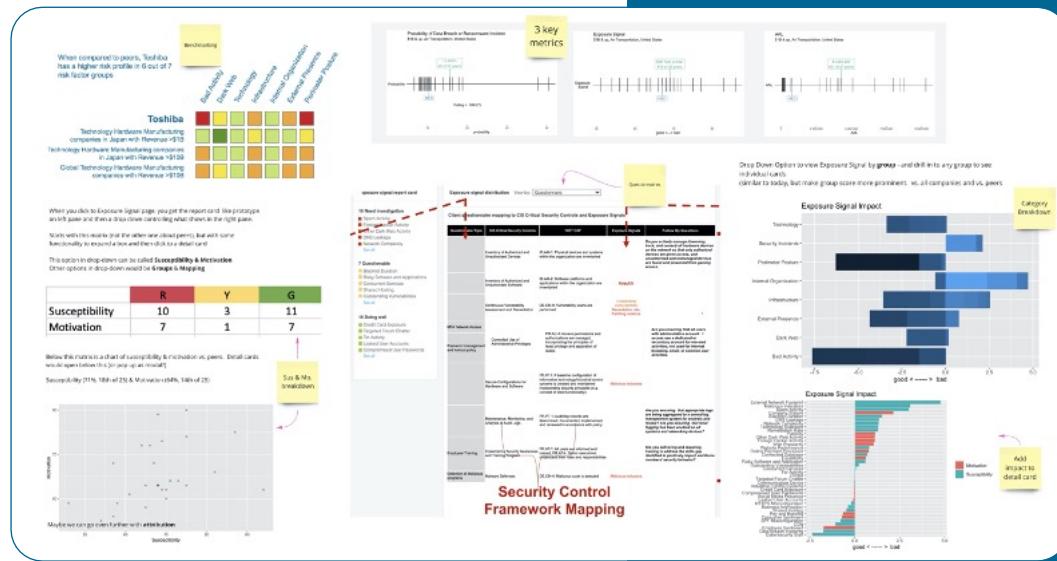


Found the UX and printable report old and outdated

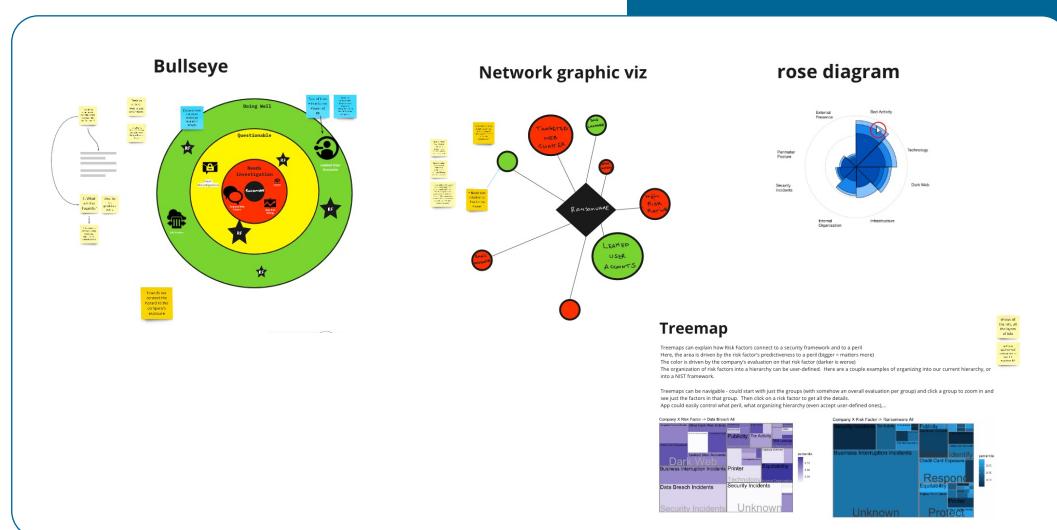
Proposed Solution

- Provide users a clear representation about the correlation of different data though out the UI.
 - Provide a new overview page with most important information in order to increase productivity.
 - Provide help text to users in order to understand the usage of information along with actionable steps which can them to move further in process.
 - Provide users a new experience for the downloadable report format like new UI.

Ideation board



Data visualization exploration



Company Overview Page

Problems with old UX

01

A primary metrics which is usually misunderstood by underwriters

02

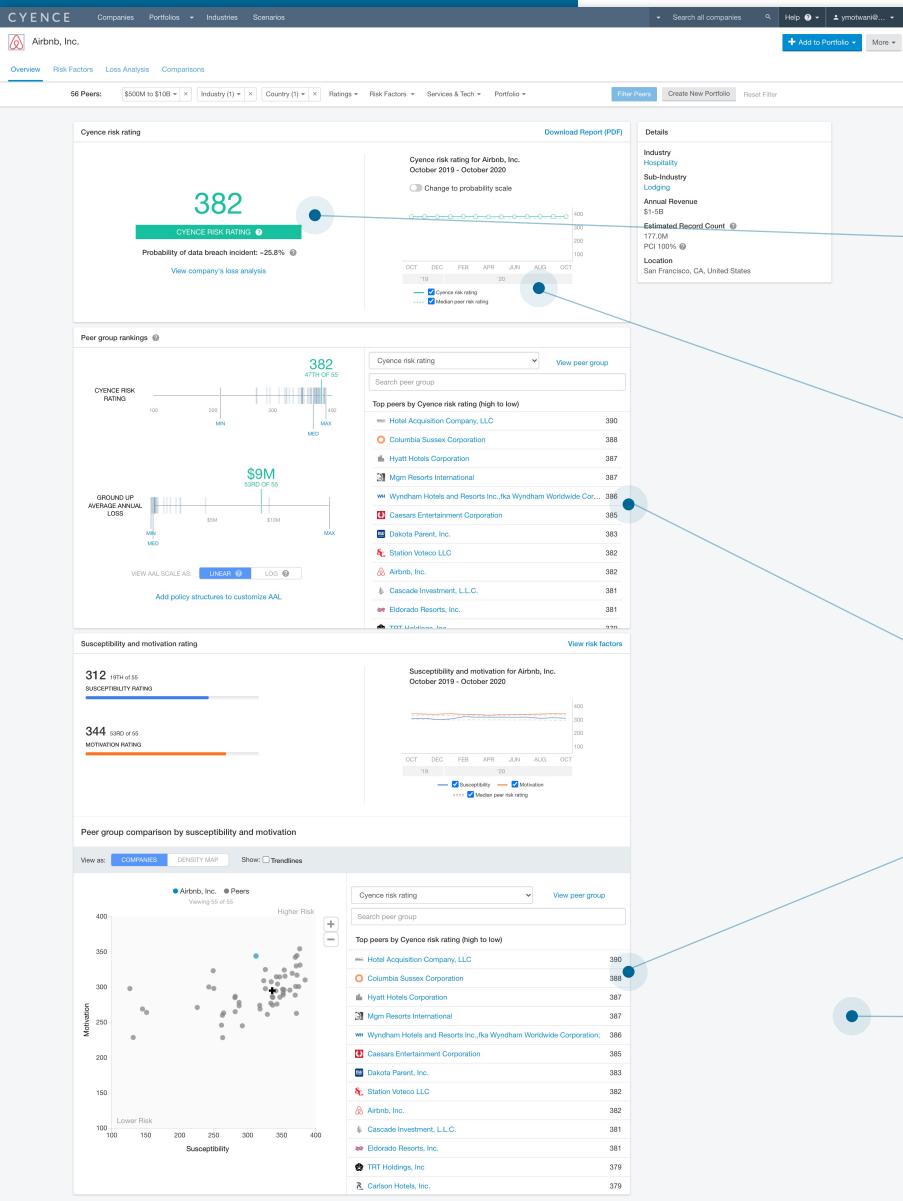
Historical trend is a secondary information but highly emphasized

03

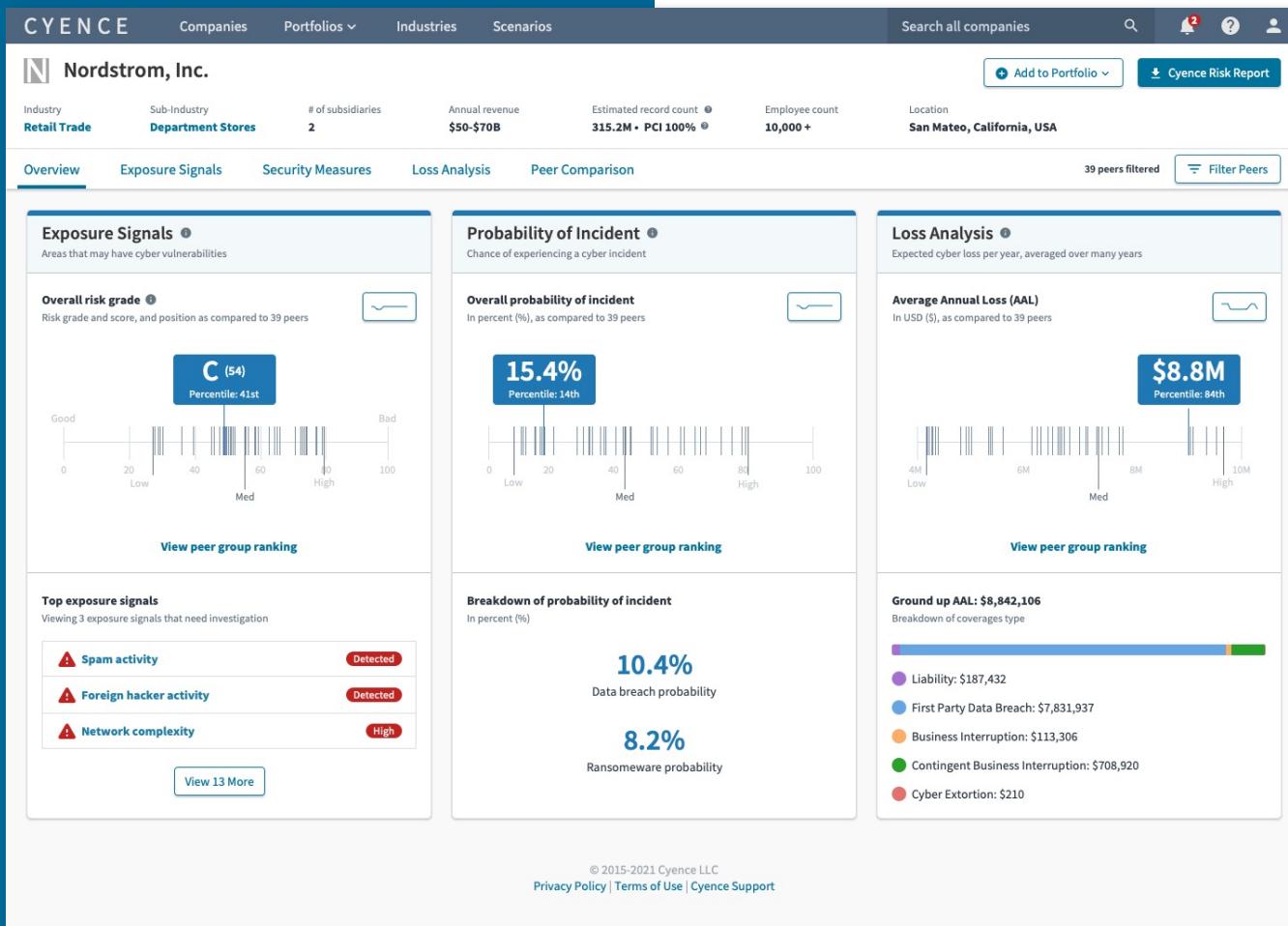
Repeated information and list of ranking which is not used that often

04

A lot of white space and unnecessary scrolling



Company Overview Page



New UX

New Information Architecture

New hierarchy of information to highlight the most important information up front.

Simplified Layout & Insights

New 3 column layout to provide the distinction of 3 different data points to identify risk.

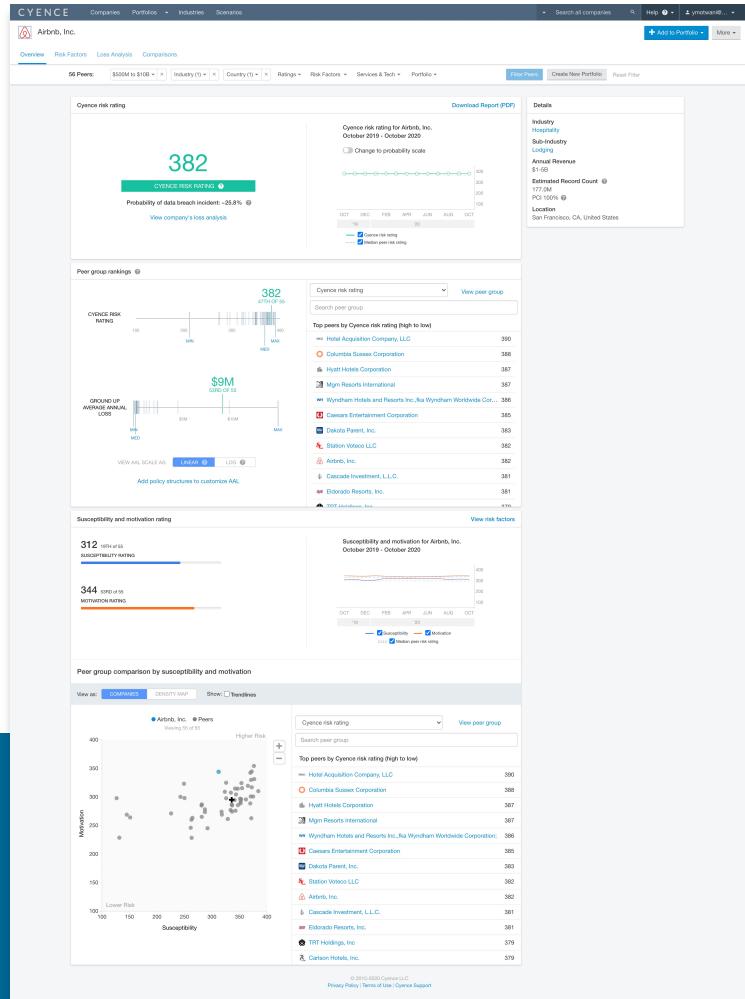
Simplified Data Visualization

Sparkline graphs to show the history trendlines for different data points to further simplify the experience.

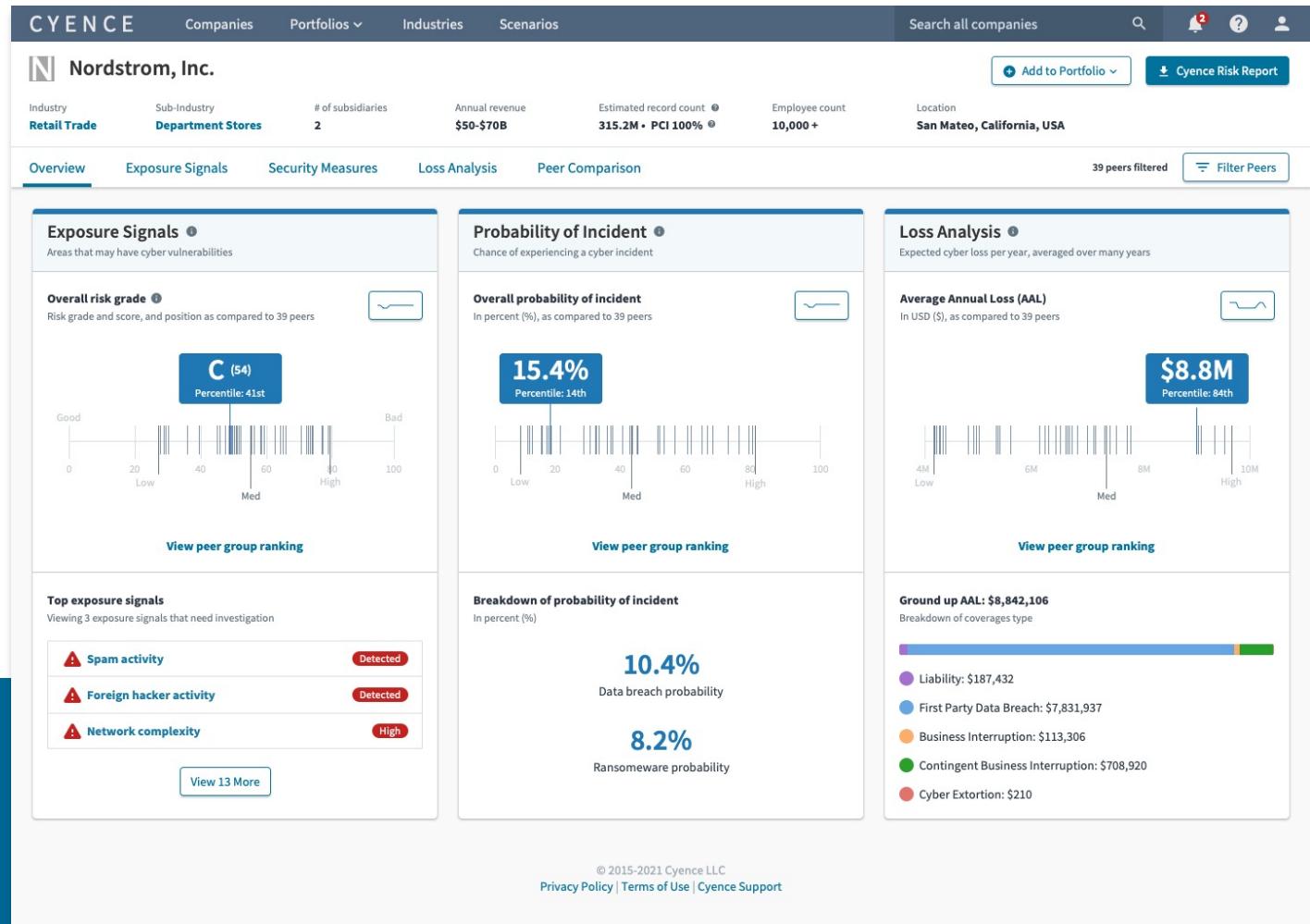
Old vs New UX

Company Overview Page

Old UX



New UX



CYENCE Companies Portfolios Industries Scenarios Search all companies Help ymotwani@... Add to Portfolio More

Airbnb, Inc.

Overview Risk Factors Loss Analysis Comparisons

56 Peers: \$500M to \$10B Industry (1) Country (1) Ratings Risk Factors Services & Tech Portfolio Filter Peers Create New Portfolio Reset Filter

Top risk factors

Positive Risk Factors

- Infrastructure
 - CDN (Present)
 - CDNs offer redundancy and the ability to absorb or neutralize potential threats to a site (like DOS), diversifying the company's risk through an added layer of security.
- Internal Organization
 - Employee Sentiment (Happy workforce)
 - Employees are responsible for a significant portion of cybersecurity breaches, either deliberately (by performing the attack themselves or collaborating with an outside threat), or unwittingly (by engaging in risky behavior or falling victim to social engineering tactics). Poor internal sentiment increases not only the likelihood of inside job hacks, but also the risk of external attacks that prey on human error.
- SPF Misconfiguration (Not detected)

Negative Risk Factors

- Dark Web
 - Compromised User Passwords (Detected)
 - Combinations of employee usernames and passwords may be used by malicious actors to gain access to corporate accounts, especially given the prevalence of password reuse.
- Leaked User Accounts (Detected)
- External Presence
 - Company Statute (Extensive footprint)
 - A company who holds top-of-mind awareness with the public also makes a more striking target in the eyes of criminal hackers.

All risk factors

Bad Activity (Improved)

Bad activity traced back to the company's network generally indicates substandard security hygiene or an infected/compromised network.

Dark Web (Unchanged)

The Dark Web is a popular resource among malicious actors, providing them the latest information on hacking innovations and security vulnerabilities. Dark web activity linked to a company generally shows evidence of hacker interest and could indicate that a breach has already occurred or that there is an increased likelihood of an upcoming breach.

Technology (Unchanged)

Technologies comprising the company network may reflect the complexity of its systems, general exposure to threats and vulnerabilities, and the sophistication and posture of the company's IT staff.

Infrastructure (Worsened)

Website design, server performance, and network configurations may reflect the company's IT sophistication and overall security posture.

Internal Organization (Unchanged)

The manner in which an organization is run affects the conduct, efficiency, and reliability of its human capital, which is a critical part of the defense against cyber attacks.

External Presence (Improved)

A ubiquitous public presence or unfavorable reputation may expose a company to increased risk of being targeted for an attack.

Perimeter Posture (Unchanged)

A company's risk increases with the number of attack vectors and exploitable vulnerabilities present in the network. Vulnerabilities on the company's internet-facing systems may allow access to other parts of the network. Perimeter security, which is the first layer of defense in a company's network, may also indicate overall security hygiene and strength of cyber defenses.

Security Incidents (Unchanged)

Past occurrences of security incidents may reflect a company's general exposure to cyber risk. No recent security incidents, 19 peer incidents

Services & Technologies

- Service provider (5)
 - Akamai (All Regions)
 - Cloudflare (All Regions)
 - Amazon Virginia (East US/Canada)
 - (Cloud service provider)
- Show More
- Software (17)
 - Apache HTTP Server
 - Microsoft IIS
 - Dovecot
 - Mail server
 - Drupal
 - Web application
- Show More
- Payment processor (13)
 - Adyen
 - Alipay
 - American Express
- Show More

© 2015-2020 Cyence, LLC Privacy Policy Terms of Use Cyence Support

Exposure Signals Page

Problems with old UX

01

Underwriters didn't care about positive risk factors

02

Showed high impact risk categories but didn't tell users any actionable insights

03

A lot of white space and unnecessary scrolling

CYENCE Companies Portfolios Industries Scenarios Search all companies

Nordstrom, Inc.

Industry: Retail Trade Sub-Industry: Department Stores # of subsidiaries: 2 Annual revenue: \$50-\$70B Estimated record count: 315.2M • PCI 100% Employee count: 10,000+ Location: San Mateo, California, USA

Add to Portfolio Cyence Risk Report

Overview Exposure Signals Security Measures Loss Analysis Peer Comparison 39 peers filtered Filter Peers

Exposure Signal Breakdown

Overall Exposure Signal: C (54) Categories: Technology Risk Grade: D (74) Peer Comparison: 79% of peers are better

Exposure Signals	Status	Impact
Online Payment Processor	Detected	High
Risky Software and Applications	Restrained	Medium
Connected Database	Not Detected	Low
Technology Exposure	Low	Medium
Communication Device	Not detected	Medium
Exposed Printers	Not detected	Low

Exposure Signal Report Card

Total Exposure Signals: 39

Worse than Peers	Similar to Peers	Better than Peers
6	2	2
9	4	13
1	1	1

Needs investigation (16) View All

- ⚠ Spam Activity
- ⚠ Compromised User Passwords
- ⚠ DNS Leakage

Suspicious (7) View All

- ⚠ Network Complexity
- ⚠ Risky Software and Applications
- ⚠ Shared Hosting

No issues (16) View All

- ✓ HTTPS Misconfiguration
- ✓ Targeted Forum Chatter
- ✓ Connected Database

All (39) Pinned (2)

Search Exposure Signal Expand All

Spam Activity Detected

Propagation of unsolicited junk email distributed to a large number of recipients

Mail servers being used to distribute spam may indicate system misconfiguration or compromised user credentials, which puts the company at risk

IP Address detected

48.155.250.79
214.46.244.249
196.64.8.69
109.219.90.255

Signal Category: Bad Activity
Signal type: Susceptibility
Signal impact: High

Peer group comparison

NOT DETECTED: 55% peers
DETECTED: This company, and 45% peers

Status in last 3 months: Unchanged

SEP 2020 OCT 2020 NOV 2020

Security control mapping
CIS: CSC7, CSC13, CSC17
NIST: ID-AM, DE-CM, PR-DS, PR-AC

Was it helpful?

Exposure Signals Page

New UX

Exposure Signals is the most used page in the app, and as part of improvement we wanted to make this more effective and useful for our users by introducing:

① Updated Prioritization

The new prioritization was based on type of signal and severity. Now users can also pin them.

② Introduced Report Card

To enable users easily navigate through most concerning risks.

③ Simplified Data Visualization

A tree view for underwriters to identify the most vulnerable risk through grading and risk impact.

④ Actionable Security Measures

We provided our users a set of follow up questions they can ask to their customers to mitigate the risk.

Old vs New UX

Exposure Signal Page

Old UX

This screenshot shows the old CYENCE platform's exposure signal page for AirbnB, Inc. The top navigation bar includes links for Companies, Portfolios, Industries, Scenarios, and a search bar. Below the header, there are tabs for Overview, Risk Factors, Loss Analysis, and Comparisons. The main content area is divided into several sections:

- Top risk factors:** A grid showing Positive Risk Factors (e.g., Infrastructure, Internal Organization) and Negative Risk Factors (e.g., Dark Web, Compromised User Passwords).
- Services & technologies:** A sidebar listing Service provider (5), Software (17), and Payment processor (19) categories.
- All risk factors:** A large section listing various risk factors like Bad Activity, Technology, Infrastructure, Internal Organization, External Presence, Perimeter Posture, and Security Incidents, each with a brief description and a status indicator.

New UX

This screenshot shows the updated CYENCE platform's exposure signal page for Nordstrom, Inc. The top navigation bar is similar to the old version. The main content area is organized into several sections:

- Overview:** Displays key company information: Industry (Retail Trade), Sub-Industry (Department Stores), # of subsidiaries (2), Annual revenue (\$50-\$70B), Estimated record count (315.2M), Employee count (10,000+), and Location (San Mateo, California, USA).
- Exposure Signals:** The primary focus, showing an overall exposure signal grade C (54) with 41% of peers being better. It includes a breakdown by category: Technology (D 74), Security Incidents (D 79), Perimeter Exposure (B 28), Internal Organizations (A 18), Infrastructure (B 33), External Presence (C 64), Dark Web (A 12), and Bad Activity (C 69). Each category has a detailed description and a peer comparison chart.
- Exposure Signal Report Card:** A summary card showing counts for different risk levels: Worse than Peers (6 red, 2 yellow, 2 green), Similar to Peers (9 red, 4 yellow, 13 green), and Better than Peers (1 red, 1 yellow, 1 green).
- Needs investigation (16):** A list of items requiring attention, including Spam Activity, Compromised User Passwords, and DNS Leakage.
- Suspicious (7):** A list of items flagged as suspicious, including Network Complexity, Risky Software and Applications, and Shared Hosting.
- No issues (16):** A list of items with no significant issues, including HTTPS Misconfiguration, Targeted Forum Chatter, and Connected Database.
- All (39) Pinned (2):** A list of pinned exposure signals, including Spam Activity (Detected), Compromised User Password (Detected), DNS Leakage (Detected), Network Complexity (High), Risky Software and Application (Moderate), Shared Hosting (Significant), and Foreign Hacker Activity (Detected).

Downloadable Report

Old UX

Nordstrom, Inc.
Cyence Unique ID: b10e9f91
Report generated on December 14, 2020
with data from November 2020

Company Overview
Nordstrom, Inc.
Cyence Unique ID: b10e9f91

Company Overview

Cyence Risk Rating	Susceptibility Rating	Motivation Rating
388 Out of 400	368 Out of 400	347 Out of 400
Peer range: 335-390	Peer range: 290-379	Peer range: 231-357
Peer median: 376	Peer median: 334	Peer median: 311

See following report for further details.

Company Details

Details

Industry: Retail Trade
Sub-Industry: Apparel Retailers
Annual Revenue: \$10-50B
Estimated Record Count: 262.4M
PCI 100%
Location: Seattle, WA, United States

Services & Technologies

Service provider (13 found)
Software (22 found)
Payment processor (5 found)
Auditor (1 found)

Refer to the Appendix for full listing of Services and Technologies.

This document and any recommendations, analysis, or advice provided by Cyence LLC ("Cyence") (collectively, the "Analysis") is intended solely for the entity identified as the recipient and is not to be distributed outside of that entity without the express written consent of Cyence and is intended for your internal use only, and may not be shared with any third party without Cyence's prior written consent. Any statements concerning professional advice, including recommendations and analyses, set forth in the Analysis are based on information and data that has been collected and analyzed by Cyence. The Analysis is not based upon any professional advice, for which you should consult your own professional advisors. Any mention of specific companies, products, services, or technologies is for illustrative purposes only and does not imply endorsement. The Analysis is not intended to be comprehensive and may not be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources believed to be reliable, but its accuracy or completeness cannot be guaranteed or assured. All representations and warranties, express, implied, or statutory, including any implied warranty of merchantability, fitness for a particular purpose, title, non-infringement, and implied warranties of fitness for a particular purpose, are disclaimed and the Analysis is provided "as-is." Without limiting the foregoing, Cyence makes no warranty, guarantee, or representation, express or implied, that the Analysis will meet your or any other party's requirements, or achieve any intended result. Cyence shall have no obligation to update the Analysis and shall have no liability to you or any other party with respect to the Analysis or any other information or data provided in the Analysis. By accepting and/or using this report, you acknowledge and agree to the terms, conditions and disclaimers set forth above.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 3 of 39

Company Overview
Nordstrom, Inc.
Cyence Unique ID: b10e9f91

Company Overview

Cyence Risk Rating	Susceptibility Rating	Motivation Rating
388 Out of 400	368 Out of 400	347 Out of 400
Peer range: 335-390	Peer range: 290-379	Peer range: 231-357
Peer median: 376	Peer median: 334	Peer median: 311

Risk Overview

Cyence Risk Rating	Risk Rating
388 Out of 400	The Cyence Risk Rating is a measure of a company's cyber risk, or the likelihood that it would experience a data breach or other cybersecurity incident due to the handling of protected information. This is derived from a combination of technical and non-technical indicators, including the company's Susceptibility, Motivation, and Risk Factors. Based on a 100-400 scale, a higher Risk Rating indicates greater risk.

Probability of Data Breach
~36.4%

37th of 39
Among its peer group of 39 companies

Peer Risk Comparison

Peer of Nordstrom, Inc., have Risk Ratings ranging from 335 to 390. The median Risk Rating among peers is 376.

Refer to the Appendix for peer group details.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 4 of 39

Company Overview: Risk Overview
Nordstrom, Inc.
Cyence Unique ID: b10e9f91

Risk Overview

Cyence Risk Rating	Risk Rating
388 Out of 400	The Cyence Risk Rating is a measure of a company's cyber risk, or the likelihood that it would experience a data breach or other cybersecurity incident due to the handling of protected information. This is derived from a combination of technical and non-technical indicators, including the company's Susceptibility, Motivation, and Risk Factors. Based on a 100-400 scale, a higher Risk Rating indicates greater risk.

Probability of Data Breach
~36.4%

37th of 39
Among its peer group of 39 companies

Risk Rating

The Cyence Risk Rating is a measure of a company's cyber risk, or the likelihood that it would experience a data breach or other cybersecurity incident due to the handling of protected information. This is derived from a combination of technical and non-technical indicators, including the company's Susceptibility, Motivation, and Risk Factors. Based on a 100-400 scale, a higher Risk Rating indicates greater risk.

Probability of Data Breach
The Probability of Data Breach is mapped to the Cyence Risk Rating. This represents the probability of a company having at least one breach over the next 12 months. Actual historical data estimates and actual probabilities may vary.

Peer Risk Comparison

Peer of Nordstrom, Inc., have Risk Ratings ranging from 335 to 390. The median Risk Rating among peers is 376.

Refer to the Appendix for peer group details.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 4 of 39

Company Overview: Risk Overview
Nordstrom, Inc.
Cyence Unique ID: b10e9f91

Historical Rating Over Time

Risk

NOV '19 JUN '20 NOV '20

Historical Probability Over Time

Probability

NOV '19 JUN '20 NOV '20

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 5 of 39

Risk Factors: Top Risk Factors
Nordstrom, Inc.
Cyence Unique ID: b10e9f91

Top Risk Factors

Top Risk Factors are the most significant factors impacting a company's Risk Rating. Positive Risk Factors are those that reduce a company's Risk Rating, while Negative Risk Factors are those that increase a company's Risk Rating.

Positive Risk Factors

- Infrastructure
- Cloud Environment
- CDNs offer redundancy and the ability to absorb or neutralize potential threats to a site like DDoS, diversifying the company's risk through an added layer of security.

Negative Risk Factors

- SPP Misconfiguration - Not detected
- A carefully tailored SPP record in the Domain Name System protects the company against email spoofing. The absence or improper configuration of SPP exposes the company to fraudulent use of its domain name for spam and phishing emails carrying fake sender addresses.
- Internal Organization
- Employee Sentiment - Content workforce
- Employees are responsible for a significant portion of cybersecurity breaches, either deliberately (by performing the attack themselves or collaborating with an outsider), or unwittingly (by engaging in risky behavior or falling victim to social engineering tactics). Poor internal sentiment increases not only the likelihood of inside job hacks, but also the risk of external attacks that prey on human error.
- Dark Web
- Compromised User Passwords - Detected
- Combinations of employee usernames and passwords may be used by malicious actors to gain access to corporate accounts, especially given the prevalence of password reuse.
- External Proxies
- Competitor Status - Extensive Footprint
- A company who holds top of mind awareness with the public also makes a more striking target in the eyes of criminal hackers.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 10 of 39

Downloadable Report

New UX

GUIDEWIRE

Cyence Risk Report for
Care Wear, Inc.

Unique ID: bdqoeybjreq
Report generated on February 26, 2020
with data from November 2019

This document and any recommendations, analysis, or advice provided by Cyence LLC ("Cyence") (collectively, the "Analysis") is intended solely for the entity identified as the recipient herein ("you"). This document contains proprietary, confidential information of Cyence and is intended for your internal use only, and may not be shared with any third party without Cyence's prior written consent. Any statements concerning professional advice, including but not limited to actuarial, tax, accounting, or legal matters, are not to be relied upon as professional advice, for which you should consult your own professional advisor. Cyence makes no representations or warranties regarding the accuracy of the Analysis. The Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy or completeness. All representations and warranties made by Cyence, including implied warranties of merchantability, fitness for a particular purpose, title, non-infringement of intellectual rights, from course of dealing, usage or trade practice, are disclaimed and the Analysis is provided "as-is." Without limiting the foregoing, Cyence makes no warranty of any kind that the Analysis, or any results of the use thereof, will meet your or any other party's requirements, or achieve any intended result. Cyence shall have no obligation to update the Analysis and shall have no liability to you or any other party with regard to the Analysis or to any services provided by a third party to you by Cyence. By accepting and/or using this report, you acknowledge and agree to the terms, conditions and disclaimers set forth above.

Care Wear, Inc.
Cyence Unique ID: bdqoeybjreq

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 2 of 35

Company Overview

Care Wear, Inc.

Company Overview

Industry: Retail Trade
Sub-Industry: Apparel Retailers
Annual Revenue: \$10-50B

Estimated Record Count: 262.4M
PCI 100%
Location: Seattle, WA, United States

Risk Overview

Risk Rating

310 of 400
Based on 15.4% probability

51st Percentile
Peer range: 290-400
Peer median: 320

Probability of Incident

15.4%
Probability in percent (%)

26th Percentile
Peer range: 12% - 49%
Peer median: 24%

Average Annual Loss

\$8.1m
Losses in USD (\$)

72nd Percentile
Peer range: \$3.1 - 9.4m
Peer median: \$5.3m

Change in history



Nov Jan Mar May Jul Sep Nov
'19 '20

Change in history



Nov Jan Mar May Jul Sep Nov
'19 '20

Change in history



Nov Jan Mar May Jul Sep Nov
'19 '20

Care Wear, Inc.
Cyence Unique ID: bdqoeybjreq

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 2 of 35

Top Exposure Signals

Top Exposure Signals

Based on peer comparison

Needs investigation

Spam activity Propagation of unsolicited junk email distributed to a large number of recipients Detected

Foreign hacker activity Discussions about the company conducted in non-English forums (such as Russian, Chinese, etc.) Detected

Network Complexity Measure of breadth and intricacy of the company's external network based on an evaluation of its DNS (Domain Name System) hierarchy High

Suspicious

Network Complexity Lorem ipsum is simply dummy text of the printing and typesetting industry. Detected

Risky Software and Applications Lorem ipsum is simply dummy text of the printing and typesetting industry. Lorem ipsum has been the industry's standard dummy. Detected

Shared Hosting Lorem ipsum is simply dummy text of the printing and typesetting industry. Lorem ipsum has been the industry's standard dummy text ever since the 1500s. High

Care Wear, Inc.
Cyence Unique ID: bdqoeybjreq

Confidential - Presented to Cyence LLC - For Internal Use Only

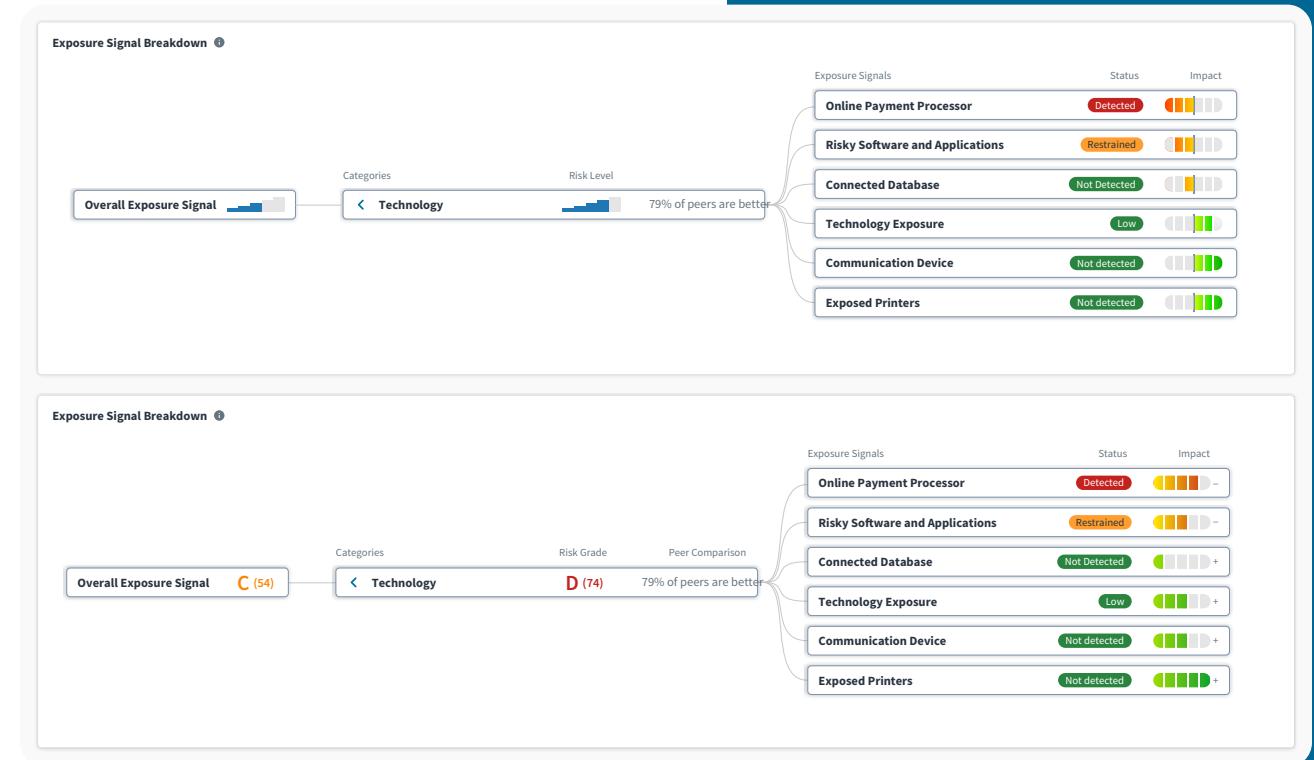
Page 3 of 35

Usability and A/B Testing

Risk Rating (Graph vs Grading)

We conducted A/B testing for deciding different data visualization and risk scaling system.

We ended up with Grading system because users were interested in granular differences of different risk level.



Onboarding Design Process

List features & define steps

Create & review content

Create & publish guide

Topics	Changes	Pendo Walkthrough
Overview page (3 column layout)	<ul style="list-style-type: none"> 1. Top 3 exposure signals and security measures questionnaire snippet 2. Probability of incident including DB and RW breakdown along with Risk Rating. 3. Loss Analysis with AAL and Breakdown of coverages 	<p>Step 1: Highlevel 3 layout</p> <p>Step 2: New historical trend line</p>
Exposure Signal page	<ul style="list-style-type: none"> 1. Interactive Report Card <ul style="list-style-type: none"> ◦ View by peer comparison ◦ View by Sus/Mo. ◦ Top 3 exposure signals of High, Medium, Low type 2. Exposure signal detail changes <ul style="list-style-type: none"> ◦ Icons in addition to color for High, Medium, Low ◦ Updated UI view on closed card ◦ Past 3 month changes instead of 2 previously ◦ Security Measure questionnaire ◦ Security control mapping 	<p>Step 3: Report Card</p> <p>Step 4: In context security measures and control mapping.</p>
Security Measures page	<ul style="list-style-type: none"> 1. NIST/CIS Security Measures <ul style="list-style-type: none"> ◦ Common questionnaire for both frameworks ◦ Downloadable questionnaire ◦ Search for ESig withing Security Measures ◦ Default sorting of ESig from High-Low 	<p>Step 5: What is Security Measures?</p> <p>Step 6: Downloadable questionnaire.</p>
Peer Comparison page	<ul style="list-style-type: none"> 1. Sus/Mo (previously in overview page) in collapsed container 2. List of filtered peers 3. Company compare (Same as before) 	Step 7: Moved Sus/Mo.

Cyence Onboarding Guide

1. What's New

We are proud to announce several new features for Cyence. 😊

1. On-demand assessments for new companies can be made directly ~~from the application~~ from within the application

2. Introducing the Underwriter Dashboard in the company 'Overview' page

3. Risk Factors are ~~now referred to as Exposure Signals~~

4. Exposure Signals are mapped to NIST & CIS cyber security frameworks and include actionable next steps

We encourage you to walk through the Quick Guide to familiarize yourself with the new user experience.

[Start Quick Guide](#)

Hunter Nielsen "for" instead of "to"
Hunter Nielsen "from within the application"
Hunter Nielsen Should this say, "Risk Factors are no longer referred to as Exposure Signals?"
 Were they before?
Hunter Nielsen You need ending punctuation here (.) May 28, 2021

2. On-Demand Assessments 📈

<GIF on how to access and request an assessment>

Unable to find a company in Cyence? You can now request an On-Demand Assessment for a new company directly ~~from the application~~ from within the application and review the results in minutes!

Next: Updates to the company Overview page

[Continue](#)

Hunter Nielsen "from within the application"

3. Introducing Underwriters Dashboard

The company overview page is now updated to highlight the three methods by which to evaluate cyber risk. These include:

1. Exposure Signals
2. Probability of Incident (Risk Rating)
3. Loss Analysis

You can learn more about each method ~~by clicking help icons (?) within dashboard~~ by clicking help icons (?) within the dashboard

Next: Updates to the Cyence Risk Report (PDF)

[Back](#) [Continue](#)

Hunter Nielsen "We've updated the company 'Overview' page to highlight three methods that you can use to evaluate cyber risk."
Hunter Nielsen "by clicking the help icons (?) within the dashboard."



We are proud to announce several new features for Cyence. 😊

1. introducing the **Overview dashboard** for underwriting and risk selection
2. **Risk Factors** are now referred to as **Exposure Signals**
3. **Exposure Signals** are mapped to NIST & CIS cyber security frameworks and include actionable next steps

We encourage you to walk through the Quick Guide to familiarize yourself with the new user experience.

[Start Quick Guide](#)

Onboarding Design Samples

Onboarding Guide

The screenshot shows the Cyence platform's onboarding guide. At the top, there's a navigation bar with 'CYENCE' and links for 'Companies', 'Portfolios', 'Industries', and 'Scenarios'. Below the navigation is a user profile section showing 'Hello, Yogesh Motwani' and 'Last login: 09 Jun 2021 11:50:15 AM'. The main content area has sections for 'My managed items' (0 Company Policy Structures), 'Recently viewed' (Companies: Apple Inc., Guidewire Software Inc., Karam, Inc., Alphabet Inc.), and 'I want to...' (View scenarios, View groups and portfolios, Compare portfolios, Create a portfolio, Run a scenario). A central callout box titled 'WHAT'S NEW' announces new features like the Overview dashboard, Risk Factors, and Exposure Signals. It also encourages users to walk through the Quick Guide. The footer includes a copyright notice: '© 2019-2021 Cyence LLC'.

In-App UI Feedback

The screenshot shows a feedback modal window. The header includes the 'CYENCE' logo and navigation links. The main content asks for a rating on changes to the underwriter dashboard, with a scale from 1 (Horrible) to 5 (Awesome). Below the rating is a text input field for comments and a 'Submit' button. The background of the modal is semi-transparent, showing the Cyence interface with sections for 'My managed items' (0 Company Policy Structures, 1 Portfolio, Create Portfolio groups, Run Scenarios), 'Recently viewed' (Companies: Apple Inc., Guidewire Software Inc.), and 'Portfolios' (Sample Portfolio). The footer of the modal also includes a copyright notice: '© 2019-2021 Cyence LLC'.

Product Success Metrics

The process of defining success metrics

 Define

 Review

 Track & Report

 Reflect

 Design Backlog

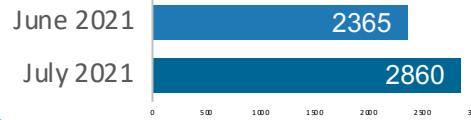
Some key insights

Month-over-month comparison

JUNE 2021 TO JULY 2021

Unique Companies Viewed

 21%



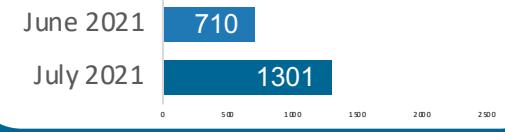
Time spent on new pages

 49%



Report Downloads

 83%





Thank You!

CYENCE Companies Portfolios Industries Scenarios Search all companies

Nordstrom, Inc.

Industry: Retail Trade Sub-Industry: Department Stores # of subsidiaries: 2 Annual revenue: \$50-\$70B Estimated record count: 315.2M • PCI 100% Employee count: 10,000+ Location: San Mateo, California, USA

Add to Portfolio Cyence Risk Report

Overview Exposure Signals Security Measures Loss Analysis Peer Comparison 39 peers filtered Filter Peers

Exposure Signals Areas that may have cyber vulnerabilities

Overall risk grade: C (54) Percentile: 41st

View peer group ranking

Probability of Incident Chance of experiencing a cyber incident

Overall probability of incident In percent (%), as compared to 39 peers

15.4% Percentile: 14th

View peer group ranking

Loss Analysis Expected cyber loss per year, averaged over many years

Average Annual Loss (AAL) In USD (\$), as compared to 39 peers

\$8.8M Percentile: 94th

View peer group ranking

Ground up AAL: \$8,842,106 Breakdown of coverages type

Liability: \$187,432 First Party Data Breach: \$7,831,937 Business Interruption: \$113,306 Contingent Business Interruption: \$708,920 Cyber Extortion: \$210

Top exposure signals Viewing 3 exposure signals that need investigation

Spam activity Detected

Foreign hacker activity Detected

Network complexity High

View 13 More

Breakdown of probability of incident In percent (%)

10.4% Data breach probability

8.2% Ransomware probability

© 2015-2021 Cyence LLC
Privacy Policy | Terms of Use | Cyence Support