

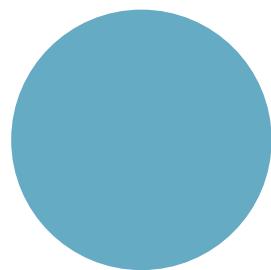


A graphic element consisting of three overlapping circles. One circle is light gray and positioned at the top. Another is black and positioned below and to the right of the first. A third circle is also black and overlaps both, centered between them.

- **Cyence  
Risk  
Analytics**

A risk assessment tool for  
cyber underwriting

# Background



Persona, application & project background



## 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.

# Persona

## Cyber Underwriter

### 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.

# About Cyence Risk Analytics

- Cyence for cyber is a risk analytics tools used by underwriters to evaluate a risk of a given business.
- 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.

## A typical underwriting workflow



# Project Needs and Goals

## NEEDS:

- Cyence is one of the Guidewire's acquisition product which had a different design language and had a lot of **accessibility issues**.
- Additionally, the product had range of risk analytics and insights which was **hard to consume for our end users**.

## GOALS:

- Enable users to **get the most important information about a business in a glance**.
- Enable users to **take actionable next steps** based on their risk findings within application.
- New user experience along with **meeting the AA accessibility standards**.

# Design Process

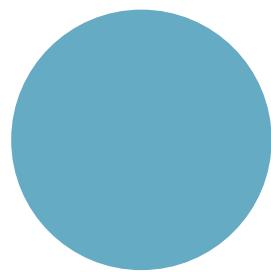
## Phase - 1



## Phase - 2



# User Research



Insights, goals, and problems

# UX Research

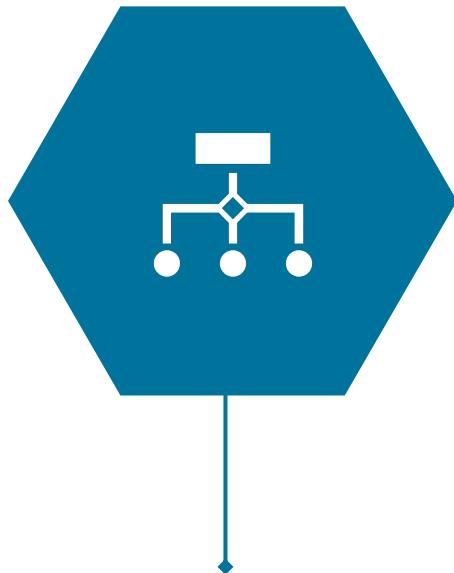
## Research Insights:

- # 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.

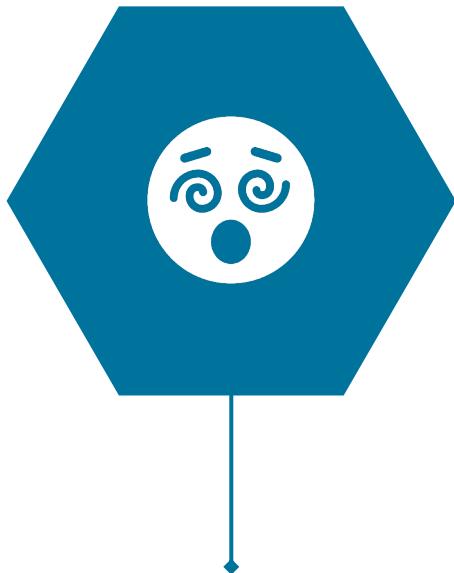
# 4 key identified problems...



Hard to understand the correlation between data



Hard to find impactful & most concerning information

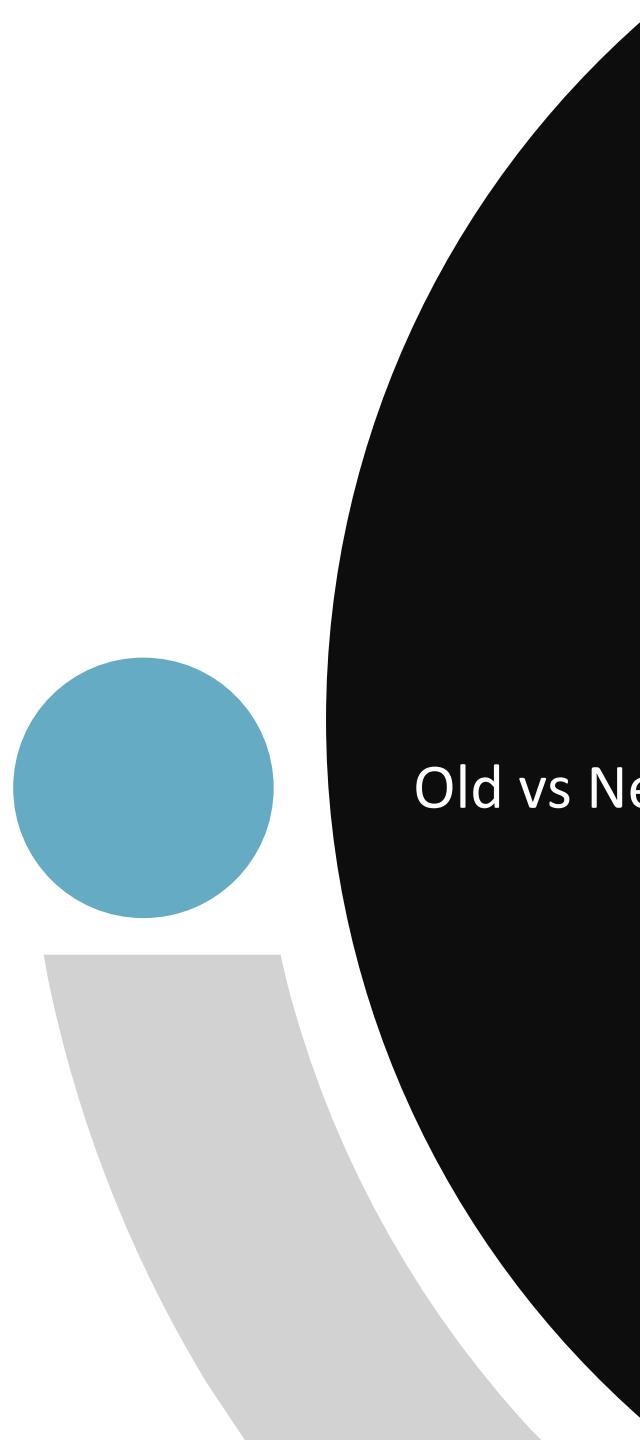


Don't know what to do with certain information



Found the UX and printable report old and outdated.

# Design



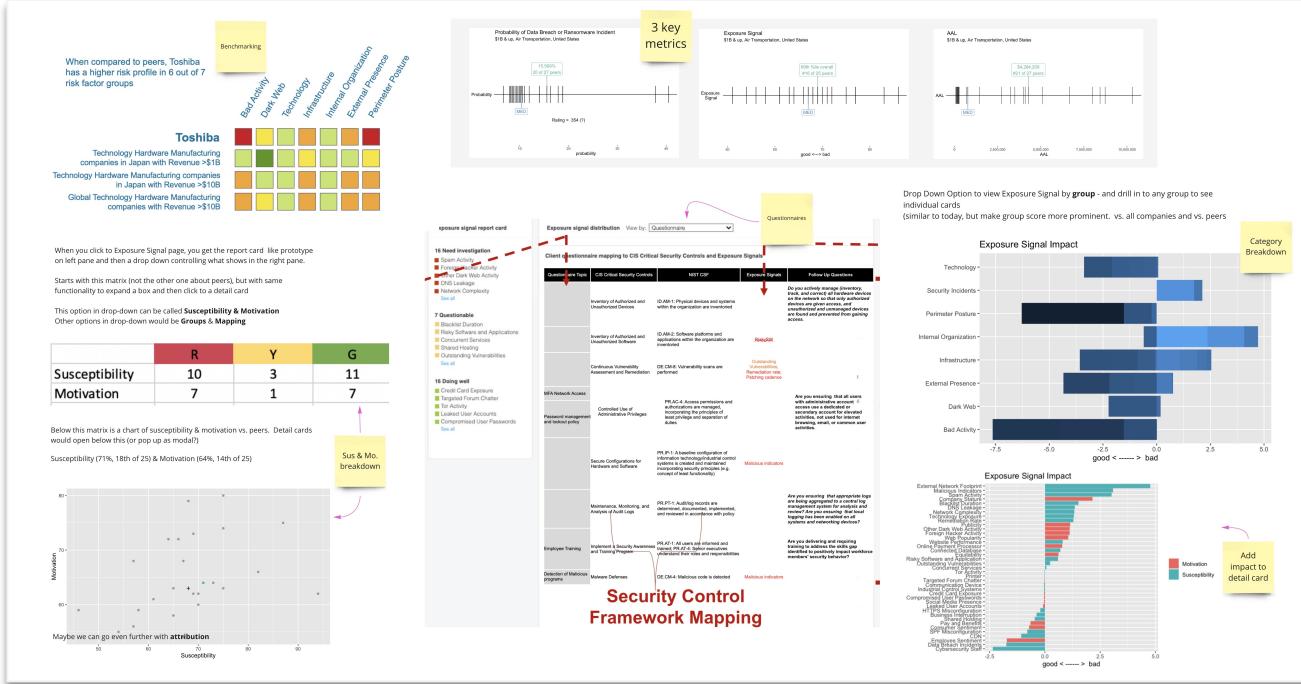
Old vs New User Experience

# Proposed Solution

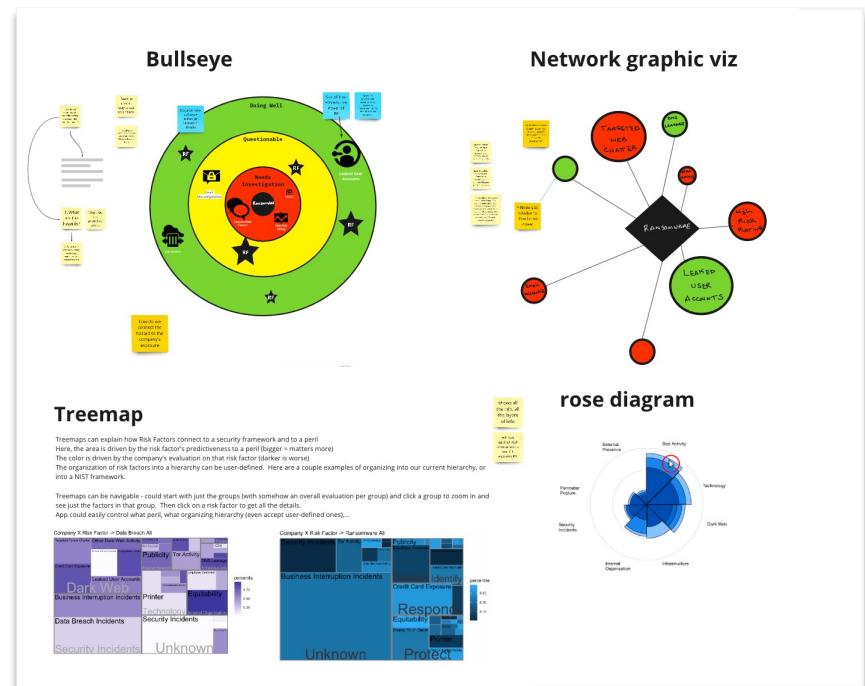
- Provide users a clear representation about the correlation of different data though out the UI.
- Provide a new overview page with most important information in order to increase productivity.
- Provide help text to users in order to understand the usage of information along with actionable steps which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

# Ideation Board

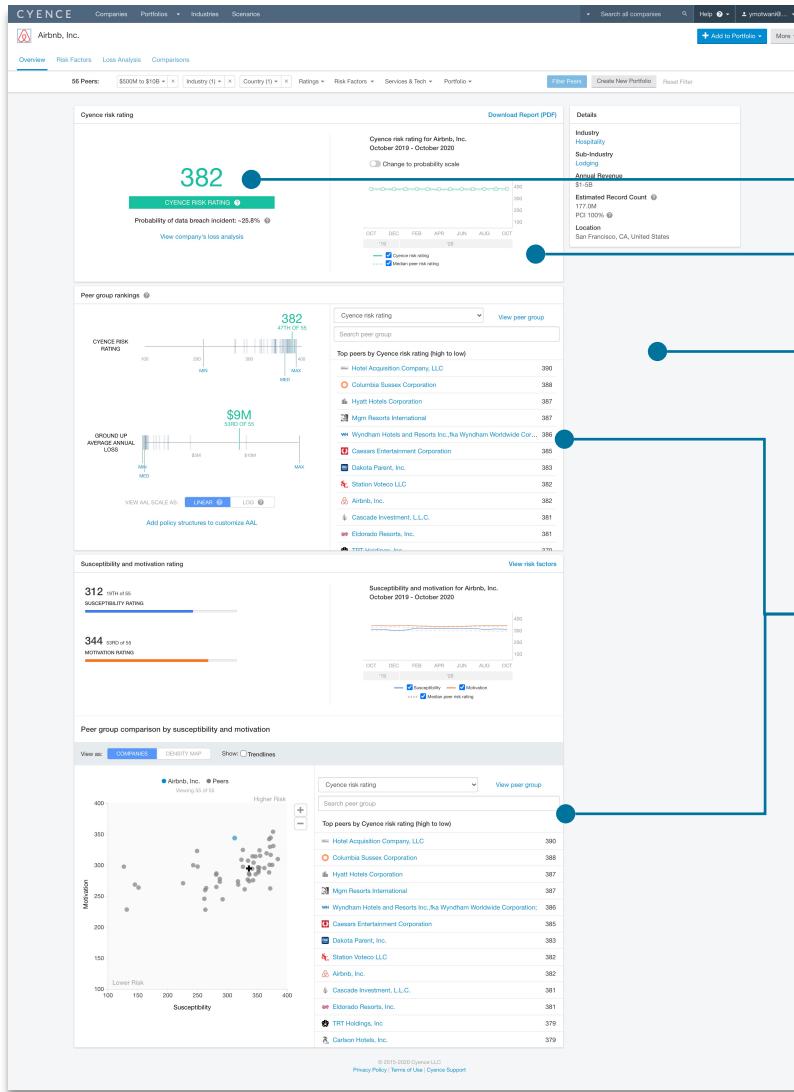
## Ideas brainstorming



## Data viz explorations

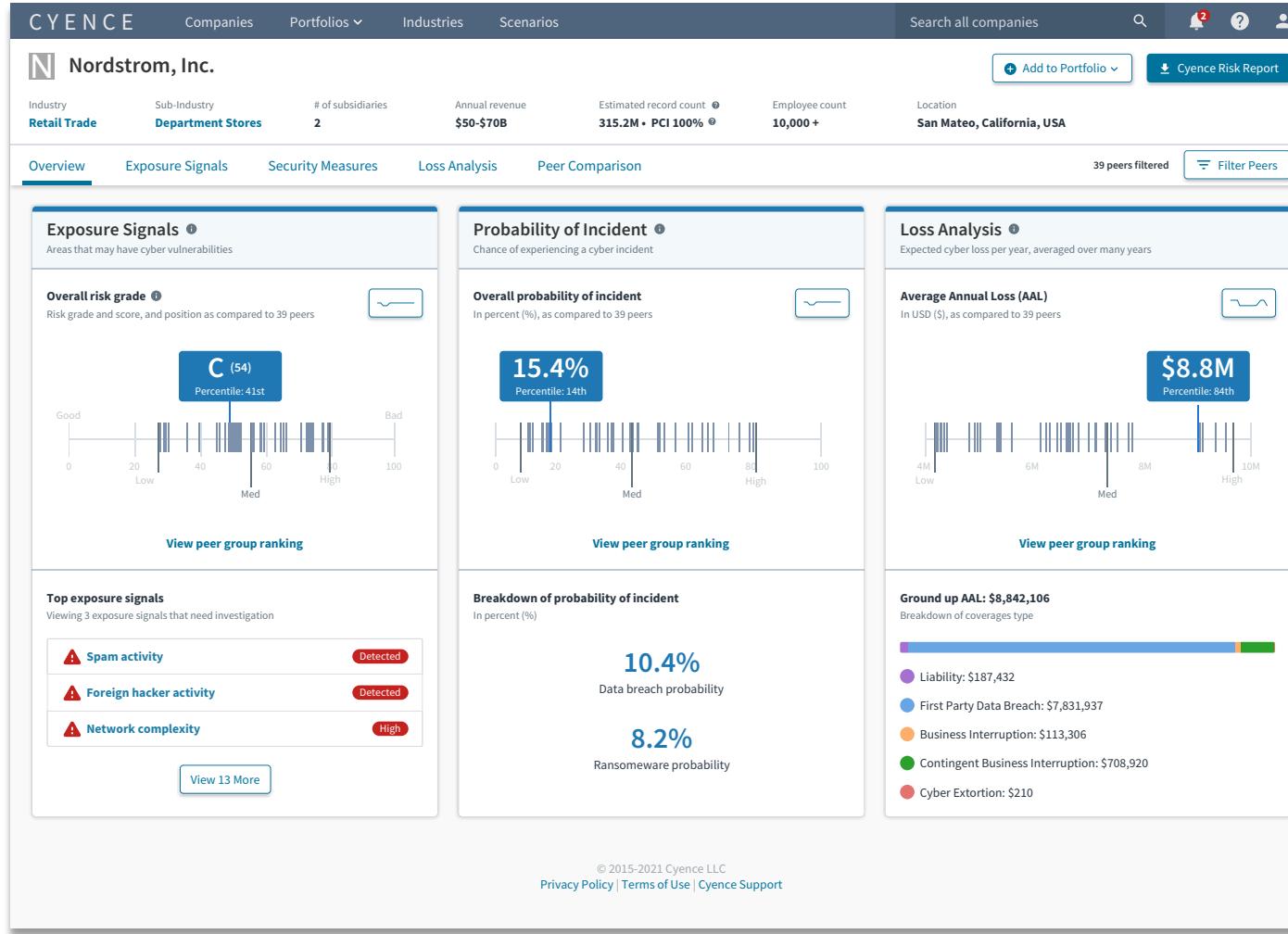


# Problem with older UX



- A primary metrics which is usually misunderstood by underwriters
- Historical trend is a secondary information but highly emphasized
- A lot of white space and unnecessary scrolling
- Repeated information and list of ranking which is not used that often

# Company Overview

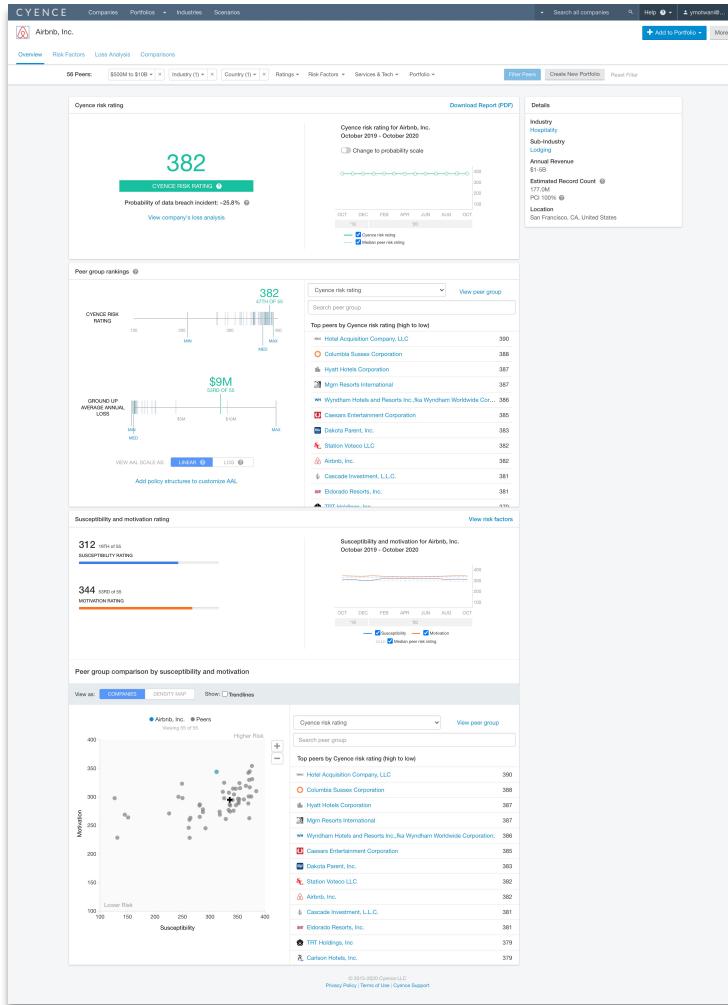


As part of the overview refresh, we introduced following improvements:

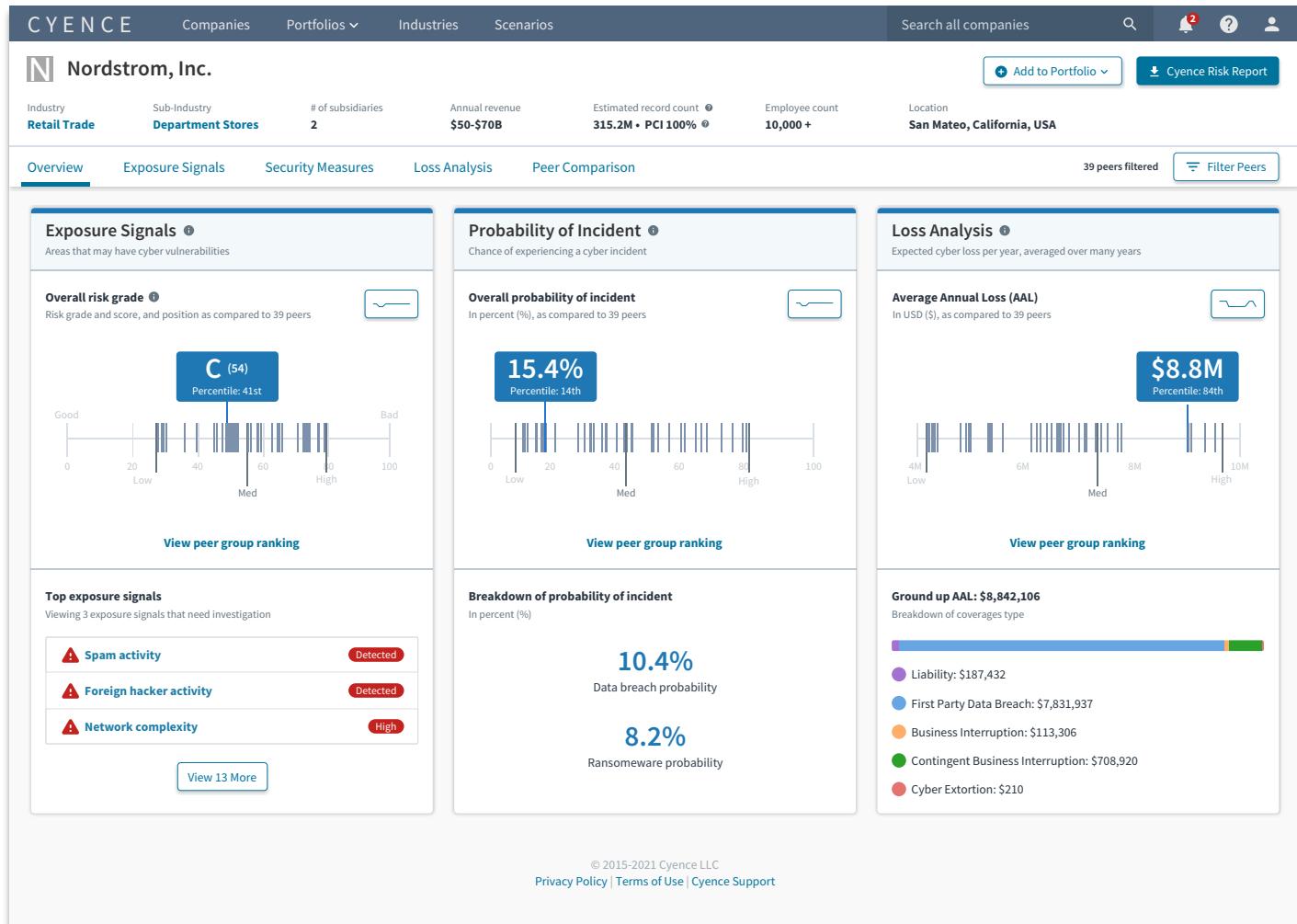
- New **hierarchy of information** to highlight the most important information up front.
- New **3 column layout** to provide the distinction of **3 different data points** to identify risk.
- New **data points** to replace some older ones and to provide further details on others.
- **Sparkline graphs to show the history** trendlines for those risk data points which helped UX to be more sleek and newer.

# Company Overview – Old vs New UX

## Old UX



## New UX



# Problem with older UX

The screenshot shows the CYENCE platform interface for Airbnb, Inc. The top navigation bar includes 'Companies', 'Portfolios', 'Industries', 'Scenarios', 'Search all companies', 'Help', and a user account. Below the navigation is a search bar and filter options: '56 Peers', '\$500M to \$1B+', 'Industry (1)', 'Country (1)', 'Ratings', 'Risk Factors', 'Services & Tech', 'Portfolio', 'Filter Peers', 'Create New Portfolio', and 'Reset Filter'. The main content area is titled 'Top risk factors' and is divided into 'Positive Risk Factors' and 'Negative Risk Factors'. Under 'Positive Risk Factors', there is one item: 'Infrastructure' with 'CDN @ - Present'. Under 'Negative Risk Factors', there are two items: 'Dark Web' with 'Compromised User Passwords @ - Detected' and 'Leaked User Accounts @ - Detected'. To the right of these sections is a 'Services & technologies' sidebar listing 'Service provider (5)', 'Software (17)', and 'Payment processor (13)'. At the bottom of the page, there is a section titled 'All risk factors' with various categories like 'Bad Activity @ - Improved', 'Dark Web @ - Unchanged', 'Technology @ - Unchanged', etc., each with a progress bar and a percentage of peers being better.

Underwriters didn't care about positive risk factors

A lot of white space and unnecessary scrolling

Showed high impact categories but not individual risk factors.  
Users didn't know how to find most concerning risk factor.

# Exposure Signals (Risk Factors)

The screenshot shows the CYENCE platform interface for Nordstrom, Inc. The top navigation bar includes links for Companies, Portfolios, Industries, Scenarios, and a search bar for 'Search all companies'. Below the header, company details are displayed: 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+), and Location (San Mateo, California, USA). A 'Add to Portfolio' button and a 'Cyence Risk Report' button are also present.

The main content area is titled 'Exposure Signals' and features a 'Report Card' section. The 'Overall Exposure Signal' is shown as a 'C (54)' grade, with '41% of peers are better'. Below this, a 'Risk Grade' section lists categories: 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)).

The 'Exposure Signal Report Card' provides a summary of findings across three peer comparison 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). It also lists specific issues under 'Needs investigation' (16 items) and 'Suspicious' (7 items), along with a section for 'No issues' (16 items).

The right side of the page displays a 'Pinned (2)' list of detected risks:

- Spam Activity (Detected): Propagation of unsolicited junk email distributed to a large number of recipients.
- Compromised User Password (Detected): Login credentials consisting of username and password pairs, which may be used to hack into private accounts.
- DNS Leakage (Detected): Internal network information is openly available on the Internet, and indicates a network misconfiguration or malicious signaling.
- Network Complexity (High): Measure of breadth and intricacy of the company's external network based on an evaluation of its DNS (Domain Name System) hierarchy.
- Risky Software and Application (Moderate): Underlying technologies of a website which are perceived to carry greater risk because they are more prone to vulnerabilities and/or they contain advertising tools.
- Risky Software and Application (Moderate): Underlying technologies of a website which are perceived to carry greater risk because they are more prone to vulnerabilities and/or they contain advertising tools.
- Shared Hosting (Significant): Website is hosted on a server which is shared with websites belonging to other entities.
- Foreign Hacker Activity (Detected): Discussions about the company conducted in a non-English forums (such as Russian, Chinese, etc.).

**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:**

- The new prioritization was based on type of signal and severity. The prioritization criteria was changed and tested as part of this UX refresh.
- Report card, so the users can easily navigate through most concerning risks.
- A tree view for underwriters to identify the most vulnerable risk through grading and risk impact.
- Security Measures to provide our users a set of follow up questions they can ask to their customers to mitigate the risk.

# Exposure Signals – Old vs New UX

## Old UX

**CYENCE** Companies Portfolios Industries Scenarios Search all companies Help More Add to Portfolio More

Airbnb, Inc.

Overview Risk Factors Loss Analysis Comparisons

56 Peers: \$600M to \$1B+ Industry (I) Country (I) Ratings Risk Factors Services & Tech Portfolio Filter Peers Create New Portfolio Reset Filter

**Top risk factors**

- Positive Risk Factors**
- Negative Risk Factors**

**Infrastructure**

**CDN** – Present

CDNs offer redundancy and the ability to absorb or neutralize potential threats to sites (like DDoS), 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 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 weakness.

**Infrastructure**

**SFP Misconfiguration** – Not detected

A carefully balanced SFP record in the Domain Name System protects the company against email spoofing. The absence or improper configuration of SFP exposes the company to fraudulent use of its domain name for spam and phishing emails carrying fake sender addresses.

**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 techniques 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 also 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

98% of peers are better

23% of peers are better

4% of peers are better

82% of peers are better

5% of peers are better

73% of peers are better

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

## New UX

**CYENCE** Companies Portfolios Industries Scenarios Search all companies Help More Add to Portfolio More Cyence Risk Report

**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

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

**Exposure Signal Breakdown**

Overall Exposure Signal C (54)

Categories Risk Grade Peer Comparison

Technology D (74) 79% of peers are better

Exposure Signals Status Impact

- Online Payment Processor Detected
- Risky Software and Applications Restrained
- Connected Database Not Detected
- Technology Exposure Low
- Communication Device Not detected
- Exposed Printers Not detected

**Exposure Signal Report Card**

Total Exposure Signals: 39

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

Needs investigation (16)

- Spam Activity
- Compromised User Passwords
- DNS Leakage

Suspicious (7)

- Network Complexity
- Risky Software and Applications
- Shared Hosting

No issues (16)

- 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

Signal Category Bad Activity

Signal type Susceptibility

Signal impact

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

Ask your client:

- Do you block all email attachments entering your org's email gateway if the file types are unnecessary for the organization's business?
- Do use sandboxing to analyze and block inbound email attachments with malicious behavior?
- Do you use DNS filtering services to help block access to malicious domains?

Was it helpful?

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

# Downloadable Report

## Old UX

Nordstrom, Inc.  
Cyence Unique ID: b3d5e9f9  
Report generated on December 14, 2020  
with data from November 2020

This document and any recommendations, analysis, or advice provided by Cyence, LLC ("Cyence") (herein the "Analyst") 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 the prior written consent of Cyence. Any recommendations, analyses, or advice, including but not limited to actuarial, tax, accounting, or legal matters, are not to be relied upon for any purpose, for which you may be liable to Cyence. All recommendations, analyses, or proposals are subject to inherent uncertainty, and the Analyst could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete. Cyence makes no representations or warranties, express or implied, as to the accuracy or completeness. All representations and warranties, express, implied, or statutory, including any implied warranty of merchantability, fitness for a particular purpose, title, non-infringement of third party rights, from course of dealing, usage or trade practice, are disclaimed. Cyence shall have no liability for any damages resulting from the use of this report. No warranty of any kind that the Analyst, 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 provide support, maintenance, or updates to the Analyst, or any report with regard to the Analyst or to any services provided by a third party to you or Cyence. By accepting and using this report, you acknowledge and agree to the terms, conditions and disclaimers set forth above.

CYENCE

Confidential - Presented to Cyence LLC - For Internal Use Only

Company Overview  
Nordstrom, Inc.  
Cyence Unique ID: b3d5e9f9

**Company Overview**

Cyence Risk Rating	Susceptibility Rating	Motivation Rating
<b>388</b> Out of 400	<b>368</b> Out of 400	<b>347</b> Out of 400
Peer range: 335-390	Peer range: 290-379	Peer range: 251-357
Peer median: 376	Peer median: 334	Peer median: 311

See following report for further details.

**Company Details**

**Details**

Industry: Retail Trade  
Sub-Industry: Department Stores  
Annual Revenue: \$10.5B  
Estimated Record Count: 262.4M  
PCI 100%  
Location: Seattle, WA, United States

**Services & Technologies**

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

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

CYENCE

Confidential - Presented to Cyence LLC - For Internal Use Only

Company Overview: Risk Overview  
Nordstrom, Inc.  
Cyence Unique ID: b3d5e9f9

**Risk Overview**

Cyence Risk Rating
<b>388</b> Out of 400
Peer range: 335-390
Peer median: 376

**Risk Rating**

The Risk Rating is a measure of a company's cyber risk, or the likelihood that it would experience a network security incident or unintentional release of protected information. This is derived from a combination of three main factors: Susceptibility, Motivation, and Risk Factors. Based on a 100-400 scale, a higher Risk Rating indicates greater risk.

**Probability of Data Breach**  
**~36.4%**

The Probability of Data Breach is mapped to the Cyence Risk Rating. This represents the probability of a company having at least one incident over the next 12 months. Probabilities are estimated and actual probabilities may vary.

**37th of 39**  
Among its peer group of 39 companies

**Peer Risk Comparison**

Peers 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.

CYENCE

Confidential - Presented to Cyence LLC - For Internal Use Only

Company Overview: Risk Overview  
Nordstrom, Inc.  
Cyence Unique ID: b3d5e9f9

**Historical Rating Over Time**

Risk

NOV '19 JUN '20 MAR '20 MAY '20 JUL '20 SEP '20 NOV '20

**Historical Probability Over Time**

Probability

NOV '19 JUN '20 MAR '20 MAY '20 JUL '20 SEP '20 NOV '20

Confidential - Presented to Cyence LLC - For Internal Use Only

Risk Factors: Top Risk Factors  
Nordstrom, Inc.  
Cyence Unique ID: b3d5e9f9

**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**

Info: Present  
CDN - Present  
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.

Infrastructure  
SPF Misconfiguration - Not detected  
A correctly aligned SPF record in the Domain Name System protects the company against email spoofing. The absence or improper configuration of SPF 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 through social engineering on their co-workers, 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, and also the risk of external attacks that prey on human error.

**Negative Risk Factors**

Bad Activity - Detected  
Malicious actors using tools to distribute spam may indicate system misconfiguration or compromised user credentials, which puts the company at risk.

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 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.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 10 of 29

# Downloadable Report

## New UX



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 legal, tax, accounting, or legal matters, are not to be construed as professional advice and you should consult with your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and 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 are limited to the express terms of the contract of merchantability, fitness for a particular purpose, title, non-infringement, of third party 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 or Cyence. By accepting and/or using this report, you acknowledge and agree to the terms, conditions and disclaimers set forth above.

### 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

#### Probability of Incident

**15.4%**

Probability in percent (%)

#### Average Annual Loss

**\$8.1m**

Losses in USD (\$)

#### 51st Percentile

Peer range: 290-400  
Peer median: 320

#### 72nd Percentile

Peer range: \$3.1 - 9.4m  
Peer median: \$5.3m

Change in history

#### 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

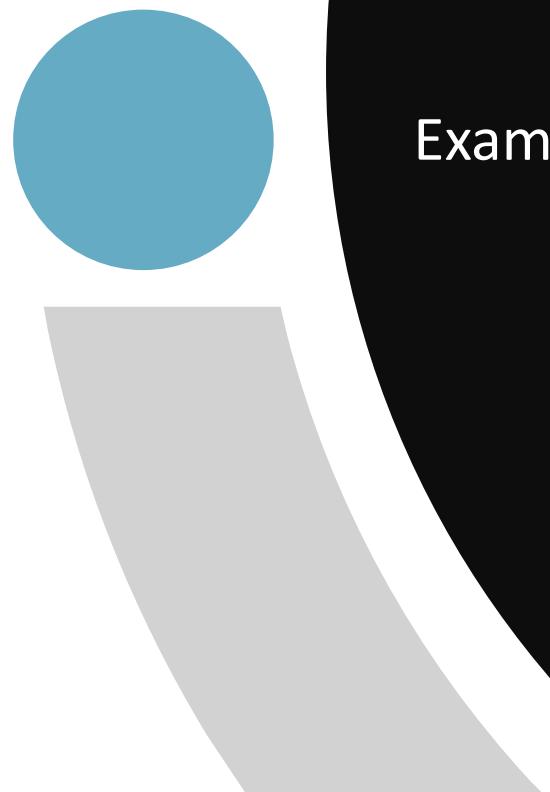
#### Suspicious

- 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 2 of 35

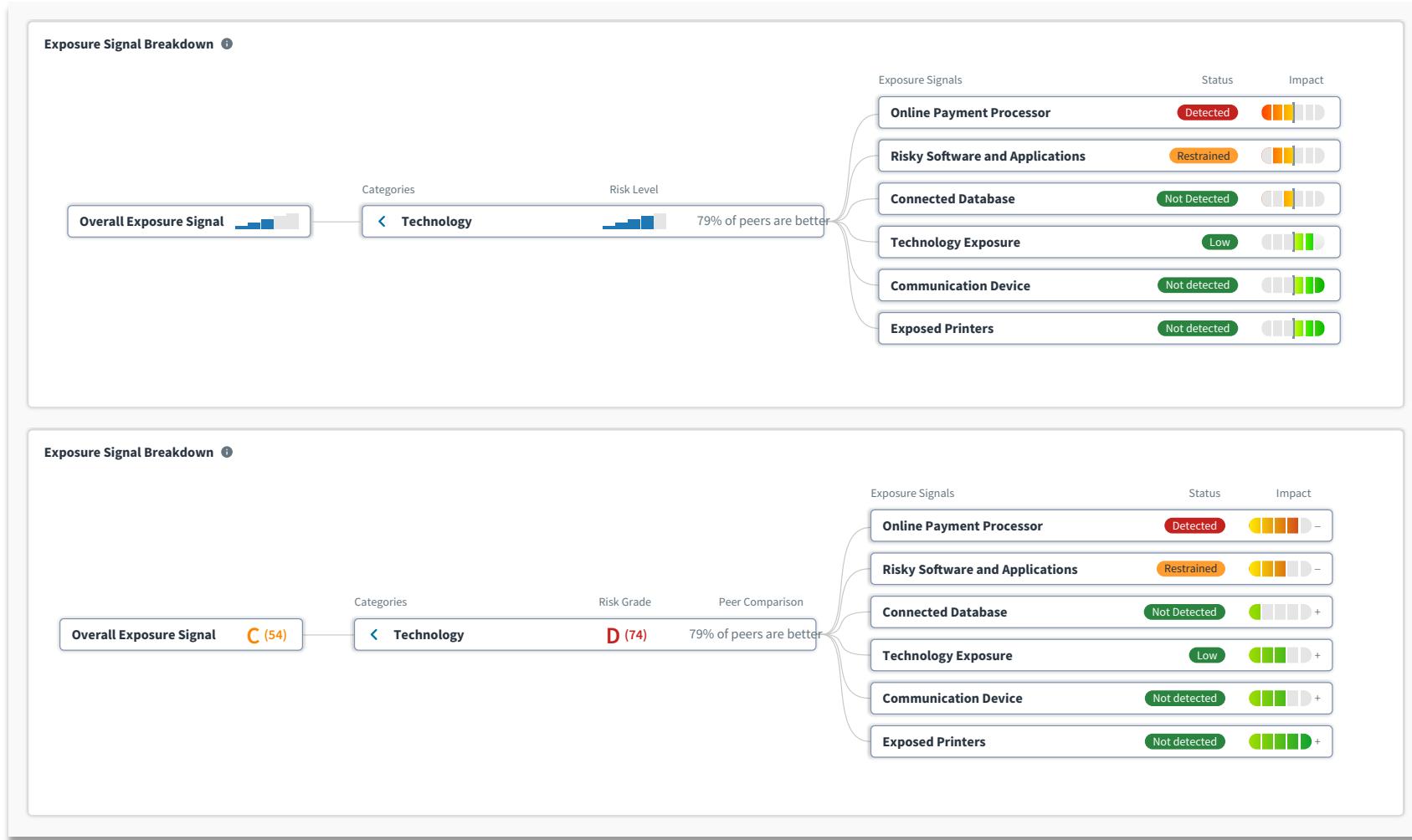
Care Wear, Inc.  
Cyence Unique ID: bdqoeybjreq  
Confidential - Presented to Cyence LLC - For Internal Use Only  
Page 3 of 35

# Usability Testing



Example of design reiteration

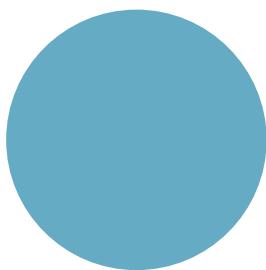
# Risk Rating (Graph vs Grading)



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



Onboarding guide and in app UI feedback

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

May 28, 2021

**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 (.)

### 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 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.

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. 😊

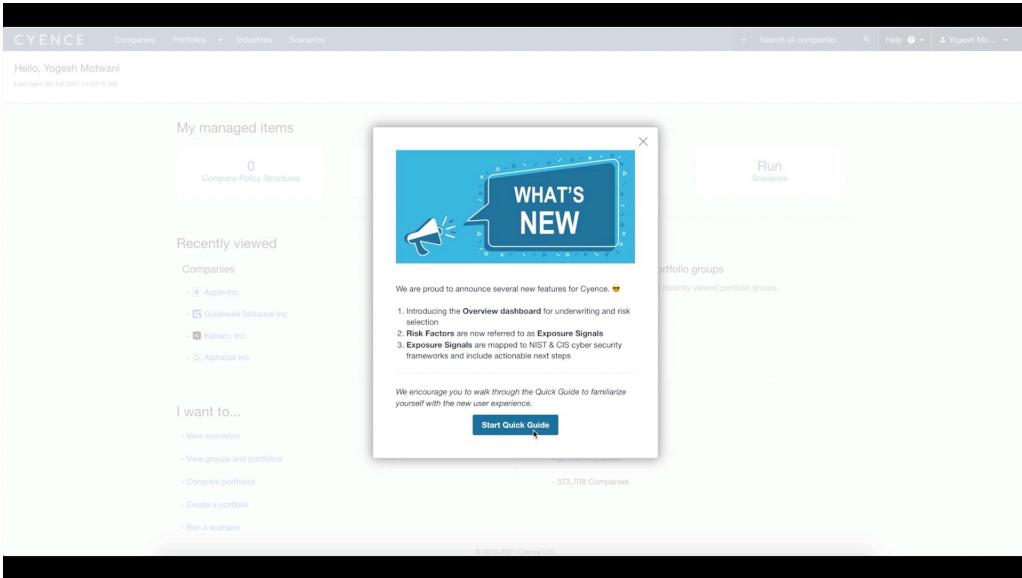
1. Introducing the **Overview dashboard** for underwriting and risk selection
2. **Risk Factors** are now referred to as **Exposure Signals**
3. **Exposure Signals** are mapped to NIST & CIS cyber security frameworks and include actionable next steps

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

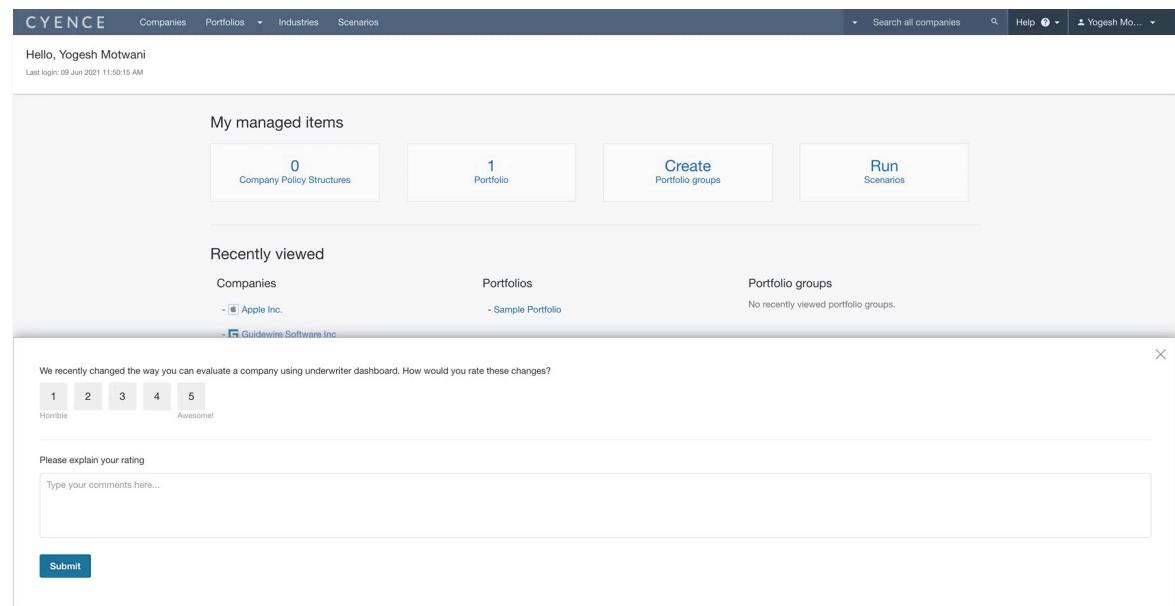
[Start Quick Guide](#)

# Onboarding Design Samples

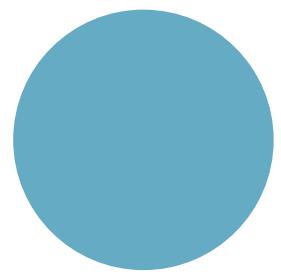
## Onboarding Guide



## In app UI Feedback

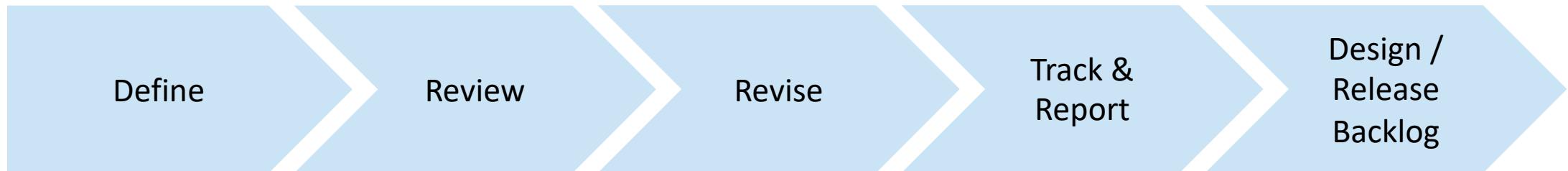


# Product Success Metrics



Process and key insights

# Defining product success matrix



## Some key insights

### Month-over-month comparison

JUNE 2021 TO JULY 2021

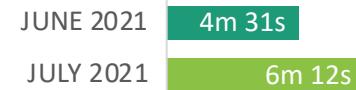
#### Unique Companies Viewed

↑ 21%



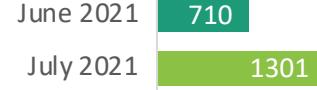
#### Average Time Spent on Company Overview page

↑ 49%



#### Report Downloads

↑ 83%





**Thank You**  
Any questions?