

# Cybersecurity disclosures

SnowFROC, March 7 2024

Andrew Hoog  
Co-Founder, NowSecure  
<https://www.andrewhoog.com/>



**Why should you  
orient to risk?**

The SEC oversee more than *\$100 trillion* in securities trading on U.S. equity markets annually

# SEC Mission

- Protect investors
- Maintain fair, orderly, and efficient markets
- Facilitate capital formation

# SEC EDGAR

- REST API
- Company Searches
- Recent filings
- Daily, Quarterly and Full Indexes
- XBRL

The screenshot shows the SEC EDGAR website interface. At the top, there is a navigation bar with the U.S. Securities and Exchange Commission logo and a search bar. Below the navigation bar, there is a sidebar menu on the left with options like 'About EDGAR', 'Quick EDGAR Tutorial', 'How To Search EDGAR', 'Company Filings Search', 'Search EDGAR Comments', 'Filings and Forms' (highlighted), 'Forms List', 'Accessing EDGAR Data', 'SIC Codes', 'Contact Filer Support', 'EDGAR - Information for Filers', and 'EDGAR - Search and Access'. The main content area is titled 'Filings & Forms' and contains a paragraph explaining that all companies are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Below this paragraph is a list of links: 'Quick EDGAR Tutorial', 'Search for Company Filings', 'Descriptions of SEC Forms', 'SEC Forms List (PDF versions)', 'About EDGAR', 'Search EDGAR Comment Letters', and 'Accessing EDGAR Data'. To the right of the main content is a 'Related Materials' section with links to 'EDGAR System Announcements' and 'Contact EDGAR Filer Support'. At the bottom right, there is a footer that says 'Modified: Jan. 9, 2017'.

# Parsing 10-Ks is a PITA



**Andrew Hoog** · You

Entrepreneur | Board Director | Cybersecurity Expert | Author | Inven...

2d · Edited · 🌐

Alphabetical order here folks! If investors are going to trust you to run a publicly traded company, you just gotta nail things like alphabetical order. Besides, all these edge cases are killing my automated scripts and I find it really inconvenient. 😓

[#sec](#) [#10k](#)

**Item 1C. Cybersecurity.**

Not Applicable.

**Item 1B. Unresolved Staff Comments.**

None.

Bob Zukis and 14 others

5 comments

IT EM 1C

I TEM 1C

ITE M 1C



# Citigroup

## MANAGING GLOBAL RISK

Overview

## CREDIT RISK<sup>(1)</sup>

Overview

Loans

Corporate Credit

Consumer Credit

Additional Consumer and Corporate Credit Details

Loans Outstanding

Details of Credit Loss Experience

Allowance for Credit Losses on Loans (ACLL)

Non-Accrual Loans and Assets

## LIQUIDITY RISK

Overview

Liquidity Monitoring and Measurement

High-Quality Liquid Assets (HQLA)

Deposits

Long-Term Debt

Secured Funding Transactions and Short-Term Borrowings

Credit Ratings

## MARKET RISK<sup>(1)</sup>

Overview

Market Risk of Non-Trading Portfolios

Banking Book Interest Rate Risk

Market Risk of Non-Trading Portfolios

Banking Book Interest Rate Risk

Interest Rate Risk of Investment Portfolios—Impact on *AOCI*

Changes in Foreign Exchange Rates—Impacts on *AOCI* and Capital

Interest Income/Expense and Net Interest Margin (NIM)

Additional Interest Rate Details

Market Risk of Trading Portfolios

Factor Sensitivities

Value at Risk (VAR)

Stress Testing

## OPERATIONAL RISK

Overview

Cybersecurity Risk

## COMPLIANCE RISK

## REPUTATION RISK

## STRATEGIC RISK

Climate Risk

## OTHER RISKS

LIBOR Transition Risk

Country Risk

Top 25 Country Exposures

Russia

Ukraine

Argentina

FFIEC—Cross-Border Claims on Third Parties and Local Country Assets

# **[New] Cybersecurity Disclosure Rules**



# Trends

1. Ever-increasing share of economic activity is dependent on ~~electronic systems~~ mobile apps
2. Substantial rise in the prevalence of cybersecurity incidents
3. Costs and adverse consequences

Item	<u>Summary Description of the Disclosure Requirement</u> <sup>30</sup>
Regulation S-K Item 106(b) – <i>Risk management and strategy</i>	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – <i>Governance</i>	Registrants must: <ul style="list-style-type: none"> <li>- Describe the board’s oversight of risks from cybersecurity threats.</li> <li>- Describe management’s role in assessing and managing material risks from cybersecurity threats.</li> </ul>
Form 8-K Item 1.05 – <i>Material Cybersecurity Incidents</i>	<p>Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its:</p> <ul style="list-style-type: none"> <li>- Nature, scope, and timing; and</li> <li>- Impact or reasonably likely impact.</li> </ul> <p>An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General (“Attorney General”) determines immediate disclosure would pose a substantial risk to national security or public safety.</p> <p>Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.</p>

10-K Item 1C  
All registrants beginning fiscal  
years ending on or after  
December 15, 2023.

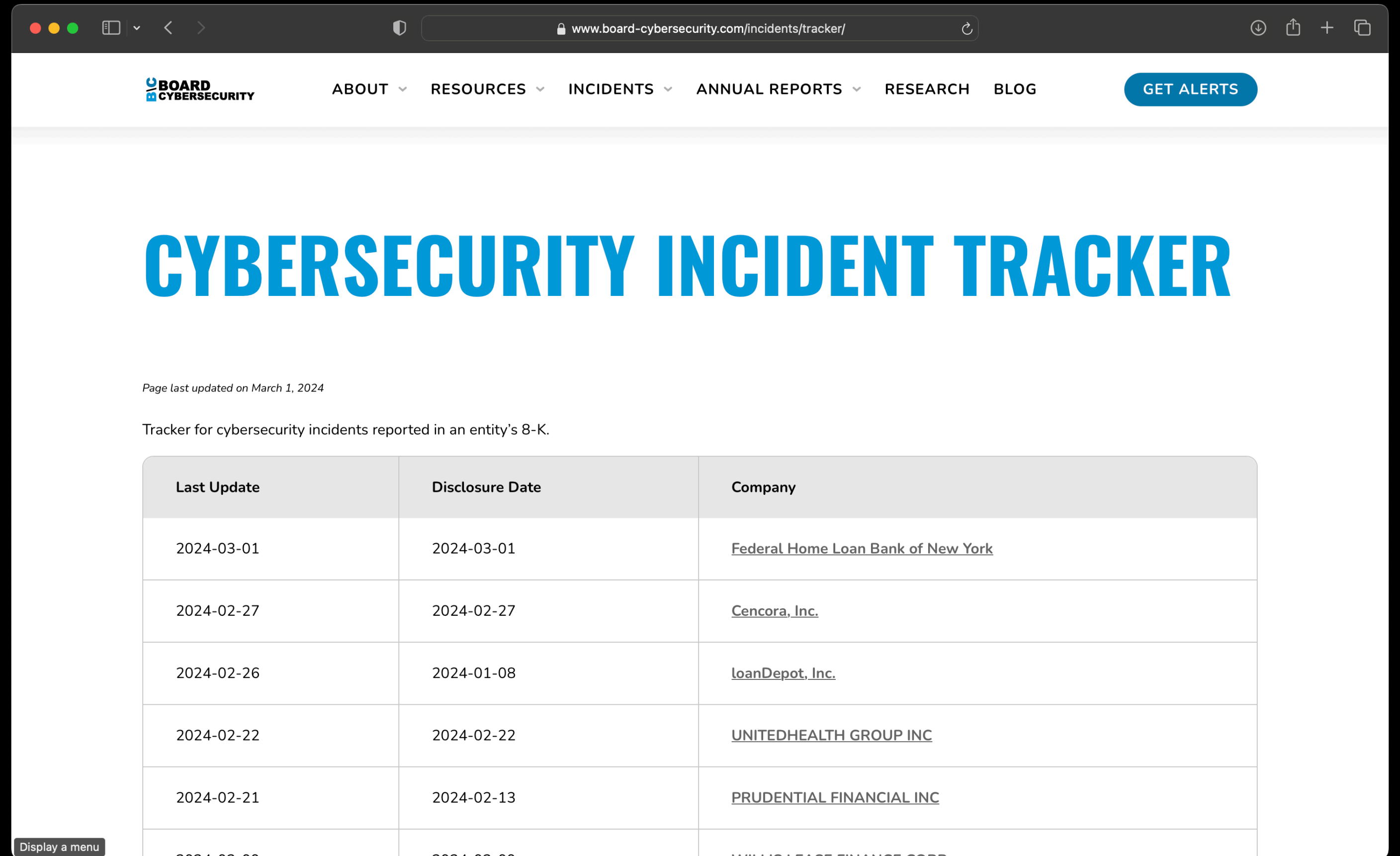
8-K Item 1.05  
December 18, 2023 (Small  
Reporting Company start June  
15, 2024)

Inline XBRL tagging  
10-K - Dec 15, 2024  
8-K - Dec 18, 2024

# Why Materiality

# 8-K Disclosures

- 11 new incidents since Dec 18
- Notable Incidents
  - VF Corp - 35.5m records
  - UnitedHealth Group - major impact
  - Microsoft - threshold



The screenshot shows the 'CYBERSECURITY INCIDENT TRACKER' page from the Board Cybersecurity website. The page is updated as of March 1, 2024. It features a table with the following data:

Last Update	Disclosure Date	Company
2024-03-01	2024-03-01	<a href="#">Federal Home Loan Bank of New York</a>
2024-02-27	2024-02-27	<a href="#">Cencora, Inc.</a>
2024-02-26	2024-01-08	<a href="#">loanDepot, Inc.</a>
2024-02-22	2024-02-22	<a href="#">UNITEDHEALTH GROUP INC</a>
2024-02-21	2024-02-13	<a href="#">PRUDENTIAL FINANCIAL INC</a>
2024-02-09	2024-02-09	<a href="#">WILLIS LEASE FINANCE CORP</a>

<https://www.board-cybersecurity.com/incidents/tracker/>

# Not Incidents?

BOARD CYBERSECURITY

ABOUT RESOURCES INCIDENTS ANNUAL REPORTS RESEARCH BLOG GET ALERTS

## CYBERSECURITY INCIDENT REPORTS

Page last updated on March 1, 2024

Cybersecurity incidents reports in the wild. Submit a [new incident report](#).

Reported Date	Company	Snippet	8-K Filed
2023-12-18	<a href="#">COM-CAST CORP</a>	Comcast suffered a data breach affected over 35.8 million customers.	No
2023-12-16	<a href="#">Mon-goDB, Inc.</a>	MongoDB is actively investigating a security incident involving unauthorized access to certain MongoDB corporate systems, which includes exposure of customer account metadata and contact information.	No
2023-10-27	<a href="#">BOEING CO</a>	Possible ransomware attack on parts business.	No

Display a menu

## Incident Reports

- Comcast
- MongoDB
- Boeing

Quite useful for understanding what some companies don't consider material.

<https://www.board-cybersecurity.com/incidents/reports/>



# 8-K Observations

# Analysis by Ezra Ortiz

	SEC 8-K Cybersecurity Requirements			SEC Order
Company	Describe the material impact or reasonably likely material impact on the registrant, including (non-exclusively) financial condition and results of operations along with qualitative factors such as harm to reputation, customer of vendor relationships, competitiveness, litigation, U.S. and non-U.S. regulatory investigations, etc.	Describe the material aspect of the nature, scope, and timing of the incident.	Disclose updated [material] incident information within four days, after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available in a Form 8-K amendment.	Civil Penalties
Federal Home Loan Bank of New York	Failed	Failed		
Cencora, Inc.	Failed	Failed		
loanDepot, Inc.	Partial	Failed	Partial	
UNITEDHEALTH GROUP INC	Failed	Failed		
PRUDENTIAL FINANCIAL INC	Failed	Failed	Partial	
WILLIS LEASE FINANCE CORP	Failed	Failed		
SouthState Corp	Failed	Failed		
BLACKBAUD INC	Failed	Failed	Partial	Y
Hewlett Packard Enterprise Co	Failed	Failed		
MICROSOFT CORP	Failed	Failed		
V F CORP	Partial	Partial	Partial	
First American Financial Corp	Failed	Failed	Partial	
Fidelity National Financial, Inc.	Failed	Partial	Partial	
MIDDLEFIELD BANC CORP	Failed	Failed	Partial	
Mr. Cooper Group Inc.	Failed	Failed	Partial	
LivaNova PLC	Partial	Failed	Failed	
23andMe Holding Co.	Failed	Failed	Partial	
Mueller Water Products, Inc.	Failed	Failed	Partial	
Inspired Entertainment, Inc.	Failed	Failed		
Johnson Controls International plc	Failed	Failed	Partial	
HENRY SCHEIN INC	Failed	Failed		
PROG Holdings, Inc.	Failed	Failed		
CLOROX CO /DE/	Failed	Failed	Partial	
Caesars Entertainment, Inc.	Failed	Failed		
MGM Resorts International	Failed	Failed		

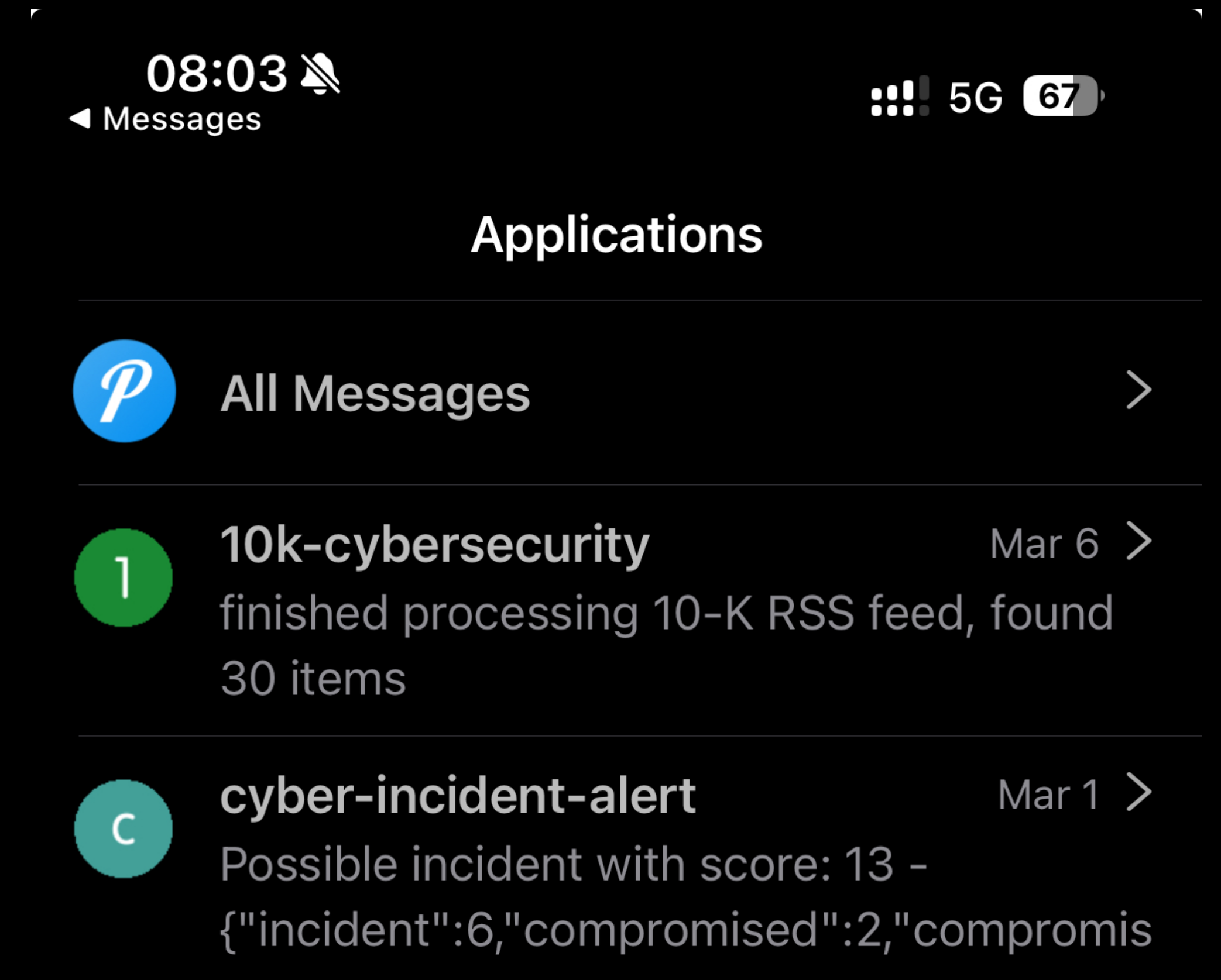
# Other Observations

- Considerable data if you 1) read closely and 2) follow over time. For example, tracking 5 different dates - Compromised, Detected, Disclosure, Contained, and Recovered
- Disclosures increasingly mentioning nation-state actors, e.g. UHG, Microsoft and HPE
- State Attorney General breach websites, e.g. Maine Attorney General - Data Breach Notifications are a trove of important data. Win for transparency.

# 10-K Analysis

# Data set

- Total 10-Ks: 2,359 (2,217 included)
  - Skipped : 107 - low word count, 125 - no word count
- Word count percentiles
  - {"0th":2,"5th":34,"50th":773,"95th":1427,"100th":2471}



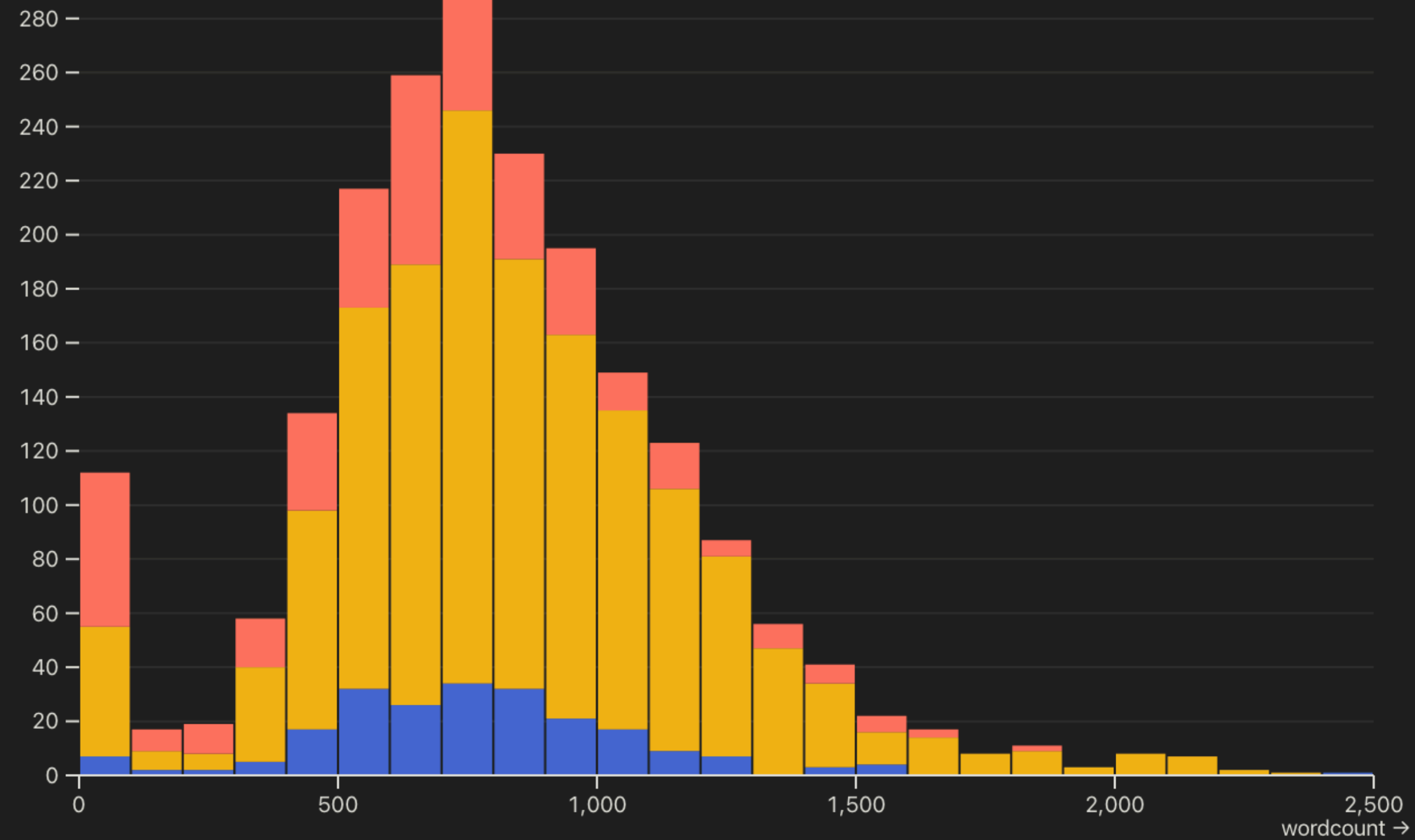


# Item 1C Word Count Histogram

10-K Item 1C word count analysis by filer category

Accelerated filer Large accelerated filer Non-accelerated filer

↑ Frequency



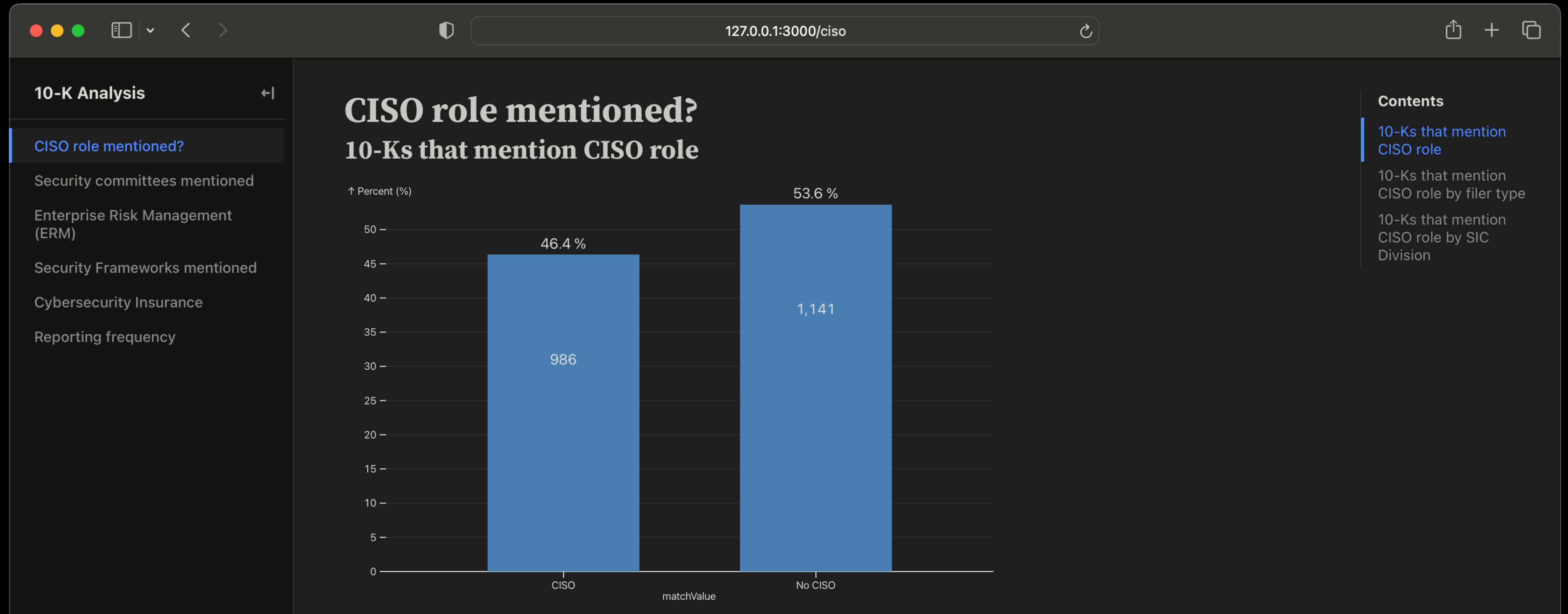
# Shortest 10-K

ITEM 1C      Cybersecurity

We do not maintain any information systems that would be subject to a cybersecurity threat. Our credit card processing is outsourced to a third party that uses a double authentication protocol.

- 34 words
- Appreciate their honesty
- But what system did you use to submit the 10-K? Or email?
- Longest 10-K so far: Fannie Mae at 2,471 words.

# Live analysis



# Best Practices

**Learn from public disclosures!**



# 8-K Best Practices

# 1. Define materiality in advance

Include qualitative and quantitative factors

## 2. Don't forget *reasonably likely* *impact*

This appear to be often overlooked

**3. Post an amended 8/K when  
new information is available**

Also subject to the “4 day” window

# 4. Include any system "owned or used by the registrant"

Breaches or incidents in your supply chain, SaaS providers, etc. are squarely in scope

# 5. Identify core team in advance

Don't scramble when a potential incident occurs with the added legal and regulatory pressure of proper disclosure

# 6. Tabletop exercise

They are not just for IR teams!



# 7. Please use Item 1.05

RTFM

## FILINGS

### 8-K filed on 2024-02-09

WILLIS LEASE FINANCE CORP filed an [8-K](#) at 2024-02-09 17:17:03 EST

#### Item 8.01 Other Events.

On February 9, 2024, Willis Lease Finance Corporation (“WLFC” or the “Company”) announced that on January 31, 2024, it detected unauthorized activity on portions of its information technology (IT) systems. An investigation into the nature and scope of the incident was launched with the assistance of leading third-party cybersecurity experts and the Company took steps to contain, assess and remediate the activity, including taking certain systems offline. The Company has not identified any unauthorized activity after February 2, 2024 and, as of the date of this filing, believes it has fully contained the unauthorized activity. The Company continues to operate and service customers, and has implemented workarounds for

# 10-K Best Practices

# 1. Only state factual items!

Are you really *fully* compliant with NIST 800-53

## **2. Have a dedicated security executive**

Otherwise security will be 2nd order focus

# 3. Risk Committee

Ideally have security report into a committee that specifically focuses on risk (they come in many names)

# 4. Board Cybersecurity Expert

While not an SEC requirement, having a Board Directory with cybersecurity experience will have a significant impact. Or technology/digital transformation at a minimum

# 5. Specific reporting frequency

Quarterly is best practice, biannually passable but annual or variations of “as needed”, “regularly”, etc. don’t appear sufficient



# 6. Use a framework!

NIST Cybersecurity Framework (v2.0 is out!) is most referenced. If you do significant US Government work, consider NIST 800-53 (among others)

# 7. Enterprise Risk Management

Have an ERM program and tie cybersecurity into it as another risk

# 8. Don't forget mobile risks :-)

70% of internet traffic is via mobile apps, driving significant revenue and customer stickiness with brands.

# Cybersecurity disclosures

SnowFROC, March 7 2024

Andrew Hoog  
Co-Founder, NowSecure  
<https://www.andrewhoog.com/>

