Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

November 6, 2024

XBRL US

Speakers

- **Nikkyann Berteau**, Sr. Product Manager, Broadridge Financial Solutions, Inc.
- **Nabeel Cheema**, Special Counsel, Office of Rulemaking, Division of Corporation Finance, U.S. Securities and Exchange Commission
- **Lisa Cousino**, XBRL Consulting Services and Professional Standards, Broadridge Financial Solutions, Inc.
- **Angela McTere**, Business Requirements Analyst, Donnelley Financial Solutions (DFIN)
- **Justine Robinson**, Of Counsel, Gibson, Dunn & Crutcher LLP
- **Scott Theis**, CEO, Novaworks, LLC

Agenda

- Overview of the Rule
- Practical XBRL Tagging and Preparation
- Discussion of the Rule
- Tips and Resources

Overview of the Rule

Effective September 5, 2023, registrants are required to provide disclosure in certain reports regarding cybersecurity incidents that are deemed material.

The amendments require timely disclosure of material cybersecurity incidents and annual disclosures.

Annual disclosure related to cybersecurity risk, management, strategy, and governance are required under a new Item 106 of Regulation S-K.

Overview of the Rule - continued

- Registrants must begin providing disclosure in Forms 8-K and 6-K, beginning with reports dated December 18, 2023, or later.
  - Disclose cybersecurity incidents that are material in a Form 8-K, Item 1.05 within four business days of determining that an incident is deemed material.
    - Describe the material attributes of its nature, scope, and timing, and
    - Impact or possible impact.
  - Foreign Private Issuers must provide disclosure in a Form 6-K promptly after the incident is disclosed or made public in a foreign jurisdiction, to any stock exchange or security holders.
  - Smaller reporting companies (SRC) were granted an additional 180 days from the effective date to begin compliance with Forms 8-K and 6-K disclosure. SRC's were required to begin compliance on June 15, 2024.

Overview of the Rule - continued

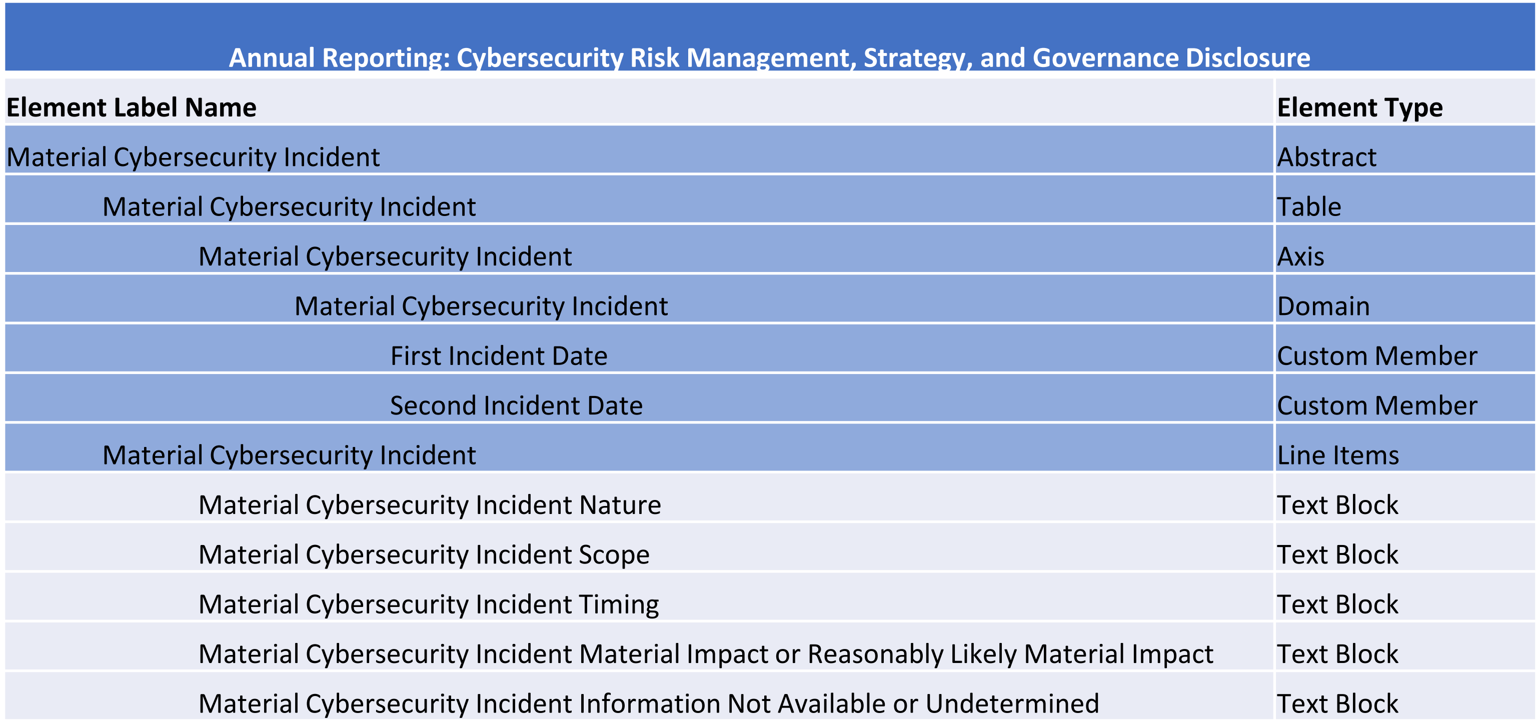
- All registrants were required to begin compliance with annual disclosure in Forms 10-K and 20-F beginning with reports for fiscal year ending on or after December 15, 2023.
- Annual disclosure required in Forms 10-K and 20-F:
    - Form 10-K: Item 1C. Cybersecurity
        - Disclose whether procedures for cybersecurity risk management and strategy were implemented and how the processes were integrated into the overall risk management processes.
        - Describe management's role in assessing and managing material risks from cybersecurity threats, and
        - Describe managements and the board of directors' oversight of cybersecurity risks.
    - Form 20-F: Item 16K. Cybersecurity
        - Describe the board of directors' oversight of cybersecurity risks.
        - Describe management's role in assessing and managing material risks from cybersecurity threats.

Overview of the Rule - continued

- Form 20-F: Item 16K. Cybersecurity
  - Describe the board of directors’ oversight of cybersecurity risks.
  - Describe management’s role in assessing and managing material risks from cybersecurity threats.
- Beginning one year after the initial compliance date, all registrants must begin tagging required disclosures in Inline XBRL.
  - Mandate of block tagging for narrative items and detailed tagging for numeric values for all registrants, including smaller reporting companies.
  - Forms 10-K and Forms 20-F, inline XBRL requirements begins annual reports for fiscal years ending on or after December 15, 2024; and
  - Forms 8-K, Item 1.05 and Forms 6-K all registrants must begin tagging responsive disclosure in Inline XBRL beginning on December 18, 2024.

Practical XBRL Tagging and Preparation

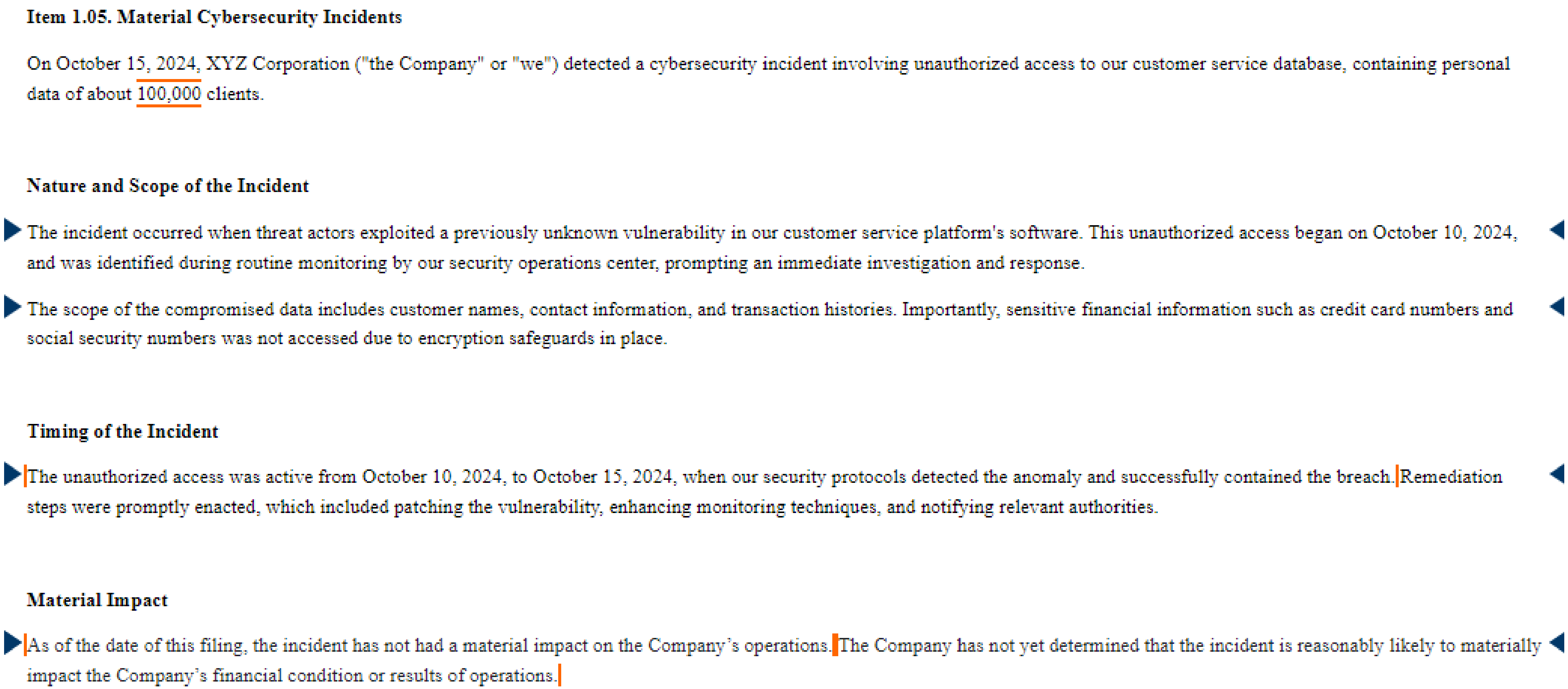
CYD Taxonomy: Current Reports (Form 8-K & 6-K)



Annual Reporting: Cybersecurity Risk Management, Strategy, and Governance Disclosure	
Element Label Name	**Element Type**
Material Cybersecurity Incident	Abstract
Material Cybersecurity Incident	Table
Material Cybersecurity Incident	Axis
Material Cybersecurity Incident	Domain
First Incident Date	Custom Member
Second Incident Date	Custom Member
Material Cybersecurity Incident	Line Items
Material Cybersecurity Incident Nature	Text Block
Material Cybersecurity Incident Scope	Text Block
Material Cybersecurity Incident Timing	Text Block
Material Cybersecurity Incident Material Impact or Reasonably Likely Material Impact	Text Block
Material Cybersecurity Incident Information Not Available or Undetermined	Text Block

As with all other Form 8-K items, the filing deadline for Item 1.05 is four business days after the trigger.

Sample Form 8-K: Tagging with CYD Taxonomy



Item 1.05. Material Cybersecurity Incidents

On October 15, 2024, XYZ Corporation ("the Company" or "we") detected a cybersecurity incident involving unauthorized access to our customer service database, containing personal data of about 100,000 clients.

Nature and Scope of the Incident

The incident occurred when threat actors exploited a previously unknown vulnerability in our customer service platform's software. This unauthorized access began on October 10, 2024, and was identified during routine monitoring by our security operations center, prompting an immediate investigation and response.

The scope of the compromised data includes customer names, contact information, and transaction histories. Importantly, sensitive financial information such as credit card numbers and social security numbers was not accessed due to encryption safeguards in place.

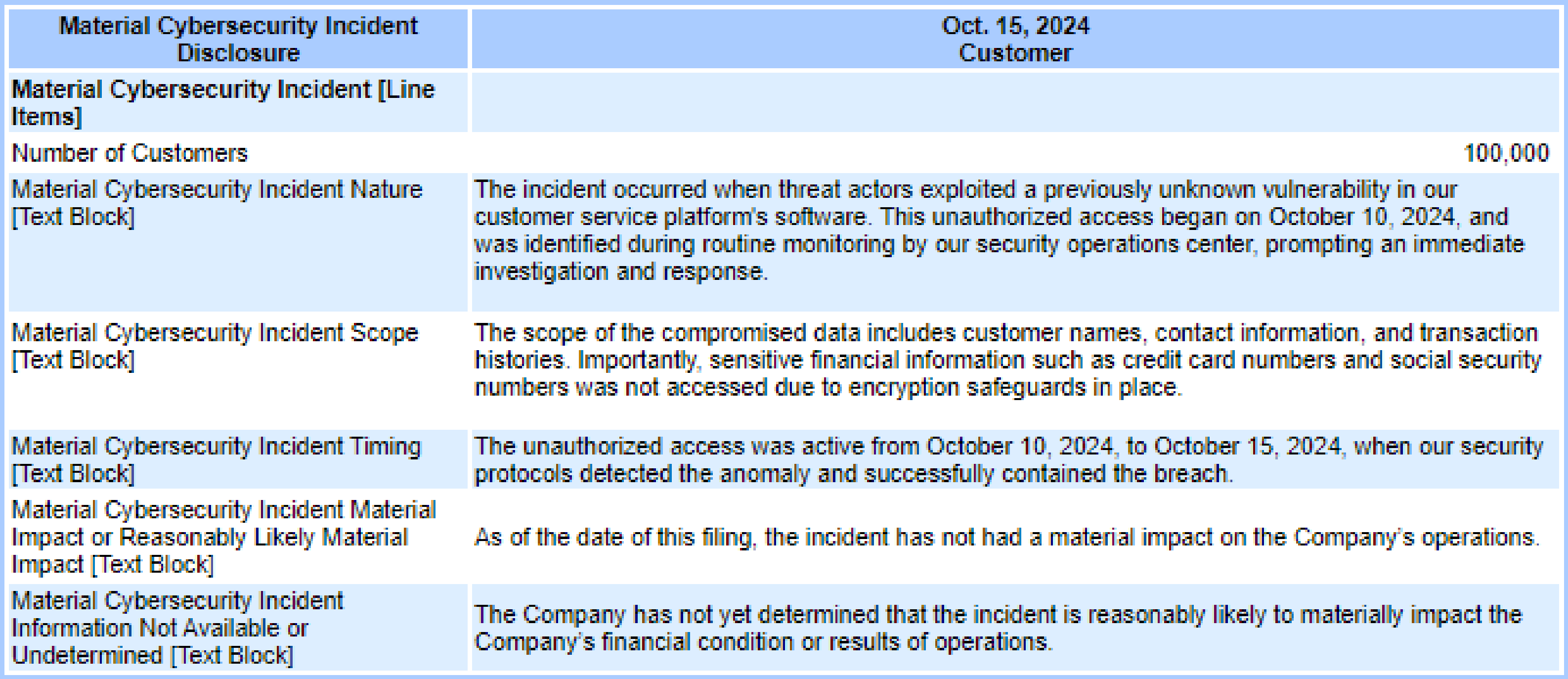
Timing of the Incident

The unauthorized access was active from October 10, 2024, to October 15, 2024, when our security protocols detected the anomaly and successfully contained the breach. Remediation steps were promptly enacted, which included patching the vulnerability, enhancing monitoring techniques, and notifying relevant authorities.

Material Impact

As of the date of this filing, the incident has not had a material impact on the Company's operations. The Company has not yet determined that the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

Sample Form 8-K: Tagging with CYD Taxonomy

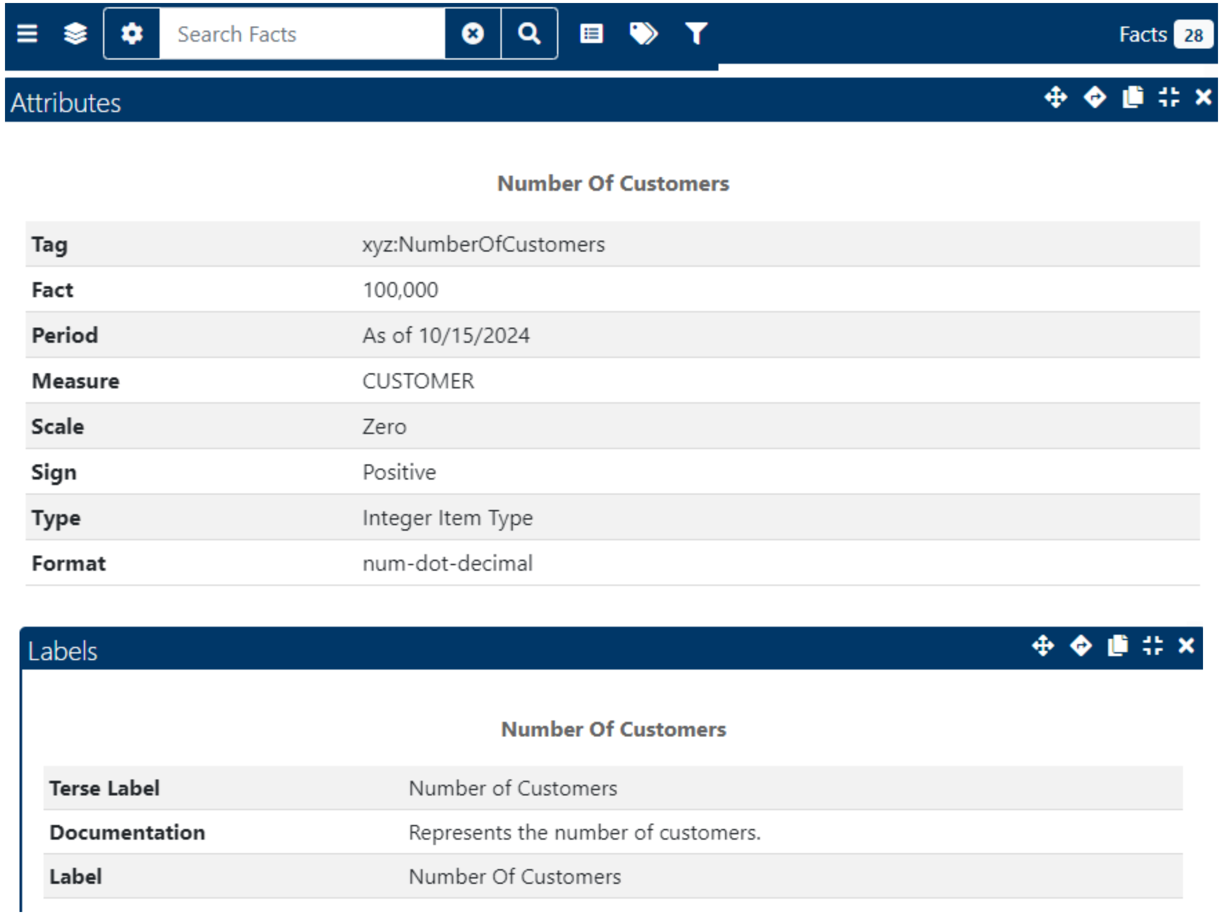


Material Cybersecurity Incident Disclosure	Oct. 15, 2024 Customer
Material Cybersecurity Incident [Line Items]	
Number of Customers	100,000
Material Cybersecurity Incident Nature [Text Block]	The incident occurred when threat actors exploited a previously unknown vulnerability in our customer service platform's software. This unauthorized access began on October 10, 2024, and was identified during routine monitoring by our security operations center, prompting an immediate investigation and response.
Material Cybersecurity Incident Scope [Text Block]	The scope of the compromised data includes customer names, contact information, and transaction histories. Importantly, sensitive financial information such as credit card numbers and social security numbers was not accessed due to encryption safeguards in place.
Material Cybersecurity Incident Timing [Text Block]	The unauthorized access was active from October 10, 2024, to October 15, 2024, when our security protocols detected the anomaly and successfully contained the breach.
Material Cybersecurity Incident Material Impact or Reasonably Likely Material Impact [Text Block]	As of the date of this filing, the incident has not had a material impact on the Company's operations.
Material Cybersecurity Incident Information Not Available or Undetermined [Text Block]	The Company has not yet determined that the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

The periods used for text blocks should be the Date of Report (Date of earliest event reported) on Form 8-K or Form 6-K.

If an amendment is filed to provide more information for a previously reported incident, the original date of report should be used, not the date of the amendment.

Sample Form 8-K: Tagging with CYD Taxonomy



Number Of Customers

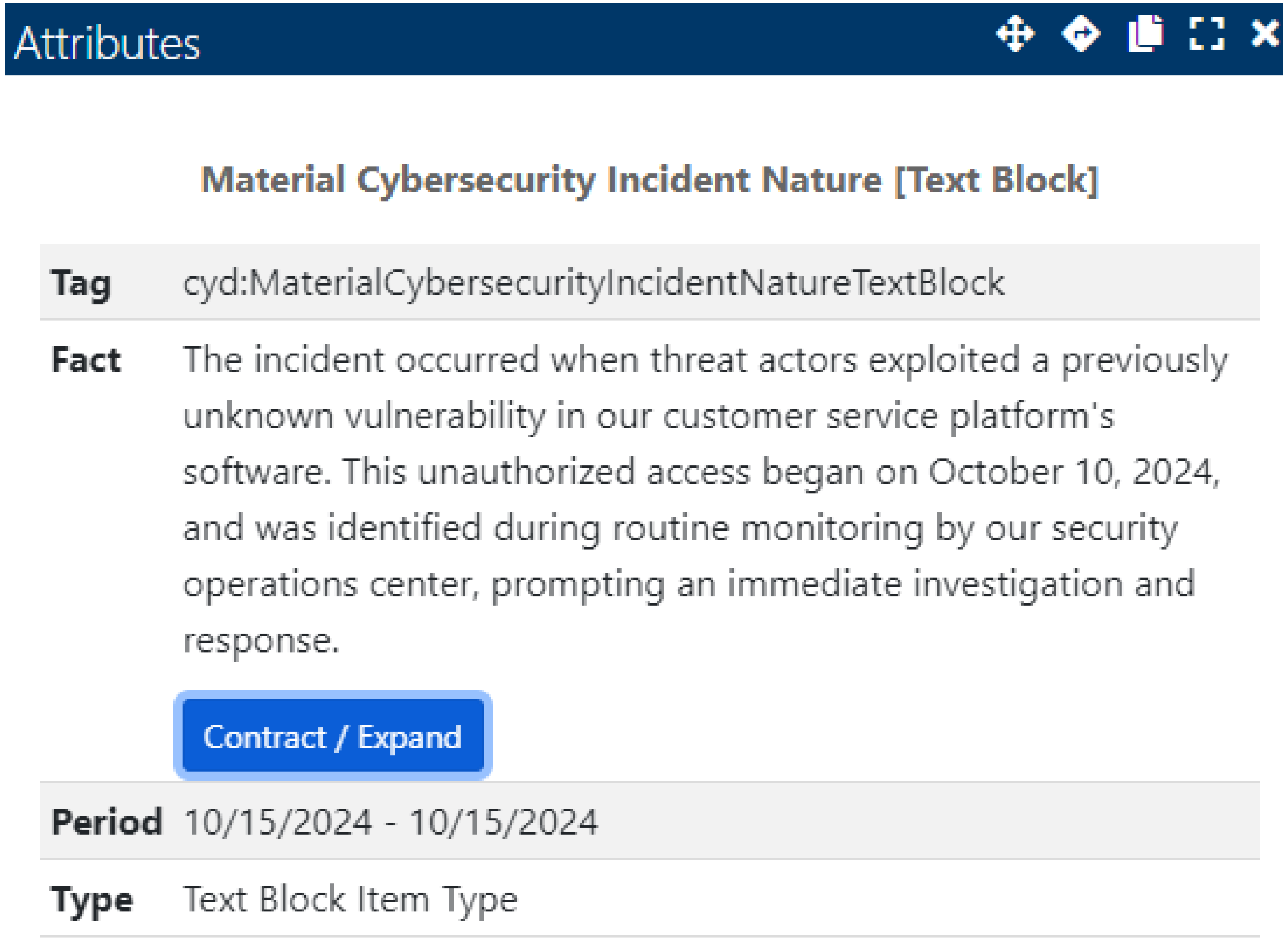
Tag	xyz:NumberOfCustomers
Fact	100,000
Period	As of 10/15/2024
Measure	CUSTOMER
Scale	Zero
Sign	Positive
Type	Integer Item Type
Format	num-dot-decimal

Number Of Customers

Terse Label	Number of Customers
Documentation	Represents the number of customers.
Label	Number Of Customers

The cybersecurity disclosure rules don't specifically ask for detailed fact values to be tagged, but if a company decides to include numbers in its report, <u>those numbers must be tagged separately along with the main text of the disclosure.</u>

Sample Form 8-K: Tagging with CYD Taxonomy



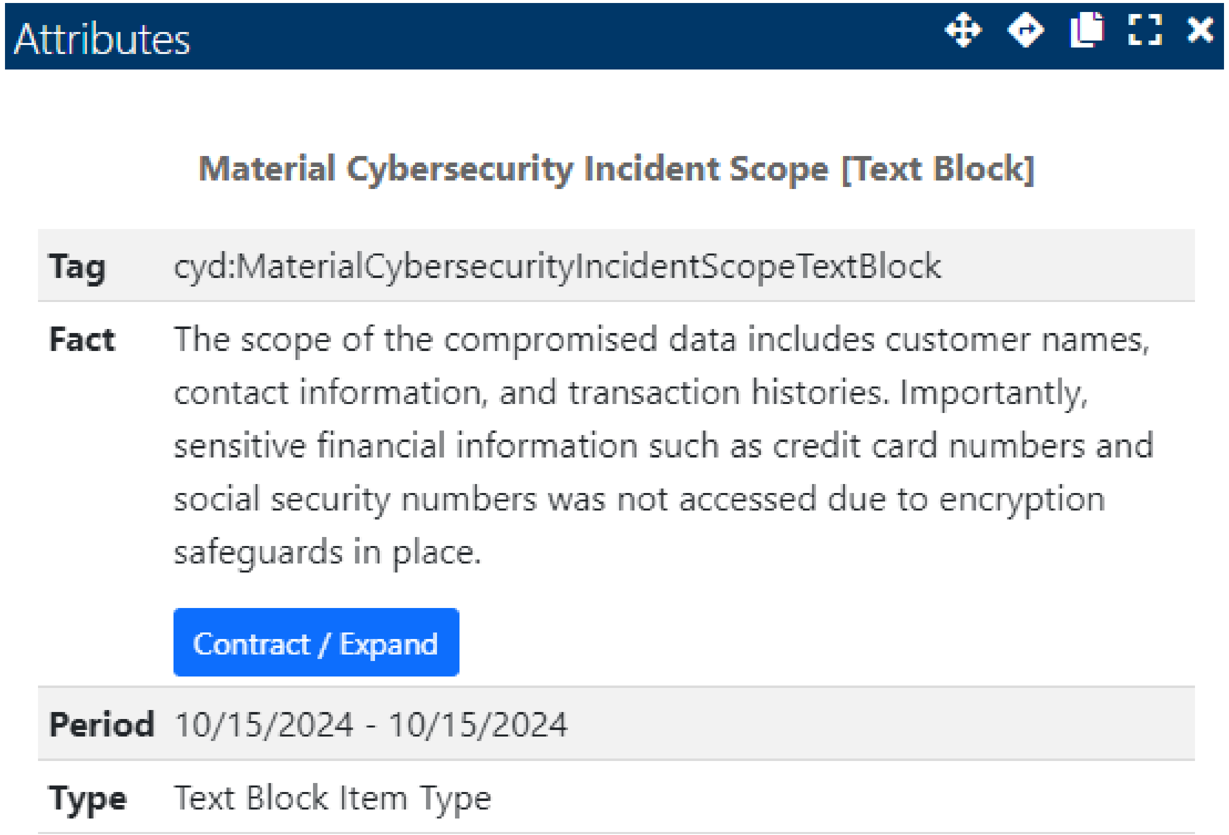
Material Cybersecurity Incident Nature [Text Block]

Tag	cyd:MaterialCybersecurityIncidentNatureTextBlock
Fact	The incident occurred when threat actors exploited a previously unknown vulnerability in our customer service platform's software. This unauthorized access began on October 10, 2024, and was identified during routine monitoring by our security operations center, prompting an immediate investigation and response.
Period	10/15/2024 - 10/15/2024
Type	Text Block Item Type

If there are multiple incidents, for each incident, the Material Cybersecurity Incident Axis must be used to separate disclosures.

Each incident disclosure (Nature, Scope, etc.) would be disaggregated using a customer domain member element (i.e., First Incident October 10, 2024 [Member], Second Incident October 20, 2024 [Member].

Sample Form 8-K: Tagging with CYD Taxonomy



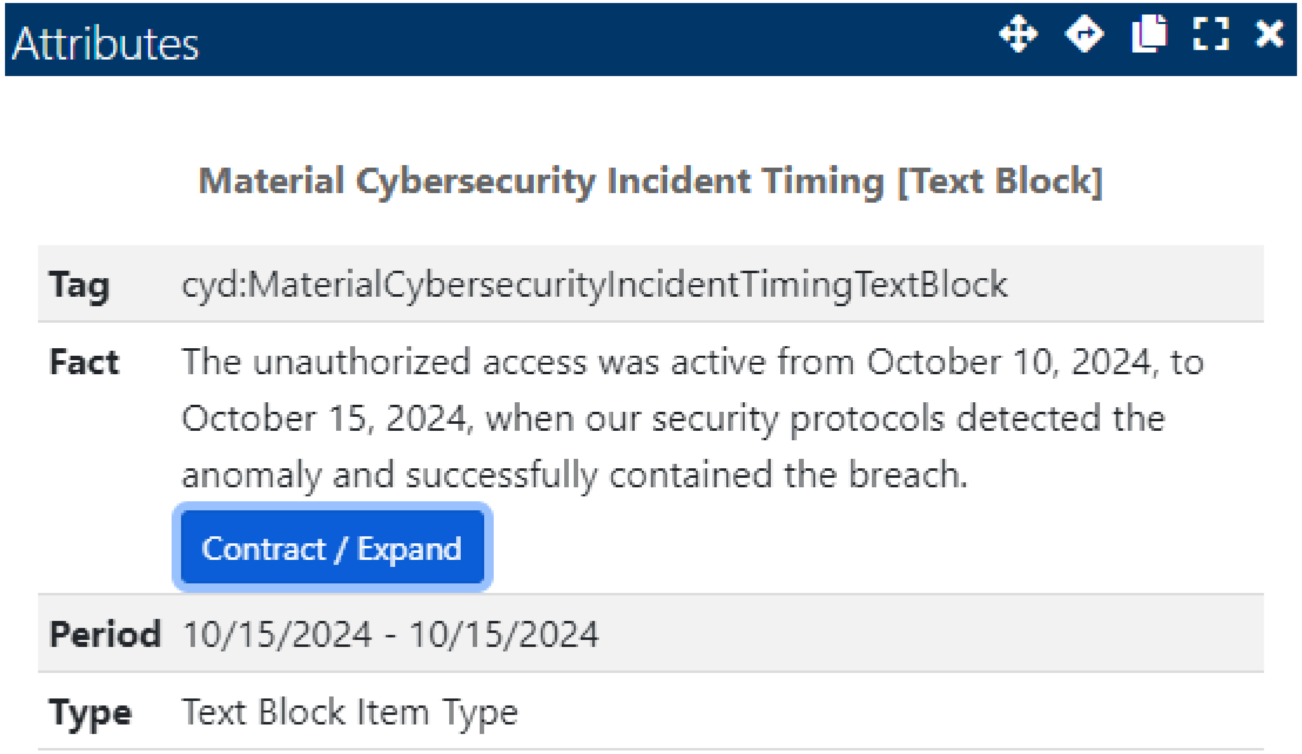
Material Cybersecurity Incident Scope [Text Block]

Tag	cyd:MaterialCybersecurityIncidentScopeTextBlock
Fact	The scope of the compromised data includes customer names, contact information, and transaction histories. Importantly, sensitive financial information such as credit card numbers and social security numbers was not accessed due to encryption safeguards in place. Contract / Expand
Period	10/15/2024 - 10/15/2024
Type	Text Block Item Type

The content iXBRL tagged which captures the nature of the incident will not always be clearly presented, as you see in this example.

The <u>textblock content could be a fragment within a sentence </u>or fragments of a paragraph.

Sample Form 8-K: Tagging with CYD Taxonomy



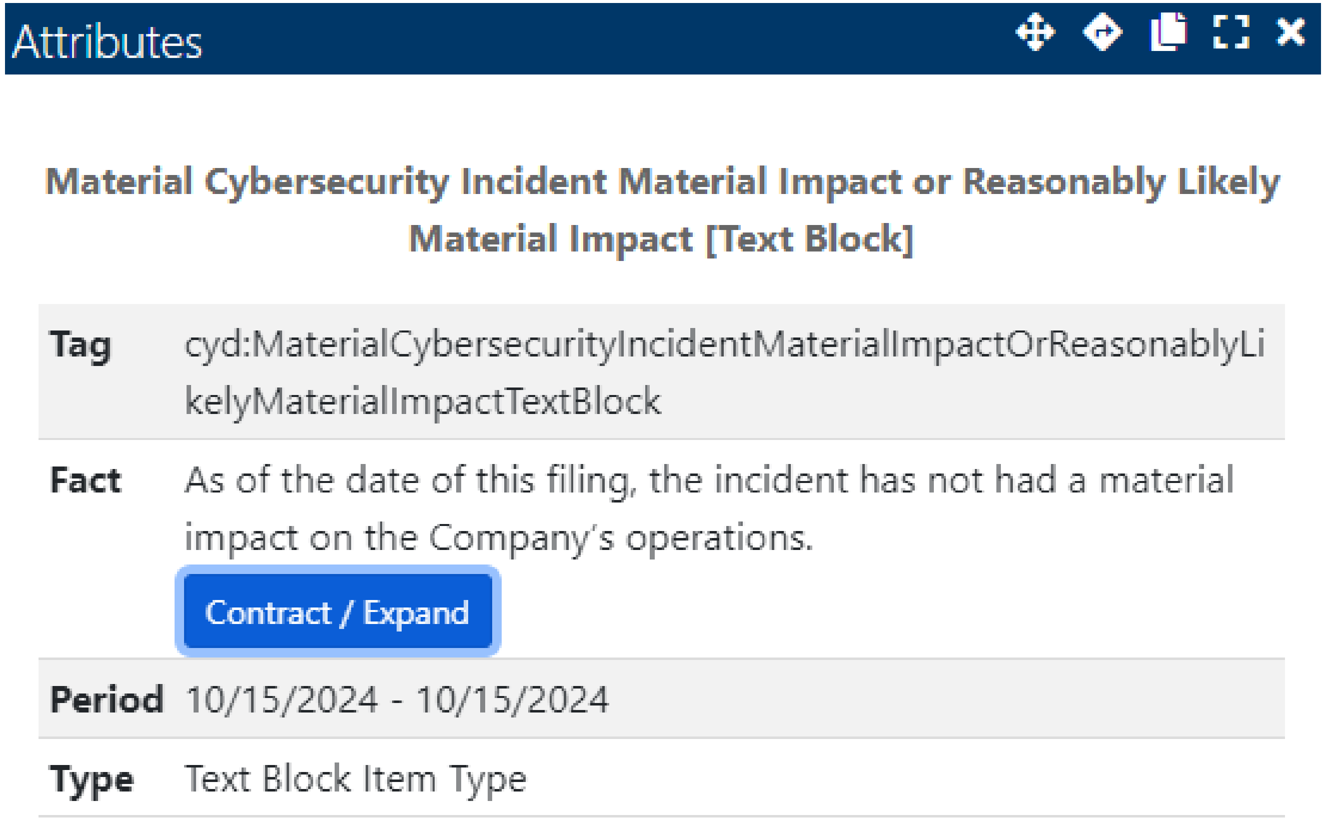
Material Cybersecurity Incident Timing [Text Block]

Tag	cyd:MaterialCybersecurityIncidentTimingTextBlock
Fact	The unauthorized access was active from October 10, 2024, to October 15, 2024, when our security protocols detected the anomaly and successfully contained the breach.
Period	10/15/2024 - 10/15/2024
Type	Text Block Item Type

Another common example of where detailed fact values could be located, is in Incident timing disclosure.

If this disclosure included the number of days until containment of a cybersecurity incident, <u>that detailed fact value must be iXBRL tagged.</u>

Sample Form 8-K: Tagging with CYD Taxonomy



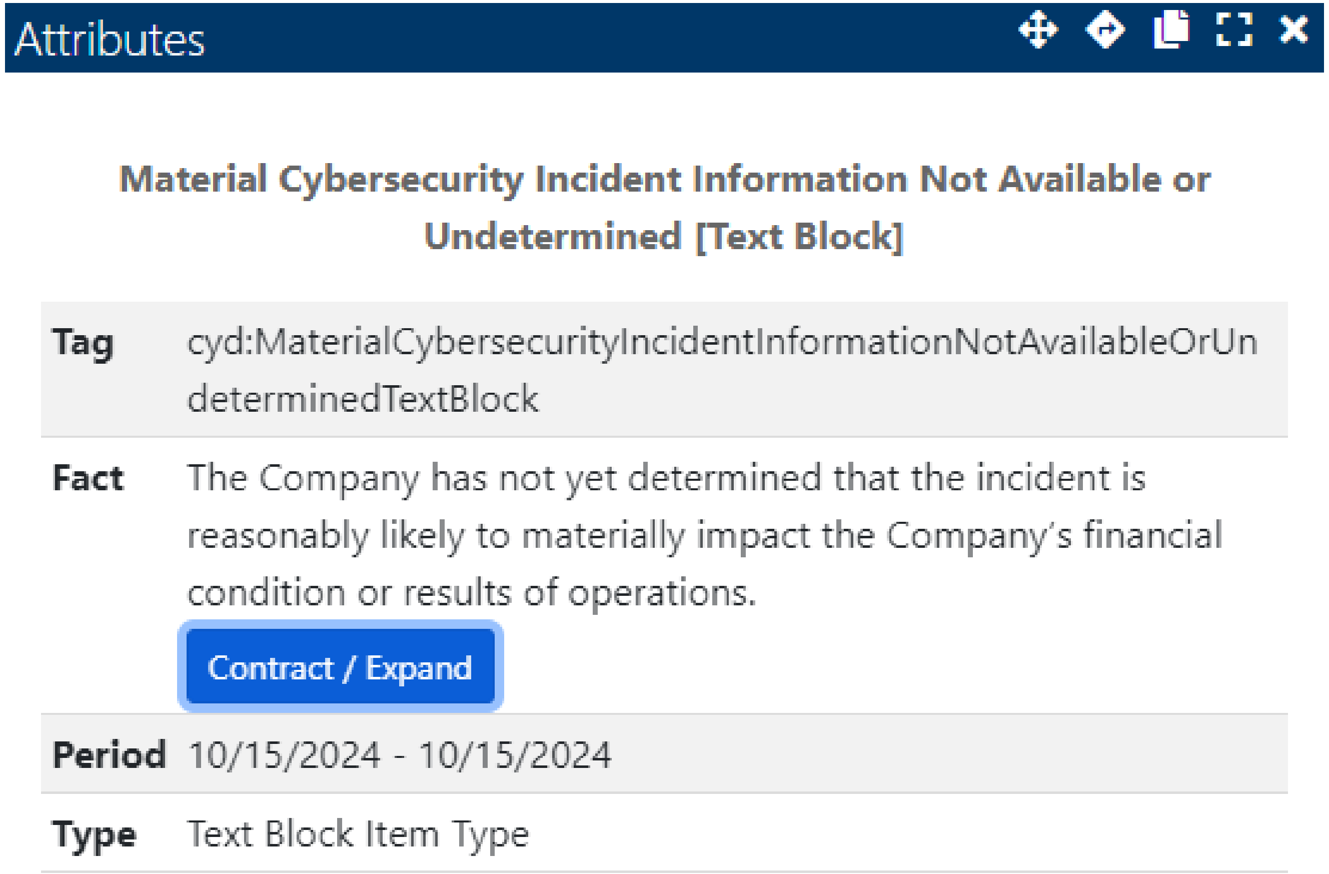
Material Cybersecurity Incident Material Impact or Reasonably Likely Material Impact [Text Block]

Tag	cyd:MaterialCybersecurityIncidentMaterialImpactOrReasonablyLikelyMaterialImpactTextBlock
Fact	As of the date of this filing, the incident has not had a material impact on the Company's operations.
Period	10/15/2024 - 10/15/2024
Type	Text Block Item Type

Focus disclosure on the material impact or reasonably likely material impact of the incident rather than the specific or technical details of the incident itself.

Also, the rule includes "financial condition and results of operations" but this is not exclusive. Consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.

Sample Form 8-K: Tagging with CYD Taxonomy



Material Cybersecurity Incident Information Not Available or Undetermined [Text Block]

Tag	cyd:MaterialCybersecurityIncidentInformationNotAvailableOrUndeterminedTextBlock
Fact	The Company has not yet determined that the incident is reasonably likely to materially impact the Company's financial condition or results of operations.
Period	10/15/2024 - 10/15/2024
Type	Text Block Item Type

The final rules don't require companies to file an amendment to update every piece of new information on the incident.

Instead, companies should submit a Form 8-K/A only if there was information required that was not determined or was unavailable at the time of the initial Form 8-K filing.

CYD Taxonomy: Annual Reporting (Form 10-K & 20-F)

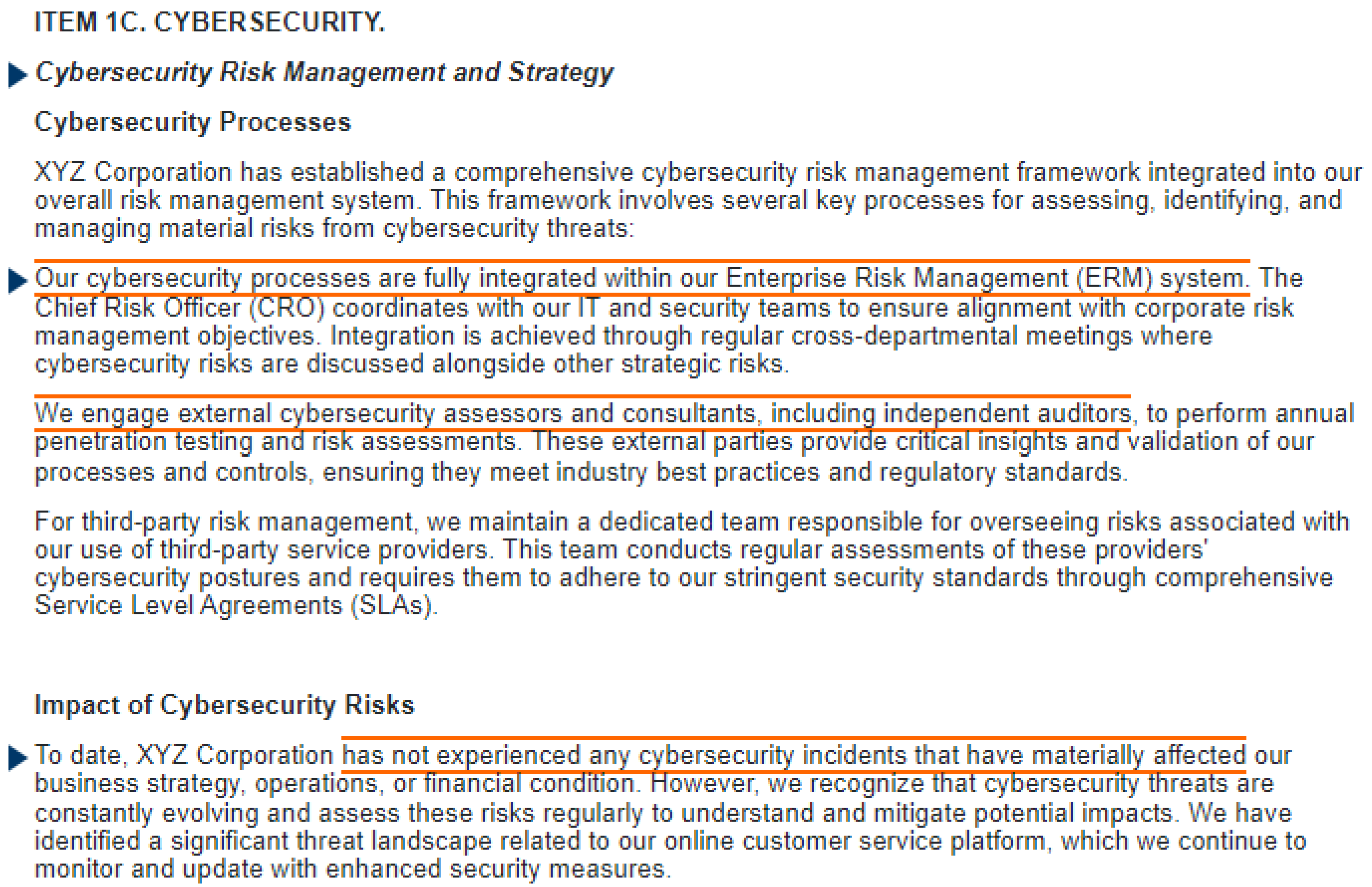
Annual Reporting: Cybersecurity Risk Management, Strategy, and Governance Disclosure	
Element Label Name	**Element Type**
Cybersecurity Risk Management, Strategy, and Governance	Abstract
Cybersecurity Risk Management, Strategy, and Governance	Table
Cybersecurity Risk Management, Strategy, and Governance	Line items
Cybersecurity Risk Management Processes for Assessing, Identifying, and Managing Threats	Text Block
Cybersecurity Risk Management Processes Integrated	Boolean Flag
Cybersecurity Risk Management Processes Integrated	Text Block
Cybersecurity Risk Management Third Party Engaged	Boolean Flag
Cybersecurity Risk Third Party Oversight and Identification Processes	Boolean Flag
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant	Boolean Flag
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant	Text Block
Cybersecurity Risk Board of Directors Oversight	Text Block
Cybersecurity Risk Board Committee or Subcommittee Responsible for Oversight	Text Block
Cybersecurity Risk Process for Informing Board Committee or Subcommittee Responsible for Oversight	Text Block
Cybersecurity Risk Role of Management	Text Block
Cybersecurity Risk Management Positions or Committees Responsible	Boolean Flag
Cybersecurity Risk Management Positions or Committees Responsible	Text Block
Cybersecurity Risk Management Expertise of Management Responsible	Text Block
Cybersecurity Risk Process for Informing Management or Committees Responsible	Text Block
Cybersecurity Risk Management Positions or Committees Responsible Report to Board	Boolean Flag

These disclosure items are non-exclusive. Companies should additionally disclose whatever information is necessary, based on their facts and circumstances.

For foreign private issuers, a substantially similar disclosure requirement is found in Item 16K to Form 20-F.

XBRL US

Sample Form 10-K: Tagging with CYD Taxonomy



ITEM 1C. CYBERSECURITY.

Cybersecurity Risk Management and Strategy

Cybersecurity Processes

XYZ Corporation has established a comprehensive cybersecurity risk management framework integrated into our overall risk management system. This framework involves several key processes for assessing, identifying, and managing material risks from cybersecurity threats:

Our cybersecurity processes are fully integrated within our Enterprise Risk Management (ERM) system. The Chief Risk Officer (CRO) coordinates with our IT and security teams to ensure alignment with corporate risk management objectives. Integration is achieved through regular cross-departmental meetings where cybersecurity risks are discussed alongside other strategic risks.

We engage external cybersecurity assessors and consultants, including independent auditors, to perform annual penetration testing and risk assessments. These external parties provide critical insights and validation of our processes and controls, ensuring they meet industry best practices and regulatory standards.

For third-party risk management, we maintain a dedicated team responsible for overseeing risks associated with our use of third-party service providers. This team conducts regular assessments of these providers' cybersecurity postures and requires them to adhere to our stringent security standards through comprehensive Service Level Agreements (SLAs).

Impact of Cybersecurity Risks

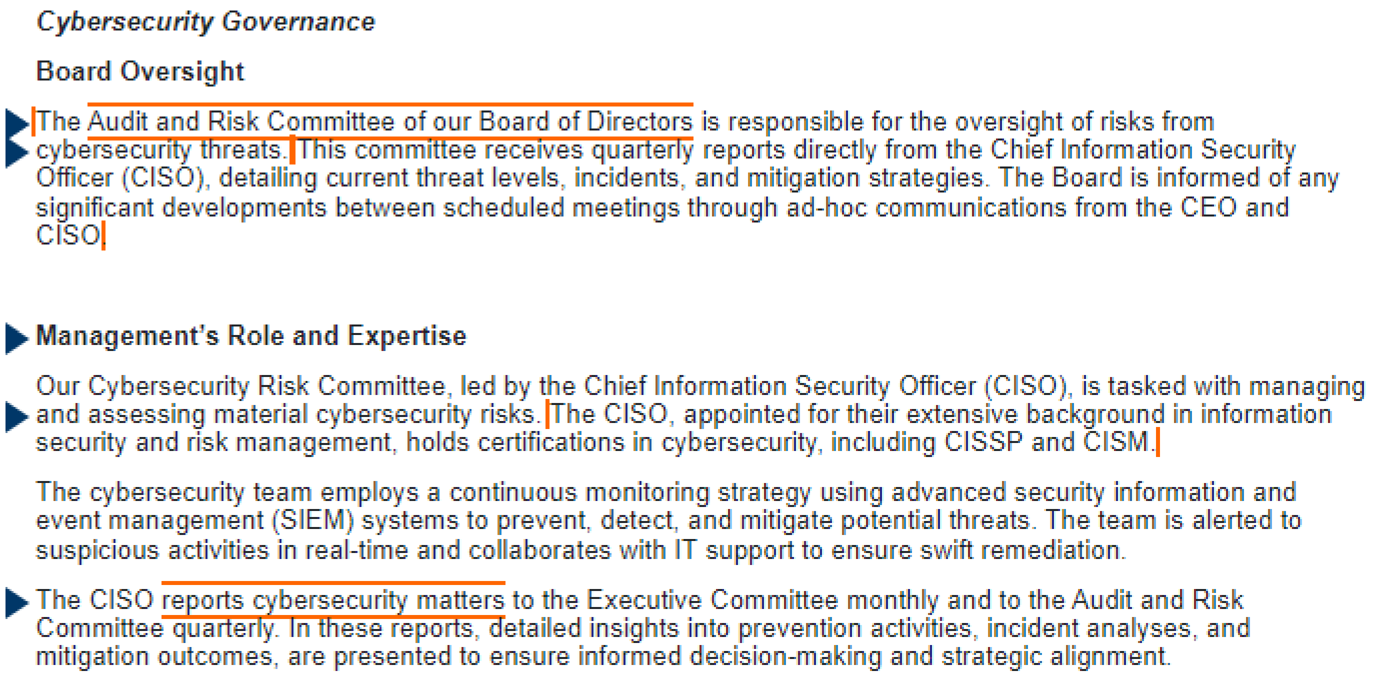
To date, XYZ Corporation has not experienced any cybersecurity incidents that have materially affected our business strategy, operations, or financial condition. However, we recognize that cybersecurity threats are constantly evolving and assess these risks regularly to understand and mitigate potential impacts. We have identified a significant threat landscape related to our online customer service platform, which we continue to monitor and update with enhanced security measures.

The disclosure requires a narrative, which is represented by text block concept **cyd:CybersecurityRiskManagementProcessesForAssessingIdentifyingAndManagingThreatsTextBlock**.

Within that disclosure, the Boolean flag **cyd:CybersecurityRiskManagementProcessesIntegratedFlag** represents whether the processes have been integrated.

If the flag is “true”, then the text block **cyd:CybersecurityRiskManagementProcessesIntegratedTextBlock** contains the description of “how” the processes have been integrated.

Sample Form 10-K: Tagging with CYD Taxonomy



Cybersecurity Governance

Board Oversight

The Audit and Risk Committee of our Board of Directors is responsible for the oversight of risks from cybersecurity threats. This committee receives quarterly reports directly from the Chief Information Security Officer (CISO), detailing current threat levels, incidents, and mitigation strategies. The Board is informed of any significant developments between scheduled meetings through ad-hoc communications from the CEO and CISO.

Management's Role and Expertise

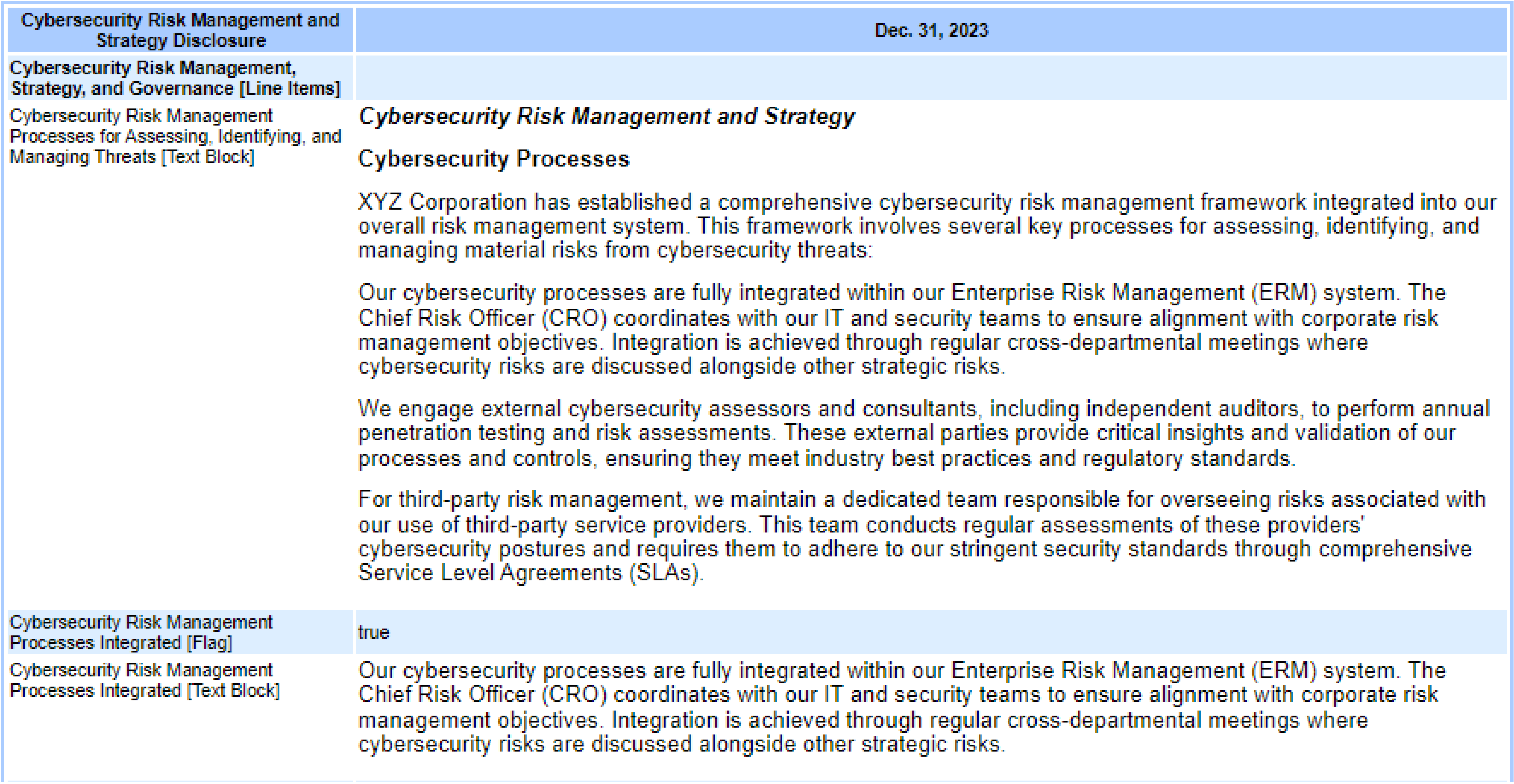
Our Cybersecurity Risk Committee, led by the Chief Information Security Officer (CISO), is tasked with managing and assessing material cybersecurity risks. The CISO, appointed for their extensive background in information security and risk management, holds certifications in cybersecurity, including CISSP and CISM.

The cybersecurity team employs a continuous monitoring strategy using advanced security information and event management (SIEM) systems to prevent, detect, and mitigate potential threats. The team is alerted to suspicious activities in real-time and collaborates with IT support to ensure swift remediation.

The CISO reports cybersecurity matters to the Executive Committee monthly and to the Audit and Risk Committee quarterly. In these reports, detailed insights into prevention activities, incident analyses, and mitigation outcomes, are presented to ensure informed decision-making and strategic alignment.

The Inline XBRL transformation registry formats **ixt:booleantrue** and **ixt:booleanfalse** can be used to mark a section of text and “flag” it as either true or false.

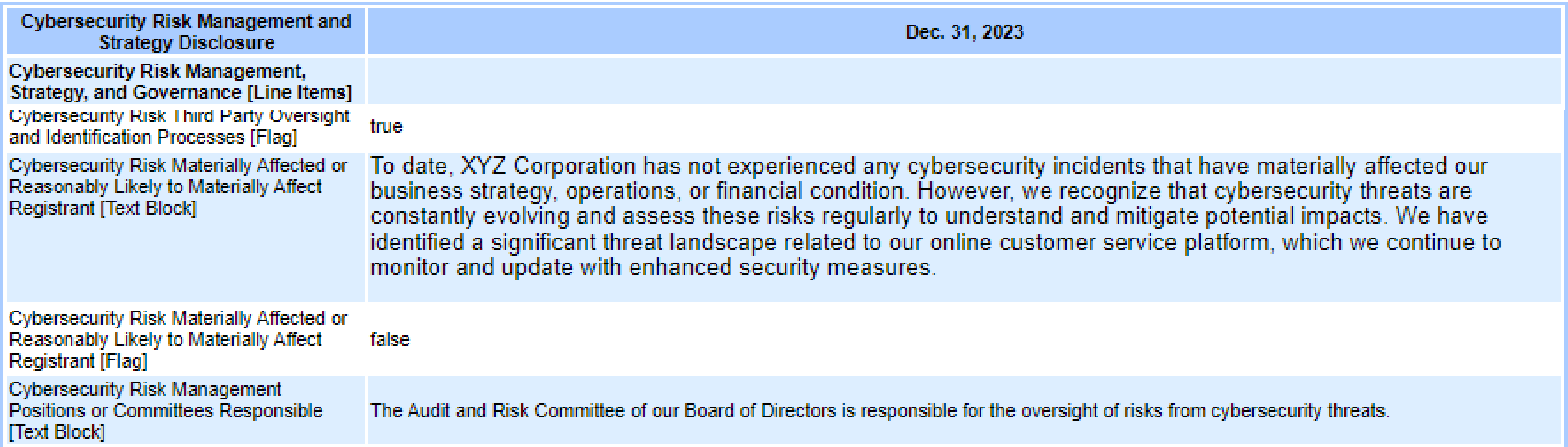
Sample Form 10-K: Tagging with CYD Taxonomy



Cybersecurity Risk Management and Strategy Disclosure	Dec. 31, 2023
Cybersecurity Risk Management, Strategy, and Governance [Line Items]	
Cybersecurity Risk Management Processes for Assessing, Identifying, and Managing Threats [Text Block]	***Cybersecurity Risk Management and Strategy*** **Cybersecurity Processes** XYZ Corporation has established a comprehensive cybersecurity risk management framework integrated into our overall risk management system. This framework involves several key processes for assessing, identifying, and managing material risks from cybersecurity threats: Our cybersecurity processes are fully integrated within our Enterprise Risk Management (ERM) system. The Chief Risk Officer (CRO) coordinates with our IT and security teams to ensure alignment with corporate risk management objectives. Integration is achieved through regular cross-departmental meetings where cybersecurity risks are discussed alongside other strategic risks. We engage external cybersecurity assessors and consultants, including independent auditors, to perform annual penetration testing and risk assessments. These external parties provide critical insights and validation of our processes and controls, ensuring they meet industry best practices and regulatory standards. For third-party risk management, we maintain a dedicated team responsible for overseeing risks associated with our use of third-party service providers. This team conducts regular assessments of these providers' cybersecurity postures and requires them to adhere to our stringent security standards through comprehensive Service Level Agreements (SLAs).
Cybersecurity Risk Management Processes Integrated [Flag]	true
Cybersecurity Risk Management Processes Integrated [Text Block]	Our cybersecurity processes are fully integrated within our Enterprise Risk Management (ERM) system. The Chief Risk Officer (CRO) coordinates with our IT and security teams to ensure alignment with corporate risk management objectives. Integration is achieved through regular cross-departmental meetings where cybersecurity risks are discussed alongside other strategic risks.

Concepts in the risk management, strategy, and governance disclosure are generally narrative text blocks, paired with Boolean flags and both corresponding to disclosure requirements.

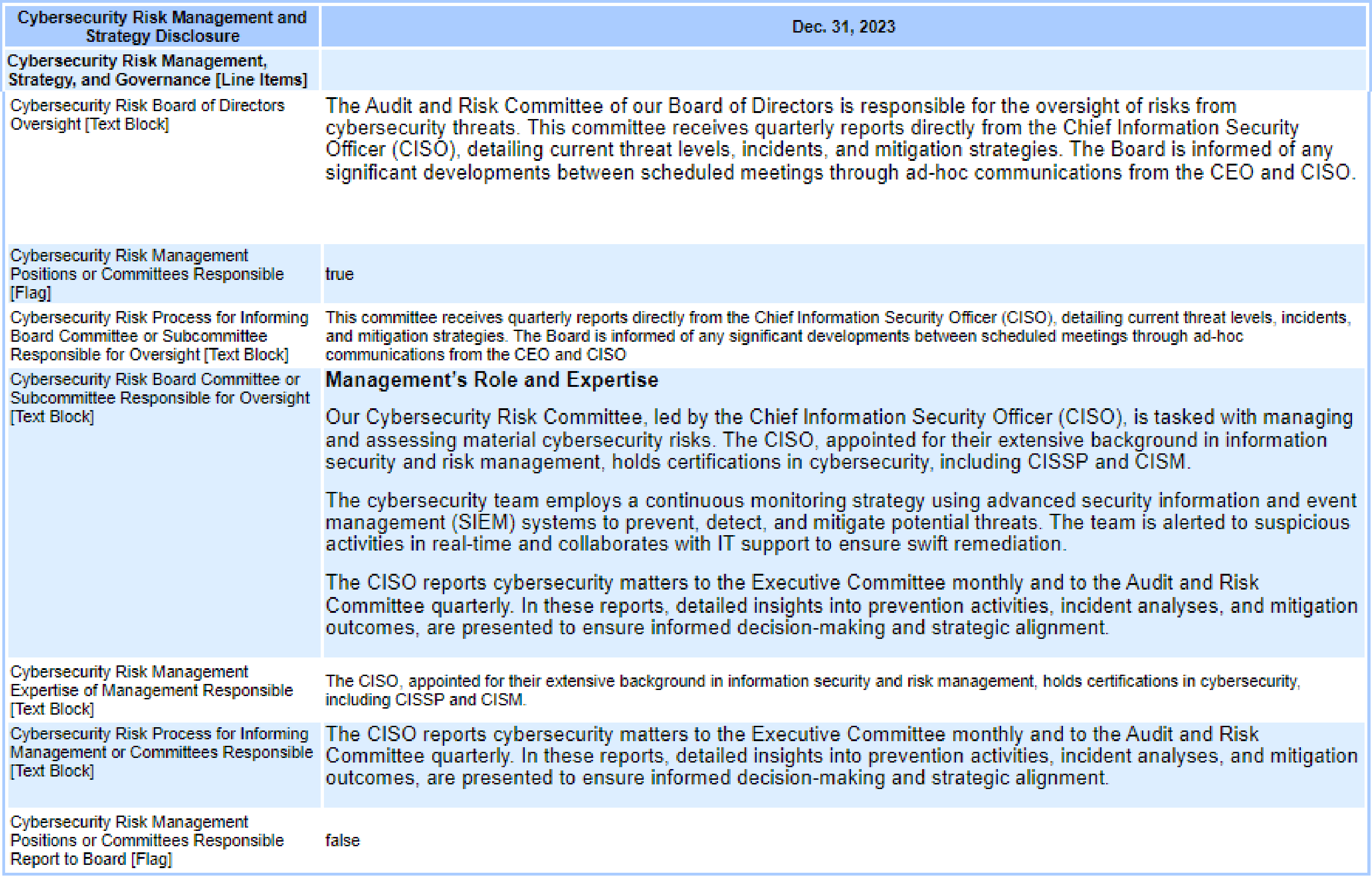
Sample Form 10-K: Tagging with CYD Taxonomy



Cybersecurity Risk Management and Strategy Disclosure	Dec. 31, 2023
Cybersecurity Risk Management, Strategy, and Governance [Line Items]	
Cybersecurity Risk Third Party Oversight and Identification Processes [Flag]	true
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Text Block]	To date, XYZ Corporation has not experienced any cybersecurity incidents that have materially affected our business strategy, operations, or financial condition. However, we recognize that cybersecurity threats are constantly evolving and assess these risks regularly to understand and mitigate potential impacts. We have identified a significant threat landscape related to our online customer service platform, which we continue to monitor and update with enhanced security measures.
Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Flag]	false
Cybersecurity Risk Management Positions or Committees Responsible [Text Block]	The Audit and Risk Committee of our Board of Directors is responsible for the oversight of risks from cybersecurity threats.

Textblock tagging might be challenging.

Sample Form 10-K: Tagging with CYD Taxonomy



Cybersecurity Risk Management and Strategy Disclosure	Dec. 31, 2023
Cybersecurity Risk Management, Strategy, and Governance [Line Items]	
Cybersecurity Risk Board of Directors Oversight [Text Block]	The Audit and Risk Committee of our Board of Directors is responsible for the oversight of risks from cybersecurity threats. This committee receives quarterly reports directly from the Chief Information Security Officer (CISO), detailing current threat levels, incidents, and mitigation strategies. The Board is informed of any significant developments between scheduled meetings through ad-hoc communications from the CEO and CISO.
Cybersecurity Risk Management Positions or Committees Responsible [Flag]	true
Cybersecurity Risk Process for Informing Board Committee or Subcommittee Responsible for Oversight [Text Block]	This committee receives quarterly reports directly from the Chief Information Security Officer (CISO), detailing current threat levels, incidents, and mitigation strategies. The Board is informed of any significant developments between scheduled meetings through ad-hoc communications from the CEO and CISO
Cybersecurity Risk Board Committee or Subcommittee Responsible for Oversight [Text Block]	**Management's Role and Expertise** Our Cybersecurity Risk Committee, led by the Chief Information Security Officer (CISO), is tasked with managing and assessing material cybersecurity risks. The CISO, appointed for their extensive background in information security and risk management, holds certifications in cybersecurity, including CISSP and CISM. The cybersecurity team employs a continuous monitoring strategy using advanced security information and event management (SIEM) systems to prevent, detect, and mitigate potential threats. The team is alerted to suspicious activities in real-time and collaborates with IT support to ensure swift remediation. The CISO reports cybersecurity matters to the Executive Committee monthly and to the Audit and Risk Committee quarterly. In these reports, detailed insights into prevention activities, incident analyses, and mitigation outcomes, are presented to ensure informed decision-making and strategic alignment.
Cybersecurity Risk Management Expertise of Management Responsible [Text Block]	The CISO, appointed for their extensive background in information security and risk management, holds certifications in cybersecurity, including CISSP and CISM.
Cybersecurity Risk Process for Informing Management or Committees Responsible [Text Block]	The CISO reports cybersecurity matters to the Executive Committee monthly and to the Audit and Risk Committee quarterly. In these reports, detailed insights into prevention activities, incident analyses, and mitigation outcomes, are presented to ensure informed decision-making and strategic alignment.
Cybersecurity Risk Management Positions or Committees Responsible Report to Board [Flag]	false

A single paragraph can contain information that would need more than one text block tag applied.

A section of text can contain partial information that could be tagged by one text block and then explained later in another section.

CPE Questions

XBRL | US

Discussion of the Rule

- **Nabeel Cheema**, Special Counsel, Office of Rulemaking, Division of Corporation Finance, U.S. Securities and Exchange Commission
- **Justine Robinson**, Of Counsel, Gibson, Dunn & Crutcher LLP
- **Lisa Cousino**, XBRL Consulting Services and Professional Standards, Broadridge Financial Solutions, Inc.

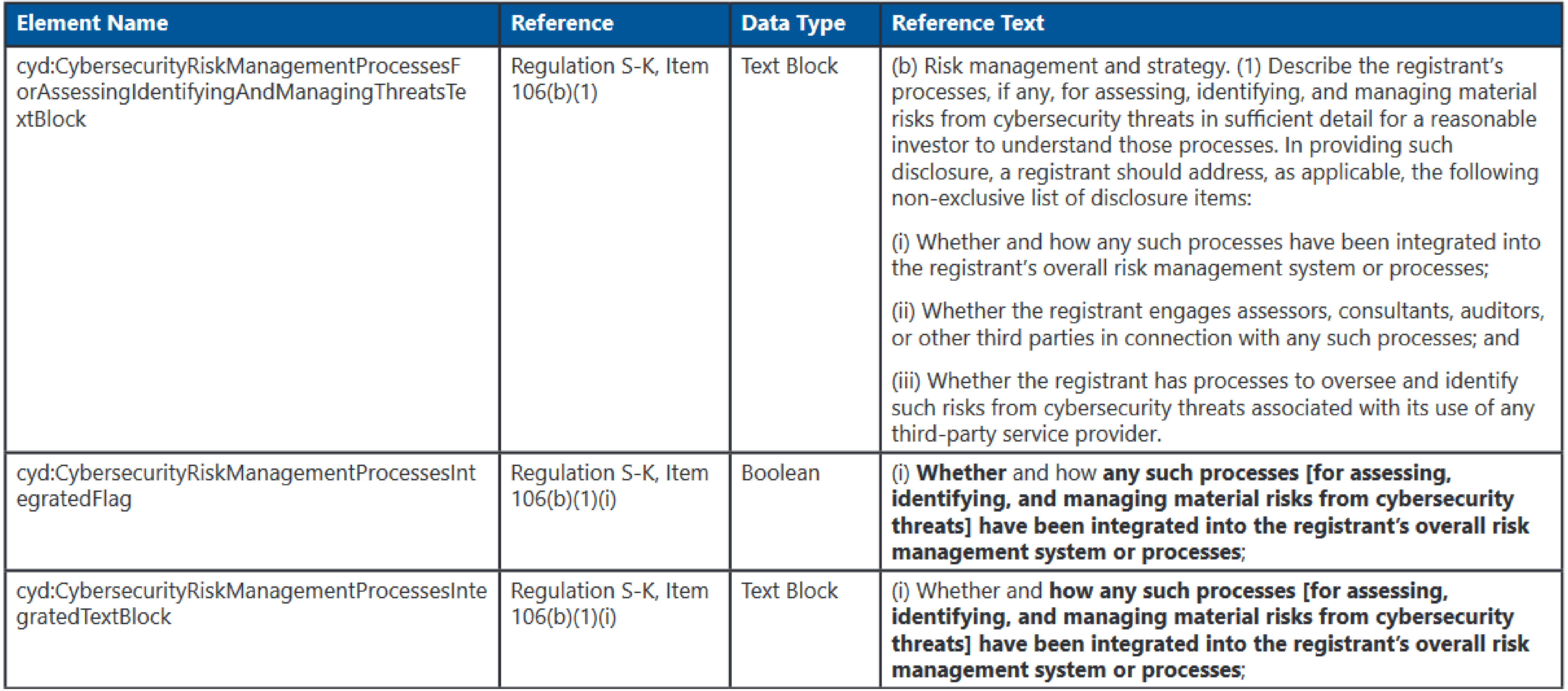
Tips and Resources

What Does CYD Tagging Look Like?

- Both types have text blocks
- Risk Management also has Boolean concepts
- Tagging consists of largely of text blocks and TRUE/FALSE affirmations
- It’s easy to differentiate the concepts by the suffix “TextBlock” or “Flag”
- Boolean items are paired with a text block
  - Whether it “has” a policy or characteristic
  - Text is “how”

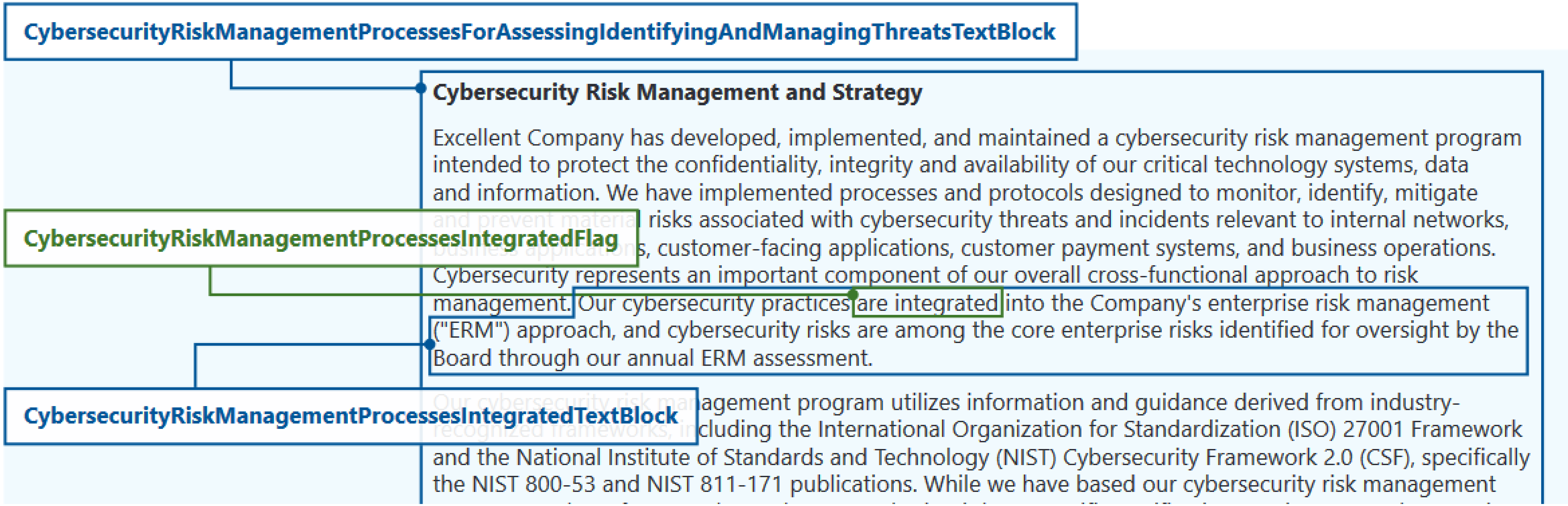
XBRL US

Sample of Concepts/Reference/Data Type



Element Name	Reference	Data Type	Reference Text
cyd:CybersecurityRiskManagementProcessesForAssessingIdentifyingAndManagingThreatsTextBlock	Regulation S-K, Item 106(b)(1)	Text Block	(b) Risk management and strategy. (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: (i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes; (ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and (iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
cyd:CybersecurityRiskManagementProcessesIntegratedFlag	Regulation S-K, Item 106(b)(1)(i)	Boolean	(i) **Whether** and how **any such processes [for assessing, identifying, and managing material risks from cybersecurity threats] have been integrated into the registrant's overall risk management system or processes**;
cyd:CybersecurityRiskManagementProcessesIntegratedTextBlock	Regulation S-K, Item 106(b)(1)(i)	Text Block	(i) Whether and **how any such processes [for assessing, identifying, and managing material risks from cybersecurity threats] have been integrated into the registrant's overall risk management system or processes**;

What’s Being Tagged


CybersecurityRiskManagementProcessesForAssessingIdentifyingAndManagingThreatsTextBlock
CybersecurityRiskManagementProcessesIntegratedFlag
CybersecurityRiskManagementProcessesIntegratedTextBlock

Cybersecurity Risk Management and Strategy

Excellent Company has developed, implemented, and maintained a cybersecurity risk management program intended to protect the confidentiality, integrity and availability of our critical technology systems, data and information. We have implemented processes and protocols designed to monitor, identify, mitigate and prevent material risks associated with cybersecurity threats and incidents relevant to internal networks, business applications, customer-facing applications, customer payment systems, and business operations. Cybersecurity represents an important component of our overall cross-functional approach to risk management. Our cybersecurity practices are integrated into the Company's enterprise risk management ("ERM") approach, and cybersecurity risks are among the core enterprise risks identified for oversight by the Board through our annual ERM assessment.

Our cybersecurity risk management program utilizes information and guidance derived from industry-recognized frameworks, including the International Organization for Standardization (ISO) 27001 Framework and the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (CSF), specifically the NIST 800-53 and NIST 811-171 publications. While we have based our cybersecurity risk management

Tag an Existing Disclosure

- Does your current cyber risk/incident disclosure match the XBRL data model?
- When authoring the section, avoid mixed conceptual data that spans multiple items to be tagged — *avoid continuations!*
- Use last year’s 10-K or 20-F as a test case
    - Are the required elements present
    - Is there any special items
- Use the preparers guide and any third-party data
- When you’re tagging, watch for nested or overlapped items

Check List

- Understand your role with respect to the organization of data or preparing and tagging
- Familiarize yourself with the proof being provided by your preparer: Do you know how to identify the fields?
- What fields are required for each type of disclosure:
  - 8-K/6-K Item 1.05/General Instruction B disclosure, vs
  - 10-K/20-F periodic disclosure
- As always, test file prior to the actual deadline (actual or self-imposed)

Be Ready for Item 1.05, If Needed

- Disclosure is fairly quick, be ready
- Have a check list or template ready — both for narrative and tagging
- Consider incorporating the disclosure into your cybersecurity incident response plan/process

Resources

- SEC Rule:
  - https://www.sec.gov/files/rules/final/2023/33-11216.pdf
- CYD Preparer’s Guide:
  - https://xbrl.sec.gov/cyd/2024/cyd-taxonomy-guide-2024-09-16.pdf
- Presentation Materials:
  - CYD Fact Sheet (download from session materials)

CPE Questions

Digital Reporting for Measurable Results

Climate, Corporate, Government

Thursday, November 14
Washington, DC

- Featuring keynote *U.S. Congressman Patrick McHenry,* Chairman of the House Financial Services Committee (R-NC)

- Special video remarks from *U.S. Senator Mark Warner (D-VA)*

https://xbrl.us/digital-reporting-2024/

Other speakers:

- International Sustainability Standards Board (ISSB)
- London Stock Exchange Group (LSEG)
- FactSet
- Data Foundation
- Global LEI Foundation
- Federal Energy Regulatory Commission (FERC)
- BNY
- KPMG