TRENDS IN INVESTOR COMMUNICATIONS

What You Need to Know About the US SEC's Proposed Cybersecurity Rules

IN THIS THOUGHT PIECE

In March 2022, the U.S. Securities and Exchange Commission (SEC) proposed new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

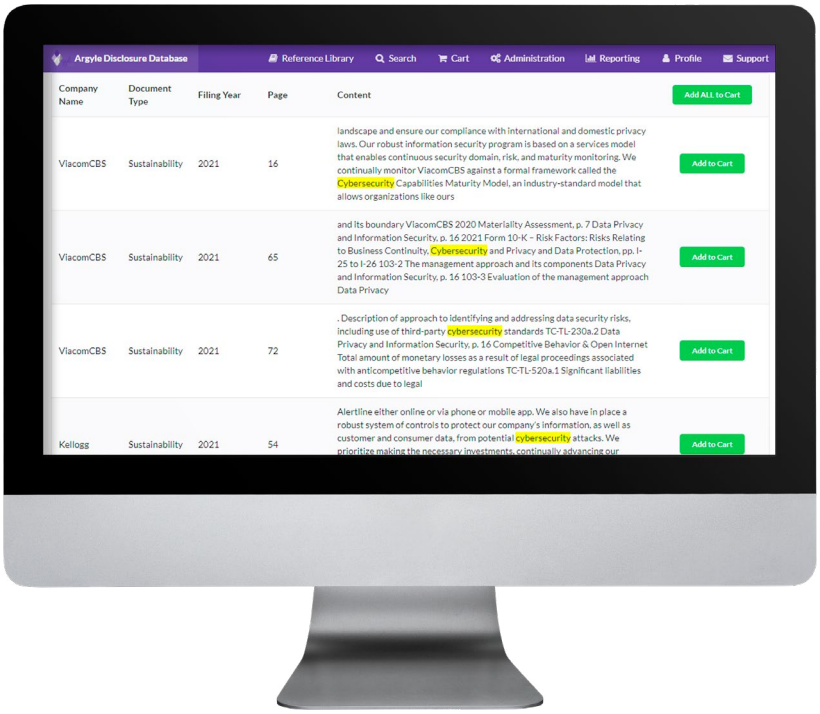
This thought pieces discusses these proposed rules and gives examples of corporate cybersecurity disclosures to date.

Benchmark for Hot Topics with the Argyle Disclosure Database

Dive deeper into hot topics like cybersecurity and run benchmarks with the Argyle Disclosure Database. Search text, and parse graphics by theme within the industry's only user-accessible graphic disclosure database.

Review online or compile and download your selected disclosures as a PDF report.

Learn more and sign up at add.argyleteam.com



Contents

Introduction

In March 2022, the U.S. Securities and Exchange Commission (SEC) proposed new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. Based on the SEC's recently released Reg Flex Agenda, final rules are expected in April 2023, with many practitioners anticipating little change to the proposed governance disclosures when the final rules are adopted.

> "The proposed amendments are designed to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents. Consistent, comparable, and decision-useful disclosures would allow investors to evaluate registrants' exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents."[1]

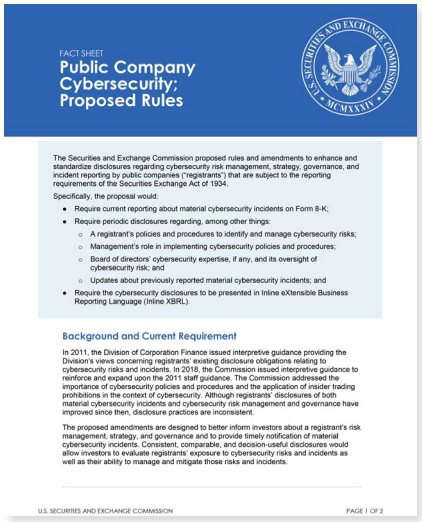
Under the proposal, companies will be required to:

1. provide current reporting on Form 8-K within four business days after a company determines that it has experienced a material cybersecurity incident,
2. update any incident disclosures in subsequent periodic filings,
3. include annual cybersecurity governance and risk management disclosures, and
4. tag the new disclosures in Inline XBRL, including block tagging of narrative disclosures and detail tagging of any quantitative amounts included in such discussions.

[1] U.S. Securities and Exchange Commission. *Fact Sheet Public Company Cybersecurity; Proposed Rules* (March 9, 2022).

Focus on the New Risk Management, Strategy, and Governance Disclosure Requirements

In light of the increasing risks that cybersecurity threats and incidents pose for public companies, the elevated focus of such risks for boards of directors and management teams, and the potential impact of such events on investors' return on investment, the SEC believes that how a company is managing its cybersecurity risks is decision-useful information and that investors would benefit from greater availability and comparability of disclosures across industries regarding cybersecurity risk management, strategy and governance practices so that they can assess if and how well companies are managing these risks.[1]



FACT SHEET

Public Company Cybersecurity; Proposed Rules

The Securities and Exchange Commission proposed rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies ("registrants") that are subject to the reporting requirements of the Securities Exchange Act of 1934.

Specifically, the proposal would:

- Require current reporting about material cybersecurity incidents on Form 8-K;
- Require periodic disclosures regarding, among other things:
  - A registrant's policies and procedures to identify and manage cybersecurity risks;
  - Management's role in implementing cybersecurity policies and procedures;
  - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
  - Updates about previously reported material cybersecurity incidents; and
- Require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

Background and Current Requirement

In 2011, the Division of Corporation Finance issued interpretive guidance providing the Division's views concerning registrants' existing disclosure obligations relating to cybersecurity risks and incidents. In 2018, the Commission issued interpretive guidance to reinforce and expand upon the 2011 staff guidance. The Commission addressed the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity. Although registrants' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since then, disclosure practices are inconsistent.

The proposed amendments are designed to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents. Consistent, comparable, and decision-useful disclosures would allow investors to evaluate registrants' exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents.

U.S. SECURITIES AND EXCHANGE COMMISSION PAGE 1 OF 2

With the new disclosures, the SEC is pushing companies to move beyond general statements or references about cybersecurity and board oversight and instead to provide investors with greater transparency of a company's strategies and actions to manage cybersecurity risks to allow investors to:

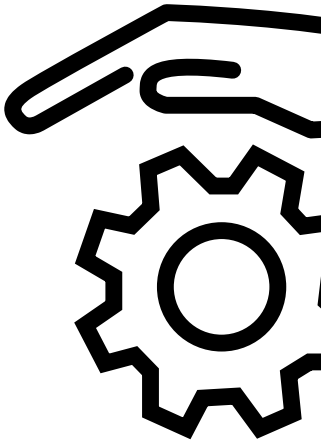
1. understand the potential impact on a company's business model, strategy, financial condition, financial planning, results of operations and allocation of capital and

2. assess a company's resiliency or vulnerability to cybersecurity risks in the future.[1]

[1] *SEC Proposed Rule Release No. 33-11038, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,* page 11.

[2] *Id.*, page 36.

Risk Management and Strategy

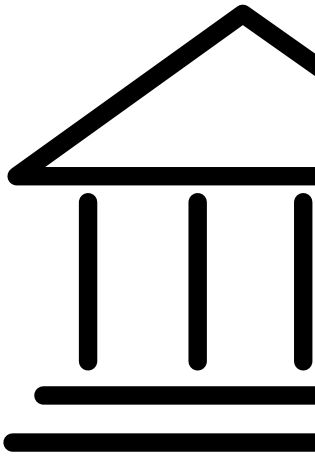


Under proposed Item 106(b), companies will be required to disclose policies and procedures, if any, to identify and manage cybersecurity risks and threats, including operational risk, intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws and other litigation and legal risk, and reputational risk.

Specifically, companies must discuss whether:

- they have a cybersecurity risk assessment program and if so, provide a description of the program,
- they engage assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program,
- they have policies and procedures to oversee and identify the cybersecurity risks associated with use of any third-party service provider (including, but not limited to, those providers that have access to customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers,
- they undertake activities to prevent, detect, and minimize effects of cybersecurity incidents,
- they have business continuity, contingency, and recovery plans in the event of a cybersecurity incident,
- previous cybersecurity incidents have informed changes in their governance, policies and procedures,
  or technologies,
- cybersecurity related risk and incidents have affected or are reasonably likely to affect their results of operations or financial condition and, if so, how, and
- cybersecurity risks are considered as part of their business strategy, financial planning, and capital allocation and, if so, how.

Governance



The proposed rules are also designed to provide more detailed disclosure regarding board oversight of a company's cybersecurity risk and the role of management in the implementation of the company's related policies, procedures, and strategies to allow investors to understand how the company "prepares for, prevents, or responds to cybersecurity incidents."[3]

Under the rules as proposed, companies will be required to provide specific disclosure on cybersecurity governance, including the board's oversight of and management's role in assessing and managing cybersecurity risks as well as the relevant expertise of management and its role in implementing the registrant's cybersecurity policies, procedures, and strategies.

[3] *Id.*, page 38.

Item 106(c)(1) will require companies to discuss the following regarding its board's oversight of cybersecurity risk:

- whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks,
- the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic, and
- whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

Additionally, proposed Item 106(c)(2) will require companies to describe management's role in assessing and managing cybersecurity-related risks and in implementing cybersecurity policies, procedures, and strategies. The SEC has indicated that, at a minimum, companies should discuss:

- whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members,
- whether the company has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the company's organizational chart, and the relevant expertise of any such persons,
- the processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents, and
- whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Directors' Cybersecurity Expertise

Lastly, the proposed rules amend Item 407 of Regulation S-K to require disclosure about the cybersecurity expertise of members of the board of directors, if any. In addition to what companies may already be providing in board biographies or skills matrices, they will have to disclose the name(s) of any director and include a detailed description of the nature of the expertise for any member of the board who is determined to have cybersecurity expertise.

While the rule does not define what constitutes "cybersecurity expertise," it does include the following non-exclusive list of criteria that companies should consider in reaching a determination on whether a director has expertise in cybersecurity:

- prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner,
- certifications or degree in cybersecurity, and
- knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

Examples of Existing Cybersecurity Disclosures in Proxy Statements and ESG Reports

In anticipation of the new disclosure requirements, companies could begin to consider what their disclosure will say if the rules are adopted as proposed. Fortunately, given the increased focus on board oversight of cybersecurity risks in many proxy statements as well as discussions of cybersecurity programs in companies' Environmental, Social and Governance (ESG) reports, issuers have examples already covering many of these topics to look to as they begin developing their disclosures.

2021 Aflac Business & Sustainability Report

Aflac Incorporated

ABOUT AFLAC | FINANCIAL HIGHLIGHTS | ESG HIGHLIGHTS | GOVERNANCE | INVESTMENTS | ENVIRONMENT | SOCIAL | APPENDIX

Protecting Our Customers and Data with Cybersecurity

At Aflac, safeguarding the information collected on behalf of the individuals and businesses we serve is of crucial importance. We are committed to the privacy of individuals and the protection of data, and we do this by placing great importance on information security to protect against threats both external and internal.

Governance

This commitment begins at the top of Aflac. Our Board provides oversight of Aflac's Global Information Security Program (the Program) and has approval rights for our governing policy. Responsibility for the Program is vested in the office of the Global Chief Security Officer (GCSO). The GCSO updates the Board's Audit and Risk Committee quarterly on the state of the Program, compliance with applicable laws and regulations, current and evolving threats, and updates to the Program strategy.

The GCSO is supported by a team of risk management and security professionals whose responsibilities encompass the development, implementation, operation, maintenance, and continuous improvement of the Program. Aflac has a comprehensive set of information and cybersecurity policies and standards structured around the National Institute of Standards and Technology Cybersecurity Frameworks (NIST CSF). Policies are reviewed and approved annually to ensure the organization is up to date with changing cybersecurity and privacy regulations, as well as any changes to technology and industry best practices.

Risk Management

Aflac has a comprehensive risk management program that performs initial evaluations and ongoing monitoring of the information security and privacy risk associated with data usage, the sharing of Aflac information with third parties and the system configuration of critical applications and infrastructure. The team carries out an initial assessment and evaluates mitigating controls to determine a final risk rating. Compliance processes are established to escalate identified risks and to ensure transparency and proper accountability for risk treatments. Reassessment cadence is determined in alignment with the risk rating process.

35 2021 BUSINESS & SUSTAINABILITY REPORT

Aflac Incorporated

ABOUT AFLAC | FINANCIAL HIGHLIGHTS | ESG HIGHLIGHTS | GOVERNANCE | INVESTMENTS | ENVIRONMENT | SOCIAL | APPENDIX

Compliance

Aflac has processes in place to evaluate business practices against security and privacy policies and standards. We have a Cyber Security Assurance Program that regularly tests a comprehensive library of security controls that map to NIST-CSF. Additionally, we complete an annual SSAE 18 SOC 2 (Statements on Standards for Attestation Engagements No. 18 Service Organization Control 2 report) examination with an independent external firm.

Cybersecurity and privacy continue to be an area of evolving focus for legislation and regulatory activity. The Company has a cross-functional team that tracks and monitors new and emerging legislation to ensure privacy and cybersecurity programs are evaluated and comply with regulatory requirements.

Security Operations

While Aflac has traditional systems and controls in place to ensure alignment with regulatory requirements and industry best practices, we constantly work to mature our security posture and keep pace with business change. Our layered defenses, which include the use of identity and access management systems, role based access, multifactor authentication, key and certificate management services, firewalls, as well as cloud, network and end-point security tools are implemented to ensure the protection and availability of information. Regular access reviews are performed, and records are maintained and audited.

Aflac also leverages a host of intrusion detection, prevention and data protection tools to safeguard our most sensitive information and assets. Across the program, continuous monitoring is in place to support our ability to detect and respond to internal and external anomalies. We have mature vulnerability scanning and patch management processes and provide detailed dashboard readouts on remediation activities to business leads on a quarterly basis.

Our team actively participates in multiple threat intelligence sharing consortiums that involve collaboration with our peers in the financial services and insurance industries, as well as local and federal law enforcement. The team also operates as a contributing member in multiple open source intelligence forums and groups to monitor environmental changes of note.

Resiliency and Response

Aflac's business resilience program is based on leading practices and industry standards, primarily ISO22301. The program implements controls and measures to prepare the Organization to manage disruptive events. It is a company-wide program that ensures Aflac employees, customers, shareholders, business partners, information, assets, and business operations are adequately protected in the event of an unplanned business disruption. Resilience is accomplished through an integrated business continuity, disaster recovery, and incident/crisis management structure. In 2021 Aflac completed a successful annual cyber incident response table top exercise which included broad participation from global executives and tested our response to a global cyber event.

Our incident response team is staffed by skilled security and forensics professionals who enact a comprehensive Incident Response Framework. The framework consists of coordinated procedures and tasks that are executed to ensure timely and accurate resolution of security and privacy incidents. Aflac has a formal process to investigate and notify individuals and authorities, as required by law, in the event that personal information has been compromised.

Security Awareness and Training

Aflac's cyber security awareness training program is designed to help employees, contractors and producers recognize information, cybersecurity, and privacy concerns and respond accordingly. Our program provides all personnel with the knowledge and skills to prevent, identify and escalate cybersecurity risks. In 2021 all employees, contractors and producers who had access to Aflac systems or data completed annual security and privacy training. In addition, role-based security training was required for individuals with elevated entitlements.

Aflac's security operations and threat intelligence teams partner closely with our awareness program to send all users monthly phishing exercises that are representative of actual threats we see in our environment. Performance metrics are tracked to provide a real-time view of the risks associated with phishing susceptibility. Additional training is required if users fail an exercise. In 2021, our average performance in phishing exercises far outpaced the performance of our industry peers, with over a 99% pass rate for employees and contractors.

Our security education approach extends beyond training and strives to embed security as a core part of Aflac's culture. We maintain strong executive support and have 130 Cyber Security Ambassadors throughout the organization who help to extend the reach of our awareness messaging. In 2021, we had more than 120 direct communications, portal stories, contest, panels and cyber events. For National Cyber Security Awareness Month, we hosted events attracting participation from over 1,600 individuals.

36 2021 BUSINESS & SUSTAINABILITY REPORT

2022 Aflac Proxy Statement

CORPORATE GOVERNANCE MATTERS 2022 PROXY STATEMENT 29

Spotlight on Information Security Risk Oversight

The Board has adopted an information security policy directing management to establish and operate an information security program with the goal of ensuring that the Company's information assets and data, and the data of its customers, are appropriately protected. The Board has delegated oversight of the Company's information security program to the Audit and Risk Committee. The Company's senior officers, including its Global Security and Chief Information Security Officer, are responsible for the operation of the information security program and communicate quarterly with the Audit and Risk Committee on the program, including with respect to the state of the program, compliance with applicable regulations, current and evolving threats, and recommendations for changes in the information security program. The information security program also includes a cybersecurity incident response plan that is designed to provide a management framework across Company functions for a coordinated assessment and response to potential security incidents. This framework establishes a protocol to report certain incidents to the Global Security and Chief Information Security Officer and other senior officers, with the goal of timely assessing such incidents, determining applicable disclosure requirements and communicating with the Audit and Risk Committee. The incident response plan directs the executive officers to report certain incidents immediately and directly to the Lead Non-Management Director.

For more information, see the Aflac Incorporated Cybersecurity Disclosure at investors.aflac.com under the "Sustainability" tab.

2021 Analog Devices Environmental, Social and Governance Report

Enterprise Information Security

In order to minimize the likelihood and impact of a cybersecurity incident we have deployed cybersecurity protections to protect ADI's networks, devices and data from external & internal threats. These protections are deployed in accordance with global privacy regulations.

ADI's Enterprise Security program has been developed based on industry standards, including those published by International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST). Highlights of the ADI program include:

POLICIES

We have developed a comprehensive set of enterprise security policies and procedures to guide our protection strategy.

PROGRAM ELEMENTS

ADI protects against threats by adopting all five elements of the NIST framework including:

- Identifying critical assets and high-risk threats
- Implementing cybersecurity detection with a 24x7x365 operations center
- Implementing security controls and remediation practices
- Having an Incident Response and Disaster Recovery capability
- Evaluating our partners' cyber posture through the implementation of a Third-Party Risk Management program

Risks identified by our cybersecurity program are analyzed to determine the potential impact on us and the likelihood of occurrence. Such risks are continuously monitored to ensure that the circumstances and severity of such risks have not changed. We evaluate our security program effectiveness by performing internal audits and periodic external audits by an independent information systems expert to determine both the adequacy of, and compliance with, controls and standards. We will continue integrating the Maxim and ADI programs over the upcoming 12-18 months.

GOVERNANCE

ADI's Board of Directors includes four members with cybersecurity expertise to assist the Board in its oversight of the Company's information security program. Senior leadership and Internal Audit regularly provide the Audit Committee with updates on the performance of our cyber program. At least annually, the Chief Information Officer updates the full Board of Directors on information security matters and risk, including cybersecurity.

EXTERNAL INPUTS

ADI regularly conducts threat assessments and benchmarks best practices. Intel sharing is conducted with leading global security providers, the National Defense Information Sharing and Analysis Center as well as industry peers, which help all participating companies improve their cybersecurity programs.

SECURITY AWARENESS & TRAINING

Education is an important part of our overall program. We conduct regular workforce training to instruct our employees to identify cyber concerns and to take the appropriate action. We install and regularly update antivirus software on all company managed systems and workstations to detect and prevent malicious code from impacting our systems.

EXTERNAL CERTIFICATION

Cybersecurity Maturity Model Certification (CMMC) is a unified standard for the implementation of cybersecurity across an enterprise that is designed to help protect sensitive unclassified information. It was developed by the US Department of Defense (DoD) and is expected to apply to the 300,000 companies supplying the DoD. The framework covers 110 controls specified in NIST 800-171. Analog Devices is pursuing its CMMC certification and is awaiting the publication of the final rule in the Federal Register.

2022 Bank of America Proxy Statement

Board oversight of cybersecurity and information security risk

Our Board recognizes the importance of maintaining the trust and confidence of our clients and employees. As a part of its objective, independent oversight of the key risks facing our company, the Board devotes significant time and attention to data and systems protection, including cybersecurity and information security risk.

The Board, which includes members with cybersecurity, technology, and information security experience, oversees management's approach to staffing, policies, processes, and practices to gauge and address cybersecurity and information security risk. Our Board and Enterprise Risk Committee each receive regular presentations and reports throughout the year on cybersecurity and information security risk. These presentations and reports address a broad range of topics, including updates on technology trends, regulatory developments, legal issues, policies and practices, information security resources and organization, the threat environment and vulnerability assessments, and specific and ongoing efforts to prevent, detect, and respond to internal and external incidents and critical threats. At least twice each year, the Board discusses cybersecurity and information security risks with our Chief Technology Officer and our Chief Information Security Officer.

The Board receives prompt and timely information from management on any cybersecurity or information security incident that may pose significant risk to our company and continues to receive regular reports on the incident until its conclusion.

Additionally, our Board receives timely reports from management on key developments and incidents involving large global corporations, as well as specific information about financial services peers and vendors.

Our Enterprise Risk Committee also annually reviews and approves our Global Information Security Program and our Information Security Policy, which establish administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of client information in accordance with the Gramm-Leach-Bliley Act and the interagency guidelines issued thereunder, and applicable laws globally. Our Enterprise Risk Committee's charter makes explicit that the Committee is responsible for reviewing cybersecurity and information security risk and the steps taken by management to understand and mitigate such risk.

Cybersecurity governance highlights

- Comprehensive reporting (including performance metrics which allow for quantitative assessment) to our Board and Enterprise Risk Committees (both scheduled and real-time) in response to key developments.
- Multi-format reporting approach, with presentations to Board as well as memoranda addressing key issues.
- Cross-functional approach to addressing cybersecurity risk, with Global Technology, Risk, Legal, and Corporate Audit functions presenting on key topics.
- Global presence, with employees and 24/7 cyber threat operations centers around the world.
- Collaborative approach, working with a wide range of key stakeholders to manage risk, and share and respond to intelligence.

Under the Board's oversight, management works closely with key stakeholders, including regulators, government agencies, law enforcement, peer institutions, and industry groups, and develops and invests in talent and innovative technology in order to manage cybersecurity and information security risk. Our company has information security employees across the globe, enabling us to monitor and promptly respond to threats and incidents, maintain oversight of third parties, innovate and adopt new technologies, as appropriate, and drive industry efforts to address shared cybersecurity risks. All employees, contractors, and those with access to our company's systems receive education on responsible information security, data security, and cybersecurity practices and how to protect data against cyber threats through our Security Awareness For Everyone program.

Going Forward

With concerns regarding wide-spread adoption of digital technologies and the proliferation of ever-changing cyber-attacks, cybersecurity risks will remain at the top of the list of concerns for companies, their boards of directors and management teams. The proposed rules are only the latest efforts by the SEC to ensure that public companies are providing their investors information on the risks and impacts of cyber events and incidents.[4] Stakeholders will continue to seek more and higher quality disclosures on governance issues related to key risks facing companies with which they invest, as well as those on whom they rely and with which they do business.

As a result, while the final rules are not anticipated in advance of the filing of the 2022 Annual Report on Form 10-K for year-end companies, many companies will continue to include enhanced disclosures related to board oversight of risks, including cybersecurity, in their 2023 proxy statements, as well as strengthen and evolve discussions of their cybersecurity programs in their ESG reporting.

Prior to the finalization of the rules, companies could review their existing policies and programs, or consider formalizing their practices if not already documented, to determine what the current procedures are within the organization and if any changes are desired prior to having to provide detailed public disclosures. Governance practitioners could consider each of the required elements, prepare the related disclosures and confirm with others within the organization that the draft disclosures are consistent with actual practices. Boards and management teams could use the time before adoption of the rules to think about the existing governance structure and composition of the board of directors, what will be required to be discussed if the rules are adopted as proposed, and any needs of the company to optimize their practices.

[4] See Division of Corporation Finance, *CF Disclosure Guidance: Topic No.2 Cybersecurity* (October 13, 2011), and U.S. Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cyber Security Disclosures* (February 26, 2018).

Citations

U.S. Securities and Exchange Commission. (March 9, 2022). *SEC Proposed Rule Release No. 33-11038, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.*

U.S. Securities and Exchange Commission. (March 9, 2022). *Fact Sheet, Public Company Cybersecurity; Proposed Rules.*

Morrison & Foerster. (March 11, 2022). *SEC Proposed Cybersecurity Disclosure Rules for Public Companies.*

Michael A. Kleinman. (March 14, 2022). *SEC Releases New Proposal for Public Company Disclosures of Cybersecurity Incidents, Risk Management, and Governance Policies and Procedures.* Fried, Frank, Harris, Shriver & Jacobson LLP.

Deloitte & Touche LLP. (March 16, 2022). *SEC Proposes New Requirements for Cybersecurity Disclosures.* Heads Up, Volume 29, Issue 1.

William L. Horton, Jr., Joan C. Conley, Carolyn Frantz, and Kevin Richards. (June 23, 2022). *Cybersecurity in the New World.* Presentation to the Society of Corporate Governance Professionals.

www.argyleteam.com

Argyle Company
100 Burma Rd.
Jersey City, NJ 07305
(201) 793 5400

About Argyle

We are a creative communications firm offering end-to-end, in-house execution capabilities.

Our experienced and passionate team is composed of attorneys, designers, project managers, thinkers and web developers. We collaborate together around a process that encompasses drafting, editing, designing and publishing across all digital and print channels.

We are thrilled that communications prepared by Argyle have contributed to trustful relationships between our clients and their readers, whether investors, employees or other stakeholders.

In turn, our commitment to our clients has resulted in meaningful long-term relationships with some of the most respected public and private companies in the world.