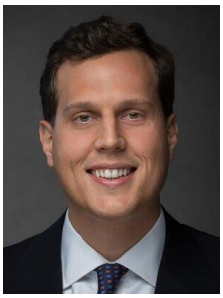
ESG's Silent C: Make Cybersecurity A Governance Priority

By **Frederick Davis, Turquoise Early and Nicholas Alvarez** (October 19, 2023)



Frederick Davis

Turquoise Early

Nicholas Alvarez

An uncontroversial issue lurks quietly beneath the more turbulent environmental, social and corporate governance waters: cybersecurity.

Regulators are actively releasing guidance on security measures and best practices, prescriptions that have broadened beyond institutional resiliency to include proactive monitoring and management of vendors and suppliers.

This trend stems in part from broadly applied international and state consumer privacy laws requiring disclosure of related parties that handle data[1] and permitting individuals to bring lawsuits for unreasonable security.[2] Here we discuss some recent examples.

CPPA Releases Draft Audit and Risk Assessment Regulations

On Sept. 8, under the California Consumer Privacy Act, the California Privacy Protection Agency board discussed and released draft regulations for cybersecurity audits[3] and risk assessments.[4]

Formal rulemaking processes for these proposed regulations will soon begin, and once finalized, regulated businesses processing personal information must perform annual cybersecurity audits and submit risk assessments to the CPPA.

Specifically, the CCPA directs the agency to issue rules requiring businesses "whose processing of consumers' personal information presents significant risk to consumer's privacy or security, to:"

- "Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent."

- "Submit ... on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."[5]

The FTC Amends the GLBA Safeguard Rule

The Federal Trade Commission recently amended[6] the Gramm-Leach-Bliley Act Safeguard Rule[7] to reflect developments in new technologies, and it required nine security updates to company policies and procedures by June 9, 2023:

- Designating a "qualified individual" to oversee the institutions' information security system;
- Ensuring that individual reports regularly to the board of directors regarding the state of the institutions' information security programs;
- Conducting risk assessments of their information security programs;
- Implementing additional administrative, technical and physical safeguards to address risks;
- Regularly testing security controls and safeguards;
- Ensuring personnel is adequately trained on security policies and procedures;
- Assessing and overseeing third-party service providers to ensure they are following the proper standards in their security programs;
- Establishing written incident response plans; and
- Keeping the procedures current.[8]

SEC Rules for Public Companies and Investment Entities

On July 26, the U.S. Securities and Exchange Commission adopted final rules for public companies implementing new disclosure obligations about cybersecurity incidents and risk oversight processes.[9]

Among other things, the rules create a new triggering event on Form 8-K, requiring disclosure of material cybersecurity incidents within four business days of a determination that such incident is material, subject to narrow exceptions. Public companies — other than smaller reporting companies — will be required to comply with the new 8-K disclosure obligations starting on Dec. 18.

In addition, the SEC implemented new annual disclosure obligations regarding cybersecurity processes and oversight, including disclosures regarding: (1) company processes for assessing, identifying and managing risks from cybersecurity threats[10]; (2) any risks of cybersecurity threats that have materially affected or are reasonably likely to materially affect the company; (3) the board of directors' oversight of cybersecurity risks and any board committee or subcommittee responsible for such oversight; and (4) management's role in assessing and managing material risks from cybersecurity threats, including a description of management positions and/or committees responsible for oversight and their relevant expertise.

For domestic public companies, these new disclosure obligations will apply to their annual reports on Form 10-K covering fiscal years ending on or after Dec. 15.[11]

Also of note, the SEC has proposed rules for investment advisers and funds,[12] amending Rule 10[13] and Form SCIR,[14] that would require periodic risk assessments; minimization of user-related risks; protection of information from third-party service providers; cybersecurity threat and vulnerability management; and measures to respond and recover from cybersecurity incidents.

And under proposed enhancements to Regulation S-P,[15] broker-dealers, investment companies and similar entities would face similar policy and breach incident reporting requirements.[16]

Financial Institution Guidance on Third-Party Relationships

Numerous regulators have released guidance on third-party relationships.

The Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation[17] and the Board of Governors of the Federal Reserve System finalized their "Interagency Guidance on Third-Party Relationships: Risk Management" in early June to recommend best practices for relationships with third-party service providers.[18]

The agencies framed the guidance in terms of the "third-party relationship life cycle," which includes planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination.

Similarly, the Federal Financial Institutions Examination Council published an "IT Examination Handbook Infobase" to provide guidance on tackling major issues,[19] including information security[20] and outsourcing technology services.[21]

These booklets provide guidance to identify, measure, mitigate and monitor information

security risks, especially when it comes to unauthorized third parties. Finally, the Consumer Financial Protection Bureau has issued bulletins guiding financial institutions to oversee their third-party relationships to ensure compliance with federal consumer finance laws.[22]

Bank and Credit Union Incident Notification

Regulators are also shortening breach notification requirements.

The OCC, FDIC and Federal Reserve Board released the Computer Security Incident Notification Rule[23] to incentivize banks and bank service providers to timely notify regulators of "notification incidents," material "computer security incidents" likely to materially disrupt or degrade a bank's (1) ability to carry out operations, activities or processes or deliver products or services to a material portion of its customer base; (2) business lines resulting in material loss of revenue, profit or franchise value; or (3) critical operations, discontinuance of which would pose a threat to the country's financial stability.[24]

A bank must notify its regulator within 36 hours after discovering that a notification incident has occurred, and a bank service provider must notify its consumers as soon as possible after an incident causes material service disruption of four or more hours.[25]

The National Credit Union Administration released a final rule effective Sept. 1, requiring federally insured credit unions to report cyber incidents no later than 72 hours[26] after the credit union "reasonably believes" that it has experienced a reportable cyber incident.[27]

Takeaways

Whether mandated or not, these standards affect all businesses.

Regulated companies must achieve reasonable compliance. But any company that does not implement some cybersecurity initiatives — including active vendor and supplier management — will be left defending decisions to ignore evolving standards supported by lower-cost solutions.[28]

And for those businesses planning to acquire or sell, cybersecurity affects deal value and time to close, and good governance generally signals sophistication and trust. [29]

So, in this and coming years, don't forget the C in ESG and make cybersecurity a corporate governance priority. Here are some practical first steps:

- Take one bite at a time. The core functions of any governance program include clear policies and procedures, as well as education, board oversight, effective audits, and stakeholder and community trust. Get started in that order and set realistic timelines and attainable goals.

- Commit resources. Consider hiring additional project management or administrative support to help tackle your timelines and goals.

- Do not have a 0-1 mindset. Governance should fit your company but leverage available resources and expertise on best practices.

- Sell governance return on investment. Investments in governance, especially risk management, breed resiliency and long-term success and affect the bottom line. Security program oversight enables companies to educate business partners, provide merger and acquisition deal insight, defend against breach lawsuits, and even correct or advocate accurate risk quantification to potential cyber carriers.

- Increase engagement through education and board-friendly reports. While regulators have retreated from explicitly requiring cybersecurity expertise on the board,[30] utilize partners who can educate and effectively communicate with the board.

- Don't forget that many data incidents trace back to weakest-link vendors and suppliers. Any governance program that does not consider third parties has a critical flaw and may not meet your industry's current standard of care.

- Include scalable third-party validation. While white-glove security audits and certifications like SOC2 and HITRUST are becoming the standard for larger enterprises, consider also new players to the security space that provide practical security risk assessment and governance through automation and AI at commensurately scaled rates.

- Consider the customer's perspective. What security functions would your customer consider most important? Prioritize the protection of third-party data and the systems and controls designed to protect that data.

- Think like a litigator. Through the lens of a simple negligence standard — standard of care and breach — what actions can you take now that will preempt allegations of security negligence? What are your peer companies doing? Call them and ask. Do they have any recommended security vendors? How about larger companies?

- Learn from incidents. While incident notification is the rule, don't forget to learn from mistakes and implement strategies to avoid them in the future. Companies must address and triage incidents when they occur, but the best programs follow through

on improving programs after security incidents exposing current vulnerabilities. Failure to do so could be evidence of negligence.

Frederick Davis is a partner, Turquoise Early is an associate and Nicholas Alvarez is a partner at Kutak Rock LLP.

Washington University law student Lauren Campbell contributed to this article.

[1] See, e.g., GDPR art. 28 (requiring sub-processor disclosure).

[2] See, e.g., Cal. Civ. Code § 1798.150(a)(1).

[3] https://cppa.ca.gov/meetings/materials/20230908item8.pdf.

[4] https://cppa.ca.gov/meetings/materials/20230908item8part2.pdf.

[5] Cal. Civ. Code § 1798.185(a)(15) (stating also that "[n]othing in this section shall require a business to divulge trade secrets.").

[6] 86 Fed. Reg. 70272 (January 1, 2022) (codified at 16 C.F.R. pt. 314). Other GLBA enforcement agencies are also balancing between consumer access and data security. The Consumer Financial Protection Bureau ("CFPB") recently proposed a rule under Dodd-Frank section 1033 that would require financial service companies to provide consumers and authorized third parties with greater access and control over data. At this point, the CFPB is not going beyond the security requirements found in the GLBA Safeguard Rules, except for authenticating the authorized third party before disclosing customer information. While these proposed rules are still a couple of years from potentially going into practice, it is clear that financial regulators are thinking about the privacy and security implications of their information practices, especially when it comes to third-party involvement. See "Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights, CFPB (October 27, 2022), available at https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf (last visited June 29, 2023).

[7] The Safeguard Rule applies to companies that offer financial products or services and sets forth standards for protecting consumer's financial information. See 15 U.S.C. §6801; 16 C.F.R. § 312.3.

[8] Large financial institutions (greater than 5,000 customers) must also document their efforts to reach compliance. Smaller financial institutions do not have to document their efforts and are also exempted from certain provisions of the updated rules.) For a more detailed look into this rule, see this recent client alert: https://www.kutakrock.com/newspublications/publications/2023/july/ftc-final-rule-amending-standards.

[9] See 88 Fed. Reg. 51896 (codified at 17 CFR pts. 229, 232, 239, 240, and 249). The SEC amended Regulation S-K Items 106 and 601, Regulation S-T Rule 405, and the Securities and Exchange Acts Rules 13a-11, 15d-11, Forms 20-F, 6-K, 8-K, 10-K, and S-3.

[10] Of course, under the Sarbanes Oxley Act, public companies are already required to maintain adequate internal controls, which include systems for overseeing cybersecurity risks and protecting sensitive information. 15 U.S.C. §7241 ("Section 302"); 15 U.S.C. §7262 ("Section 404").

[11] The SEC published a helpful small entity compliance guide, here: https://www.sec.gov/corpfin/secg-cybersecurity.

[12] 88 Fed. Reg. 20212 (April 5, 2023) (to be codified at 17 C.F.R. pts. 232, 240, 242, 249).

[13] 17 C.F.R. § 242.10 (amending Rule 10).

[14] 17 CFR § 249.642 (amending Form SCIR to notify the SEC of "significant cybersecurity incidents" and providing for later updates on these incidents).

[15] 88 Fed. Reg. 20616 (April 6, 2023) (to be codified at 17 C.F.R. pts. 240, 248, 270, 275).

[16] The SEC's proposed enhancements change the previous regulation in four major ways: covered institutions must: (1) adopt an incident response under the Safeguard Rule; (2) notify affected individuals when it is reasonably likely that an unauthorized actor accessed their sensitive customer information; (3) maintain written records documenting compliance with cybersecurity compliance, and (4) the expansion of "customer information" to include records containing "nonpublic personal information" received from customers and from third-party financial institutions.

[17] The FDIC also publishes institutional letters to guide members through tough issues. For example, FIL 19-2019, FIL-13-2014, and FIL-44-2008 all provide guidance for navigating third party risk management. See "Regulatory Guidance: Risk Management Supervision," FDIC, available at https://www.fdic.gov/regulations/resources/director/risk.html.

[18] 88 Fed. Reg. 37920 (June 9, 2023); "Interagency Guidance on Third-Party Relationships: Risk Management," FDIC (June 2023), available at https://www.fdic.gov/news/financial-institution-letters/2023/fil23029a.pdf.

[19] "IT Examination Handbook Infobase," FFIEC, available at https://ithandbook.ffiec.gov/ (last visited June 29, 2023).

[20] "Information Security," in FFIEC Information Technology Handbook, FFEIC (September 2016), available at https://ithandbook.ffiec.gov/it-booklets/information-security/.

[21] "Outsourcing Technology Services" in FFIEC Information Technology Handbook, FFEIC (June 2004), available at https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/.

[22] "Compliance Bulletin and Policy Guidance; 2016-02, Service Providers" Consumer Finance Protection Bureau (February 2016), available

at https://files.consumerfinance.gov/f/documents/102016_cfpb_OfficialGuidanceService ProviderBulletin.pdf.

[23] 86 Fed. Reg. 66424 (November 23, 2021) (codified at 12 CFR pts. 53, 225, and 304).

[24] CSIs are "occurrence[s] that result in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits." All three agencies have versions of this: for the OCC see 12 C.F.R. § 53.2(4)); for the FDIC see 12 C.F.R. § 304.22(4)); for the Federal Reserve Board see 12 C.F.R. § 225.301(b)(4)).

[25] With the short 36-hour period, the agencies sought to ease administrative burden in four ways: updating key language to narrow the focus on incidents that do or likely will materially impact customers; providing examples of incidents that would trigger notification, such as widespread system outages, hacking incidents, malware, and ransomware; not requiring particular content or format; and allowing the notifier to amend and update its initial notification.

[26] The NCUA chose to align its rule with the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022, which will also require disclosure of cyber incidents within 72 hours once that rule making process is completed by 2025. Pub. L. No. 117-103 (March 15, 2022), available at https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[27]88 Fed. Reg. 12811 (March 1, 2023) (codified at 12 C.F.R. pt. 748). The rule was first proposed in July 2022. 87 Fed. Reg. 45029 (July 27, 2022). Reportable incidents include those that disrupt operations, lead (or could lead to) to unauthorized access to sensitive data or disrupt members' access to accounts or services. The rule specifically requires credit unions to report to the NCUA when a third-party with whom the credit union has a relationship identifies an incident. The required reporting is an early alert and credit unions are not required to provide a detailed incident assessment.

[28] See, e.g., Wilson, et al. v. J.B. Hunt Transport, Inc., No. 5:21-CV-5194, 2022 WL 20273042, at *1 (W.D. Ark. Oct. 6, 2022).

[29] Chirantan Chatterjee and D. Daniel Sokol, "Don't Acquire a Company Until You Evaluate Its Data Security," Harvard Business Review (April 16, 2019) https://hbr.org/2019/04/dont-acquire-a-company-until-you-evaluate-its-data-security; Shilpi Gupta & Stuart D. Levi, "The Emerging Need for Cybersecurity Diligence in M&A," Harvard Law School Forum on Corporate Governance (May 2, 2017) https://corpgov.law.harvard.edu/2017/05/02/the-emerging-need-for-cybersecurity-diligence-in-ma/.

[30] See 87 Fed. Reg. 16590 (March 9, 2022).