AN A.S. PRATT PUBLICATION
FEBRUARY 2026
VOL. 12 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: A STRATEGIC GUIDE
Victoria Prussen Spears

NAVIGATING MINORS' PRIVACY AND ONLINE SAFETY LAWS: A STRATEGIC GUIDE FOR BUSINESSES
Maki DePalo and Hyun Jai Oh

CYBERSECURITY RESOURCES FOR BOARDS IN THE UNITED STATES, UNITED KINGDOM, AND EUROPEAN UNION
Kelly Hagedorn, Cara M. Peterman, Alice Portnoy, Sierra Shear, Hanna Hewitt and John Evan Laughter

COMMUNICATING WITH THE SECURITIES AND EXCHANGE COMMISSION WHEN YOUR ORGANIZATION SUFFERS A CYBERSECURITY INCIDENT
Haimavathi V. Marlier, Michael D. Birnbaum and Miriam H. Wugmeister

THE BENEFITS AND RISKS OF NOTIFYING LAW ENFORCEMENT
Miriam H. Wugmeister, David A. Newman and Robert S. Litt

CALIFORNIA EXPANDS THE IMPACT OF THE CALIFORNIA CONSUMER PRIVACY ACT WITH SWEEPING NEW RULES ON CYBERSECURITY AUDITS, AUTOMATED DECISIONMAKING TECHNOLOGIES, AND PRIVACY RISK ASSESSMENTS
Katherine Doty Hanniford, David C. Keating, Kimberly Kiefer Peretti, Lance Taubin and Santiago "Santi" Villar

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 2** **February 2026**

Editor's Note: A Strategic Guide 29
Victoria Prussen Spears

Navigating Minors' Privacy and Online Safety Laws: A Strategic Guide for Businesses 31
Maki DePalo and Hyun Jai Oh

Cybersecurity Resources for Boards in the United States, United Kingdom, and European Union 38
Kelly Hagedorn, Cara M. Peterman, Alice Portnoy, Sierra Shear, Hanna Hewitt and John Evan Laughter

Communicating with the Securities and Exchange Commission When Your Organization Suffers a Cybersecurity Incident 50
Haimavathi V. Marlier, Michael D. Birnbaum and Miriam H. Wugmeister

The Benefits and Risks of Notifying Law Enforcement 54
Miriam H. Wugmeister, David A. Newman and Robert S. Litt

California Expands the Impact of the California Consumer Privacy Act With Sweeping New Rules on Cybersecurity Audits, Automated Decisionmaking Technologies, and Privacy Risk Assessments 58
Katherine Doty Hanniford, David C. Keating, Kimberly Kiefer Peretti, Lance Taubin and Santiago "Santi" Villar

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Cybersecurity Resources for Boards in the United States, United Kingdom, and European Union

By Kelly Hagedorn, Cara M. Peterman, Alice Portnoy, Sierra Shear, Hanna Hewitt and John Evan Laughter*

In this article, the authors explain that boards in the United States, United Kingdom, and European Union face increasing pressure to oversee cybersecurity risks amid evolving regulatory expectations. The authors highlight key resources, frameworks, and reporting obligations shaping board-level cybersecurity governance across jurisdictions.

Boards across the United States, United Kingdom, and European Union are under growing pressure to demonstrate effective oversight of cybersecurity risks. As incidents become more frequent and impactful, boards must not only understand their responsibilities but also stay informed about evolving legal obligations, best practices, and governance expectations.

Last year, the French national cybersecurity regulator (ANSSI) hosted a first-of-its-kind tabletop exercise involving over 5,000 professionals from 1,000 public and private organisations. The event underscored the critical need for companies and their leadership teams to embed robust crisis-management strategies to prepare for and respond to cybersecurity incidents.

Cybersecurity resources, frameworks, and regulatory developments are increasingly relevant to boards that oversee operations in the U.S., UK, and EU. Practical guidance, legal requirements, and emerging trends continue to shape how boards should approach cyber-risk management, incident response, and disclosure obligations. By synthesising materials from government agencies, industry bodies, and legal experts, this resource aims to support directors in better fulfilling their fiduciary duties and enhancing organisational resilience in the face of cyber threats.

---

* The authors, attorneys with Alston & Bird LLP, may be contacted at kelly.hagedorn@alston.com, cara.peterman@alston.com, alice.portnoy@alston.com, sierra.shear@alston.com, hanna.hewitt@alston.com and johnevan.laughter@alston.com, respectively.

GENERAL GUIDANCE FOR BOARDS

Cybersecurity oversight has become a core boardroom issue in the U.S., UK, and EU, driven by regulatory developments and heightened expectations around risk governance. Several board-level professional associations have published guidance for directors on implementing and overseeing their organisations' cybersecurity programs. In the UK, government bodies and regulators have issued resources to help boards navigate their cybersecurity responsibilities, while across the EU, national cybersecurity agencies have developed targeted resources to support board-level engagement with cyber risk. Collectively, these resources reflect a growing recognition that cybersecurity is not merely a technical issue but a core component of corporate governance and organisational resilience.

United States	The National Association of Corporate Directors' (NACD) Handbook on Cyber-Risk Oversight[1] sets out key principles for board engagement, emphasising the need for directors to understand and manage cyber risks as part of their fiduciary duties. The NACD's 2025 Public Company Survey[2] analyses the priorities of over 200 boards of directors and identifies emerging trends in AI and cybersecurity oversight. The Cybersecurity Law Report,[3] in an article authored by our team, outlines five actionable steps boards can take to prepare for and respond to cyber incidents.
United Kingdom	The Cyber Security Code of Practice[4] outlines governance principles tailored to board-level oversight, while the National Cyber Security Centre (NCSC) Board

[1] https://www.nacdonline.org/globalassets/public-pdfs/nacd_cyber-risk-oversight-handbook_pages_web-compressed.pdf.

[2] https://www.nacdonline.org/all-governance/governance-resources/governance-surveys/surveys-benchmarking/2025-public-company-board-practices--oversight-survey/.

[3] https://www.cslawreport.com/21030571/five-steps-for-effective-board-oversight-on-cybersecurity-breach-response.thtml.

[4] https://www.gov.uk/government/publications/cyber-governance-code-of-practice/cyber-governance-code-of-practice.

	Toolkit offers practical tools and key questions to guide boardroom discussions. Sector-specific guidance is also available: • Financial institutions: The FCA's SYSC Handbook[5] outlines expectations for senior management systems and controls. Although published in 2019, the FCA's Industry Insights[6] also offers relevant observations on systems and controls that financial institutions may consider implementing. • Auditors and actuaries: The UK Corporate Governance Code[7] emphasises accountability and risk management. These materials reflect a broader regulatory trend towards embedding cyber resilience into corporate governance frameworks.
European Union	In France, the SME cybersecurity memorandum[8] published by the French Confédération des Petites et Moyennes Entreprises, along with the accompanying executive guidance,[9] provides tailored advice for directors and senior managers, emphasising the strategic importance of cybersecurity. In addition, cloud service providers, under the "SecNumCloud" framework[10] (established by the national

[5] https://handbook.fca.org.uk/handbook/SYSC.pdf.

[6] https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf.

[7] https://media.frc.org.uk/documents/UK_Corporate_Governance_Code_2024_a2hmQmY.pdf.

[8] https://www.cybermalveillance.gouv.fr/medias/2024/09/20240926Memento_ImpactCYBER_SCREEN.pdf.

[9] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/gestion-cybersecurite-dirigeants.

[10] https://cyber.gouv.fr/enjeux-technologiques/cloud/.

	cybersecurity regulator, ANSSI), can certify the resilience of their solutions against cyberattacks. The framework establishes broad organisational requirements, including personnel standards that must be addressed by the management body. Germany's Cyber Risk Management Handbook[11] and Cyber-Risk Oversight Toolkit[12] offer a comprehensive framework for executive-level risk oversight, emphasising principle-based compliance that aligns with the NACD Handbook on Cyber-Risk Oversight. Italy's National Cybersecurity Agency has issued both executive-level guidance[13] and a governance fundamentals guide[14] to help boards integrate cybersecurity into corporate strategy.

SECURITY CONTROLS

In the wake of high-profile data breaches over the last decade, organisations are not only encouraged but often required to maintain safeguards that protect internal, proprietary, and customer data. They must implement technical defences against cyberattacks and educate employees on cybersecurity best practices. Accordingly, all organisations should adopt certain policies to prevent cyber incidents, as well as industry-specific measures to protect highly sensitive consumer records and information. Government entities in the U.S., UK, and EU have published control frameworks that organisations can use to minimise vulnerabilities, safeguard confidential information, and protect customers, corporate integrity, and business.

United States	The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has developed a comprehensive catalogue of controls,

[11] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/NACD/managing_cyber_risk_en.pdf?__blob=publicationFile&v=4.

[12] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/NACD/toolkit_managing_cyber_risk_en.pdf?__blob=publicationFile&v=2.

[13] https://www.acn.gov.it/portale/cybersicurezza-pmi#dirigenti.

[14] https://www.acn.gov.it/portale/w/cybersecurity-governance-fundamentals-definizione.

	Security and Privacy Controls for Information Systems and Organizations,[15] for entities to consider when developing corporate policies and procedures. NIST has also established its Cybersecurity Framework[16] as a hub of resources for cybersecurity practices more broadly. The Center for Internet Security, a nonprofit organisation focusing on controls and benchmarks, has developed its 18 CIS Critical Security Controls as pillars of enterprise information security.
United Kingdom	In the UK, the Information Commissioner's Office has developed a range of resources and guidance[17] regarding situation-specific cybersecurity measures and broader best practices. Similarly, the National Cyber Security Centre (NCSC) has published its Cyber Assessment Framework[18] (available as a PDF on the NCSC website)[19] to help organisations assess and improve their cybersecurity and resilience. In addition, the NCSC's 10 Steps to Cybersecurity[20] offers guidance for medium to large organisations to strengthen their information management protocols.

[15] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[16] https://www.nist.gov/cyberframework.
[17] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/.
[18] https://www.ncsc.gov.uk/collection/cyber-assessment-framework.
[19] https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf.
[20] https://www.ncsc.gov.uk/collection/10-steps.

European Union	For financial institutions, the FCA Handbook Chapter 5.1[21] provides industry-specific guidance regarding data security. In the EU, the European Union Agency for Cybersecurity provides a repository[22] of best practices and controls for the EU Cyber Security Incident Response Teams network to help manage the responsible reporting, coordination, and remediation of cybersecurity vulnerabilities. Country-specific resources are also available: • The French Cybersecurity Agency has published guidance[23] on preventing and responding to ransomware attacks. • The Belgian Federal Service for Economy has published a comprehensive guide[24] on cybersecurity protocols for corporations.

CYBER REPORTING AND DISCLOSURE OBLIGATIONS

Cybersecurity reporting obligations are a regulatory priority across the U.S., UK, and EU, with increasing regulatory expectations for transparency, resilience, and board-level accountability. Reporting requirements are increasingly stringent, often requiring rapid notification of significant cyber events to national authorities, sector regulators, and, in some cases, affected stakeholders. Sector-specific and product-level responsibilities are also expanding, particularly in financial services and digital product manufacturing, where organisations must report vulnerabilities and operational disruptions. Boards should remain informed about these evolving disclosure and reporting requirements and proactively ensure that their organisations are prepared to respond to developing reporting and disclosure obligations.

[21] https://handbook.fca.org.uk/handbook/fcg5.

[22] https://github.com/enisaeu/CNW?tab=readme-ov-file#csirts-network---security-guidance.

[23] https://messervices.cyber.gouv.fr/guides/attaques-par-rancongiciels-tous-concernes.

[24] https://economie.fgov.be/sites/default/files/Files/Publications/files/Manuel-Cybersecurite-votre-entreprise-est-elle-prete.pdf.

United States	The SEC's rule on Risk Management, Strategy, Governance and Incident Disclosure, which became effective in 2023, governs public disclosures related to material cyberwsecurity risks, material cybersecurity incidents, and cyber-risk governance. The National Association of Corporate Directors has produced guidance as to how directors can align oversight practices with the SEC's expectations.[25] They have also published a piece exploring how organisations can combine the use of regulatory guidance with AI-driven analysis[26] to help comply with the SEC's disclosure requirements. Our team provides a summary of the SEC's rule[27] and describes how companies should consider updating and revising their protocols in light of the rule.
United Kingdom	The ICO provides detailed guidance on how and when to report incidents,[28] including under the Network and Information Systems (NIS) Regulations.[29] Other UK regulators have also published guidance: • The UK's energy regulator, Ofgem, has published guidance for downstream gas and electricity operators of essential services,[30] as has

[25] https://www.nacdonline.org/all-governance/governance-resources/directorship-magazine/winter-2024-issue/is-the-board-ready-for-the-secs-new-cyber-disclosure-rules/.

[26] https://www.nacdonline.org/all-governance/governance-resources/directorship-magazine/online-exclusives/2024/september-2024/the-goldilocks-approach-to-sec-cybersecurity-disclosures-combine-regulatory-guidance-with-ai-analysis-to-get-it-just-right/.

[27] https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

[28] https://ico.org.uk/media2/migrated/2614816/responding-to-a-cybersecurity-incident.pdf.

[29] https://ico.org.uk/for-organisations/the-guide-to-nis/.

[30] https://www.ofgem.gov.uk/sites/default/files/2022-04/NIS%20Guidance%20for%20 Downstream%20Gas%20and%20Electricity%20Operators%20of%20Essential%20Services%20 in%20GB%20v2.0.pdf.

	the Department for Energy Security & Net Zero (available on the department's website).[31] Ofgem's website[32] also includes reporting templates and resources on applying appropriate security measures using the NCSC's Cyber Assessment Framework. • The UK's communications regulator, Ofcom, has published guidance for companies operating in the digital infrastructure sector,[33] including information on security and incident-reporting duties and how operators of essential services are defined. Financial institutions face additional obligations, including promptly notifying the Financial Conduct Authority (FCA) of significant cyber events (see Chapter 15 of the FCA Handbook).[34]
European Union	The EU continues to advance its cybersecurity framework, including incident-reporting obligations, through several legislative measures: • The NIS2 Directive[35] expands the scope and enforcement of cybersecurity obligations across EU Member States and requires certain "essential"

[31] https://assets.publishing.service.gov.uk/media/6530f145927459000df959e3/implementation-of-the-network-and-information-systems-regulations-guidance.pdf.

[32] https://www.ofgem.gov.uk/guidance/nis-directive-and-nis-regulations-2018-ofgem-guidance-operators-essential-services.

[33] https://www.ofcom.org.uk/siteassets/resources/documents/phones-telecoms-and-internet/information-for-industry/network-and-information-systems-regulations/ofcom-guidance-for-oes-in-the-digital-infrastructure-sector.pdf?LinkSource=PassleApp&v=323207.

[34] https://handbook.fca.org.uk/handbook/SUP/15/14.pdf.

[35] https://www.nis-2-directive.com/.

	and "important" entities working in critical sectors to report cybersecurity incidents. As a directive, NIS2 must be transposed into local law by each Member State. Implementation remains fractured, so organisations should continue to monitor local developments. • The Digital Operational Resilience Act (DORA)[36] targets the financial sector and requires financial entities to report major ICT-related cybersecurity incidents. • The Cyber Resilience Act (CRA)[37] targets organisations that manufacture or place products with digital elements (PDEs) on the EU market. Such organisations are required to report actively exploited vulnerabilities and cybersecurity incidents.

CYBER TRENDS

Most jurisdictions track the evolving cyber threat landscape through a combination of regulator data and industry research. In the U.S. and EU, these trends are centralised in databases. In the UK, annual surveys and regulator trends are published to help organisations understand and better protect against cyber risks. Whilst particularly useful for security and IT personnel, these resources also enable boards to gain a clear understanding of the cyber threat landscape and associated cyber risks.

[36] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
[37] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

United States	The CISA Known Exploited Vulnerabilities Catalog[38] is an authoritative, regularly updated list of security vulnerabilities that have been actively exploited in the wild, designed to help organisations prioritise remediation efforts and strengthen their cybersecurity posture. The Government Accountability Office has released a report[39] detailing the types of incidents that the government encounters and the need to address those vulnerabilities.
United Kingdom	The ICO's Data Security Incident Trends[40] provide insight into the types and frequency of reported breaches, helping boards understand sector-specific risks. The NCSC's Annual Cyber Security Breaches Survey[41] offers a broader view of how UK organisations are managing cyber threats, including board-level engagement and investment trends.
European Union	The European Vulnerability Database (EUVD)[42] provides a real-time view of known vulnerabilities affecting European systems, offering boards a technical perspective on emerging risks. The 2024 ENISA Report on the State of Cybersecurity in the Union[43] presents a comprehensive overview of threat trends, regulatory developments, and strategic priorities across member states – an essential resource for boards operating in or across the EU.

[38] https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[39] https://www.gao.gov/products/gao-24-107231.
[40] https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-security-incident-trends/.
[41] https://www.ncsc.gov.uk/cyber-governance-for-boards/training.
[42] https://euvd.enisa.europa.eu/.

	The 2025 ENISA Threat Landscape Report[44] analyses 4,875 cybersecurity incidents recorded between July 2024 and June 2025, highlighting the most significant threats and trends currently impacting the EU.

BOARD LIABILITY

As attempted cyberattacks and data breaches become a routine expectation rather than an anomaly in the corporate environment, boards may be exposed to potential liability arising from their actions before and after a cybersecurity incident. Board liability varies across the U.S., UK, and EU.

In the UK, for example, directors owe general duties to an organisation under the Companies Act which would apply when managing a cybersecurity incident. Directors must act in good faith, promote the success of an organisation, exercise independent judgment, and avoid conflicts of interest.

In the U.S., directors are bound by their fiduciary duties to act in the best interests of an organisation, place the interests of the organisation above their own, ensure the organisation has systems in place to monitor potential risks, and respond appropriately to any red flags indicating significant cyber risks. Accordingly, boards should be aware of their obligations to institute management training for cybersecurity incidents, oversee the execution of response protocols, and report on outcomes. Equally important, boards should recognise when failure to do so may result in director liability.

United States	Our team reviews U.S. law to provide a synopsis[45] of how boards can fulfil their role after a cyber breach. We also provide practical recommendations[46] for boards responding to a cyber incident.
United Kingdom	In the UK, Sections 172 and 174 of the Companies Act[47] govern boards' duties, which apply to cyber risk and oversight.

[44] https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf.

[45] https://www.alston.com/en/insights/publications/2024/04/board-oversight-and-cyber-breach-response.

[46] https://www.alston.com/en/insights/publications/2024/04/tips-for-balanced-board-oversight.

[47] https://www.legislation.gov.uk/ukpga/2006/46/contents.

European Union	In the EU, the European Voice of Directors Association has published its Guide to Directors' Duties and Liabilities,[48] which offers a helpful overview of the scope of board obligations. Belgium has also published useful guidance in this area: • The Federation of Belgian Companies has published an article[49] summarising specific duties that arise in the cybersecurity context. • The Centre for Cybersecurity Belgium has released a directive[50] for management and leadership on their duties and responsibilities.

CONCLUSION

The importance of cybersecurity oversight for boards in the U.S., UK, and EU continues to grow. As cyber threats evolve and regulations tighten, boards must remain informed and be proactive in managing cyber risks. Leveraging resources from government agencies, industry bodies, and legal experts can enhance both the understanding and execution of cybersecurity responsibilities. Doing so helps ensure compliance and strengthens organisational resilience, making effective cybersecurity governance an essential component of corporate strategy and risk management in today's digital environment.

[48] https://eimf.eu/wp-content/uploads/2015/10/ecoDa_Directors-Duties-Final.pdf.

[49] https://www.vbo-feb.be/fr/nouvelles/cybersecurite-quelle-responsabilite-pour-les-dirigeants-dentreprise/#:~:text=La%20directive%20NIS2%20visant%20%C3%A0,de%20cybers%C3%A9curit%C3%A9%20dans%20les%20entreprises.

[50] https://atwork.safeonweb.be/sites/default/files/2024-10/NIS2%20Brochure%20FR.pdf.