Skadden

The Informed Board

Winter 2024

The oversight obligations of boards continue to expand. Recent enforcement actions and new laws in areas such as cybersecurity, artificial intelligence and supply chains create new challenges, as we explain in this issue of *The Informed Board*. In another article, we outline potential pitfalls for companies that want to lend financial support to political conventions, transitions or inaugural events in this election year.

We also track the explosion of shareholder activism in Europe, including a wave in Germany.

In our podcast, our panelists discuss best practices for succession planning, and why it should be an annual affair.

Emerging Expectations: The Board's Role in Oversight of Cybersecurity Risks

- New SEC rules from 2023 require public companies to report material cybersecurity incidents promptly and detail their cybersecurity risk management strategies in annual reports — requirements that increase the risk of litigation over misstatements relating to cybersecurity.
- The fallout from the SEC's enforcement action against SolarWinds and shareholder litigation over the company's alleged failure to manage cybersecurity risks highlight the need for thoughtful board governance in this area.
- Boards should review how oversight responsibility for cybersecurity risk is assigned and coordinated within the board and with management to facilitate clear lines of communication in the event of a cybersecurity incident.

What role are boards expected to play in protecting their companies against cyberattacks?

New rules issued by the Securities and Exchange Commission (SEC) and an enforcement action by the agency against SolarWinds, a software developer that was the victim of a serious cyberattack, provide detailed guidelines. They make clear that directors need to understand the risks and actively engage in cybersecurity oversight. The SEC's actions are also likely to shape the expectations of shareholders, customers and other stakeholders.

New SEC Cyber Disclosure Rules in a Nutshell

Overview

The SEC adopted final rules in 2023, which are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incident reporting by public companies. Specifically, the amended rules require:

- Prompt public reporting of material cybersecurity incidents on Form 8-K.
- Disclosures in annual reports about the company's processes for identifying, assessing and managing the risks of cybersecurity threats, management's role in assessing and managing those risks, and the board's oversight of cybersecurity risks.

For companies with public floats of more than $250 million, the Form 8-K incident disclosure obligations took effect on December 18, 2023. For those companies, the cybersecurity risk management, strategy and governance disclosures must be included in annual reports for fiscal years ending on or after December 15, 2023 — and thus, for many companies, in annual reports issued in early 2024.

Key Considerations for Boards of Directors

Incident reporting. Under the new rules, a company must disclose a "cybersecurity incident" experienced by the company within four business days of determining that the incident is material.

This requirement has led many companies to evaluate whether their current incident response and disclosure procedures are designed to help ensure compliance with the rules. Management teams and boards are asking whether their company's procedures are integrated and designed to facilitate streamlined communication between cybersecurity business functions, management and the board in the event of a cybersecurity incident and any steps the board or a committee would need to take in its oversight role.

Cybersecurity governance. Annual reports must now disclose information on the board's oversight of cybersecurity risk management. In particular, companies must describe:

- The board's oversight of risks from cybersecurity threats and, if applicable, any board committee or subcommittee responsible for that oversight.
- How the board or board committee is informed about such risks.

Accordingly, boards should review how oversight responsibility is assigned within the board and make sure that board and committee discussions regarding cybersecurity risks are documented. Those discussions should include regular briefings and updates from management.

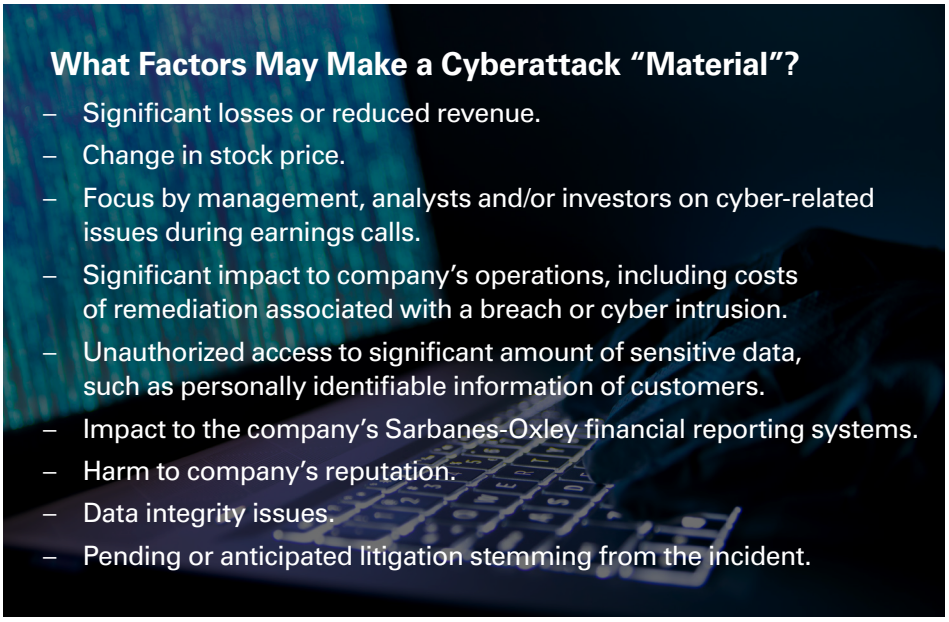
The detailed disclosure requirements under the new rules will necessitate robust oversight by boards.

SEC Cyber Litigation and Enforcement: SolarWinds

Companies with inadequate board oversight of cybersecurity practices may face serious consequences.

On October 30, 2023, the SEC filed a complaint against SolarWinds, a software development company, and Timothy Brown, its chief information security officer (CISO), alleging that both SolarWinds and Brown made materially misleading statements and omissions about the company's cybersecurity practices and risks. The SEC claimed this ultimately led to a drop in SolarWinds' stock when a large-scale cybersecurity attack known as SUNBURST was revealed.

The SEC's complaint alleges that SolarWinds and Brown inaccurately claimed on a website security statement that the company followed cybersecurity standards like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, used Secure Development Lifecycle practices (industry-developed standards to minimize software vulnerabilities), enforced strong password policies, and maintained adequate access controls. The SEC also alleged that SolarWinds's SEC filings, including the first disclosure of the SUNBURST incident, included only generic and



What Factors May Make a Cyberattack "Material"?

- Significant losses or reduced revenue.
- Change in stock price.
- Focus by management, analysts and/or investors on cyber-related issues during earnings calls.
- Significant impact to company's operations, including costs of remediation associated with a breach or cyber intrusion.
- Unauthorized access to significant amount of sensitive data, such as personally identifiable information of customers.
- Impact to the company's Sarbanes-Oxley financial reporting systems.
- Harm to company's reputation.
- Data integrity issues.
- Pending or anticipated litigation stemming from the incident.

hypothetical statements that failed to address known cybersecurity risks and vulnerabilities.

The SEC also accused SolarWinds of having deficient cybersecurity controls and known vulnerabilities that left its systems susceptible to attack. Before the attack, SolarWinds and Brown purportedly knew about vulnerabilities and attacks involving its Orion software, used by thousands of SolarWinds customers, but these were not remediated or disclosed.

The SolarWinds case is the first time the SEC has charged a CISO with fraud and highlights the increasing importance of cybersecurity under federal securities law. The SEC's complaint seeks not only corrective actions but also significant penalties, including injunctions and a prohibition against Brown serving as an officer or director of any public company. These charges reflect how seriously the agency views these alleged infractions.

In addition to the SEC's action, two shareholder derivative actions were filed against SolarWinds's directors for failure to oversee operations, and the company agreed to a $26 million settlement in a securities class action filed by its shareholders. The derivative suits were dismissed.

Board and Senior Executive Cyber Risk and Disclosures Checklist

The rules and the SolarWinds case suggest certain basic steps boards should take.

- **Evaluate internal controls:** The SolarWinds action underscores the need for companies to scrutinize internal controls relating to cybersecurity. Regulators, customers and the market expect certain market-standard security practices, like NIST. Companies should develop mechanisms for assessing and elevating issues and ensure that internal cybersecurity weaknesses are promptly addressed, given adequate resources and are promptly brought to the attention of counsel responsible for disclosures. Third-party testing and assessments are critical to identifying gaps in those controls and processes.
- **Proper cybersecurity oversight is in place:** Responsibility for the company's cybersecurity risk should be clearly assigned and coordinated within the board and have established procedures. The board or committee overseeing cyber issues should ensure that management has conducted tabletop exercises to test and assess

the company's incident response and its processes for disclosures.

- **Consider the SEC's expansive view of materiality:** Whether a cybersecurity event is considered material will hinge on quantitative and qualitative factors, including:
  - The extent to which the attack uncovered significant deficiencies in the company's overall cybersecurity infrastructure.
  - The extent to which the attack shows weaknesses in systems associated with Sarbanes-Oxley (SOX) compliance and financial reporting, including the integrity of the information processed by these systems.
  - The scope of sensitive customer or employee data compromised.
  - Costs relating to remediation.
  - Loss of a material contract or customer business.
  - Reputational harm.
  - The impact on the company's stock when an announcement was made.
- **Evaluate the risks of statements and disclosures beyond SEC filings:** In the Solar Winds litigation, the SEC leaned heavily on the company's Security Statement, which was included on its website, alleging that it contained misstatements about the company's compliance with cybersecurity standards, its software products, and password policy and access controls. The lesson here: Companies must evaluate all their public statements, not just those in SEC filings.
- **Validate all cybersecurity assurances:** Publicly disclosed cybersecurity assurances must be defensible and consistent with the reality of the company's cyber health.
- **Weigh the cumulative cyber risks:** Individual cybersecurity issues that are not material on their own are evaluated alongside prior incidents to provide context for current incidents, ensuring that the full picture of cyber risks is conveyed to investors.
- **Involve the CISO in the disclosure process:** The company's CISO should be involved in the disclosure process to assess and explain the technical nature of any cybersecurity risks.
- **Distinguish actual from hypothetical risks:** Disclosures should accurately distinguish between actual cyber events and potential, hypothetical risks. Known exploits or vulnerabilities should not be downplayed as merely possible or speculative when there is evidence to suggest otherwise.

Authors

Anita B. Bandy, William Ridgway, David A. Simon, Brian V. Breheny, Raquel Fox, Shirley Diaz, Khadija Messina, Christian Knipfer

Seven Myths About the US Law Banning Imports Made With Forced Labor

- In light of the vigorous enforcement of the Uyghur Forced Labor Prevention Act, boards in their oversight role should ensure that their companies conduct heightened diligence on their supply chains, including upstream suppliers.
- Industrial products and components increasingly are targets — not just items traditionally seen as high risk from a forced labor standpoint, such as textiles and solar panels — and the vast majority of shipments detained have countries of origin other than China.
- The U.S. government pays close attention to NGO and other reports on products that may contain components made with forced labor in China's Xinjiang region.
- The U.K., Germany and Canada have implemented their own forced labor prevention laws, and the EU is considering one.

The U.S. law targeting forced labor and other alleged human rights abuses in the Xinjiang region of China has upended supply chains worldwide since it took effect in June 2022. In the first year and a half that this law has been in force, U.S. Customs and Border Protection (CBP) denied entry to 2,500 shipments worth a combined $2.2 billion. Moreover, the vast majority of the shipments came to the U.S. not from China but from other countries, and were blocked because components were traced back to Xinjiang.

This has implications for boards:

- As enforcement of the U.S. law is enhanced and other jurisdictions enact similar import controls, as part of their risk oversight role, boards should satisfy themselves that their companies have mechanisms and controls in place to provide reasonable assurance of compliance with these laws.
- Boards need to be aware that, if a company shows up in reports that note potential problems or violations, it will need a strategy to get ahead of the story to mitigate reputational risk and prepare for any government action.
- Such reports also can trigger shareholder demands to take action against management or board members, or may lead to books and records demands to find evidence of non-compliance with these laws.

The Uyghur Forced Labor Prevention Act (UFLPA) was prompted by concern within the U.S. Congress and the Biden administration that forced labor and other abuses against the Uyghur ethnic group are widespread in Xinjiang. Under the law, the CBP must presume that any goods mined, produced or manufactured in whole or in part in Xinjiang, or produced by entities blacklisted

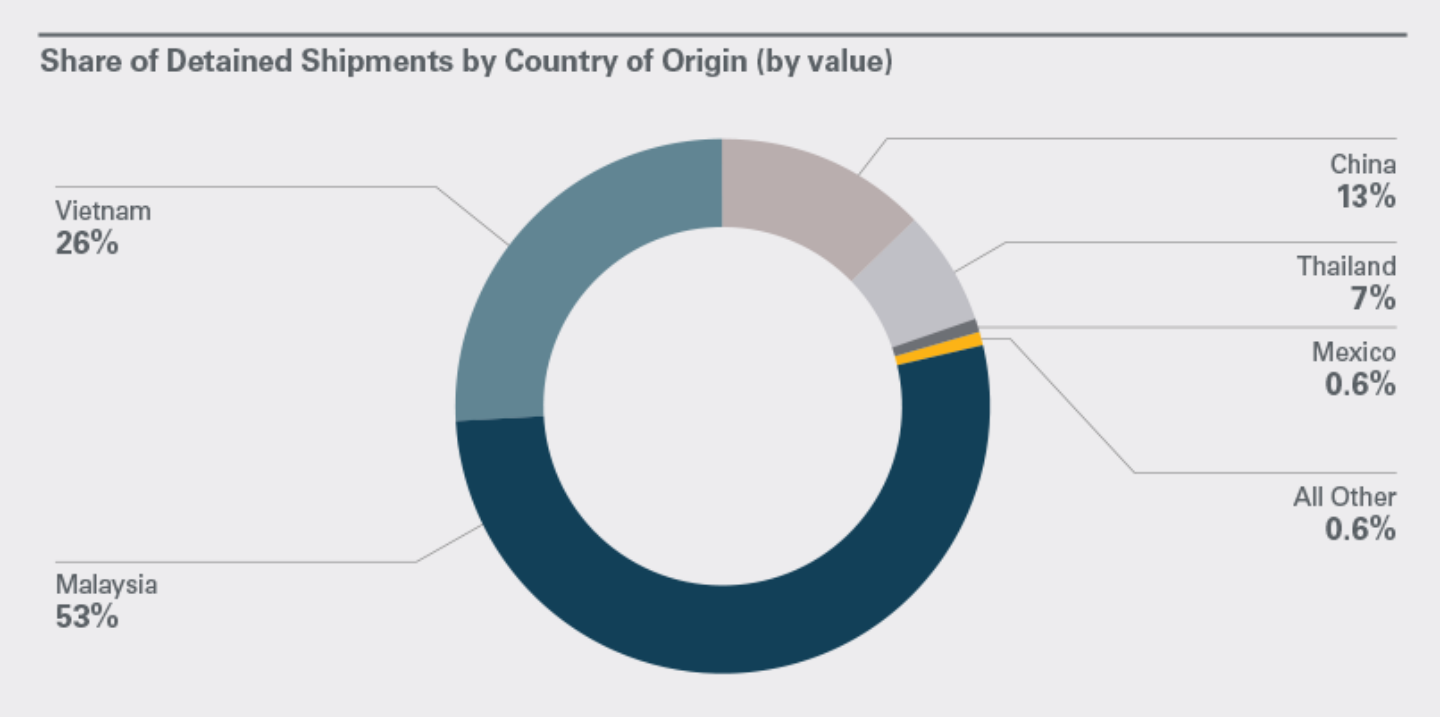
under the law, have been made with forced labor, and are prohibited from entering the U.S.

Despite the robust enforcement of the UFLPA and the resulting risk to importers, a number of myths and misconceptions persist:

The Uyghur Forced Labor Prevention Act (UFLPA) was prompted by concern within the U.S. Congress and the Biden administration that forced labor and other abuses against the Uyghur ethnic group are widespread in Xinjiang. Under the law, the CBP must presume that any goods mined, produced or manufactured in whole or in part in Xinjiang, or produced by entities blacklisted under the law, have been made with forced labor, and are prohibited from entering the U.S.

Despite the robust enforcement of the UFLPA and the resulting risk to importers, a number of myths and misconceptions persist:

Myth #1: The UFLPA only applies to imported goods whose country of origin is China. The UFLPA applies to goods that contain any inputs — no matter how small — that are made in Xinjiang or by an entity on the UFLPA "Entity List." All such goods are presumed to be the product of forced labor. The country of origin of the good as a whole is irrelevant. As the pie chart shows, China is the country of origin for only 13% of shipments detained under the UFLPA. The vast majority of detained goods were made in Malaysia (54%), Vietnam (26%) or Thailand (7%).



Myth #2: Only cotton, tomatoes and solar panels face a meaningful risk of being detained. When Congress passed the UFLPA, it identified cotton, tomatoes and polysilicon (a key element used to make solar panels) as high-priority enforcement targets. Public discourse has heavily focused on forced labor risks associated with textiles and solar panels. But a much wider array of goods are currently at risk of detention. In a 2023 report, an interagency task force determined that a wide range of additional goods are at a high risk of being tainted by forced labor:

- Some agricultural products.
- Electronics.
- Lead-acid and lithium-ion batteries.
- Automobile components.
- Downstream products of vinyl, copper, aluminum and steel.

Indeed, more shipments of industrial materials and electronics have been detained than shipments of apparel and textiles. Recent additions to the UFLPA "Entity List" mirror this: Network technology, chemical and biotechnology companies were added in 2023.

Myth #3: NGO reports on Xinjiang don't need to be taken seriously. When assessing supply chain risks, companies ignore at their peril the reports of journalists, academics and non-governmental organizations (NGOs). The task force mentioned above and CBP pay close attention to NGO reporting on forced labor in Xinjiang. The task force has "extensive engagements" with NGOs to understand forced labor schemes in Xinjiang. Similarly, the State Department has cited numerous NGO reports on forced labor abuses. Beyond their influence with the government, NGO reports can harm a company's reputation. For instance, an October 2023 NGO report mapped the Xinjiang mining industry and identified hundreds of large companies that may indirectly source gold from these entities.

Myth #4: ESG certifications adequately address forced labor risk. In assessing whether a supplier uses or benefits from forced labor, companies may be tempted to rely on third-party certifications that are based on environmental, social or governance (ESG) considerations other than forced labor. For instance, the London Base Metals Association's Responsible Sourcing Programme and the Responsible Minerals Initiative provide certifications based largely on whether a company is operating in or sourcing from a conflict-affected, high-risk area. But given their focus on conflict minerals, these certifications are not reliable measures of potential forced labor risk. They are not a substitute for supply chain due diligence targeting forced labor.

Myth #5: CBP doesn't have the resources to implement the UFLPA. CBP received increased funding in FY 2022 to enforce the UFLPA, and the administration has urged Congress to allocate additional resources. Going forward, CBP's enforcement efforts will likely continue to widen in scope and become more sophisticated, reflecting new hires, new technology

and enhanced training. This increases the likelihood that CBP will be able to accurately trace shipments of goods with a Xinjiang nexus further up the supply chain, and highlights the importance of having robust diligence measures in place to preemptively identify any such goods before they are detained at the border.

Myth #6: Small shipments won't be scrutinized. Currently, shipments of goods valued below the de minimis threshold of $800 are exempt from import duties and do not go through the formal entry process at the border. CBP has historically applied less scrutiny to these "informal entries," as it generally has less reportable information on them. This can make it difficult for CBP to assess the possible forced labor risk associated with such shipments, and detentions rarely occur. But there is growing interest on Capitol Hill in changing the de minimis regime and the administration has signaled that it may increase scrutiny of de minimis entries using its existing authority.

Myth #7: Companies need only focus on complying with U.S. law. Several other countries have adopted or are considering laws targeting the problem of forced labor. These laws broadly fall into two camps.

- **Reporting requirements.** Under the U.K.'s 2015 Modern Slavery Act, companies that meet certain financial thresholds must publicly disclose their efforts to eradicate forced labor from their supply chains. The government can "name and shame" companies that don't produce the required statement, but it is not empowered to detain or investigate goods that may have been made with forced labor. Similarly, the 2021 German Supply Chain Act, Canada's new Act on Fighting Against Forced Labour and Child Labour, and the EU's proposed Corporate Sustainability Due Diligence Directive all impose diligence and reporting obligations on certain companies.
- **Import prohibitions.** In 2020, Canada implemented an import ban on goods mined, manufactured or produced wholly or in part by forced labor. Likewise, the EU is currently considering a similar regulation that would prohibit the importation and sale of goods in the EU that are made with forced labor.

How Should Companies Respond?

CBP continues to ramp up its enforcement of the UFLPA, and an increasingly broad range of goods are now under scrutiny. To avoid the risk of goods being detained at the border, companies should implement robust policies and procedures to identify any supply chain links with Xinjiang. Companies should adopt a risk-based approach to forced labor diligence, taking into account the specific characteristics of the supply chains at issue. Among other steps, companies should consider the following:

Supply Chain Mapping

- Work with first-tier suppliers — especially high-volume suppliers or suppliers of high-risk items — to map their supply chains.
- Regularly screen these suppliers against the UFLPA Entity List.
- Review NGO reporting to identify any high-risk entities or goods.

Collect Key Documents

- For high-risk items, work with suppliers to collect documents for each stage of the supply chain, such as bills of lading, purchase orders, payment records, etc.

Establish Enforceable Standards

- Create a supplier code of conduct that prohibits the use of forced labor.
- Include contractual provisions that prohibit forced labor and ensure that this prohibition is heeded by upstream suppliers.

Authors

Brooks E. Allen, Jack P. DiCanio, Brian J. Egan, Ellie M. Fain, Stephen A. Floyd, Christian Knipfer

AI Executive Order: The Ramifications for Business Become Clearer

- In the months since the Biden administration issued a sweeping executive order directing government departments to implement policies to address the opportunities and risks associated with artificial intelligence (AI), its implications for the private sector have become clearer.
- Some agencies have now issued detailed guidance and proposals that affect not only government contractors but also companies developing large AI models, with large computing clusters or with businesses tied to critical infrastructure.
- With AI now a central focus of governments around the world, boards will need to oversee their companies' AI efforts to ensure they comply with new regulations and mitigate risks.

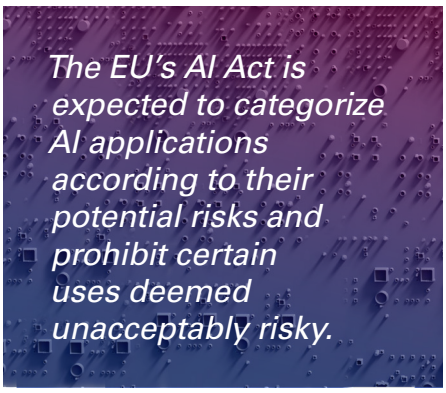
On October 30, 2023, the White House issued a wide-ranging executive order establishing a framework for regulation of AI. The executive order aims to support the development of AI and promote innovation and competition, while establishing safeguards to minimize the risks of the new technology.

The nearly 20,000-word executive order included detailed instructions and set deadlines for departments and agencies across the federal government. In recent months, as various arms of the government have begun to carry out the mandates of the executive order, its full impact across the technology, financial and life sciences sectors and beyond is becoming clearer.

Companies Directly Subject to the Executive Order

While much of the executive order was directed to government agencies, some provisions applied directly to the private sector from the outset. For example:

- Companies developing large AI models that could pose a serious risk to security or national public health or safety must report to the Department of Commerce on the training and "red-team" adversarial safety testing of the models.
- Companies that have certain large-scale computing clusters must inform the government of the clusters' existence, locations and sizes.
- U.S. IaaS companies (and possibly their foreign subsidiaries) must collect "know your customer" information from any foreign customers using the IaaS to train large AI models and report that activity to the federal government.



Other Businesses Affected by Government Actions in Response to the Executive Order

The White House confirmed that federal agencies have met all of the 90-day deadlines set forth in the executive order, with agencies issuing more detailed guidelines and rules that will impact the private sector. For example,

- Companies looking to supply AI products or services to government agencies will need to consider a draft memorandum with guidance from the Office of Management and Budget (OMB) that was issued shortly after the executive order. Among other things, it would:
  - Require agencies to treat raw and modified data as a critical asset to which the government should maintain sufficient rights to avoid vendor lock-in and facilitate further design, development, testing and operation of AI.
  - Encourage government agencies to tailor contracts for generative AI to have risk management requirements such as red-teaming and other safety testing and the ability to label and establish the provenance of AI-generated content.
- In December 2023, the Department of Health and Human Services published guidelines for companies developing or deploying AI in health care. These address potential bias in algorithms and establish a framework to evaluate AI's use in drug development, public health and health care delivery.
- The Department of Labor invited public comment in December 2023 on a proposal to include AI-related occupations on a list of classifications qualifying for an expedited immigration visa process due to a labor shortage. The list, known as Schedule A, is currently limited to nurses, physical therapists and foreign workers with demonstrated exceptional ability required for jobs in the sciences, arts or performing arts.
- The "secure by design" principles in the Guidelines for Secure AI System Development issued in November 2023 are likely to serve as benchmarks for companies developing AI. The guidelines were issued jointly by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.K.'s National Cyber Security Centre and a number of agencies and ministries from across the world, including all members of the G7. AI developers should also consult CISA's Roadmap for Artificial Intelligence, detailing the agency's national plan to address the opportunities and threats posed by AI with respect to critical infrastructure.

In addition to assessing the business impacts of guidance issued to date, boards and management should continue to monitor agency activity over the coming months, as additional deadlines set in the executive order approach. For example, financial services companies should note the March deadline for the Secretary of the Treasury to detail best practices for financial institutions to manage AI-related cybersecurity risks.

How Management and Boards Should Respond

The executive order will have a broad impact on companies developing and deploying AI, but the U.S. government is not alone in focusing on AI regulation. For example, the EU is finalizing details of the EU AI Act, which will broadly govern AI development and use in the EU. The EU AI Act is expected to take a distinct approach, categorizing AI applications according to their potential risks and prohibiting certain uses deemed unacceptably risky, including those that have significant potential for manipulation through subconscious messaging or by exploiting vulnerabilities, such as socioeconomic status or age. Additionally, while the executive order lacks specific penalties, penalties for violations of the EU AI Act could be costly, with expected fines up to €35 million or 7% of annual worldwide revenue, which ever is greater.

Management and boards should therefore:

- Develop and implement appropriate governance processes to assess on a regular basis the impact of global AI regulations and the related guidance, rules and regulations on current and future company operations.
- Establish accountability and reporting regarding material AI-related matters.
- Develop and regularly update corporate AI policies and training.
- Consider not only the risks and obligations created, but also the opportunities for businesses aligning with the new requirements.
- Where AI is a material component of current or future business plans, make AI a regular board agenda item.

Further Reading

"What Is Generative AI and How Does It Work?" (*The Informed Board*, Spring 2023)

"Biden Administration Passes Sweeping Executive Order on Artificial Intelligence" (Skadden client alert, November 3, 2023)

"Latest Text of EU AI Act Proposes Expanding Obligations for High-Risk and General AI Systems and Banning a Third Category" (Skadden client alert, February 5, 2024

Authors

Ken D. Kumayama, Pramode Chiruvolu, Anita Oh

A Guide for Directors to Political Law Issues in This Election Year

- With the 2024 election season underway, corporations may want to support the presidential nominating conventions as well as transition efforts and inaugural activities for incoming federal, state and local administrations.
- These opportunities may come before boards, so it is critical for directors to understand the rules of the road — for their companies as well as for their own individual involvement and that of executives — because these activities can fall under an array of campaign finance, pay-to-play and government ethics rules.
- Violations not only risk financial penalties and reputational damage, but government contractors that are subject to pay-to-play rules can be barred from state and local government business for years as a result of providing support to certain officials and other political entities.

National Party Conventions

The presidential nominating conventions are just months away and both host cities — Milwaukee, where Republicans will gather in July, and Chicago, which welcomes Democrats in August — are hoping for a return to pre-COVID levels of attendance. Conventions are expensive events, and corporations have increasingly become an important source of support.

The conventions are primarily financed by convention committee accounts of the Republican and Democratic national committees and by separate host committees, which are nonprofit organizations established to promote commerce in the convention city and project a favorable image of it to attendees.

Convention Committees

The convention committees are responsible for paying the costs of producing the conventions, and federal law treats them the same way it does other accounts of the national parties in terms of prohibited sources of support: Contributions by corporations, foreign nationals, federal contractors and nationally chartered organizations are forbidden.

These sources are also not allowed to pay for expenses such as travel and accommodations for convention speakers and delegates. There are, however, certain limited interactions that corporations may have with the convention committees, including providing:

- Goods and services to the committees in exchange for promotional consideration.
- Certain items of de minimis value, such as samples, pens, tote bags or other items to be distributed to convention attendees.

Individuals and political action committees (PACs) are permitted to contribute to convention committees, within limits. However, companies

subject to strict liability pay-to-play laws should be mindful that their contributions may be governed by those laws if they are solicited by or linked to state or local candidates or officeholders.

Host Committees

The cities' host committees, on the other hand, may accept unlimited monetary or in-kind contributions from corporations but are limited to paying costs associated with a city bidding for, and subsequently, hosting the convention. The types of expenses that a host committee may pay for include those promoting the city and its commerce, as well as certain "behind the scenes" infrastructure and logistical needs for the convention.

If a corporation provides in-kind contributions to a host committee, the resources furnished must be used exclusively for purposes that are appropriate and permissible for the host committee, such as:

- Security and construction services (*e.g.*, camera platforms, lighting and electrical equipment and press tables).
- Welcome booths for convention attendees.
- Providing accommodations for host committee members.

However, permissible host committee expenses generally do not include items appearing on the broadcast of the convention (*e.g.*, the balloons and confetti televised dropping on the nominee) or travel and accommodations for convention speakers.

It is a best practice to memorialize any agreement in writing with the host committee to ensure that in-kind contributions will be used in a permissible fashion.

Private Events During the Conventions

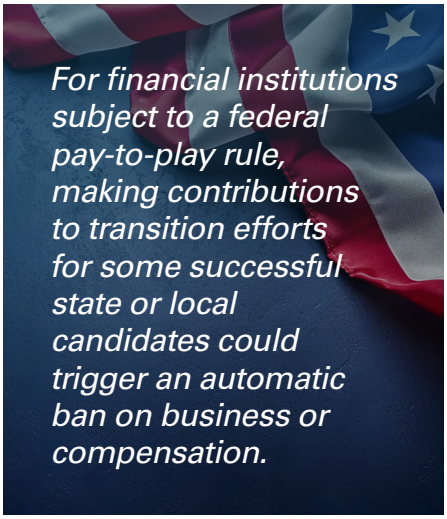
In addition to supporting the convention and host committees, companies sometimes consider hosting or supporting parties and other private events during the conventions. If the event — even if organized by a third party — is coordinated with, or held for the purpose of benefiting, a candidate's campaign, party committee or political committee, financial support of the event may constitute an in-kind contribution.

Such a contribution may be impermissible or subject to limits under campaign finance law and could also trigger an automatic ban on government contracts if the relevant jurisdiction maintains a strict liability pay-to-play law.

Even if that is not a concern, given the likely attendance of public officials at these events, companies should also vet potential implications under federal, state and local gift laws.

Transition Efforts

Changes of administration at the federal, state and local levels can present opportunities for individuals and companies to contribute to and get involved in the efforts of transition teams.



Contributions to Transition Committees

Transition efforts are usually run out of separately designated nonprofit organizations that are typically allowed to accept unlimited contributions from individuals and corporations. However, some jurisdictions impose bans and limits on these contributions, such as the $5,000 limit under federal law on contributions to a presidential transition committee.

Moreover, there are instances in which transition teams are operated from campaign committees, parties or PACs, in which case contributions would trigger all applicable campaign finance limits and prohibitions in the relevant jurisdiction.

For financial institutions subject to a federal pay-to-play rule (*e.g.*, broker-dealers that underwrite municipal securities and investment advisers that manage state or local government money), soliciting or making contributions to transition efforts for a successful state or local candidate is covered under those rules and thus could trigger an automatic ban on business or compensation.

Certain state and local pay-to-play laws also apply to support for transition efforts. As a result, companies that do business with state or local government entities should carefully evaluate the legal implications of any such support.

Corporate Executives Serving on Transition Teams

A corporate executive serving on a transition team (such as for a governor-elect) could pose legal risks.

Conflict of interest. Depending on the jurisdiction, a transition team member may be treated as a public official and, as a matter of law or policy, become subject to some or all of that jurisdiction's conflict of interest laws.

Campaign finance and pay-to-play. Use of corporate resources, volunteering during working hours or an executive personally paying for expenses related to their volunteer activity may result in an in-kind contribution to the committee with the ramifications described above.

Procurement ethics. Conflict of interest provisions in many jurisdictions prohibit a company from obtaining an unfair advantage by assisting in the preparation of the terms or specifications of a request for proposal (RFP) and then bidding on that RFP. This conflicts issue may arise if the volunteer helps or advises the transition on RFPs or the bidding process.

Lobbying. If a corporate executive's transition activities include communications with government officials, and the communications are for the purpose of influencing decisions on behalf of their employer, there may be registration and/or reporting implications under applicable lobbying laws.

Inaugural Committees

Following the elections, successful candidates will also begin to prepare and fundraise for inaugural events in celebration of taking office. Support for the inaugural committees running these events can raise some of the same issues that arise from involvement in a transition of administrations.

In particular, while inaugural committees tend to be set up as distinct nonprofit organizations that are not subject to limits, there are jurisdictions that impose dollar limits on contributions to inaugural committees. Additionally, as with some transition teams, inaugural committees are sometimes funded by a campaign committee, political party or PAC, triggering campaign finance restrictions.

Finally, regardless of how they are formed, soliciting or making contributions in support of inaugural activities for successful state or local candidates is covered under the federal, as well as some state and local, pay-to-play rules.

Authors
Charles M. Ricciardelli, Melissa L. Miles

Shareholder Activism Continues To Increase and Spread in Europe

- The number of activist campaigns launched against European companies rose again in 2023, with a new focus on German targets.
- Many activists surveyed believe that France offers them good opportunities.
- Most of the companies surveyed said they have moved to install defenses against activists, or plan to in the near future.

The boards of listed European companies increasingly find themselves faced with pressure from activist investors. A record number of new public activist campaigns were launched in 2023 and a number of new activist players entered the scene, Skadden's fourth annual survey of the European activist landscape reports. Germany saw the most dramatic increase in activity, with 26 companies targeted in 2023.

In addition, activists in Europe are now more likely to make their demands publicly rather than approaching companies privately, companies report.

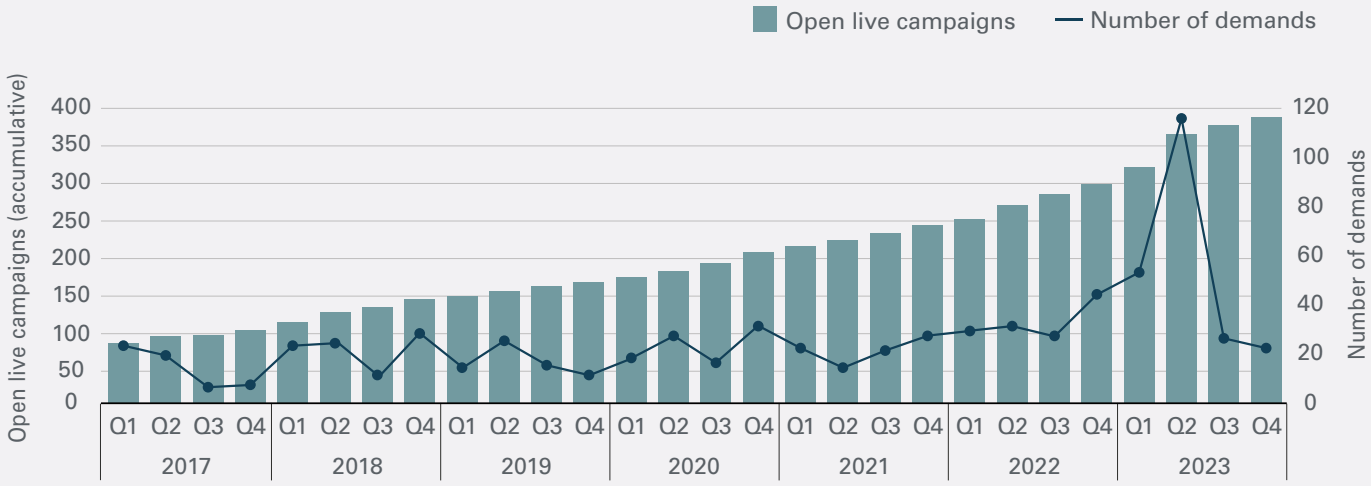
The report, conducted in collaboration with Activistmonitor, combines statistics with a survey of 35 corporate executives of listed companies and 15 activist investors conducted in the fourth quarter of 2024. Below are excerpts. The full report can be found here.

Some of the report's findings were striking — even surprising.

New campaigns and cumulative live campaigns were up significantly again in 2023. The number of new public activist campaigns soared in 2023, to 89, sharply up from the 53 launched in 2022, a 68% increase. That brought the cumulative total of open live campaigns to 380 at the end of 2023, versus 291 a year earlier.

Because some campaigns include multiple demands, the increase in new campaigns in 2023 pushed up the number of new demands issued to 225, up 62% from 132 in 2022.

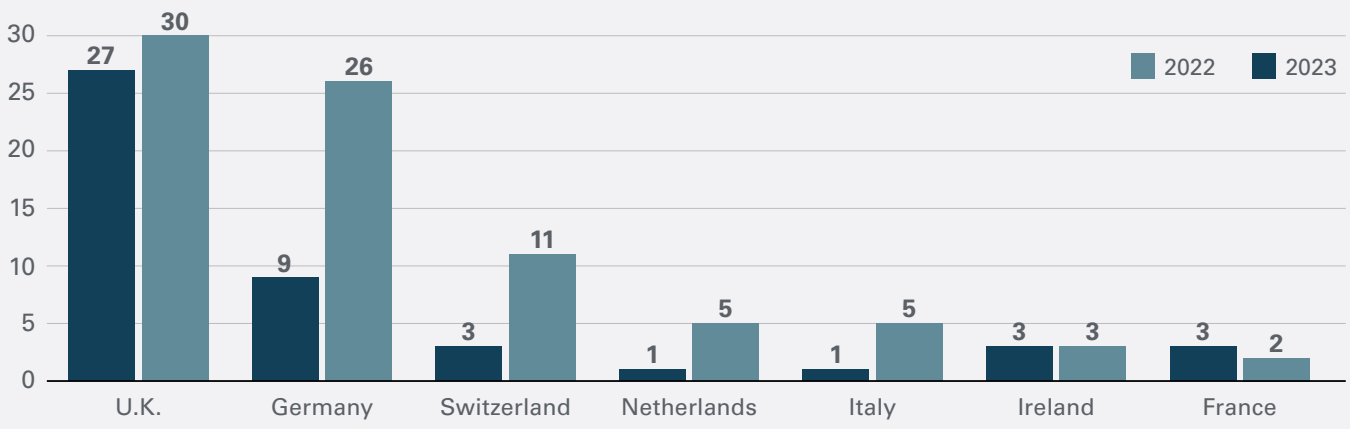
Activism Is on the Increase in Europe



A large majority of corporations report that they have faced an activist recently. Seventy-four percent of corporate respondents said their companies faced one or two activists approaches in the past 12 months, and 8% said they had received demands from three or four such investors.

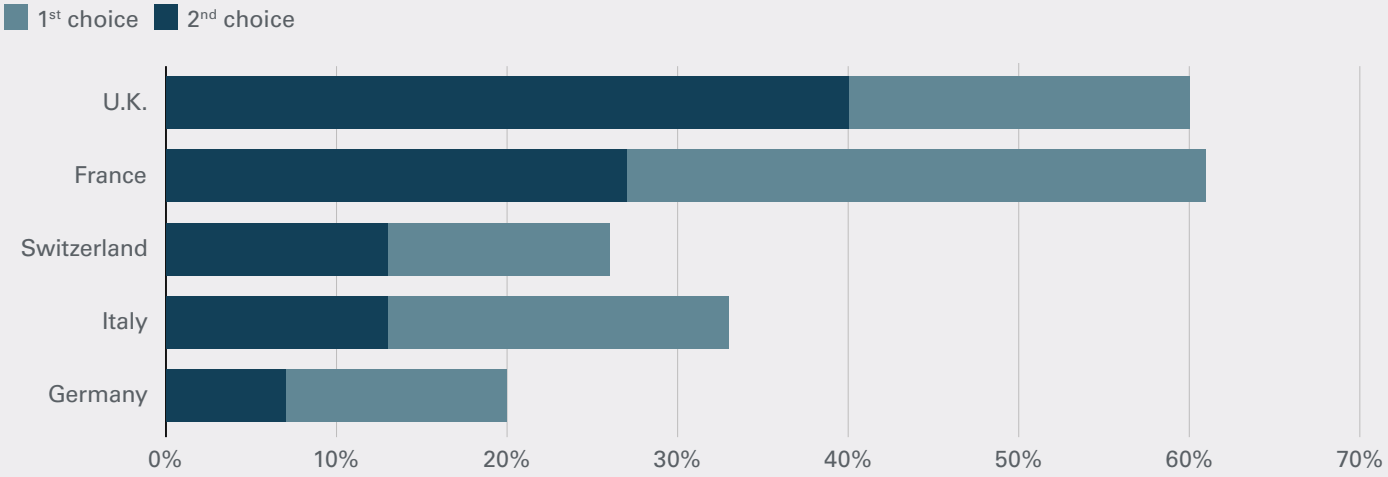
Germany emerged as an important market for activists in 2023. Twenty-six new campaigns were launched against German companies in 2023 — nearly as many as in the U.K. (30), where there is a longer tradition of activist pressure.

Countries With Most Targets (New Campaigns)



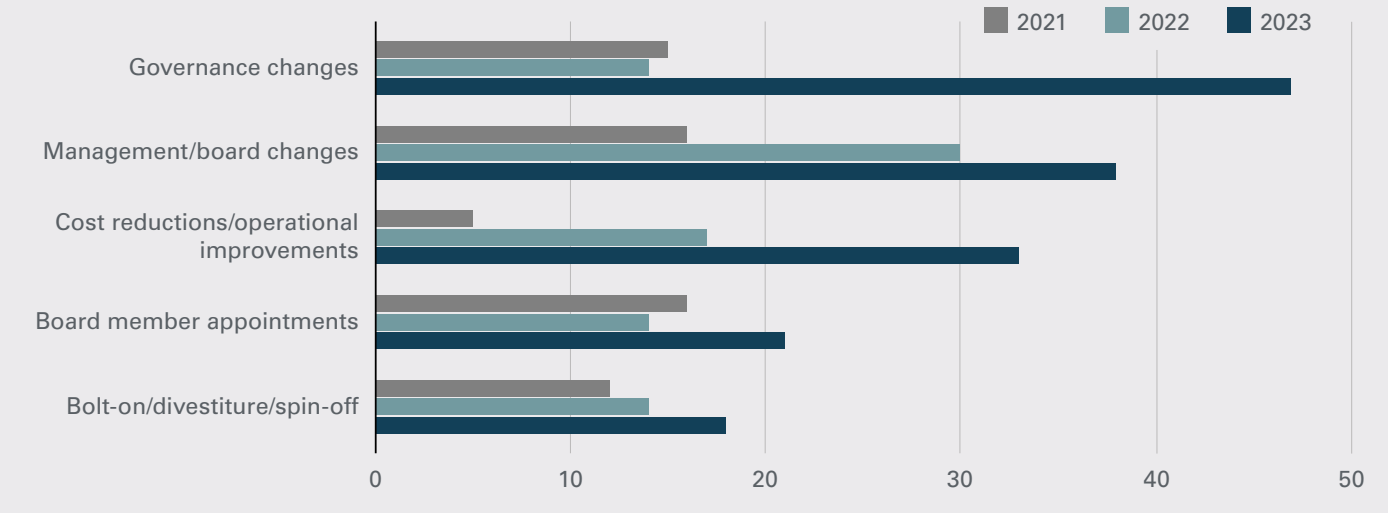
French companies could be targets. Notwithstanding the sharp rise in German targets, the 15 activists surveyed ranked France second to U.K. as the jurisdiction offering the most opportunities in the year ahead, and put Germany behind Switzerland and Italy.

Countries Where Activists See the Best Opportunities in the Next 12 Months



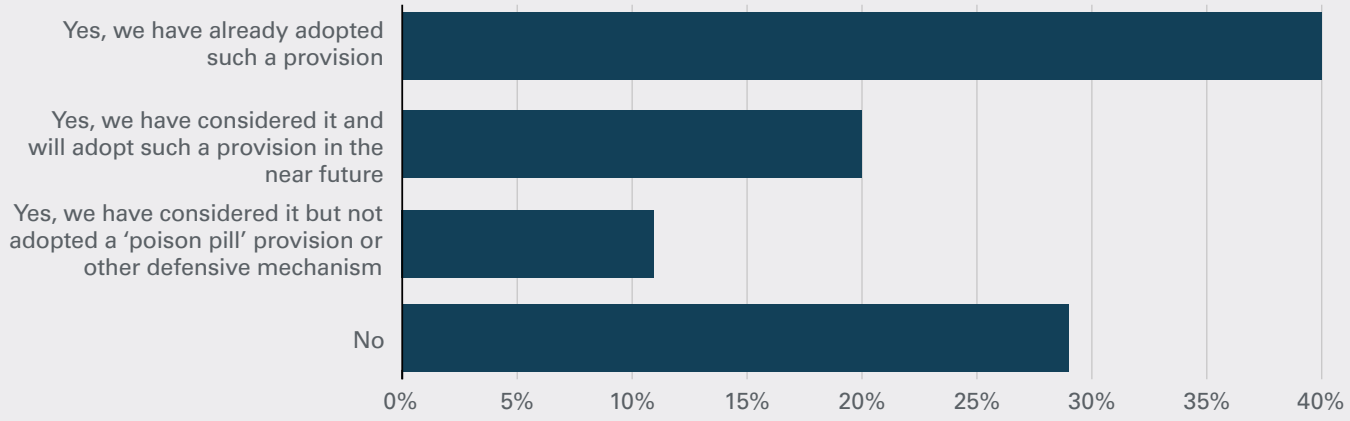
Governance changes (including board or management changes), cost and operational changes and transactions topped the lists of demands.

Most Common Demands in Open Live Campaigns



Many European companies are moving to install defenses. A majority of companies responding (40%) said they have recently added, or enhanced, their corporate defense mechanisms or plan to (20%) "in the near future." These mechanisms are typically less aggressive than the "poison pill" tools that many U.S. corporations utilize and may just require notification of a holding of voting rights at a lower threshold. However, the wider prevalence of these measures indicates that companies are more concerned; last year, only 3% reported installing such defenses.

Use of Defense Mechanisms: Over the last 12 months, has your board considered adopting a 'poison pill'-type provision or other defense mechanisms?



Insights From Skadden Partners

"In the past, activists would usually demand that the CEO and chair go. Today, the more common demand is for the appointment of a 'challenger' non-executive director offering alternative perspective. Companies facing attempts to remove their lead executives would naturally fight back, whereas adding a fresh voice to the board may be something to be welcomed. "In almost all cases there is a benefit to engaging with activists. It shows the company is willing to talk with its investors, and some of the ideas may be worthwhile. The company will learn something from the dialogue."

– George Knighton / London

"German corporates are suffering from supply-chain issues, as well as decoupling and derisking. These and other factors have brought to light needs for reorganization, spin-offs, M&A and other corporate transactions. Activists are seeing these needs and have increasingly used them for their campaigns."

– Matthias Horbach and Holger Hofmeister / Frankfurt

"Given the significant gap that persists between public and private market valuations — and the resulting temptation for activists to pressure corporates to divest non-core assets to realize short-term value — it is unsurprising that more financial sponsors are looking at this space."

— Katja Butler / London

"The continuing market headwinds and unpredictable macro environment are likely to increase pressure on corporates experiencing periods of underperformance or a challenge to the execution of their business strategy. Activists will continue to be on the hunt for these opportunities in Europe in 2024."

— Simon Toms / London

"Public campaigns force companies to engage with activists as well as non-activist investors. This can be a significant source of pressure and commitment in terms of timing, communication and investment."

— Pascal Bine / Paris

"While lawmakers are pretty busy with a lot of topics, new laws that are targeted at governing activist campaigns are not, and likely will not be at least short term, atop their priority lists. Nonetheless, given the publicity and steady increase of campaigning activity, lawmakers and policy makers should be expected to monitor the developments and take note of potential areas of action — they will likely not hesitate to act should dysfunctions become apparent."

— Bruce Embley / London

"With increased tensions feeding the public debate, boards may find themselves in the crossfire between activists' differing — and potentially contradictory — views for the same company in campaigns in 2024."

— Armand Grumberg / Paris / head of Skadden's European M&A practice

Authors

Armand W. Grumberg, Pascal Bine, Katja Butler, Bruce Embley, Holger Hofmeister, Matthias Horbach, George Knighton

Podcast: CEO Succession Planning on a Clear Day

Listen to the podcast

"There's certainly an argument to be made, that the moment you name a new CEO, then you ought to be starting to think about who the next person is," says Blair Jones.

In this episode of the *Informed Board* podcast, our host, Skadden M&A partner Ann Beth Stebbins, is joined by guests, Blair Jones, a managing director at Semler Brossy Consulting Group LLC, and Erica Schohn, partner and head of the Executive Compensation and Benefits Practice at Skadden, to explore best practices in CEO succession planning. They highlight the importance of preparedness, noting that a well-conceived succession plan should serve as a contingency program for unforeseen events, as well as for orderly retirement of a CEO.

The trio emphasize that succession planning should be an annual event, allowing for adjustments as business strategy evolves. They also discuss the necessity of having multiple candidates and keeping them incentivized, including those not selected for the CEO position. A key issue is the current CEO's role in succession planning. Typically, the CEO will be involved, but ultimately it falls to the board to make the final decision.

The guests also highlight emerging trends in succession planning, including the use of external assessments, the role executive chairs and the development of next-level candidates. They conclude that, while companies lean toward internal candidates during planned successions, external candidates are more likely to be considered in the case of unexpected transitions or shifts in business strategy.

Authors

Ann Beth Stebbins, Erica Schohn, Blair Jones

Contacts

Anita B. Bandy
Partner / Washington, D.C.
202.371.7570
anita.bandy@skadden.com

Pascal Bine
Partner / Paris
33.1.55.27.11.01
pascal.bine@skadden.com

Brian V. Breheny
Partner / Washington, D.C.
202.371.7180
brian.breheny@skadden.com

Katja Butler
Partner / London
44.20.7519.7151
katja.butler@skadden.com

Jack P. DiCanio
Partner / Palo Alto / Los Angeles
650.470.4660 / 213.687.5000
jack.dicanio@skadden.com

Brian J. Egan
Partner / Washington, D.C.
202.371.7270
brian.egan@skadden.com

Bruce Embley
Partner / London
44.20.7519.7080
bruce.embley@skadden.com

Raquel Fox
Partner / Washington, D.C.
202.371.7050
raquel.fox@skadden.com

Armand W. Grumberg
Partner / Paris
33.1.55.27.11.95
armand.grumberg@skadden.com

Holger Hofmeister
Partner / Frankfurt
49.69.74220.117
holger.hofmeister@skadden.com

Matthias Horbach
Partner / Frankfurt
49.69.74220.118
matthias.horbach@skadden.com

George Knighton
Partner / London
44.20.7519.7062
george.knighton@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Charles M. Ricciardelli
Partner / Washington, D.C.
202.371.7573
charles.ricciardelli@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Brooks E. Allen
Counsel / Washington, D.C.
202.371.7598
brooks.allen@skadden.com

Pramode Chiruvolu
Counsel / Palo Alto
650.470.4569
pramode.chiruvolu@skadden.com

Melissa L. Miles
Counsel / Washington, D.C.
202.371.7836
melissa.miles@skadden.com

Shirley Diaz
Associate / Washington, D.C.
202.371.7362
shirley.diaz@skadden.com

Ellie M. Fain
Associate / Washington, D.C.
202.371.7034
ellie.fain@skadden.com

Stephen A. Floyd
Associate / Washington, D.C.
202.371.7145
stephen.floyd@skadden.com

Christian Knipfer
Associate / Washington, D.C.
202.371.7331
christian.knipfer@skadden.com

Khadija L. Messina
Associate / Chicago
312.407.0116
khadija.messina@skadden.com

Anita Oh
Associate / New York
212.735.2499
anita.oh@skadden.com

View past editions / You can find all *Informed Board* articles here.

One Manhattan West / New York, NY 10001
212.735.3000

skadden.com