Senior executives still hold divided views on generative AI’s potential. BCG’s 2023 Digital Acceleration Index (DAI) survey of 2,000 global executives found that more than 50% discourage GenAI adoption. But while the debate over the potential and perils of GenAI goes on, the technology continues to advance. Most companies need to plan for GenAI’s becoming a more pervasive and powerful part of everyday business. This means that all C-suite members need to climb the GenAI learning curve.
As has been widely documented, the GenAI opportunities are significant, but leaders need to focus equally on the risks. Privacy and cyber security are already regular fixtures on boardroom agendas, and compromised privacy and data breaches are two of the top reasons why executives in BCG’s survey said they discourage broader adoption. Risks also extend to operations, safety, compliance, and reputation. We have already seen plenty of cases of hijacked software, misguided chatbots, and cyber defense breaches—and we are still in the early days. The bad guys are climbing their own learning curve. Regulators are watching, determining if they should step in and if so, when, where, and how.

Beyond bringing themselves up to speed, though, what is a responsible C-suite member supposed to do? When it comes to AI risk, what exactly are the CEO’s responsibilities? Or the COO’s or CIO’s?

Companies need a strategy and plan for implementing GenAI, but equally important, they need clear accountabilities for each member of the top management team to ensure that they cover all the bases—relating to the risks as well as the rewards. Here’s our hands-on guide to where C-suite members should focus their efforts as GenAI becomes a bigger part of everyday business reality.

**Heightened Risk and Exposure**

AI, and especially GenAI, increases a company’s exposure to technology risks and expands the potential attack surfaces beyond just digital systems. Much of GenAI’s power comes from the ease with which anyone can use it, the unstructured data it can quickly organize, and the insights it can generate. But GenAI models are still works in progress: bias and hallucinations (tech speak for mistakes) are commonplace.

GenAI presents or heightens five types of material business risk:

- **Safety:** Biased or inaccurate AI decision making
- **Data Loss:** Theft, disclosure, or misdirection of private or confidential information
- **Operational Failure:** Inaccurate solutions or nonresilient systems
- **Reputational Damage:** Business failures, safety issues, data loss, and eroded customer trust
- **Regulatory:** Privacy violations and noncompliance

In addition, GenAI boosts the capabilities and productivity of criminals, just as it does that of companies. Fraud, malware, social engineering attacks (such as phishing) are already common threats. Now they can all be automated, and their quality and precision enhanced with the same types of algorithms that companies use to improve their processes. Corporate data, confidentiality, integrity, and privacy are all in the crosshairs.
Implementing GenAI is partly a matter of marrying it with the company’s current AI capabilities and determining the best use cases for scaling up. But companies also need to ensure that the GenAI models they build, buy, and implement have appropriate guardrails to ensure data protection, privacy, and responsible use. They must put three elements in place. The first is enterprise-wide security and privacy capabilities tailored to the relevant use cases. Second is model security and secure application design. Models in development need to be made safe against AI-specific vulnerabilities, such as in the algorithm supply chain and the integrity of training data. At the same time, all GenAI application development teams should be following standardized DevSecOps processes and integrating AI safety measures throughout the application development process. The third priority is ensuring that companies understand the GenAI security practices of their vendors and partners and require that they are sufficiently robust.

These priorities cross multiple organizational lines. Getting them right requires clear responsibilities and accountabilities, starting in the C-suite.

**Chief Executive Officer**

The top executive’s job is to ensure that the company realizes the full business value of GenAI solutions while maintaining customer trust and a high standard of responsible use. As a practical matter, he or she must oversee the development of the objectives for GenAI and lead the effort to make them clear to the organization.

CEOs need a basic understanding of GenAI, particularly with respect to security and privacy risks, since they are responsible for holding their C-suite colleagues accountable for implementing security and privacy processes with measurable effectiveness across the organization. They must have confidence that all decisions strike the right balance between risk and business benefit. One key requirement is the establishment of a formal GenAI operating model for security and privacy that includes third-party vendors and platform providers.

> The top executive’s job is to ensure that the company realizes the full business value of GenAI solutions while maintaining customer trust and a high standard of responsible use.
The CEO ensures that product, legal, and security teams collaborate across all phases of GenAI deployment, including acquisition, building, and implementation of GenAI models. If disagreement or conflict arises in goals or incentives, CEOs need to bring functions and business units into alignment. Multiple important constituencies will be watching, including the board, shareholders, competitors, regulators, and customers.

Chief Operating Officer

The COO’s primary responsibility is to ensure that deployed GenAI use cases are aligned with business objectives and implemented in a resilient fashion. COOs establish GenAI objectives for business operations, ensuring that measurable security and privacy processes are included. They oversee development of the desired operational structure and capability building to support GenAI-enabled operations.

COOs rely heavily on the enterprise’s security capabilities to prevent malicious activity and avoid operational disruptions. As GenAI becomes more embedded in the ways that companies operate, the COO must ensure that the organization has the ability to troubleshoot and resolve disruptions in GenAI-enabled processes.

Chief Risk and Information Security Officers

These two executives are directly responsible for controlling the risk of GenAI to the organization. Working hand in hand, they identify threats and implement the proper controls upfront to mitigate hazards while also promoting innovation. In addition, CROs and CISOs manage the organization’s risk appetite and advise other C-suite members on tradeoffs between the value of GenAI and the new risk exposure it creates. They help develop and implement low-friction solutions while maintaining an appropriate risk profile.

GenAI presents CROs and CISOs with particular challenges, among them using the new technology to be better and faster at achieving basic cybersecurity goals, managing the dynamic nature of new capabilities that support both protection and attacks, and addressing the urgent need to reskill or upskill security staff amid a general talent shortage.

CROs and CISOs have a long list of immediate security and privacy priorities, which include:

- Establishing a security strategy with defined risk tolerance levels
- Establishing (with the COO) measurable criteria to evaluate GenAI use cases against potential value and risks
• Ensuring that they have the appropriate skills to identify, manage, govern, and report on GenAI risks and controls
• Ensuring that current data governance and provenance guidelines are sufficiently robust and baked into current GenAI development processes
• Ensuring that secure-by-design standards are updated and applied to the machine-learning operations process used for building custom GenAI applications
• Ensuring compliance with data governance and provenance guidelines and legislative and regulatory requirements
• Dedicating resources and funding to develop GenAI security capabilities
• Evaluating how GenAI solutions embedded in cybersecurity solutions can help the organization detect attacks, protect data, and retain business value
• Putting in place strong vendor management procedures, including the vetting of new GenAI vendors
• Ensuring that they have defined appropriate incident response mechanisms in the event of a security or regulatory breach involving GenAI
• Refreshing learning and development plans and the talent within their organizations to account for the skill sets required to manage GenAI cybersecurity and privacy risks

Chief Information, Technology, and Data Officers

Technology and data are the enablers of AI. The responsible executives must ensure that product, technology, and cybersecurity teams have access to the necessary technology infrastructure, systems, applications, services, and data—at a reasonable cost-value ratio. It’s a delicate balance: improper implementation could hinder innovation and put the organization at risk of stagnation.

The responsible executives must ensure that teams have access to the necessary technology infrastructure, systems, applications, services, and data—at a reasonable cost-value ratio.
CIOs, CTOs, and CDOs need to monitor both the provenance and security of data and plan for GenAI systems that can assemble data into answers and outputs that exceed the data security classifications of the data inputs. A robust data office with visibility into the data being used in these systems and an understanding of critical intellectual property is extremely important.

CIOs, CTOs, and CDOs are also actively involved in setting up environments for development and experimentation and establishing guidelines for how new GenAI-enabled products or services can begin to be used. They create the organization’s inventory of GenAI technologies and communicate with the workforce on the use (by both business users and developers) of these new tools. They must collaborate closely with the risk, legal, and information security functions.

**Chief Legal and Privacy Officers**

Legal and privacy executives make sure that the use of GenAI adheres to company standards and privacy regulations and that security practices meet legal and regulatory requirements. They are responsible for data provenance, access, and governance, as well as for governance of GenAI processes that ensure compliance without hindering exploration. They need to stay up to date on new legislation and regulation regarding the use of GenAI products and systems and translate them into practical standards and procedures. Putting in place, updating monitoring, and reporting mechanisms are priorities for confirming that standards and procedures are followed.

**Chief Product Officer**

Innovation must serve a purpose. The chief product officer makes sure that whatever uses GenAI is put to aren’t just “cool” experiments but add value to products, services, or processes (such as through new customer value propositions or lower costs). The chief product officer also works with the CRO, CISO, and each product owner to ensure that responsible AI and secure-by-design practices are implemented and resourced within each product team. It is critical that metrics and key performance indicators are established to measure the value, impact, security, and responsible deployment of GenAI products.

**Chief Marketing Officer**

The CMO’s principal security responsibility is ensuring that marketing materials developed using GenAI, whether internally or by outside agencies or contractors, are “clean” and do not use copyrighted content or text, graphics, videos, or other materials that the company may not have the rights to. The risk of misuse or unauthorized use is vastly heightened because virtually anyone can use GenAI tools to generate marketing or communications content without checking for provenance or ownership of the materials that result.
Chief Financial Officer

GenAI promises big benefits in productivity and costs, but these do not come without investment. Much as they did during the initial cloud migration two decades ago, CFOs need to establish a good handle on how the technology is being used within the organization and its effect on costs.

CFOs need to establish a good handle on how the technology is being used within the organization and its effect on costs.

The CFO needs to negotiate contract rates, collaborate with legal to ensure that appropriate contract terms for cybersecurity and privacy are in place, and work with the chief information security officer to ensure that outside services are vetted for their cybersecurity and privacy practices as part of procurement. Since GenAI systems require significant computing and data resources, the teams using them need to understand their costs and how they are allocated. Budgeting has quickly become a key step in the GenAI development or acquisition process. Business cases for GenAI investments should include allocations for integration of security and data privacy practices. The CFO also needs to request an investment business case from the chief information security officer on the augmented security capabilities needed to deal with the new GenAI landscape. Once the value of GenAI is realized, either by enabling cost cutting or adding new revenue streams, the CFO must be ready to ask where the savings will be reallocated.

Chief Human Resources Officer

Training and personnel policies governing use are important for any organization taking on GenAI. It is up to HR to work with developers, IT, and security to implement these policies and provide appropriate training on the use of GenAI solutions.

A Lesson from History

Remember the great cloud migration? Almost 20 years ago, the development of the commercial cloud promised to eliminate technology capex and reduce overall tech spending. The cloud was heralded as the future of enterprise IT.
But the rush to shift both computing capability and data storage to third parties was confusing and sometimes chaotic. Individual teams set up their own leases in commercial clouds, starting up and shutting down vendor accounts as needed, with little regard for compatibility, not to mention security or other risks and implications. In some cases, the only way for management to know who was doing what was by analyzing the bills.

With GenAI, we need to move with deliberate speed, but the emphasis should be on deliberate. There is a lot about the technology that we don’t know. A team of people with diverse capabilities is a must to ensure that all the bases are covered. The lesson of the rapid and sometimes irresponsible rush to the cloud is that we should move into GenAI responsibly, carefully, and with discretion.

Because GenAI has so many potential use cases, C-suite leaders need to be aware of all projects, capabilities, data requests, and developments. Establishing an AI leadership team, backed by a well-resourced center of excellence, is one way to organize oversight. But it is still incumbent on each C-suite member to climb the GenAI learning curve in his or her area of responsibility so that top executives can manage implementation in an informed and thoughtful manner with customer trust, resilience, and safety front of mind.
ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

© Boston Consulting Group 2024. All rights reserved.

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and X (formerly Twitter).