



How to balance opportunity and risk in adopting disruptive technologies

Authors

Todd Marlin

Jim McCurry

Contributors

Alan Gibson

12 minute read

30 Nov 2023

Related topics

AI

Forensics



The successful adoption of disruptive technologies requires a balance between the pursuit of opportunities and the management of risks.

In brief

- Laws and guidelines often struggle to keep up with the rapid pace of technological evolution, making it essential for organizations to be proactive.
 - Investment in compliance technology is growing, but it may not be sufficient.
 - Organizations need to prioritize ethical technology use and incorporate innovation into their broader compliance strategy.
-

Artificial intelligence (AI), automation and other advancements are transforming both the enterprise and its compliance function as they optimize operations and extract new insights from data. But these technologies amplify existing risks such as data breaches and reputational damage while creating new threats. Generative AI (GenAI), along with other advances, can help compliance and legal departments better manage risk, with the right investment. But GenAI and other disruptive technologies can also lead to serious business challenges such as creating biased or false content, violating copyright laws and exploiting personal data.

One of the top corporate challenges in the privacy era is keeping up with regulatory changes across many jurisdictions, but in the case of AI, development has far outpaced legislative action. This gap has led stakeholders to demand that organizations proactively develop an ethics-based framework for using AI and other emergent technologies.

How can businesses foster a culture of compliance while staying competitive?

Companies need to develop a cohesive strategy for responsibly using technology and data, in much the same way as they prioritize their sustainability agenda. Organizations can adopt many of the measures used to set targets for, manage and report on initiatives such as protecting the environment and advancing the wellbeing of their stakeholders and communities. This strategy should align with an organization's core values rather than relying on constantly changing regulations that vary among jurisdictions. Technology adoption is critical for business growth, but failure to prioritize its ethical use could mean legal and reputational risks outpace any rewards.

Why relying on the legislation isn't enough

AI systems collect and analyze vast amounts of data, raising the risks from cyber-attacks and data breaches. AI used for surveillance can also impact the right to privacy. Using it to generate images and videos may mislead the public and violate copyright laws. Other risks include generating fictitious content (hallucinations) and the lack of transparency in data-driven decisions. AI systems can also amplify societal biases to discriminate against a bank customer seeking credit or a job applicant.

These risks have far outpaced the capacity of lawmakers and regulatory bodies to rein them in. Nearly 40 AI-related laws were passed globally in 2022,¹ before the use of GenAI exploded, and new regulations that address GenAI are pending in many key jurisdictions, including the EU, whose AI Act is poised to serve as a global model, much like the General Data Protection Regulation (GDPR).

New regulatory requirements

AI-related laws passed globally in 2022

Changing regulatory requirements are the top challenge for large companies when considering adopting technology to support data governance, responsible AI use and cybersecurity, according to a **2023 EY survey produced by EI Studios, a division of Economist Impact.**

Methodology

+

Many multinational companies would like to apply the strongest data protection regulations holistically, but there can be jurisdictional conflicts. Organizations need to decide what is the most defensible position while minimizing data moving from one geography to another.

An EY study of **eight jurisdictions that are leading the way in developing AI regulations** shows differing approaches but similar goals: to reduce potential AI harm while facilitating its use to benefit citizens. The jurisdictions are all taking a risk-based approach to creating regulations that safeguard human rights, privacy and data security while demonstrating transparency and sustainability. For example, the EU AI Act mandates that GenAI systems disclose content generated by AI and publish summaries of copyrighted data used for training.²

But companies increasingly face reputational risks even if there are no laws in place. Growing fears around AI are bringing new demands from stakeholders. Corporate investors, employees, partners, and customers, while pressing regulators to move more quickly, are simultaneously calling on companies to be proactive in using AI and other technologies responsibly.

World leaders are also pressuring organizations for ethical AI use. As a precursor to national US regulations, the Biden Administration is asking for voluntary commitments to develop AI responsibly.³ UN Secretary-General Antonio Guterres has called on Security Council members to join “a race to develop AI for good.”⁴ These kinds of growing demands mean organizations can’t afford to wait for regulators to catch up before setting their AI strategy.

Investment grows in compliance technology, but is it sufficient and strategic?

Regulators increasingly expect companies to use advanced technologies to objectively demonstrate sound compliance. For example, the US Department of Justice (DOJ) calls on companies to use data analytics

in periodically evaluating their compliance.⁵ Failure to do so is a consideration for prosecutors.

Data analytics, AI and automation greatly improve the ability to detect legal and reputational risks, describe them (typically in a quantitative way) and provide actionable insights. Relying on manual systems just isn't an option for most companies.

That's because customer data, the lifeblood of most industries, is coming in at greater volumes than ever before, and the pace is increasing. Data professionals say data volumes are growing 63% every month on average in their organizations, with data coming from 400 different sources, according to a 2022 Matillion and IDG Research survey.⁶ Governing this data effectively is a basic requirement that typically doesn't attract enough investment.

Nearly half of chief data officers surveyed in 2022 said clear and effective data governance is a top concern.⁷ Before companies invest in technology, they need to assess how they manage information. Who has access to what type of data? How is data minimized, tracked, validated and transferred? How is it protected? Many organizations may need to put more money into data governance before investing in AI.

Most companies are increasing their spending on legal and compliance technology, with 87% investing in AI and machine learning, according to the **2023 EY-commissioned EI Studios survey**. However, most of the organizations surveyed spend less than 10% of their IT budget on technologies used to identify and manage legal and compliance risk.

Legal and compliance technology

0%

of companies are investing in AI and machine learning

IT budget allocation

< 0%

spent on technologies used to identify and manage legal and compliance risk

Any investment in compliance technology should include safeguards to make sure the technology is working properly and effectively. For example, machine learning can help a company detect fraud patterns in sales transactions or flag problematic vendors, but using biased or insufficient data could result in false positives.

Criminals are also leveraging AI. AI systems can develop sophisticated malware, learn from unsuccessful attacks and create more believable phishing campaigns. Companies using AI and automation to detect and respond to these attacks discover data breaches much more quickly than those that don't, reducing their cost of a breach by nearly US\$2 million, according to IBM research.⁸ Despite this, only half of the organizations studied planned on increasing security investment after a breach.

Organizations should also consider spending more on internal controls, which restrict data access and provide accountability. Inadequate controls are the highest-ranked internal risk reported in the **2023 EY-commissioned EI Studios survey**. Embedding workflows with built-in controls reduces mistakes and fraud, creating digitized compliance scorecards that provide detailed insights into key risk areas.

Advanced data analysis also enables an enterprise to integrate risk management with strategy and performance management. For example, a comprehensive analysis of risk exposure for emerging scenarios helps a board determine whether its strategies and business models are viable, as described in the **EY Global Board Risk Survey 2023**, which found that highly resilient boards leverage data and technology effectively to detect risks early and improve decision-making.

Developing a sustainable data and technology strategy that aligns with core values

The responsible use of technology may not always be a strategic priority for many companies. Nearly half of respondents in the **2023 EY-commissioned EI Studios survey** reported their organization lacks a corporate strategy for data privacy, which is well-regulated in most jurisdictions and requires sound data governance.

Organizations need to develop a comprehensive strategy and vision for managing technology and data ethically, just as many companies have done with their sustainability agenda. But progress in this area is alarming. Less than one-third of board directors believe their oversight

of the risks arising from digital transformation is very effective, according to the EY Global Board Risk Survey (GBRS) 2023.

A mission statement is essential for showing how an enterprise manages technology and data in an appropriate and defensible way that aligns with their core values. For example, Adobe has clearly communicated its commitment to advancing the responsible use of technology for the good of society. Its AI Ethics Principles describes the actions the software maker is taking to avoid harmful AI bias and align its work with its values.⁹

Microsoft's approach to creating responsible and trustworthy AI is guided by both ethical and accountability perspectives.¹⁰ It calls on technology developers to establish internal review bodies to provide oversight and guidance so that their AI systems are inclusive, reliable, fair, accountable, transparent, private and secure.

Ethical use of technology isn't possible without fostering a culture where integrity is just as important as profits. For example, Volkswagen Group states that integrity and compliance have the same strategic and operational priority as sales revenue, profit, product quality and employer attractiveness.¹¹

The average cost of a data breach grew to nearly US\$4.5 million in 2023, according to an IBM study.¹² Regulatory fines are also on the increase, with Meta hit with a €1.2 billion sanction for GDPR violations.¹³

Organizations looking to create an ethical and sustainable strategy for technology and data use can adapt measures used for other

sustainability initiatives, such as environmental protection and good governance. This includes setting targets and budgets, measuring performance and reporting progress publicly. Robust sustainability efforts can go a long way toward addressing stakeholder concerns and even attracting job applicants.

Some sustainability activities such as climate action are already moving from voluntary commitments into compliance as regulators set disclosure requirements for public companies.¹⁴ Corporate strategy and principles for ethical technology are expected to have the same focus as that of the sustainability agenda if they don't already.

Ensuring confidence in AI with a robust governance approach is one of **five strategic initiatives EY teams recommends for organizations** looking to maximize AI's potential while meeting its challenges. This approach includes:

- Establishing an AI council or committee along with ethical principles to guide policies and procedures
- Tracking all relevant existing regulations and ensure any new use cases comply
- Defining controls to address emerging risks
- Preparing for pending legislation

Prioritizing the ethical use of AI and other emergent technologies means leaders must be careful not to fall into the "say-do" gap in which they pay lip-service to doing the right thing. This gap was clearly apparent in the **EY Global Integrity Report 2022** in which 58% of board members said they would be very or fairly concerned if their decisions were subject to public scrutiny and 42% reported their

company is willing to tolerate unethical behavior from high or senior performers.

Rise in GenAI brings new opportunities and risks

Imagine two doorways – one labeled “technology opportunity,” the other “technology risk.” Which door do you open first? Which is more important to your organization? What blocks your path and who may be nipping at your heels?

GenAI has made it more difficult than ever to balance opportunity and risk in adopting technology. Its widespread adoption in 2023 raised awareness of the potential for all types of AI, along with shortcomings. The public wants to know how AI can be prevented from creating false information, biased results and taking their jobs.

Large language models (LLMs) like ChatGPT are becoming a game changer for legal and compliance functions with their ability to analyze and summarize vast numbers of documents. But professionals well-versed in privacy and cybersecurity risks may struggle to assess new threats stemming from AI. We’ve already seen lawyers cite cases invented by AI, making it essential that outputs be validated by other intelligent tools and/or people

Organizations that seek to reduce GenAI risks by prohibiting its use may see this strategy backfire. More than a quarter of employees responding to an online Reuters-Ipsos poll in July 2023 said they regularly used OpenAI ChatGPT at work, even though only 22% of those users said their employers explicitly allowed it.¹⁵ Limiting employees to company-approved GenAI tools may result in

workarounds, making it critical to develop policies, standards, and procedures no matter how AI is accessed throughout an organization.

Even companies that authorize GenAI usage may not have a full picture of how it's being deployed and the accompanying risks. More than half of AI failures come from "shadow AI" or third-party tools, which are used by 78% of organizations globally, according to MIT research.¹⁶

Companies looking at GenAI investments must focus on the problems they're trying to solve and the role data will play. Does the organization have the required data? Does it understand how the data was generated, its limitations, and what it represents? Can the data be used to create LLMs? A lack of good data governance can cause a host of risks – from biased outcomes to data breaches. Even if a company gets all this right, there's often a breakdown in communicating actions in a form that leadership, investors, employees and other stakeholders understand.

The reality is no matter which door you open first, you're bound to end up in the same room. Emergent technologies with game-changing potential will always be intertwined with a bevy of legal and reputational risks that must be addressed strategically.

Takeaways

New regulatory requirements and growing stakeholder expectations are driving companies to better address the risks arising from adopting new technologies. But they aren't doing enough. The **2023 EY-commissioned EI Studios survey** reveals alarming gaps in strategies to address digital threats and insufficient IT investment in

managing risk and maintaining compliance.

A robust, cohesive strategy to use technology and data responsibly throughout an enterprise supported with proper governance and investment is essential. We believe organizations should consider modeling their information and technology governance efforts after leading sustainability initiatives.

Leaders who invest in protecting data and using technology responsibly can more effectively address growing digital threats such as data breaches, privacy violations and AI misuse. They can also use technology to drive more effective decision-making and embed risk management into business strategy and compliance, building a more resilient, successful enterprise.

Show article references

Summary

In the face of rapid technological innovation, organizations are navigating a complex landscape of opportunities and risks. Technologies like AI are transforming operations but also amplifying risks such as data breaches and ethical concerns. While GenAI can aid compliance and legal departments in managing risk, an investment in ethical technology usage may lag. With the rapid development of AI,

How EY can help

Integrity and Compliance

As regulatory enforcement and public intolerance of corporate...

Read more

regulations struggle to keep pace, necessitating organizations to proactively establish ethics-based frameworks for technology use. Organizations that prioritize data protection and ethical technology usage can better navigate the digital landscape, mitigating risks and driving more effective decision-making.

About this article

Authors

Todd Marlin

EY Global Forensic & Integrity Services Technology & Innovation
Leader

Jim McCurry

EY Global Forensic & Integrity Services Deputy Leader

Contributors

Alan Gibson

Related topics

AI **Forensics**



Connect with us

Our locations

My EY

Site map

Legal and privacy

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.