

EQUITY RESEARCH

November 30, 2023

ESG

AI In Tech

An ESG Threat & Opportunity

Our Conclusion

AI has been the hot topic in tech for 2023, and we believe it's safe to say we've officially entered the 'Age of AI'. With that context, we attempt to assess the impact of widespread use of AI tools on the three prongs of ESG, with a focus on generative AI. While the technology sector has historically been favoured by ESG-conscious investors, we see potential for broad-based adoption of GenAI to impact the tech sector's "ESG-friendly" reputation when it comes to energy consumption, workplace composition, cybersecurity and data privacy. On the other hand, we also see potential for the technology to provide opportunity to improve the environmental, social, and governance ratings of tech companies if applied in the right areas.

Key Points

Environmental Impact Is A Twofold Problem: Data centres are well known to require massive amounts of electricity to power their servers and to run the significant cooling systems needed to support them. As generative AI becomes more commonly adopted, the widespread use and training of these models is expected to have an impact on the environmental footprint of data centres. Large language models (LLMs) require substantial levels of energy to train, and require memory storage for the data they are fed as well as the data they produce. More energy means more heat generated by the data centres that house these AI systems, which leads to increased water consumption from additional cooling. However, research has shown that the choice of energy supplying the cloud data centres for LLMs can significantly reduce the carbon footprint.

AI Will Change The Workplace: The social component of ESG places heavy emphasis on workforce composition, specifically gender and diversity targets. It is no surprise that generative AI will disrupt the workforce; however, the impact is likely to be felt disproportionately within certain occupations and demographics. Beyond job displacement, many occupations will see changes in the skills needed to perform day-to-day tasks. Over the next few years, employees across many functions will likely be required to understand how to work and interact with AI. On the flip side, AI is also expected to generate new jobs centred around AI implementation, training, and maintenance.

Privacy Concerns Are On The Rise: Concerns around personal data privacy have been on the rise for years as businesses, particularly tech companies and social media platforms, have increased the amount of personal data they are collecting. This concern is not entirely unfounded. The most common type of data stolen in data breaches continues to be customer and employee personal identifiable information. As generative-AI models become more widely used and more and more personal data is stored, we expect increased regulation around data privacy and cybersecurity incidents as the world races to regulate AI. In the U.S., [Biden's AI Executive Order](#) is the first example of this.

All figures in U.S. dollars unless otherwise stated.

For required regulatory disclosures please refer to "Important Disclosures" beginning on page 19.

Stephanie Price, CFA
Analyst
+1 416-594-7047
Stephanie.Price@cibc.com

Scott Fletcher, CPA, CA
Analyst
+1 416-956-3229
Scott.Fletcher@cibc.com

Erin Kyle, CPA
Associate
+1 416-313-9851
Erin.Kyle@cibc.com

Sam Schmidt, CPA
Associate
+1 416-980-5448
sam.schmidt@cibc.com

Sector:

Information Technology



Environmental



Social



Governance



Artificial Intelligence Vs. Data Analytics

The AI frenzy has resulted in the term “AI” being misused often. It is important to distinguish between AI and analytics before discussing the ESG impact of AI. Different than data analytics, pure AI is able to make assumptions, to test, and to learn on its own. AI systems are dynamic, improving as they analyze more data and learn from experience.

Data Analytics

Traditional data analytics involves the aggregation of vast volumes of data in order to report results, find patterns or identify relationships. Data analytics does not make its own assumptions and functions by traditional scientific method: an individual makes an assumption (forms a hypothesis); data is collected to test the theory; and if the theory is validated or proven, then more testing is performed on additional data.

Predictive Analytics

Predictive analytics is the next step after data analytics. Predictive analytics uses collected data, often from a variety of sources, to predict some future outcome. Companies often use predictive analytics to gain further insight into areas such as customer behaviour. A key distinction between predictive analytics and AI is that traditional predictive analytics still requires human interaction to create and test its assumptions, and the algorithms still require a pre-determined set of rules (i.e., humans form the assumptions).

Machine Learning

Machine learning is the next leg up from predictive analytics, and it is where artificial intelligence truly starts. In machine learning, the system can make its own assumptions, test them and learn from them. The algorithm is simply provided the data and is not told what to look for in the data. Machine learning models are designed to continuously learn and evolve from mistakes as they process more data.

Generative AI

Generative AI, which builds on machine learning and is what’s really behind the recent “AI boom”, is a machine-learning-based content generation model. Users enter data or a question into the system, and the system generates newly synthesized content such as text, images, video, sounds, or animations. Generative-AI models can learn unsupervised, taking a large set of unlabeled data to form foundation models. The early foundation models, sometimes also called general-purpose AI, are GPT-3, GPT-4, BERT, T5 and DALL-E, and can be built upon to develop more advanced and complex models: ChatGPT was built on GPT-4.

Environmental: More Data = More Energy & Water

Data centres consume massive amounts of energy, and the need for more of them has been steadily increasing over the past few years thanks to the growth of cloud-based technologies and the increase in remote work. According to data from the International Energy Agency (IEA), global data centre electricity consumption in 2022 was estimated to be between 240-340 TWh, or around 1%-1.3% of global final energy consumption (excluding energy used for cryptocurrency mining). Overall global energy consumption has increased significantly in recent years, and data centre energy usage is a key contributor to that. Energy consumption from data centres increased in the range of 20%-70% over 2015 to 2022 (Exhibit 1). A notable statistic from the International Energy Agency (IEA) is that combined electricity use by tech giants Amazon, Microsoft, Google, and Meta has more than doubled from 2017 to 2021.

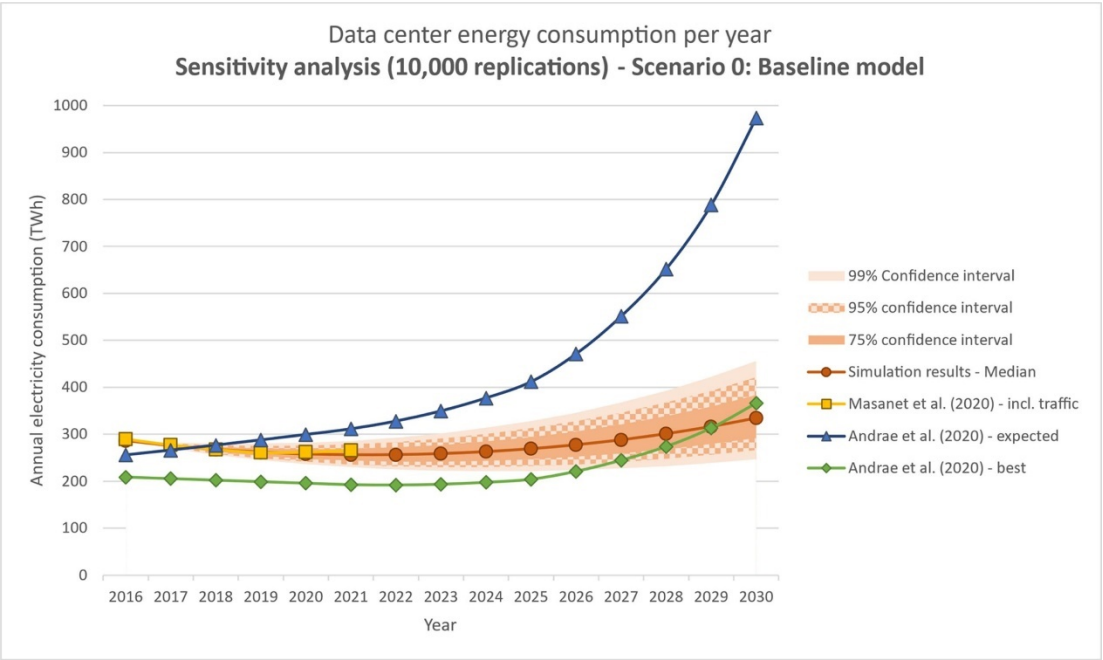
Exhibit 1: Global Trends In Digital And Energy Indicators, 2015 Vs. 2022

	2015	2022	Change
Internet Users	3 Billion	5.3 Billion	78%
Internet Traffic	0.6 ZB	4.4 ZB	600%
Data Centre Workloads	180 million	800 million	340%
Data Centre Energy Usage (excluding crypto)	200 TWh	240-340 TWh	20%-70%
Crypto Mining Energy Use	4 TWh	100-150 TWh	2300%-3500%
Data Transmission Network Energy Use	220 TWh	260-360 TWh	18%-64%

Source: IEA and CIBC World Markets.

Data centres are projected to continue to increase in their electricity consumption, both from increased computing capacity and the addition of more data centres globally. According to research conducted at the University of Twente and published by Elsevier, electricity usage of data centres is projected to increase to close to 1,000 TWh by 2030, as displayed by the chart in Exhibit 2.

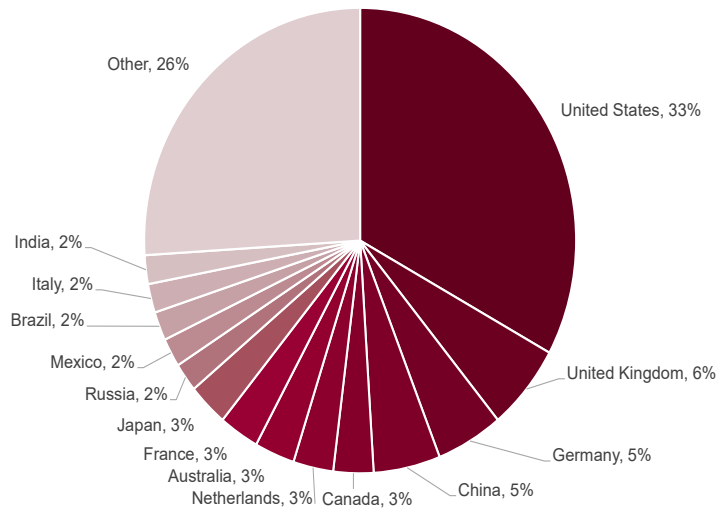
Exhibit 2: Global Data Centre Electricity Usage, 2016-2030E



Source: Elsevier, Applied Energy, Volume 291, June 2021.

The United States has the largest share of data centres globally, at 33%, per the circle chart in Exhibit 3. As of 2021, there were ~8,000 data centres globally, with ~2,600 data centres in the U.S. Using the IEA’s reported 2022 global data centre energy consumption average of 290 TWh, and assuming 8,000 data centres globally (while also assuming even consumption across each, which is unlikely considering differing electrical grids as well as the varying sizes of each data centre), one data centre consumes approximately 3,600 MWh annually on average.

Exhibit 3: Share Of Global Data Centres By Major Country (%)



Source: CloudScene and CIBC World Markets.

AI Is An Energy Intensive Business

As advanced AI tools become more common, energy consumption is set to climb sharply due to the requirements of AI applications, specifically generative-AI models which burn more energy than conventional software given the additional compute power required. Generative-AI models run on GPU chips which require 10-15 times more energy than traditional CPU chips. GPU chips, or graphics processing units, are used in a wide range of applications but are most well known for their use in gaming for graphics and video rendering. They've now become popularized for generative AI for the rendering of images, animations and other outputs. GPU chips are designed to break down complex tasks into smaller subtasks that can be continuously performed – necessary for AI models, which require running computations on massive amounts of data quickly.

The generative-AI sector is growing incredibly fast and has limited transparency given its relative lack of regulation so far. As such, it is difficult to estimate the environmental impact of generative-AI models; however, researchers are currently suggesting that AI's carbon footprint could be as bad or worse than crypto mining. To put that into context, crypto mining consumed 100-150 TWh in electricity in 2022 based on data from the IEA. Research from Gartner also suggests that if current AI practices remain unchanged, the energy needed for machine learning training, data storage and processing could account for 3.5% of global electricity consumption by 2030. However, we believe GenAI is much more likely to create value compared to crypto mining.

Determining the overall environmental impact is further complicated by the fact that the level of emissions depend on what type of power feeds the grid of the data centre running the model, driving large variations. The type of model being run and the number of parameters on which it is trained are also factors. That being said, research conducted by Dr. Sasha Luccioni, AI Researcher & Climate Lead at HuggingFace Inc., estimated that training OpenAI's GPT-3 model consumed 1,287 MWh, which is roughly equivalent to the annual household energy consumption of 120 U.S. homes. Data from this study is summarized in Exhibit 4 below.

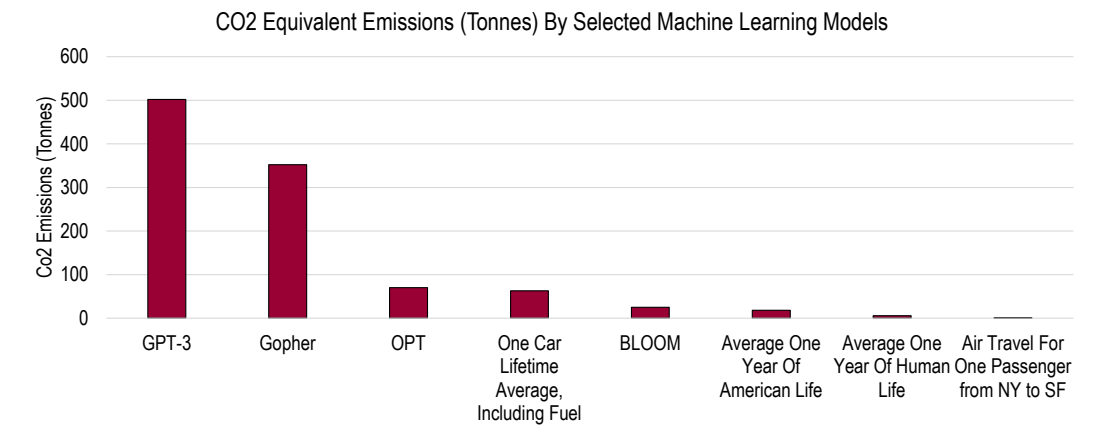
Exhibit 4: Environmental Impact Of Machine Learning Models

Model	Number Of Parameters	Datacentre Power Usage Effectiveness (PUE)	Grid Carbon Intensity	Power Consumption	CO2 Equivalent Emissions	CO2 Equivalent Emissions X PUE
Gopher	280B	1.08	330 gCO2eq/kWh	1,066 MWh	352 tonnes	380 tonnes
BLOOM	176B	1.20	57 gCO2eq/kWh	433 MWh	25 tonnes	30 tonnes
GPT-3	175B	1.10	429 gCO2eq/kWh	1,287 MWh	502 tonnes	552 tonnes
OPT	175B	1.09	231 gCO2eq/kWh	324 MWh	70 tonnes	76.3 tonnes

Source: Luccioni et al., 2022.

The bar graph in Exhibit 5 compares the carbon emissions from each of the models tested relative to real-life examples. Notably, training GPT-3 emits carbon emissions equivalent to the lifetime emissions of almost 100 people. Research suggests that GPT-4 is trained on 570 more parameters than GPT-3, meaning the total energy usage for GPT-4 (the foundation model for ChatGPT) is likely much higher.

Exhibit 5: CO2 Equivalent Emissions By Machine Learning Model, 2022

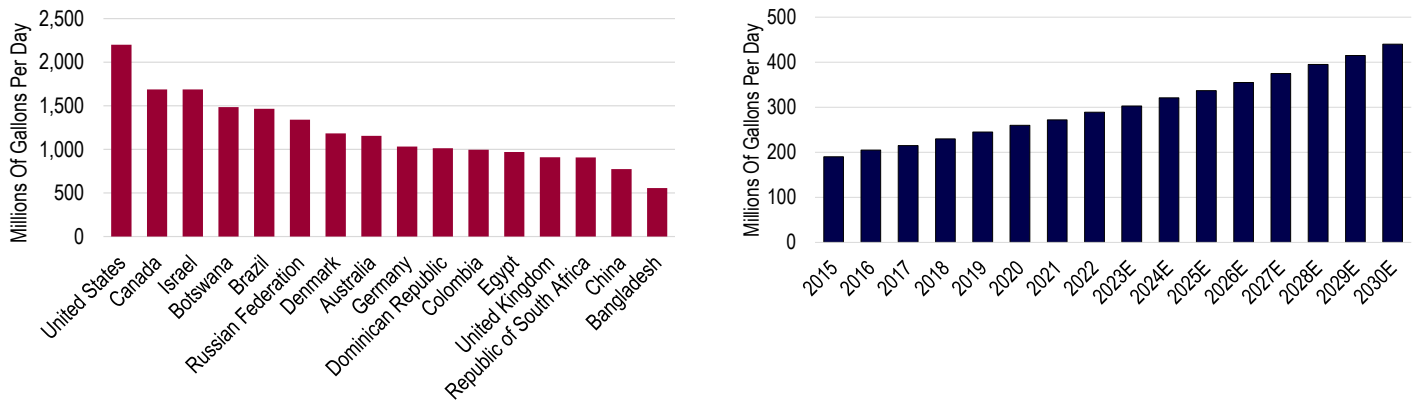


Source: Stanford University AI Index 2023 Annual Report and CIBC World Markets.

Thirsty For Fresh Water

While the electricity consumption from data centres is a key concern, experts estimate that electricity only represents ~10% of data centre CO2 emissions. The remainder comes from their infrastructure, including building and cooling systems. Given the large amount of energy that data centres require, they generate a lot of heat – which in turn requires cooling in order to prevent systems from overheating, failing, or catching fire. Currently there are two options used for cooling these systems: traditional air conditioning and evaporative cooling, which involves large quantities of water. Most data centres use evaporative cooling as it is less expensive than air conditioning. Data centres also pull from clean, freshwater sources in order to avoid corrosion or bacteria growth from seawater and to control humidity, meaning the available water supply in some regions for cooling is already a scarce resource.

Taking one tech giant as an example, Google currently has 14 data centres spread out across North America, and the company reported that it consumed 5.2 billion gallons of water for its data centres in 2022, a 20% increase over 2021 levels. Several of Google’s data centres are also located in warm states such as Texas, meaning they require even more water to cool. AI model training is expected to increase this number. Research suggests that training for GPT-3 alone consumed 185,000 gallons of water, and an average user’s conversation with GPT-3 is the equivalence of dumping out a large bottle of water. GenAI models run on thousands of high-speed GPU chips and, put simply, the faster the processing power of the chips, the hotter they become and the more cooling is required. The bar charts in Exhibit 6 show the current estimated global water usage by country and the projected global data centre water consumption in millions of gallons per day, to 2030.

Exhibit 6: Current Global Water Usage By Country (Left); Projected Global Data Centre Water Usage, 2015-2030E (Right)

Source: Water Footprint Network, Bluefield Research, and CIBC World Markets.

Searching For Greener Energy Sources For Hyperscalers

Despite these data points, it should be noted that most of the tech giants have recently set carbon-free energy targets following increased scrutiny for their water consumption. As global climate conditions worsen and water scarcity becomes a more pressing concern, water conservation from data centres has become an essential aspect of data centre sustainability. Google has pledged to operate on 24/7 carbon-free energy by 2030, and a blog post from November 2022 detailed some methods the company plans to use to achieve this target. Google reported that the company uses reclaimed or non-potable water at 25%+ of its data centre campuses by recycling local municipal wastewater. AWS has pledged to be water positive by 2030, returning more water than it uses, and Microsoft has pledged the same despite the company's water consumption jumping 34% Y/Y in 2022 due in part to generative-AI workloads.

As the cloud transition continues and we enter the 'Age of AI', the importance of the energy source for cloud providers will become even more important in reducing the carbon footprint of AI. Research from Menlo, which surveyed 450 enterprise executives across the U.S. and Europe, revealed that enterprise buyers of AI spend 35% of their infrastructure dollars on foundational models like those from OpenAI and Anthropic, and that most enterprises purchase off-the-shelf models with only 10% of enterprises pre-training their own models. Researchers from Google and the University Of California, Berkley found that the geographic location for machine-learning workload scheduling can result in carbon emissions varying by 5x-10x, even within the same country and the same organization given differences in the fraction of carbon-free energy and resulting CO2 emissions.

Providers of the large foundation models will have the largest footprint, given the energy needs discussed above and the expectation that most companies will use existing LLMs from large vendors or cloud providers. With this context, the energy source of hyperscalers' data centres can make a significant difference to total AI energy consumption. For example, Google is currently building a \$735 million data centre in Quebec, where the electricity grid is almost 100% renewable power (94% hydro and 5% wind), and has made commitments to shift to 24/7 carbon-free energy by 2030.

Applying Generative AI To Optimize Renewable Energy

Generative AI is being applied across multiple industries to further scientific research, and environmentalism is no exception. AI can be used to predict energy demand, help optimize solar and wind farms, and advance power grid reliability. Demand-forecasting AI tools are now being used to predict when demand spikes will occur, discharging energy to keep customers' grid-supplied electricity below a set point, and helping to control costs.

IBM recently developed a program for the U.S. Department of Energy Efficiency & Renewable Energy's SunShot Initiative, using self-learning weather models trained on datasets of historical weather data and real-time measurements from local weather stations, satellite imagery and cameras, to drive a 30% improvement in the accuracy of solar forecasting which helped decrease electricity generation costs. Some other examples of AI being used to improve the environment include:

- DroneDeploy is using AI to assess solar farm layouts to maximize energy generated per site and to monitor the health of solar panels and other equipment.
- The Edge Company is tracking endangered birds near offshore wind farms to provide operators with real-time suggestions to help prevent collisions and shutdowns.
- Eneryield is using AI to detect signal anomalies in undersea cables and predict equipment failures.
- Open Climate Fix has built transformer-based AI models trained on satellite data used to predict weather patterns and improve predictions of solar energy generation by 3x.
- Tying optimization back to data centres, software company Ecolibrium uses IoT, artificial intelligence and machine learning to measure ~280 different points across data centre facilities and create a digital twin, which identifies whether the centre operates efficiently and suggests ways to reduce energy, emissions, water and costs.

How Our Coverage Scores

Within our coverage, 69% of companies provide ESG reports. The majority are guided by either Sustainability Accounting Standards Board (SASB) standards or Task Force on Climate-related Financial Disclosures (TCFD) framework, and 30% of our companies include an SASB Index referencing the applicable standards within their report. Within our coverage, Open Text, CGI, and Docebo score the highest in terms of environmental disclosures, and Kinaxis and Softchoice are also among the strongest, demonstrating that strong ESG governance can be achieved within smaller companies. The table in Exhibit 7 details the environmental metrics disclosed for our coverage.

Exhibit 7: Software & Services – Disclosure Of Environmental Metrics, 2022

Company Name	Environment Disclosure							Data Availability		Targets		
	ESG Report	Guided By SASB Or FCFD	SASB Disclosure	GRI	TCFD Disclosure	UN SDGs	Energy Usage	Water Consumption	Waste Management	GHG Emission Reduction	Energy Reduction	Net-zero Goals
Altus Group Limited	Y	Y	N	N	N	N	Y	Y	N	N	N	N
Constellation Software Inc.	N	N	N	N	N	N	N	N	N	N	N	N
Converge Technology Solutions Corp.	N	N	N	N	N	N	N	N	N	N	N	N
Docebo, Inc.	Y	Y	Y	N	N	Y	Y	Y	N	Y	Y	Y
Descartes Systems Group Inc.	Y	Y	N	N	N	N	N	N	N	N	N	N
Enghouse Systems Limited	Y	N	N	N	N	N	N	N	N	N	N	N
CGI Inc. Class A	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
Kinaxis, Inc.	Y	Y	Y	N	Y	Y	Y	N	N	N	N	N
Open Text Corporation	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Softchoice Corporation	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	N
Dye & Durham	N	N	N	N	N	N	N	N	N	N	N	N
Information Services Corp	N	N	N	N	N	N	N	N	N	N	N	N
TELUS International (CDA), Inc.	Y	N	N	N	N	Y	Y	Y	N	Y	Y	Y

Source: Company reports, FactSet and CIBC World Markets Inc.

Social: Will AI Change The Workplace?

The “S” in ESG has long been associated with areas such as workforce composition, diversity targets, human rights, and health and safety. When generative AI went mainstream, it brought about the same concerns that are always raised when new technologies are debuted, namely that AI would lead to job losses. In fact, the World Economic Forum released an article in October 2020 estimating that AI would likely eliminate 85 million jobs globally by 2025. However, the same article also surmised that AI would generate 97 million new jobs. Given current generative-AI use cases (listed in Exhibit 8), it is estimated that jobs high in automation, routine and repetition (e.g., retail sales or clerical work) are the most exposed to displacement. Within that context, a key area of concern is AI’s impact on gender diversity.

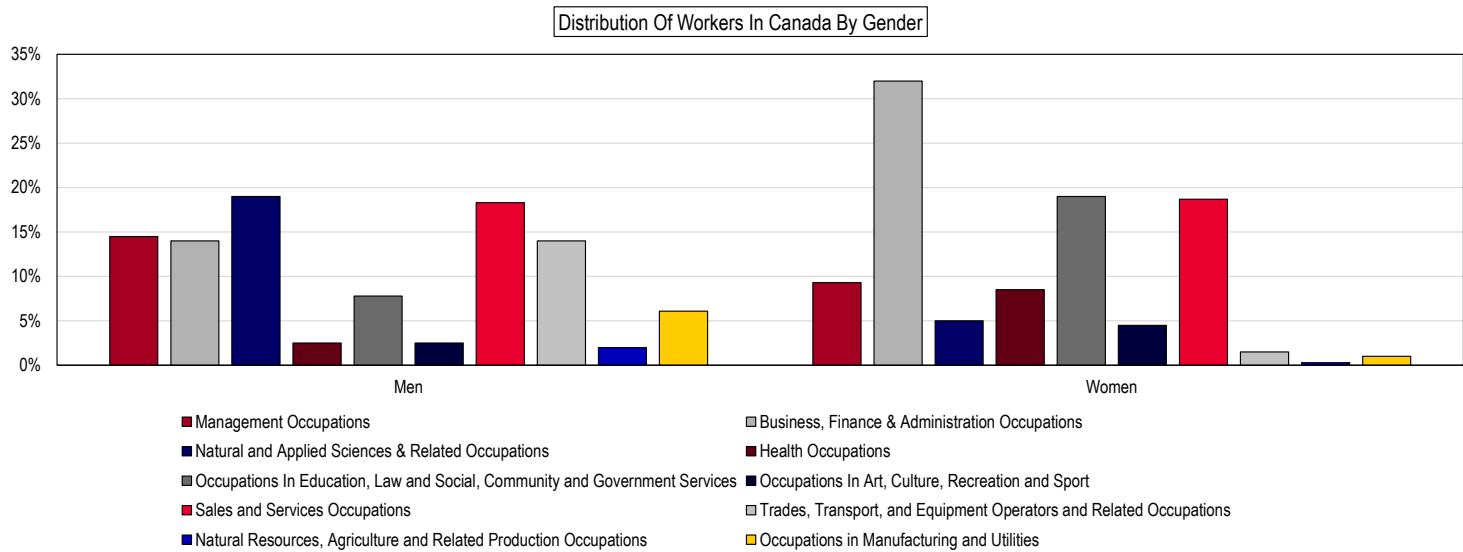
Exhibit 8: Common Generative-AI Use Cases

Language	Visual	Auditory
Content Marketing	Video Generation	Music Generation
Note Taking	3D Models	Voice Generation
Gene Sequencing	Design	
Code Development	Image Generation	
Essay Generation		

Source: Nvidia and CIBC World Markets.

A study from Statistics Canada published in 2020 found that 44.4% of women in the paid workforce faced a moderate to high risk of automation-related job transformation, compared to only 34.8% of men. This disadvantage could be in part due to the higher number of women employed in business, finance and administration operations relative to men, as well as sales and service operations, with the two accounting for roughly ~50% of the female workforce (as illustrated by the bar chart in Exhibit 9). These two categories capture retail sales and clerical work, both potential candidates for AI-related displacement.

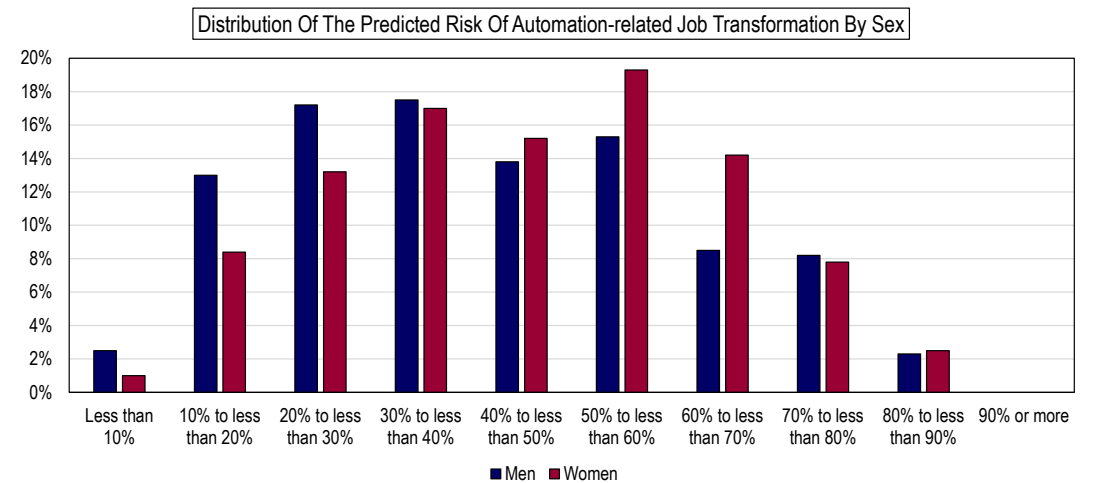
Exhibit 9: Statistics Canada Distribution Of Adult Workers In Canada By Gender, 2016



Source: Statistics Canada and CIBC World Markets.

The bar chart in Exhibit 10 shows the probability of facing automation-related job transformation for men vs. women as found by a Statistics Canada study. Results showed that women were far more likely to face a moderate to high (50%-70%) risk of job transformation vs. men, with 44.4% of women in this category vs. 34.8% of men.

Exhibit 10: Statistics Canada Distribution Of Predicted Automation Risk By Gender



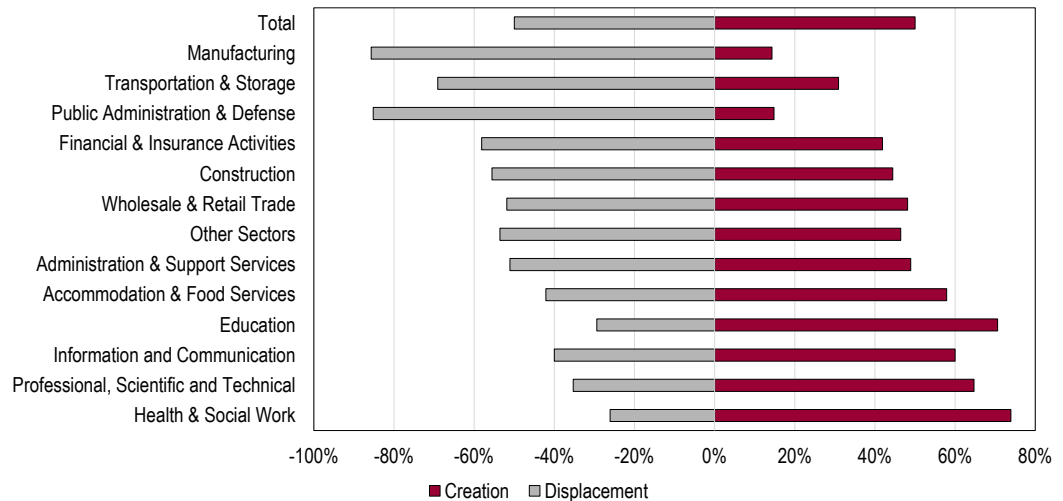
Source: Statistics Canada and CIBC World Markets.

This data is consistent with other studies on the topic, including a recent article published by Princeton University that suggested high-income, white-collar jobs were the most exposed to changes from generative AI. The study further concluded that developing policy to help minimize any disruptions from AI job losses will be important, as the effects of generative AI will most likely disproportionately impact certain demographics and occupations.

AI Will Create New Jobs Too

So far, we’ve seen some large corporations like IBM and BT Group cut jobs in favour of artificial intelligence. IBM announced plans to halt hiring and replace 7,800 jobs with AI over the next five years, and BT Group stated it expects to replace 10,000 jobs with AI by 2030. In a year where tech layoffs are already at all-time highs, AI is being seen as a helpful cost-cutting tool. Although headlines such as “AI could replace 85 million jobs” have continued to fuel fears of an AI takeover, it’s important to consider that the World Economic Forum also estimated AI would create 97 million jobs.

Widespread adoption of AI tools has accelerated demand for data scientists and engineers globally. However, the newness of the technology combined with its rapid adoption across all industries should lead to the emergence of new job positions, such as those focused on AI implementation, training, and maintenance. While many industries have been adopting machine learning technology for years, the emergence of generative-AI tools provides opportunities for even low-automation sectors to benefit from the technology. A report from PwC UK on job creation and displacement from AI estimated that the healthcare industry will benefit the most from the use of AI. The bar chart in Exhibit 11 details the estimated displacement and creation across industries.

Exhibit 11: PwC Estimated Job Displacement & Creation From AI, 2017-2037

Source: PwC and CIBC World Markets.

In total, AI and related technologies are projected to create as many jobs as they displace over 2017-2037; however, the impact by sector will vary. PwC estimates the health and social work sectors could see employment increase by around 20%, though this is in part due to an expectation that healthcare will be increasingly in demand as society becomes wealthier and the population ages.

New Tech Means New Skills

While healthcare jobs are at a lower risk of being eliminated by AI jobs, the sector may still face substantial changes in cases where machine learning is introduced. Some of the ways we've already seen healthcare organizations embrace AI include the following:

- 24/7 virtual health assistants and chatbots
- drug discovery
- AI-assisted robotic surgery
- AI-assisted clinical diagnosis
- automated workflow and administrative tasks

As AI assistance becomes more and more common in the healthcare sector, familiarity with AI tools will likely become a requirement for healthcare professionals. This will likely include understanding AI algorithms, and more specifically their limitations and biases. As AI handles more repetitive tasks and the analysis of data, it is expected that doctors and nurses will be able to spend more time on patient care. The concept of using AI-based technologies in healthcare provides an appropriate segue into our final topic: privacy and data protection.

Strong Diversity Disclosure

Our covered companies have relatively strong disclosure on diversity and inclusion. Approximately 60% of them have set specific minimum targets for women or visible minority representation on the Board or management. Our coverage has on average 38% women directors, 32% women employees, and 30% employees of a visible minority as shown in the table in Exhibit 12.

Exhibit 12: Software & Services – Disclosure Of Diversity Metrics, 2022

Company Name	Diversity Targets?	% Women Directors	% Women Employees	% Visible Minority
Altus Group Limited	Y	50%	28%	26%
Constellation Software Inc.	N	38%	36%	30%
Converge Technology Solutions Corp.	Y	33%	26%*	8%*
Docebo, Inc.	Y	29%	14%**	N/A
Descartes Systems Group Inc.	N	40%	31%	26%
Enghouse Systems Limited	N	43%	29%**	N/A
CGI Inc. Class A	Y	31%	34%	48%***
Kinaxis, Inc.	Y	43%	28%	40%
Open Text Corporation	Y	36%	30%	27%
Softchoice Corporation	N	25%	39%	33%
Dye & Durham	Y	14%	22%**	N/A
Information Services Corp	N	30%	56%**	N/A
TELUS International (CDA), Inc.	Y	80%	50%**	13%**

Note: board representation as of current board; all other data as of most recent ESG Report or Circular.

* Represent number in management positions

** Represents number in executive positions.

*** U.S. only

Source: Company reports, FactSet and CIBC World Markets Inc.

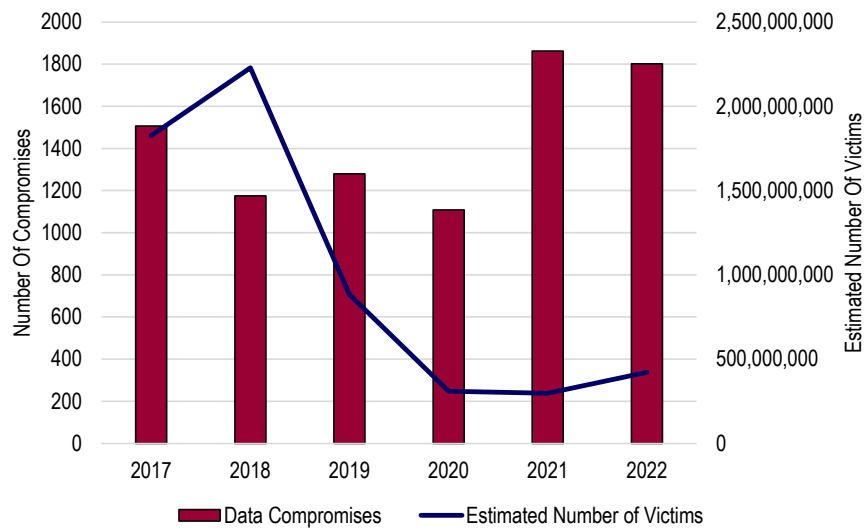
Governance: Privacy Please

As we know, AI systems require vast amounts of data to train their algorithms. Depending on the model's intended use, some of that data may be personal, sensitive and confidential. Concerns around personal data privacy have been on the rise for years as businesses, particularly tech companies and social media platforms, have been reporting increased personal data collection. This concern is not entirely unfounded; the most common type of data compromised in data breaches continues to be customer and employee personal identifiable information (PII), with 52% of cases reported in 2023 involving customer PII and 40% of cases involving employee PII according to data from IBM.

Data Breaches And Their Resulting Costs Continue To Rise

According to data from the Identify Theft Resource Centre (ITRC), 2021 represented the largest number of publicly reported data compromises in a single year in the United States, at 1,862 compromises. Year over year, the number of compromises reported in 2022 was relatively flat at 1,802; however, the estimated number of victims, 422 million, jumped significantly Y/Y. The bar graph in Exhibit 13 shows the number of compromises and estimated number of victims for the last six years.

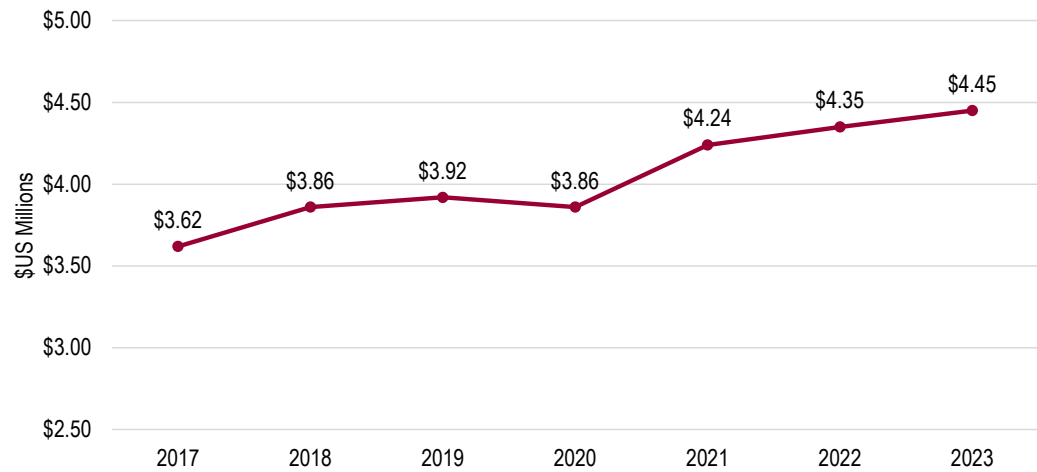
Exhibit 13: Annual Data Compromises Reported In The U.S., 2017-2022



Source: Identify Theft Resource Centre, 2022 and CIBC World Markets.

These data breaches are becoming increasingly costly to organizations. Since 2020, the average total cost of a data breach has increased 15.3%, reaching an all-time high in 2023 at \$4.5 million according to IBM's 2023 Cost of Data Breach Report. The average cost for a data breach in the U.S. specifically is even higher, at an estimated \$9.5 million for 2023. In Canada, it was \$5.6 million.

Exhibit 14: Global Average Total Cost Of A Data Breach, 2017-2023



Source: Ponemon Institute, IBM and CIBC World Markets Inc.

Cloud environments were frequent targets for cyber attacks in 2023. IBM reported that 82% of breaches in 2023 involved data stored in the cloud: public, private or hybrid environments (i.e., cloud and on-premises). Cloud breaches incurred even higher costs, averaging \$4.75 million. The largest percentage of breaches involved data stored across multiple environments, accounting for 39% of breaches in 2023, a number we expect will rise as the cloud transition continues.

Beyond that, the data used to train generative-AI systems as well as the data produced by them are likely to be stored on public or private cloud. For providers of the foundation models, we expect that most, if not all, rely on public cloud infrastructure for data storage;

OpenAI's ChatGPT, Codex and DALL-E 2 use Microsoft Azure's cloud infrastructure to run their compute, storage, database and networking requirements.

Users Are More Concerned About Their Data

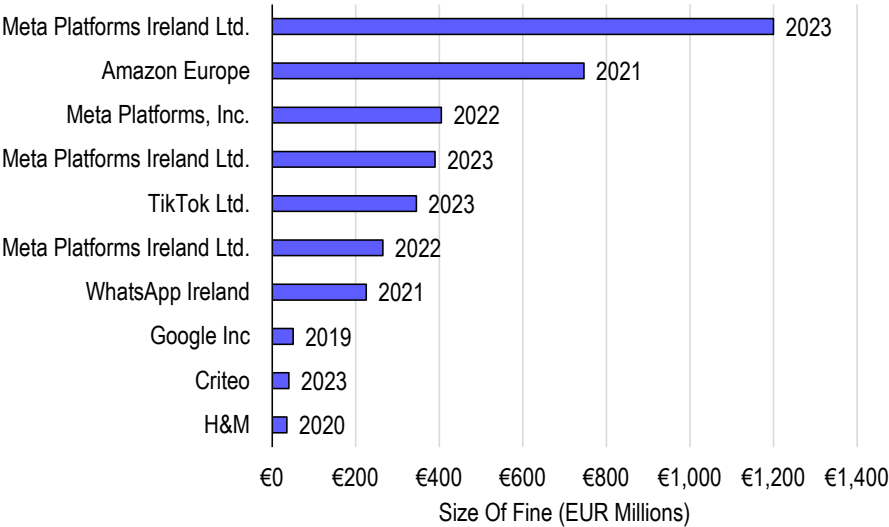
KPMG's 2022 Corporate Data Responsibility Survey revealed an unsurprising statistic: data privacy is a growing concern for 86% of survey respondents. Approximately 68% of those respondents indicated they feel the level of data collection by companies is concerning. A further 64% of respondents said they believe companies are not doing enough to protect consumer data, and ~40% said they did not trust companies to use their personal data ethically.

The AI frenzy has done nothing to slow this growing concern. Given the data-centric nature of AI systems, concerns have been raised around the collection and storage of information used by them. While the data used by generative-AI models varies by industry, in many cases training the data could include PII such as individuals' names, social insurance numbers, home addresses, medical histories, and banking or other financial information. For foundation generative-AI models, what an individual types into the chat interface matters as well. According to an FAQ page published by OpenAI, the company saves and stores ChatGPT conversations for future analysis. This could cause serious privacy issues should confidential documents be fed to ChatGPT for proofreading or summarizing, for example.

The main way to address the increasing risk of personal, private, or confidential information being compromised is through increased regulation. ChatGPT has already faced regulatory troubles: the EU is scrutinizing the application under its General Data Protection Regulation (GDPR), and Italy banned access to the service earlier this year after accusing OpenAI of violating GDPR. Meanwhile, Canada is evaluating privacy concerns under the Personal Information Protection and Electronics Documents Act (PIPEDA). More recently, President Biden unveiled the U.S.'s first [AI Executive Order](#), designed to place safeguards around the use and development of AI, with a key priority centred around cybersecurity and consumer privacy protection.

We expect privacy regulation to continue to grow (and fines to increase). GDPR fines for violations can be up to €20 million or up to 4% of total global revenue, whichever is higher. The bar graph in Exhibit 15 details the top 10 GDPR fines over the last four years.

Exhibit 15: Top 10 GDPR Fines, 2019-2023

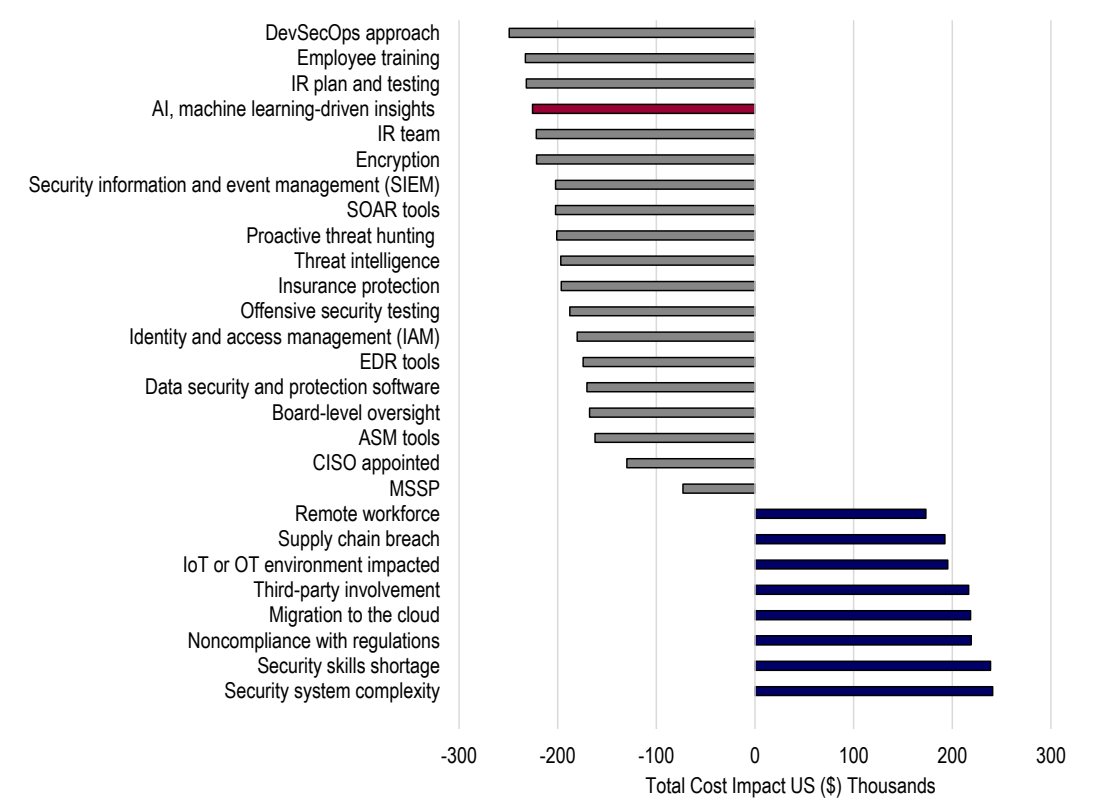


Source: Skillcast and CIBC World Markets Inc.

Adopting Artificial Intelligence In Cybersecurity Is Actually A Benefit

While widespread AI adoption poses additional personal privacy concerns, the effect of extensive use of AI in security and automation has actually been shown to reduce data breach costs and minimize the time to identify and contain security breaches, according to data from IBM. The use of machine-learning driven insights was identified as a cost mitigator to data breaches, with breaches reported by organizations using these tools having an average cost of approximately \$225,000 less than the 2023 mean (Exhibit 16).

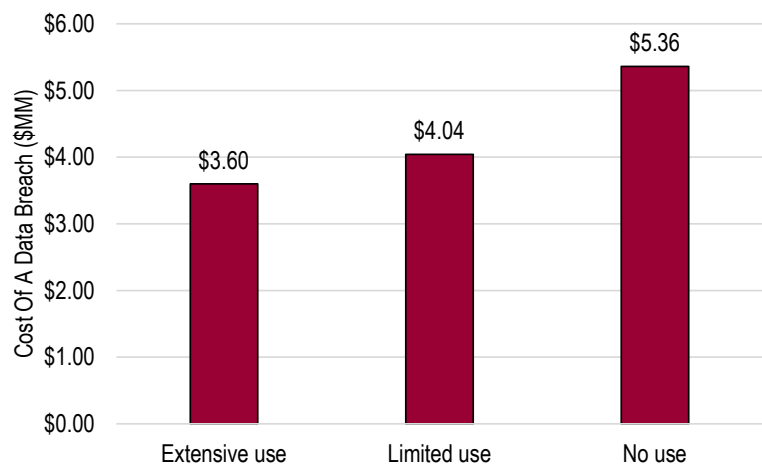
Exhibit 16: Impact Of Key Factors On Total Cost Of A Data Breach, 2023



Source: Ponemon Institute, IBM and CIBC World Markets Inc.

IBM also found that organizations using security AI and automation in their cybersecurity approach (beyond just machine-learning data insights) reported between \$1.3 million to \$1.8 million less in data breach costs compared to organizations that didn’t use those capabilities. More importantly, they were able to identify and contain a breach in 214 days, 108 days fewer than those with no use. The bar graph in Exhibit 17 shows the estimated cost of a data breach for organizations by security AI and automation usage level.

Exhibit 17: Cost Of A Data Breach By Security AI And Automation Usage Level, 2023



Source: Ponemon Institute, IBM and CIBC World Markets Inc.

Cyber Disclosure Is Less Standardized In Our Coverage

While standardizing environmental data has been a focal point for investors over recent years, disclosure around cybersecurity is less consistent. Despite this, over 50% of the companies within our coverage provide disclosure in their ESG reports around their compliance certifications (primarily ISO 27001), compliance with national privacy acts including the EU’s General Data Protection Regulation (GDPR), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), the FTC Privacy Act, the California Consumer Protection Act (CCPA) and others. Fifty-four percent of our coverage provides disclosure on annual employee cybersecurity training, and 23% discloses annual data breaches, as shown in the table in Exhibit 18.

Exhibit 18: Software & Services – Disclosure Of Cybersecurity Data, 2022

Company Name	Alignment with National Institute of Standards and Technology (NIST) Cyber Security Framework?	Compliance Certifications	Data privacy controls Compliance?	Data Breach Disclosure?	Disclosure on Employee cybersecurity training?
Altus Group Limited	Y	ISO 27001	GDPR, PIPEDA, CCPA	N	Y
Constellation Software Inc.	Y	ISO 27001, HITRUST, PCI DSS, SOC-2	PCI DSS, PIPEDA, GDPR	N	Y
Converge Technology Solutions Corp.	Y	N/A	N/A	N	N
Docebo, Inc.	N	ISO 27001, AICPA/ISAE 3000 SOC-2	EU-US and Swiss-US Privacy Shield Certification	Y	N
Descartes Systems Group Inc.	Y	ISO 27001, SOC-2	GDPR, US FTC Privacy Act, PIPEDA	N	Y
Enghouse Systems Limited	N	N/A	N/A	N	N
CGI Inc. Class A	Y	ISO 27001, 27701 at 44 sites	EU BCRs	Y	Y
Kinaxis, Inc.	Y	ISO 27001, SOC-1, SOC-2	GDPR, PIPEDA, US FTC Privacy Act	Y	N
Open Text Corporation	Y	ISO 27001	GDPR	N	Y
Softchoice Corporation	N	N/A	GDPR, CCPA, PIPDEA	N	Y
Dye & Durham	N	N/A	N/A	N	N
Information Services Corp	N	ISO 27001	N/A	N	N
TELUS International (CDA), Inc.	N	ISO 27001, HITRUST, SOC-1, SOC-2	N/A	N	Y

Source: Company reports, FactSet and CIBC World Markets Inc.

Conclusion

Overall, despite the risks that widespread AI use poses to environmental, social, and governance factors, we see significant opportunity for the technology to benefit these areas. While the technology is expected to drive higher energy consumption and create job disruption, we expect the benefit of using AI to improve energy efficiency and job productivity to outweigh these risks. Regarding data protection, despite fears that increased AI use places more personal data at risk, we expect the technology to be widely adopted by cybersecurity teams to improve the speed and accuracy of data breach detection, reducing costs over the long term.

Important Disclosures

Analyst Certification: Each CIBC World Markets Inc. research analyst named on the front page of this research report, or at the beginning of any subsection hereof, hereby certifies that (i) the recommendations and opinions expressed herein accurately reflect such research analyst's personal views about the company and securities that are the subject of this report and all other companies and securities mentioned in this report that are covered by such research analyst and (ii) no part of the research analyst's compensation was, is, or will be, directly or indirectly, related to the specific recommendations or views expressed by such research analyst in this report.

Potential Conflicts of Interest: Equity research analysts employed by CIBC World Markets Inc. are compensated from revenues generated by various CIBC World Markets Inc. businesses, including the CIBC World Markets Investment Banking Department. Research analysts do not receive compensation based upon revenues from specific investment banking transactions. CIBC World Markets Inc. generally prohibits any research analyst and any member of his or her household from executing trades in the securities of a company that such research analyst covers. Additionally, CIBC World Markets Inc. generally prohibits any research analyst from serving as an officer, director or advisory board member of a company that such analyst covers.

In addition to 1% ownership positions in covered companies that are required to be specifically disclosed in this report, CIBC World Markets Inc. may have a long position of less than 1% or a short position or deal as principal in the securities discussed herein, related securities or in options, futures or other derivative instruments based thereon.

Recipients of this report are advised that any or all of the foregoing arrangements, as well as more specific disclosures set forth below, may at times give rise to potential conflicts of interest.

CIBC World Markets Inc. does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that CIBC World Markets Inc. may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decision.

Analysts employed outside the U.S. are not registered as research analysts with FINRA. These analysts may not be associated persons of CIBC World Markets Corp. and therefore may not be subject to FINRA Rule 2241 restrictions on communications with a subject company, public appearances and trading securities held by a research analyst account.

CIBC World Markets Inc. Stock Rating System

Stock Ratings	Abbreviation	Description
Outperformer	OP	Stock is expected to outperform similar stocks in the coverage universe during the next 12-18 months.
Neutral	NT	Stock is expected to perform in line with similar stocks in the coverage universe during the next 12-18 months.
Underperformer	UN	Stock is expected to underperform similar stocks in the coverage universe during the next 12-18 months.
Tender	TR	Shareholders are advised to tender shares to a specific offer as we do not believe a superior offer will materialize.
Not Rated	NR	CIBC World Markets does not maintain an investment recommendation on the stock.
Restricted	R	CIBC World Markets is restricted (due to potential conflict of interest) from rating the stock.

Sector Ratings	Abbreviation	Description
Overweight	O	Sector is expected to outperform the broader market averages.
Marketweight	M	Sector is expected to equal the performance of the broader market averages.
Underweight	U	Sector is expected to underperform the broader market averages.
None	NA	Sector rating is not applicable.

Note: Broader market averages refer to S&P 500 in the U.S. and S&P/TSX Composite in Canada.

CIBC World Markets Inc. Price Chart

For price and performance charts, please visit CIBC on the web at <https://researchcentral.cibccm.com/#/disclaimer-central-new> or write to CIBC World Markets Inc., 161 Bay Street, 4th Floor, Toronto, ON M5H 2S8, Attn: Research Disclosure Chart Request.

Important Disclosure Footnotes

For important disclosure footnotes for companies mentioned in this report that are covered by CIBC World Markets Inc., click here: [CIBC Disclaimers & Disclosures](#)

Ratings Distribution*: CIBC World Markets Inc. Coverage Universe

(as of 30 Nov 2023)	Count	Percent	Inv. Banking Relationships	Count	Percent
Outperformer	159	52%	Outperformer	158	99%
Neutral	131	43%	Neutral	129	98%
Underperformer	7	2%	Underperformer	7	100%
Tender	1	0%	Tender	1	100%
Restricted	6	2%	Restricted	6	100%

Important disclosures for each issuer can be found by visiting the Research Central website at <https://researchcentral.cibccm.com/#/disclaimer-central-new> and then entering the issuer name. Access to our research dissemination policy can be found on the same website at <https://researchcentral.cibccm.com/#/dissemination-policy>. These important disclosures can also be obtained by writing to CIBC World Markets Inc., 161 Bay Street, 4th Floor, Toronto, ON M5H 2S8, Attention: Research Disclosures Request.

Access to CIBC Equity Research

Clients may access CIBC Equity Research online at Research Central at <https://researchcentral.cibccm.com/>, or at the following research aggregators: Bloomberg, Refinitiv, Capital IQ, and FactSet.

Legal Disclaimer

This report is issued by CIBC Capital Markets.

CIBC Capital Markets is a trademark brand name under which Canadian Imperial Bank of Commerce ("CIBC"), its subsidiaries and affiliates (including, without limitation, CIBC World Markets Inc., CIBC World Markets Corp. and CIBC Capital Markets (Europe) S.A.) provide different products and services to our customers around the world. Products and/or services offered by CIBC include corporate lending services, foreign exchange, money market instruments, structured notes, interest rate products and OTC derivatives. CIBC's Foreign Exchange Disclosure Statement relating to guidelines contained in the FX Global Code can be found at <https://cibccm.com/en/disclosures/fx-disclosure-statement/>. Other products and services, such as exchange-traded equity and equity options, fixed income securities and futures execution of Canadian securities, are offered through directly or indirectly held subsidiaries of CIBC as indicated below.

CIBC World Markets Inc. is a member of the Canadian Investor Protection Fund and the Investment Industry Regulatory Organization of Canada. In the United States, CIBC World Markets Corp. is a member of the Financial Industry Regulatory Authority and the Securities Investor Protection Fund. In Luxembourg, CIBC Capital Markets (Europe) S.A. (RCS Luxembourg: B236326) is authorised by the European Central Bank (the "ECB") and supervised by the Luxembourg Financial Supervisory Authority (Commission de Surveillance du Secteur Financier) under the oversight of the ECB. CIBC Australia Ltd (AFSL No: 240603) is regulated by the Australian Securities and Investment Commission ("ASIC"). CIBC World Markets (Japan) Inc. is a member of the Japanese Securities Dealer Association. CIBC (TSX/NYSE: CM) is a bank chartered under the Bank Act (Canada) having its registered office in Toronto, Ontario, Canada, and regulated by the Office of the Superintendent of Financial Institutions. CIBC New York Branch is licensed and supervised by the New York State Department of Financial Services. In the United Kingdom, CIBC London Branch is authorised by the Prudential Regulation Authority and subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Canadian Imperial Bank of Commerce, Sydney Branch (ABN: 33 608 235 847) is an authorised foreign bank branch regulated by the Australian Prudential Regulation Authority (APRA). Canadian Imperial Bank of Commerce, Hong Kong Branch is a registered institution under the Securities and Futures Ordinance, Cap 571, and a limited liability foreign company registered with the Hong Kong Companies Registry. Canadian Imperial Bank of Commerce, Singapore Branch is a wholesale bank licensed and regulated by the Monetary Authority of Singapore.

This report is issued and approved for distribution by (a) in Canada, CIBC World Markets Inc., a member of the Investment Industry Regulatory Organization of Canada ("IIROC"), the Toronto Stock Exchange, the TSX Venture Exchange and a Member of the Canadian Investor Protection Fund and (b) in the United States either by (i) CIBC World Markets Inc. for distribution only to U.S. Major Institutional Investors ("MII") (as such term is defined in SEC Rule 15a-6) or (ii) CIBC World Markets Corp., a member of the Financial Industry Regulatory Authority ("FINRA"). U.S. MIIs receiving this report from CIBC World Markets Inc. (the Canadian broker-dealer) are required to effect transactions (other than negotiating their terms) in securities discussed in the report through CIBC World Markets Corp. (the U.S. broker-dealer). CIBC World Markets Corp. accepts responsibility for the content of this research report.

Distribution to Institutional Customers Only

Canada

This report is provided, for informational purposes only, to institutional investor and retail clients of CIBC World Markets Inc. in Canada, and does not constitute an offer or solicitation to buy or sell any securities discussed herein in any jurisdiction where such offer or solicitation would be prohibited.

Legal Disclaimer (Continued)

United States

This report is provided, for informational purposes only, to Major US Institutional Investor clients of CIBC World Markets Corp. in the United States, and does not constitute an offer or solicitation to buy or sell any securities discussed herein in any jurisdiction where such offer or solicitation would be prohibited.

United Kingdom

The distribution of this report in the United Kingdom is being made only to, or directed only at, persons falling within one or more of the exemptions from the financial promotion regime in section 21 of the UK Financial Services and Markets Act 2000 (as amended) ("FSMA") including, without limitation, to the following:

- authorised firms under FSMA and certain other investment professionals falling within article 19 of the FSMA (Financial Promotion) Order 2005 ("**FPO**") and directors, officers and employees acting for such entities in relation to investment;
- high value entities falling within article 49 FPO and directors, officers and employees acting for such entities in relation to investment; and
- persons who receive this presentation outside the United Kingdom.

The distribution of this report to any other person in the United Kingdom is unauthorised and may contravene FSMA. No person falling outside such categories should treat this report as constituting a promotion to them or rely or act on it for any purposes whatsoever.

This report is distributed solely to eligible counterparties or professional clients and not retail clients as defined in point (8) of Article 2 of Regulation (EU) No 2017/565 as it forms part of UK domestic law by virtue of the European Union (Withdrawal) Act 2018.

All other jurisdictions

This report is distributed solely to institutional clients and not retail clients as defined by the applicable securities legislation and regulation to which CIBC Capital Markets may be subject in any jurisdiction, and only in compliance with all applicable laws and regulations.

The securities mentioned in this report may not be suitable for all types of investors. This report does not take into account the investment objectives, financial situation or specific needs of any particular client of CIBC World Markets. Recipients should consider this report as only a single factor in making an investment decision and should not rely solely on investment recommendations contained herein, if any, as a substitution for the exercise of independent judgment of the merits and risks of investments. The analyst writing the report is not a person or company with actual, implied or apparent authority to act on behalf of any issuer mentioned in the report. Before making an investment decision with respect to any security recommended in this report, the recipient should consider whether such recommendation is appropriate given the recipient's particular investment needs, objectives and financial circumstances. CIBC World Markets suggests that, prior to acting on any of the recommendations herein, Canadian retail clients of CIBC World Markets contact one of our client advisers in your jurisdiction to discuss your particular circumstances. Non-client recipients of this report who are not institutional investor clients of CIBC World Markets should consult with an independent financial advisor prior to making any investment decision based on this report or for any necessary explanation of its contents. CIBC World Markets will not treat non-client recipients as its clients solely by virtue of their receiving this report.

Legal Disclaimer (Continued)

Past performance is not a guarantee of future results, and no representation or warranty, express or implied, is made regarding future performance of any security mentioned in this report. The price of the securities mentioned in this report and the income they produce may fluctuate and/or be adversely affected by exchange rates, and investors may realize losses on investments in such securities, including the loss of investment principal. CIBC World Markets accepts no liability for any loss arising from the use of information contained in this report, except to the extent that liability may arise under specific statutes or regulations applicable to CIBC World Markets.

Information, opinions and statistical data contained in this report were obtained or derived from sources believed to be reliable, but CIBC World Markets does not represent that any such information, opinion or statistical data is accurate or complete (with the exception of information contained in the Important Disclosures section of this report provided by CIBC World Markets or individual research analysts), and they should not be relied upon as such. All estimates, opinions and recommendations expressed herein constitute judgments as of the date of this report and are subject to change without notice.

Nothing in this report constitutes legal, accounting or tax advice. Since the levels and bases of taxation can change, any reference in this report to the impact of taxation should not be construed as offering tax advice on the tax consequences of investments. As with any investment having potential tax implications, clients should consult with their own independent tax adviser.

This report may provide addresses of, or contain hyperlinks to, Internet web sites. CIBC World Markets has not reviewed the linked Internet web site of any third party and takes no responsibility for the contents thereof. Each such address or hyperlink is provided solely for the recipient's convenience and information, and the content of linked third party web sites is not in any way incorporated into this document. Recipients who choose to access such third-party web sites or follow such hyperlinks do so at their own risk.

Although each company issuing this report is a wholly owned subsidiary of CIBC, each is solely responsible for its contractual obligations and commitments, and any securities products offered or recommended to or purchased or sold in any client accounts (i) will not be insured by the Federal Deposit Insurance Corporation ("FDIC"), the Canada Deposit Insurance Corporation or other similar deposit insurance, (ii) will not be deposits or other obligations of CIBC, (iii) will not be endorsed or guaranteed by CIBC, and (iv) will be subject to investment risks, including possible loss of the principal invested. CIBC Capital Markets and the CIBC Logo Design are trademarks of CIBC, used under license.

© 2023 CIBC World Markets Inc., CIBC World Markets Corp. and CIBC Capital Markets (Europe) S.A. All rights reserved. Unauthorised use, distribution, duplication or disclosure without the prior written permission of CIBC World Markets is prohibited by law and may result in prosecution.