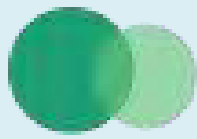
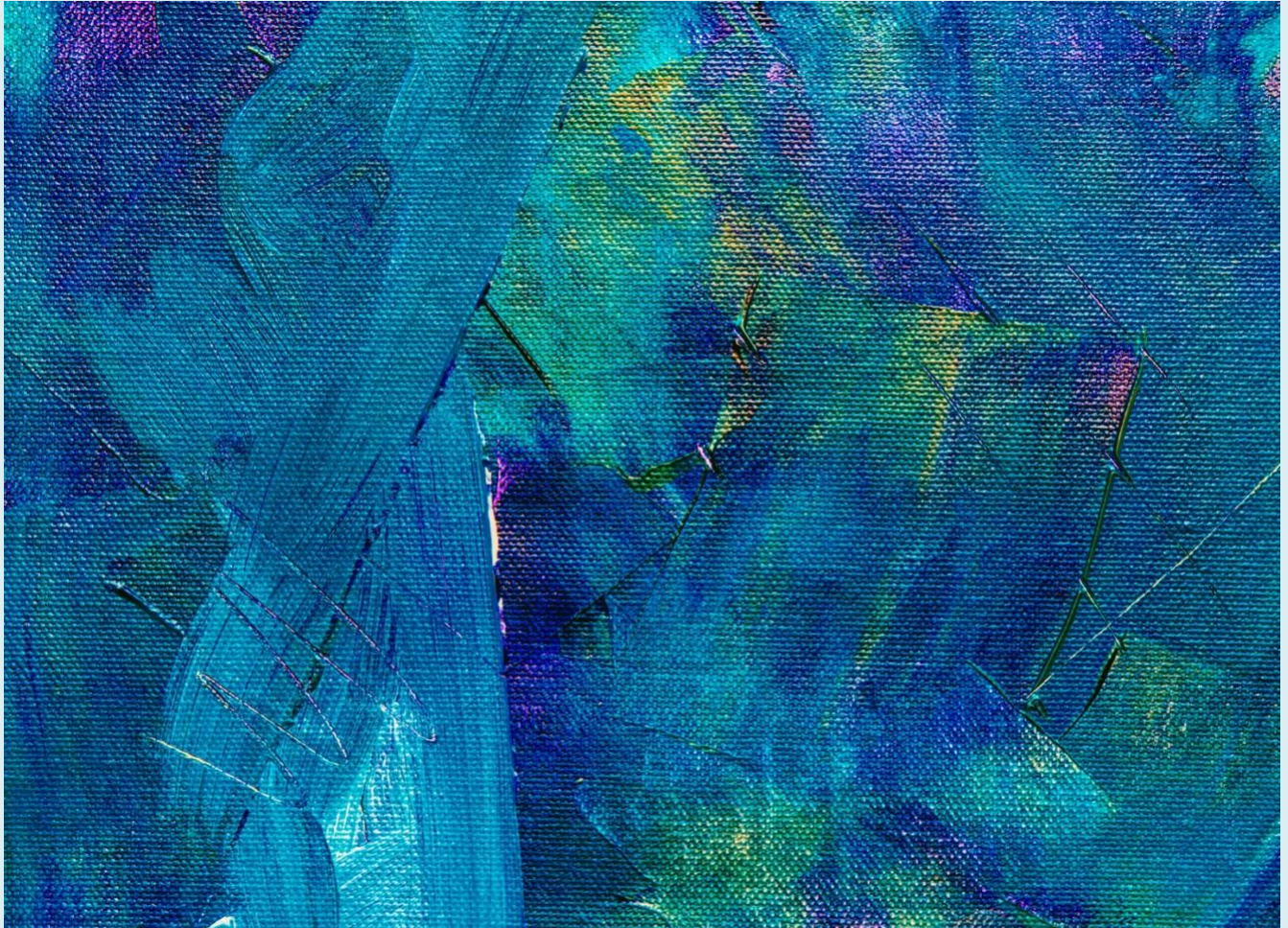


Issue No.18 Fall 2023



***Think*TWENTY20**

The Magazine for Financial Professionals



Risks and Benefits of Integrating AI Into Your Business
What Is the Future of Real-time Corporate Reporting?
Generative Artificial Intelligence and Undesirable Output: Developing a Taxonomy for
Undesirable Output with a Focus on Hallucination
The State of Cybersecurity in Canada
A Wealth Tax Proposal



Number 18, Fall 2023

Editor in Chief: Gerald Trites, Managing Editor: Gundi Jeffrey, Contributing Editor: Eric E Cohen

Email: info@thinktwenty30.com Telephone: (416) 602-3931

Subscription rate, digital edition: To subscribe or buy an issue, go to our secure online store at <https://thinktwenty20-magazine.myshopify.com>. Individual issues - \$10 CDN. Premium Subscriptions, One year - \$30, Two years - \$50.

ISSN 2563-0113

We wish to acknowledge with gratitude the financial support of Heritage Canada.

Cover picture from Pixabay.com

FOUNDING PARTNER



Deloitte.

Canada's Centre for Financial Reporting

Beyond compliance: Promoting excellence in financial reporting in Canada
Keep up to date with the latest in financial reporting at Canada's Centre for Financial Reporting.
The centre features:

- An extensive collection of news and resources on financial reporting, assurance, and regulatory developments relevant to the Canadian marketplace;
- Daily summaries of the activities of the accounting, assurance, and regulatory boards;
- Summaries of developments in the United States that are closely related or might have an impact on IFRS standards; and
- The CFO's corner, where you will find editorials on top-of-mind issues for CFOs.

Website: <https://www.iasplus.com/en-ca>
Contact us: financialreporting@deloitte.ca

A close-up photograph of a single water droplet falling from a green leaf, creating a clear reflection on the surface below. The background is softly blurred, showing more green foliage.

Table of Contents

Editorial.....Pg. 4

By Gerald Trites, FCPA, FCA, Editor in Chief

Risks and Benefits of Integrating AI Into Your Business.....Pg. 5

By Colin Wenngatz, MBA, Jason J Lee and Jeremy Beltgens, CPA, CA

In an increasingly digital and automated world, you're facing more pressure than ever to reduce costs and improve efficiency with the digital tools at your fingertips. Every day, new players are entering the AI market, forcing organizations and finance departments to navigate through an ever-expanding array of technologies and vendors to choose and/or implement the tools that suit their needs.

In Their Own Words: What Is the Future of Real-time Corporate Reporting?.....Pg.10

By Gundi Jeffrey

Real-time reporting and assurance will not only affect business measurement, but also strongly affect business assurance. External sources of data that are close to real time have the potential to progressively implement or replace current audit measures. The role of accountants will change drastically from data preparation and manipulation to information understanding, explanation, and model evaluation.

Generative Artificial Intelligence and Undesirable Output: Developing a Taxonomy for Undesirable Output with a Focus on Hallucination.....Pg. 15

By Eric E. Cohen, CPA

Chatbots based on LLMs generate content based on their internal models, developed through training, and probabilities, and not from "reality." There is no validation of input or output for suitability for specific uses. Thus, results may not be factually correct for numerous reasons.

The State of Cybersecurity in Canada Report by Grant Thornton.....Pg. 24

Summarized by Gundi Jeffrey

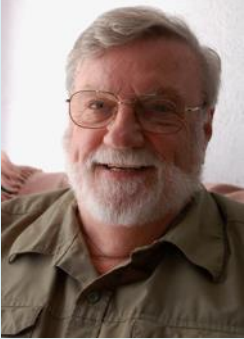
Grant Thornton LLP has released a report on the state of cybersecurity in Canada that provides insights on imminent cybersecurity threats and what businesses can do to protect themselves. According to the report, "as businesses develop new ways to protect themselves from online attacks, cybercriminals are becoming savvier – and finding new weaknesses to exploit. It's important for businesses to be aware of cybersecurity developments to prepare accordingly."

A Wealth Tax Proposal.....Pg. 32

By Jason Fleming, CPA, CA, M.Acc

This article proposes a new, administratively simple, wealth tax for Canada. The goals of this tax are to create income for the federal government and reduce the concentration of wealth. Most Canadians will not be subject to this tax and unlike current taxes it will be relatively easy to comply with.

Editorial



***Gerald Trites, FCPA, FCA, CISA
Editor-in-Chief***

There is little doubt that we are living in an age of revolutionary change, led by AI, particularly since the introduction of ChatGPT last year. In one short year, generative AI, the basis of ChatGPT, has gone from a dazzling curiosity to an important tool for business and many other fields.

After a year of much experimentation and implementation of various new AI-charged applications in business, we have come to the realization that, while gAI is impressive and powerful, it also is capable of generating ‘undesirable’ output. This includes output that is simply wrong, that is inconsistent with the facts, that contains made-up facts. Some people have been referring to many of these undesirables as hallucinations, because they bear some resemblance to human hallucinations. Eric Cohen delves into this issue and others in his article on generative AI this month.

Grant Thornton has been implementing gAI where possible and addresses some of the difficulties, including hallucinations, in their article. Others are encountering similar issues.

As we gain more experience and as gAI continues its astronomical path of growth and improvement, we will see many more issues and opportunities. Definitely the opportunities will prevail and we will see a new world where AI plays a major role is most of what we do. Some refer to it as a new industrial revolution, perhaps the fourth?

It seems to me that this misses the point, that AI is moving us into a new epoch, way beyond anything like an industrial revolution, more like the next level of human activity – an existential revolution.

/GDT

Risks and Benefits of Integrating AI Into Your Business

By Colin Wennatz, MBA, Jason J Lee and Jeremy Beltgens, CPA, CA

In an increasingly digital and automated world, you're facing more pressure than ever to reduce costs and improve efficiency with the digital tools at your fingertips. Every day, new players are entering the AI market, forcing organizations and finance departments to navigate through an ever-expanding array of technologies and vendors to choose and/or implement the tools that suit their needs.



Recent advancements in artificial intelligence through generative AI programs such as ChatGPT and Azure OpenAI have brought AI to the mainstream, further increasing its visibility, and highlighting a significant number of use-cases that have broad applicability.

AI is very good at specific activities such as pattern recognition, anomaly detection, bulk output, context-sensitive predictions, summarization and translation. Combining these strengths enables AI to generate

novel outputs that seem to hold limitless potential. It's imperative, however, to acknowledge the risks and limitations of AI programs and the impact they can have on your business. Understanding both the potential benefits and risks is key to implementing a successful AI strategy.

A primary area of concern revolves around the growing threat of data breaches and cyber-attacks. As businesses and organizations increasingly rely on cloud-based storage solutions, the integration of AI-powered systems opens the door to vulnerabilities susceptible to hacking and manipulation, thereby amplifying security risks.

There are no quick fixes, and all decisions should be made with a focus on specific business requirements. First and foremost, it's crucial to fully understand the problem and then align it with the appropriate technology.

It's imperative to acknowledge the risks and limitations of AI programs and the impact they can have on your business.

Defining AI

Traditional artificial intelligence focuses on utilizing data to automate processes and make predictions. Although these systems can learn and make decisions, that ability does not extend to generating anything new. On the other hand, Generative AI takes AI systems one step further by layering on the ability to create something altogether new – for example, what users now see with ChatGPT. This ability to generate something new has led to much broader applicability and an unprecedented adoption rate by the general public.

AI Benefits

When leveraged appropriately and with a rigorous governance program, AI has immense potential to improve quality, streamline workflows and help businesses run more effectively. It

also enables existing team members to spend less time on mundane repetitive tasks and refocus that effort into value-added and challenging tasks.

AI, particularly generative AI, can significantly enhance the efficiency of finance teams and professionals. When integrating AI into a financial setting, it's often more appropriate to view many AI applications as tools for augmentation rather than full automation. If AI can handle 70 to 80 percent of the workload or provide valuable insights, it typically places you in a better position than if the task were performed entirely manually. In today's environment, most AI systems still require finance professionals to interpret the analysis or finalize the results. This judgment and expertise remain crucial steps in the process.

Opportunities for implementing AI include:

- **Time savings:** AI can increase efficiency by taking on time-consuming tasks that would typically be done by a human. Generative AI can summarize large bodies of text into easy-to-understand language in seconds, can explain complicated topics in a simple way, can help with quick brainstorming, or complete financial workflows.
- **Cost savings:** By enabling AI technology to help with these time-consuming tasks, businesses can allocate resources more efficiently. This includes using AI tools while performing financial analysis, identifying anomalies, journal entry testing and other more repetitive tasks. While AI systems can have material costs for implementation, that often pales in comparison to the associated benefits.
- **Enhance creativity and innovation:** Generative AI helps users think outside the box through idea generation, divergent thinking, problem-solving, and collaborative opportunities.
- **Digital Assistants:** The use of digital assistants continues to gain popularity, and can be effectively applied to specific situations within your business. Examples include responding to more common questions around month-end tasks or completing simpler AR or AP functions.
- **Clearer communication:** Generative AI can provide summarized or simplified versions of complicated information or data sets in seconds, enabling you to share information with a wider audience for increased exposure and understanding.

While AI systems can have material costs for implementation, that often pales in comparison to the associated benefits.

Risks

When implemented correctly, AI can multiply the output of finance teams and organizations; however, if not carefully considered or implemented incorrectly, AI can have the opposite effect. Within the finance or accounting industry, it's imperative to consider these risks before jumping in:

- **Privacy concerns:** As with any application, it's vital to understand how the data you're incorporating into the AI system is being utilized. This includes issues related to privacy, data residency, etc. We are beginning to see many European countries investigating ChatGPT's data storage system, with Italy outright banning the program over alleged

privacy violations related to ChatGPT's collection and management of data. Canada has also introduced The Artificial Intelligence and Data Act (AIDA), which is proposing legislation on the design development and use of AI as early as 2025. Before uploading any of your organization's data into these public systems it is crucial to consider what is being shared and limit or prohibit any proprietary information from the organization being placed into the environment. Many organizations are taking strong stances on the use of systems such as ChatGPT as it can be difficult to define when it's appropriate or not to share or query a particular topic. As a response, organizations are developing their own Large Language Models (LLMs); however, this also comes at a cost and requires domain expertise.

- **Plagiarism, factual inaccuracies, and copyright issues:** While Generative AI is a useful tool for research and creative writing, as with taking from another person's work, it's important to source the information and clearly state that some or all of it came from generative AI. Text and other information provided by ChatGPT and other programs must be edited to ensure there are no incorrect statements, manufactured information, or spelling or grammatical errors. Questions remain over who owns the rights or intellectual property for AI-generated content.
- **Lacking governance:** Organizations must have a structure in place to manage the use of AI technologies to set out best practices and prevent abuse.
- **Rushing to market:** Many companies (OpenAI, Google, Microsoft, etc.) may be rushing to market before the product is safe in order to preserve market share and keep up with the competition.
- **Legal responsibility:** It's still unclear who is legally responsible for actions taken based on information and feedback provided by AI technology. For example, if your client makes a decision based on your AI chatbot with negative outcomes, would they sue you, or the AI manufacturer?
- **Blackbox systems and false positives:** Many off-the-shelf AI systems fall into the category of blackbox, with a level of mystery that can create additional work for finance professionals as they navigate their understanding of outputs and/or false positives. However, many of the leading-edge vendors are demystifying their systems and adopting an explainable AI approach. Demystifying these systems will only enhance adoption rates and lead to better implementations.

Other Considerations

Hallucinations: Hallucinations can occur when a Generative AI model becomes convinced of incorrect facts and responds to questions with made-up answers. Such hallucinations are more likely to occur when prompts are overly vague, which highlights the importance of asking clear and defined questions. The process of structuring text that can be easily interpreted and understood by a generative AI model is referred to as prompt engineering.



Generative AI programs use “temperature” parameters to determine the level of confidence in their predictions. Lower temperatures mean more creative responses, while higher

temperatures equate with greater confidence in the results. But higher temperatures don't necessarily mean the results are more precise.

Generative AI models absorb information from across the internet and from myriad sources, some of which are reliable and trustworthy, and others that are not. It's the sourcing of information, and input from humans, that can cause these programs to present incorrect, misleading and biased information, i.e., hallucinate.

False information can have significant real-world consequences and, while these hallucinations can be addressed, privacy and security concerns must be considered when fine-tuning a model against sensitive or confidential data.

AI-Generated Content, And How to Spot It:

From a risk perspective, knowing how to spot when content was authored, either partly or entirely by AI, will dictate how much you can trust the results.

Look for sentences that lack complexity or contain words that are frequently repeated. When editing content, keep an eye out for scientific facts or citations that don't match up with manual calculations or sources, seemingly correct code that looks out of date or place, and inaccurate or stale data.

Here are a few online tools that can be used to determine if copy has been AI-generated:

- **Content at Scale AI Detector** – Best for casual writing samples
- **Originality.AI** – Best for professional writing samples
- **Open AI Classifier** – In progress. Best for long writing samples

Hallucinations can occur when a Generative AI model becomes convinced of incorrect facts and responds to questions with made-up answers

Best Practices to Adopt a Risk-Based Approach to Using Generative AI

If you're considering implementing the use of ChatGPT or other chatbot programs into your business, there are a few best practices to take when building a plan.

- **Complete a risk assessment** – Identify potential hazards associated with using generative AI, assess those risks and consider steps to control them. Completing tests of its use will be helpful to record how it might work for you and how the proposed controls could mitigate or decrease risk.
- **Define the use case** – Determine how, where and when you would use generative AI and the implications of its use across all elements of your business.
- **Build a governance committee** – Creating a diverse group to provide input will enable you to better characterize what ChatGPT operations will look like and prevent biases.
- **Create policies and procedures** – Make sure to have a set of rules guiding the use and misuse of AI programs. Be proactive in mitigating unwanted or harmful behaviour and document weaknesses or vulnerabilities within the program.

- **Provide training and resources** – In line with developing policies and procedures, training employees on how and when to use chatbots and use parameters is key.
- **Communicate with customers and employees** – Be open and transparent with employees about how introducing generative AI may impact their roles and your expectations of its use. Sharing your intentions with customers and stakeholders is vital to ensuring everyone is on the same page about what role generative AI will play in your business moving forward.



Colin Wenngatz, Partner, Data & Analytics, leads MNP’s Enterprise Analytics program – supporting MNP’s clients across the Country through the development of innovative data-driven solutions. Colin draws on nearly 20 years of experience in corporate strategy, analytics, and program management across varying industries. His specialized focus is on implementing and utilizing analytical platforms and tools to gather data-driven insights in support of optimizing business models, and assessing opportunities for growth and performance improvement.



Jason Lee is a Partner with MNP’s Digital Services team in Toronto. Drawing on more than two decades of experience in technology, project and account management, and innovation labs, Jason solves complex technology and business challenges to help his clients thrive. He is experienced in 3D integration, cloud, gaming, the Internet of Things, artificial intelligence/machine learning, and data. He has been the delivery lead for large enterprise agile transformations and engagements.



Jeremy Beltgens, CPA, CA, Senior Manager, Assurance Innovation, performs a key role in the evaluation, development and deployment of technology and innovative methodologies in the firm. His work with the Assurance Innovation team has focused on transforming MNP’s assurance practice using leading edge innovative technology. He has a lead role in vendor relations, providing functionality guidance to the vendor and collaborating on team member education to maximize value on deployment of products.

Jeremy has led teams with deep skills in data engineering and science, audit execution, technology due diligence, and technology to adopt enterprise scale assurance solutions that are transforming the practice and stimulating a more data driven approach.



In Their Own Words: What Is the Future of Real-time Corporate Reporting?

By Gundi Jeffrey



Gundi Jeffrey is an award-winning business journalist specializing in writing about the accounting profession for various publications in Canada and England. In 1985, she co-founded The Bottom Line, Canada's only independent publication for the accounting and financial professions, serving as its executive editor

What is real-time, or continuous, reporting? The web defines it as a business intelligence tool related to gathering data for users immediately and allowing them to view and access important data as soon as it happens. Users may access this data through an online portal, software platform or similar option, and it's available with the most up-to-date information at all times.

According to some sources, real-time reporting platforms are a great way to stay up-to-date with the latest information and make informed decisions. Some benefits of using real-time reporting include:

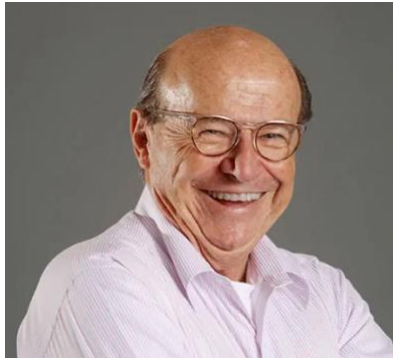
- **Accelerating the decision-making process:** Real-time reporting may help you make decisions more quickly, especially when handling a time-sensitive matter, as it provides the most current data possible.
- **Delivering better customer service:** Real-time reporting provides you with the most accurate representation of performance. This may help you better understand the business's or your client's performance, allowing you to adapt your strategies for better results.
- **Fostering more productive client meetings:** With static reports, clients may not see their performance data until the meeting, giving them little time to review the information and prepare questions.

This type of reporting and assurance are emerging with various forms and motivations. This will not only affect business measurement, but also strongly affect business assurance. External sources of data that are close to real time have the potential to progressively implement or replace current audit measures. The role of accountants will change drastically from data preparation and manipulation to information understanding, explanation, and model evaluation.

As investors are clamoring for more frequent corporate financial reporting, a number of studies are showing that that it can also have a number of negative effects. According to one

study, “frequent reporting can impose significant costs by inducing myopic behavior and distorting managerial investment decisions.”

Others point out that increased competition between businesses requires more up-to-date data to allow company decision makers to respond quickly to opportunities and threats. At the same time, it says, there are a number of challenges to overcome when moving to real-time reporting. And, so, the debate goes on.



ThinkTWENTY20 decided to investigate this controversy by interviewing a well-known expert in the field, Professor Miklos A. Vasarhelyi. He is the KPMG Distinguished Professor of Accounting Information Systems and serves as Director of the Rutgers Accounting Research Center (RARC) & Continuous Auditing & Reporting Lab (CAR Lab).

ThinkTWENTY20: *There has been much discussion about the use of real-time corporate reporting. Are you for or against it?*

Vasarhelyi: Real-time reporting (RTR) is a must to resolve the problem of anachronistic reporting. While a large percentage of stock market trades are performed algorithmically in milliseconds the measurement of business is annual or at best quarterly. Consequently, algorithmic trading uses very little of corporate reporting.

ThinkTWENTY20: *What does “real-time corporate reporting” mean to you, as there are some differences of opinion on this also?*

Vasarhelyi: The nature of RTR has not been defined although some internal corporate reporting systems have alerts and up-to-the-moment figures. Most likely “reporting apps” will emerge that will give flexibility to the users on what is to be seen, collected, distributed, etc.

External sources of data that are close to real time have the potential to progressively implement or replace current audit measures.

ThinkTWENTY20: *How does it differ from the financial reports we are seeing now?*

Vasarhelyi: Mainly up-to-the-moment measures with definable time frames and a plentitude of exogenous variables like social media, weather, foot traffic, IoT measures, sentiment of news pieces, etc.

ThinkTWENTY20: *Have you seen any attempts to use RT Reporting? How did they work out? Why?*

Vasarhelyi: Not yet.... I expect some companies to create future reporting products merging proxies for real-time information with a range of Exogenous variables (EVs).



ThinkTWENTY20: In your opinion, what benefits can real-time reporting bring to financial reporting as we see it now?

Vasarhelyi: A real time economy needs real time numbers.

ThinkTWENTY20: How can companies best use it? In what areas would it be most beneficial?

Vasarhelyi: Internally companies already measure inventory, cash, receivables, payables close to real-time for narrow

management functions and a large number of algorithms are automating some immediate actions. Exogenous variables can add some futurity to information. For example, many searches for a product predict increased sales or indicate poor sales efforts. Analytical extrapolation of historical numbers can be complemented with EV, for example bad weather forecast can predict increased sales of certain products like boards to protect windows, shovels to deal with snow, etc.

ThinkTWENTY20: What are the difficulties inherent in adopting RT Reporting? What are the risks?

The nature of RTR has not been defined although some internal corporate reporting systems have alerts and up-to-the-moment figures.

Vasarhelyi: Although corporations may have great internal reporting schemata, they will always be reluctant to externally disclose the information. I ask my students: Do you like to be graded? Furthermore, information comes with liability. Defective products, employment biases, work accidents, future actions all have their dangers as well as information value for different stakeholders. Also, information of biases against race, nationality, gender and much more is interesting for certain audiences (stakeholders) than others. A large set of the current principles of reporting would have to be completely changed – how to value assets, how frequently (if at all) to do it, how to measure accumulated wealth, how to deal with structural changes, how to measure the pulse of operations, how to compare entities, how to deal with operations in different geographies, how to measure and disclose virtual assets – etc., etc., etc.

Financial reports were created to allow honest trading of corporate stocks in the public market. The information that could be economically provided and relevant in an age of physical asset trading is very different from what can be provided today and what is of interest. Investors would much rather get raw data than data manicured with FASB rules that try to create

comparability and measurement where there is little comparability and anachronistic measurement.



Up-to-Date
List of
RealTime Reports
Dashboards



ThinkTWENTY20: Do you think the benefits outweigh the risks and why?

Vasarhelyi: These types of changes always have unintended consequences and these must be – where possible – anticipated and managed by progressive fine tuning of the rules. For example, consolidation of subsidiaries is obfuscation as it hides valuable details

out of lines of business. There is little reason why more complete information sets of lines of business cannot be provided and it is likely that much of that information can be gathered with EVs and data from data brokers. Society would benefit from some standardization of EVs and industrialization of the information.

Not sure what would be the risks except some privacy and DEI issues that can be carefully managed. Typically, more information leads to better decisions and societal benefits. When the security act of 1933-34 came out, many firms objected disclosing their profit margins as they may be bringing in competition. The disclosures clearly made for better allocation of societal resources. More efficient internal and external information and algorithms would make for a more efficient society.

ThinkTWENTY20: What are the practical limitations of going down this road?

Information comes with liability. Defective products, employment biases, work accidents, future actions all have their dangers as well as information value for different stakeholders.

Vasarhelyi: Difficult to say. Information these days is very cheap but very large amounts of information create costs for storage and processing. As always, these need to be balanced.

ThinkTWENTY20: Could it benefit capital markets overall?

Vasarhelyi: The stock trading algorithms would be more based on performance and future as opposed to price, volume and comparables. These would bring more market efficiency if some of the idiocy of the current standards could be waived. When double entry was published, that type of information was very important to run a business. Today, the financial reporting module of an ERP is not useful to run the business, it is very separate and often provides bizarre information.

ThinkTWENTY20: In your opinion, how uniform or diverse are the opinions of different types of users of this information about the usefulness and demand for such information?

Vasarhelyi: Thomas Edison: “if you asked users about illumination, they would say longer lasting less smelly candles, not the electric bulb. Users are not good evaluators of revolutionary technology.

The current methodology of accounting standard setting does not work for this but requirements and guidance by standard setters will be essential. As Lev and Gu showed in their “end of accounting” book, current published/issued information has lost much relevancy. Waterloo (Professor Efrim Boritz) recently held a “value of data” seminar that showed clearly that our current measurements are not very good and not fulfilling the market homogenization function that is needed.



ThinkTWENTY20: *How do you see this developing and when might we have a world where real-time reporting becomes the standard?*

Vasarhelyi: If you look at the report that was presented in our session, written by very reputable (but conservative) academics reporting on a survey they

performed, obviously there is very little taste for change except among the quants that work in the field. Something very dramatic will need to happen to motivate regulators and politicians to push in this direction. I do expect, however, the emergence of a data provider industry – probably out of the data broker industry.



 **ThinkTWENTY20**

The Magazine for Financial Professionals

Digital Subscriptions are available through
www.thinkttwenty20.com

Standard ads - \$375.00

Logo ads - \$100.00

Contact info@thinktwenty20.com



Generative Artificial Intelligence and Undesirable Output: Developing a Taxonomy for Undesirable Output with a Focus on Hallucination

By Eric E. Cohen



Eric E. Cohen, CPA, is a technologist with a passion for collaboration toward the goal that “a piece of business information, once entered into any system, anywhere, never needs to be retyped as it moved through the business reporting supply chain.” He’s also a prolific author, engaged in virtually every effort to standardize accounting and audit data, a national expert to a wide variety of standards efforts, and co-founder of XBRL.

The year 2023 has brought with it the rise of generative artificial intelligence (gAI), bringing the chatbot to the masses. Different gAIs interact in different ways with users – some factual, reminding the user that it is just a “large language model” (LLM), some programmed to act more like a human, with fun and familiarity, with a façade of a human with feelings, opinions, and interests.

When users feel like there is someone human on the other end, or make some other emotional attachment, they may trust the results provided by the gAI to a greater degree. That’s why it can be jarring when those results are not the ones desired or expected. These undesirable results are often called “hallucinations.”

The term “hallucination” is being used as one of the biggest concerns when using – or perhaps more directly, relying on the output of – a gAI tool based on an LLM. It may, however, be more precise and more helpful when considering how to fix, compensate for, or otherwise leverage the output from a gAI tool.

Chatbots based on LLMs generate content based on their internal models, developed through training, and probabilities, and not from “reality.” There is no validation of input or output for suitability for specific uses. Thus, results may not be factually correct for numerous reasons: the desired output may not have been developed previously, or there is insufficient training data on the topic, or there has been incorrect or adversarial input – LLMs do not inherently possess “common sense.”

Chatbots based on LLMs generate content based on their internal models, developed through training, and probabilities, and not from “reality.”

Even when gAI solutions, such as Bing AI Chat or Google Bard, incorporate search lookup or permit checking through search lookup, they are not reconciling the gAI output with the search output.

As such, responses may sound plausible but be factually incorrect. Citations and references are not drawn from a database, nor are they verified, without some manner of extension or plug in. However, the term “hallucination” may be used for a broader group of undesirable outputs than it should get credit for. Therefore, it may be helpful to develop a taxonomy of gAI undesirable output results, with a focus on hallucinations, as we will describe them.

Brief History

Chatbots are not a new phenomenon, with a start date of November 30, 2022 (when OpenAI delivered ChatGPT to the world and started the generative AI tidal wave). Eliza (1966) was the name of an early gAI chatbot out of MIT, a recent Peabody award winner,¹ often called the world’s first autonomous computer chat program. There are accounts² that the secretary of the scientist who developed the code was one of many who treated Eliza as a confidant. That scientist, Joseph Weizenbaum, went on to write on AI and the need to not rely on it for important decisions, as they lack compassion and wisdom. In his book *Computer Power and Human Reason*,³ he made a distinction between “deciding” and “choosing” – deciding is a computation activity, where choosing comes from judgment, wisdom and compassion, and not calculation. He concludes. “What emerges as the most elementary insight is that, since we do not now have any ways of making computers wise, we ought not now to give computers tasks that demand wisdom.”

Your author has been using chatbots for more than 30 years to help brainstorm and organize his thoughts. Dan E. Burns was the developer of *Thoughtline* (MS DOS) and *Write-EZ* (Windows) creativity tools, patterned after Eliza. The author wrote of this phenomenon 20 years ago, and interviewed Mr. Burns about the usefulness of the technology. Burns’ words seem as relevant today as in 2003:

“From experience, I know that being an entrepreneur and owning or managing a small business can be a lonely experience. Those managers are thinking through their communications on their own. Thinking is not a monologue, but an internal, condensed dialogue. WriteEZ provides a companion for that dialogue, so you can advance your thinking. WriteEZ makes that process explicit and easier by asking the questions for you.”

Burns’ design was based on “directed discussion” – “a heuristic technique for helping students develop essays by asking questions, challenging assumptions, requiring supporting evidence, and then critiquing a final draft.”⁴

Fast forward. gAI tools became somewhat commonplace leading up to 2022. Most of the generation was images, or art. Other than IP concerns, people did not expect fact. Then came ChatGPT. A number of more obvious kinds of undesirable results emerged.

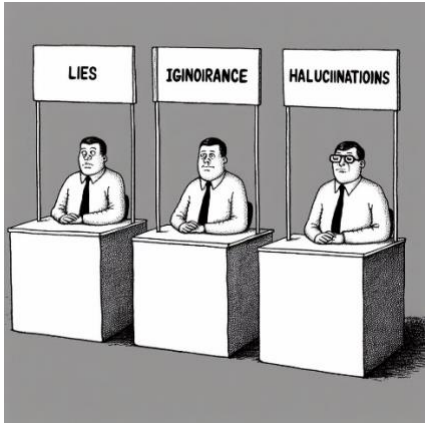


Figure 1: Created with DALL-E-4 from Bing AI Chat

Many guardrails are in place to deal with outputs that are offensive, hateful, violent or otherwise harmful.

- **Refusal to respond:** These are when chatbots say they cannot. *For example, a chatbot might say the question violated a guideline, was outside of the scope of an LLM, or that it didn't want to respond.*
- **Facts that are not facts:** These are when *chatbots* make up facts or details that are not true or supported by evidence. *For example, a chatbot might invent a research paper that does not exist or cite a source that is not reliable. However, some users would push back on correct responses to force incorrect responses to get these results.*
- **Semantic issues*:** These are when chatbots produce content that is grammatically correct but does not make sense or is irrelevant to the context. *For example, a chatbot might switch topics randomly, or use words that are out of place.* A counterpart might be as illustrated in Figure 1; DALL-E-4 sometimes refuses to provide the text it is given when creating images.
- **Stylistic issues:** These are when chatbots generate content that does not match the tone, genre or purpose of the task. *For example, a chatbot might use informal language in a formal setting, or mix up different styles of writing, harmful or inappropriate for the situation. For example, a chatbot might use hate speech, promote violence, or violate privacy.* These are often manipulation by “malicious” users. Some may feel that harmful or inappropriate outputs should be broken out as particularly egregious; many guardrails are in place to deal with these outputs that are offensive, hateful, violent or otherwise harmful. They may be due to malicious users or to problems with the model's understanding of social norms and ethical guidelines.

Hallucinations

The author has experienced many confident responses from chatbots that are not true. These include:

1. The results of a request for the biography of *ThinkTwenty20's* managing editor.
2. The lyrics for the classic 1967 hit by Vaughn Horton, *Pennsylvania Turnpike, I Love You.*

3. A list of articles by leading scholars from reputable academic journals on AI in accounting. We know the news about a New York attorney⁵ who included citations for his court filing that were completely fabricated by ChatGPT. (But why wasn't he using a real citator?)

In each case, the AI delivered a complete and confident reply that was completely wrong. It wrote a completely new song about Pennsylvania's Turnpike. It took real journal names, real (if mixed up) author names, and created plausible sounding article titles that simply didn't exist.

I do not call these hallucinations – I call them math. Others disagree. But whether hallucination or not, these results can have negative consequences for the reliability, credibility and trustworthiness of gAI applications and can potentially harm users of society.

The ISO does not currently have a definition of "hallucinations" when it comes to artificial intelligence, although it has quite a few definitions of "artificial intelligence" and a helpful technical report on testing AI (see Additional References and Glossary). Therefore, different groups can include or exclude different categories of undesirable results as hallucinations or not.

(With the example of the song above, it may not have been the result I wanted, but it could have been the result I needed – it invented a song! One person's undesirable result is another person's treasure.)

A hallucination implies that the chatbot is generating content that is not influenced by external inputs, but rather by its own internal logic and probabilities.

In a recent survey on hallucination in natural language generation,⁶ the authors credit the genesis of the term "hallucination" to *Computer Vision*,⁷ with positive meaning, but later took on more negative implications. The authors took the position that hallucination is both generated text that is *unfaithful to the provided source input* (with which the author agrees) and *nonsensical* (which the author finds troublesome, as an AI does not possess "sense"; it decides computationally, it does not choose, as Weizenbaum noted.). They do helpfully categorize hallucinations as *intrinsic* or *extrinsic*, based on whether the undesired result *disagrees with* or *cannot be verified from* source content.

Of these, the author places hallucinations largely in the Semantic issues arena. A hallucination implies that the chatbot is generating content that is not influenced by external inputs, but rather by its own internal logic and probabilities. Reasons may include "drift", "degradation" and "staleness"⁸; Bing AI Chat limits the back and forth on a topic for these reasons.

A Bard query provides definitions to these terms, and the relevance to our topic:

- **Drift** refers to the tendency of large language models to generate text that is less relevant to the topic at hand over time. This can happen because the model is not able to keep track of

the context of the conversation or because it is simply generating text based on the most likely next word in the sequence.

- **Degradation** refers to the tendency of large language models to generate text that is of lower quality over time. This can happen because the model is not able to learn from its mistakes or because it is simply being asked to generate text on topics that it is not familiar with.
- **Staleness** refers to the tendency of large language models to generate text that is outdated or inaccurate. This can happen because the model is trained on a dataset of text that is not up-to-date or because it is simply not able to keep up with the rapidly changing world around it.

Bard also suggests that “overfitting” (see glossary) can be a problem, where the model fits the training data too well and cannot generalize in response to user input accurately.

As to the other examples above, your author agrees they are undesirable results, but not hallucinations.

Take Tay, for example. The Microsoft 2016 AI experiment gone bad was not hallucinating, but rather repeating what it learned from others. Nevertheless, Tay still illustrates some of the ethical and social challenges of creating chatbots that can learn from human interactions.

Likewise, concerns about “bias” are not related to lack of faithfulness to inputs, but the nature of the training data itself.

That training data may be an issue, where there is a collapse of the AI model itself due to the model entering a feedback loop – where the AI is trained on data it generated itself, sometimes called Model Autophagy Disorder (MAD).⁹ This is a different kind of “bias,” an AI “echo chamber.”

Users should be aware that generative AI systems are not human and that they do not possess the same abilities as humans.

Developing a Taxonomy

With all of the being noted, one can begin to build a “taxonomy,” an organizational structure that may be helpful when considering how to remediate the risks of reliance on AI. We have discussed:

- Cause (e.g., drift, degradation, staleness, model issues)
- Focus (e.g., intrinsic, extrinsic)
- Classification (e.g., factual, semantic, stylistic)
- Operational (e.g., guardrails, refusal)
- Expectations (e.g., recognition it is computational, not a database/sense/choice)
- Planned uses (e.g., casual use, business communication, mission-critical operations)

- Known risks (e.g., IP violations, incorrect/biased training materials)

Note: Faithfulness can lead to undesirable results; nonsense always leads to undesirable results. A classification, or taxonomy, of undesirable output results into factual, semantic, stylistic and harmful or inappropriate categories can be helpful. Such tools can be used to develop targeted mitigation strategies. For example, to mitigate factual errors, we can develop techniques to improve the AI's ability to verify the accuracy of its output. To mitigate semantic errors, we can develop techniques to improve the AI's understanding of language and its ability to generate text that is coherent and relevant. To mitigate stylistic errors, we can develop techniques to improve the AI's understanding of different writing styles and its ability to generate text that is appropriate for the situation. To mitigate harmful or inappropriate outputs, we can develop techniques to identify and filter out harmful or inappropriate text.

Operational aspects of undesirable output results are important. For example, we need to consider how to detect undesirable output results in real time and how to respond to them. We also need to consider how to communicate the risks of undesirable output results to users. User expectations are also important, but for such a rapidly evolving environment, education is very difficult. For example, users should be aware that generative AI systems are still under development and that they may produce undesirable output results. Users should also be aware that generative AI systems are not human and that they do not possess the same abilities as humans.



Figure 2: Another image from DALL-E-4

Note: Claude (Claude.ai) recommends:

To develop the taxonomy further:

- Categories could include the type (factual, semantic, etc.), cause (e.g., lack of context, overconfidence), expected user impact (minor confusion to harm).
- Subcategories could distinguish intrinsic vs. extrinsic outputs, or examine the content (made up details, switching topics) vs non-responses.

- Causal factors, such as data biases, model deficiencies and human manipulation could be noted.
- Mitigation approaches could address the AI system design (e.g., uncertainty metrics), data & models (e.g., debiasing) and user education.
- Case examples that don't neatly fit proposed categories could help refine the taxonomy definitions.
- Real-world use scenarios could inform what level of unwanted output is acceptable.

Application

Let's take one of our examples from above: the author asks the gAI to provide a bio for the managing editor (to be used in an upcoming presentation). The AI provides a detailed description that has no connection to the managing editor's experience.

- Cause: While not a desirable result, the LLM is not a search engine. The cause is math.
- Focus: While we can't ask the LLM to tie back to the results, there was likely similar content in the training.
- Classification: Factual.
- Operational: There are no obvious operational issues.
- Expectations: We were looking for facts as if it were a database.
- Planned uses: Business communication.
- Known risks: Potential embarrassment, false claims, missing the good stuff that might influence others.

Conclusion

While more narrowly defining "hallucinations" may seem like nitpicking when generative AI is creating nonsense, presenting incorrect information as fact with great confidence, and potentially influencing users that treat the AI as an extension of themselves, helping users understand why gAI may provide unreliable and undesirable results as well as working toward plans to remediate and mitigate.

There are many dimensions to these problems. It ranges from the users themselves (decoupling them from the experience, turning on appropriate skepticism) to improving the training data, models, interfaces, guardrails and other logic.



Additional References:

[ISO/IEC TR 29119-11:2020\(en\)](#) Software and systems engineering — Software testing — Part 11: Guidelines on the testing of AI-based systems.

[ISO/IEC 23053:2022\(en\)](#) Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).

Glossary (Source is the ISO Online Browsing Platform at <https://www.iso.org/obp/ui#search> unless otherwise noted).

Artificial Intelligence –[Note: Oddly enough, defined numerous times]

ISO/IEC 2382:2015 capability of a functional unit to perform functions that are generally associated with human intelligence such as reasoning and learning

ISO/IEC 39794-16:2021: discipline concerned with the building of computer systems that perform tasks requiring intelligence when performed by humans

ISO 22458:2022: engineered system with capability to acquire, process and apply knowledge and skills

Overfitting

ISO/IEC 23053:2022(en) <machine learning> creating a model which fits the training data too precisely and fails to generalize on new data.

AI Process, as told by ChatGPT

The following is a response by ChatGPT when asked about the processes in ChatGPT. Risks and errors can be introduced at each step. The steps may be summarized in the following graphic:

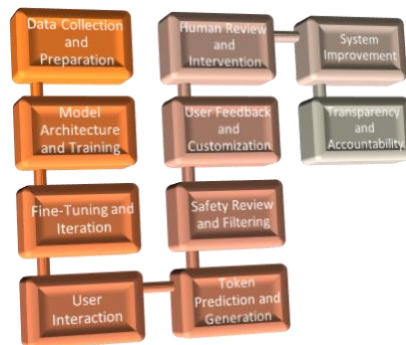


Figure 3: Steps of gAI Process from ChatGPT

ChatGPT's response begins here:

"I can provide you with a generalized depiction that can help you understand the high-level process involved in creating and using generative AI systems:

- 1. Data Collection and Preparation:**
 1. Gather a diverse and relevant dataset for training the AI model.
 2. Clean and preprocess the data to remove noise and inconsistencies.
- 2. Model Architecture and Training:**
 1. Choose a suitable architecture (e.g., transformer) for the generative AI model.
 2. Train the model on the prepared dataset using techniques like supervised or reinforcement learning.
 3. Incorporate safety measures, guidelines, and constraints into the training process.
- 3. Fine-Tuning and Iteration:**
 1. Fine-tune the model based on specific use cases or user feedback.
 2. Continuously iterate and improve the model's performance and safety.
- 4. User Interaction:**

1. Users provide prompts or input to the generative AI system.
2. The input is tokenized and processed by the model.
5. **Token Prediction and Generation:**
 1. The model predicts the next tokens in the sequence based on the input and its training.
 2. Generated tokens form a coherent response.
6. **Safety Review and Filtering:**
 1. The generated response undergoes safety review, including checking for offensive, harmful, or inappropriate content.
 2. Real-time filtering tools can be used to catch problematic outputs.
7. **User Feedback and Customization:**
 1. Users provide feedback on the generated output.
 2. Some systems allow users to customize the behavior of the AI within certain bounds.
8. **Human Review and Intervention:**
 1. In cases of uncertainty or nuanced content, human reviewers assess the generated response.
 2. Human reviewers help maintain the quality and safety of the system's outputs.
9. **System Improvement:**
 1. Feedback from users and human reviewers contributes to improving the system's safety measures and performance.
 2. Developers refine the model and update its training based on user needs.
10. **Transparency and Accountability:**
 1. Developers maintain transparency about the AI's behavior, safety mechanisms, and guidelines.
 2. Users are informed about how the AI system operates.
 - Please keep in mind that the specifics of this process can vary based on the organization, technology, and the type of generative AI system.”

ChatGPT’s response ends here.

Endnotes:

¹ [ELIZA wins Peabody Award | MIT CSAIL.](#)

² ['Please Tell Me Your Problem': Remembering ELIZA, the Pioneering '60s Chatbot \(mentalfloss.com\).](#)

³ [Computer power and human reason : from judgment to calculation : Weizenbaum, Joseph : Free Download, Borrow, and Streaming : Internet Archive.](#)

⁴ A history of the development of the software is documented in *Writing Teachers Writing Software*, taken from <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=91e63cec4f60fad9bfdedeaca52b237e9fd7e7b9> p 72-75.

⁵ [ChatGPT is not quite ready to be your lawyer \(morningbrew.com\).](#)

⁶ <https://dl.acm.org/doi/abs/10.1145/3571730>, <https://arxiv.org/pdf/2202.03629.pdf>.

⁷ S. Baker and T. Kanade. 2000. “Hallucinating Faces.” In *Proceedings Fourth IEEE International Conference on Automatic Face and Gesture Recognition (Cat. No. PR00580)*. 83–88. <https://doi.org/10.1109/AFGR.2000.840616>

⁸ [https://www.iso.org/obp/ui#iso:std:iso-iec:tr:29119:-11.](https://www.iso.org/obp/ui#iso:std:iso-iec:tr:29119:-11)

⁹ [https://arxiv.org/abs/2307.01850.](https://arxiv.org/abs/2307.01850)

The State of Cybersecurity in Canada

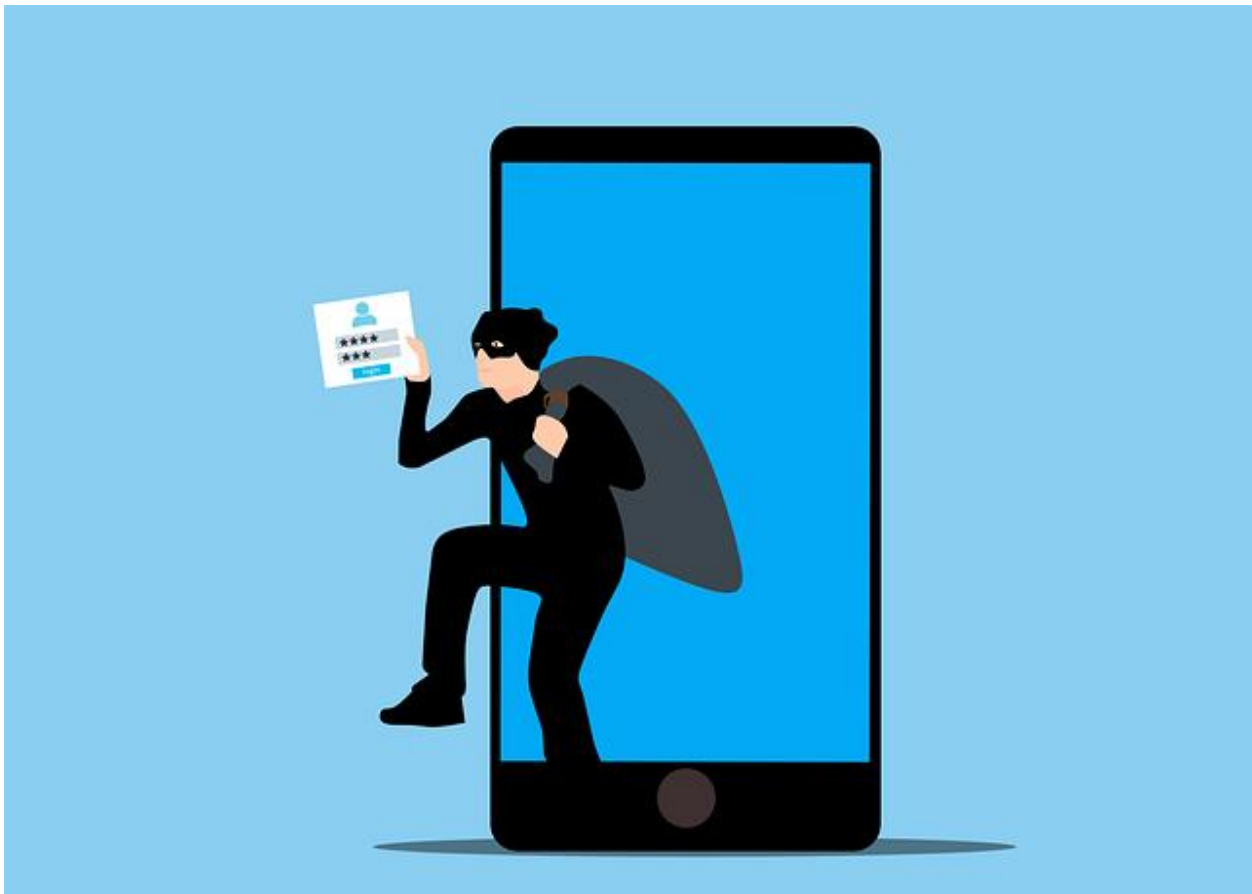
Report by Grant Thornton, summarized by Gundi Jeffrey

Grant Thornton LLP has released a report on the state of cybersecurity in Canada that provides insights on imminent cybersecurity threats and what business' can do to protect themselves. According to the report, "as businesses develop new ways to protect themselves from online attacks, cybercriminals are becoming savvier – and finding new weaknesses to exploit. It's important for businesses to be aware of cybersecurity developments to prepare accordingly."

The report addresses:

- Threats to small businesses
- Attacks on critical infrastructure
- Cybersecurity implications of AI
- Supply chain attacks

ThinkTWENTY20 has summarized the report as it contains valuable information on how organizations can prepare and protect themselves from cyberattacks now and in the future.



Smaller Businesses Under Attack

With larger organizations typically having strong controls around cybersecurity, whether in terms of training, processes or technology, small- and medium-sized businesses (SMB) are

increasingly feeling the brunt of cyber-attacks in Canada. As these businesses increasingly rely on digital infrastructure for day-to-day operations, they became enticing targets for cybercriminals seeking to exploit vulnerabilities. Phishing attacks, ransomware incidents and data breaches were among the most prevalent threats faced by SMBs. Many of these smaller Canadian businesses lacked the resources and expertise to implement robust cybersecurity measures, making them more susceptible to exploitation.

“The financial repercussions of cyber-attacks were often devastating for small businesses, with the cost of recovery and reputational damage putting their very survival at risk. The average cost of a data breach in Canada is \$5.64 million\$1 million more than the global average, and a [Mastercard study](#) showed that 99 per cent of victims said the cyber-breach impacted their business operations. Furthermore, the study noted that the most common effect of these cyber-breaches was the loss of customer data, and more than a third said the hack strained their relationships with vendors or customers.”

As small- and medium-sized businesses increasingly relied on digital infrastructure for day-to-day operations, they became enticing targets for cybercriminals seeking to exploit vulnerabilities.

Moreover, the interconnected nature of supply chains means that small businesses often became entry points for larger-scale attacks on their partners and customers. In response to this escalating threat, industry experts and governments stresses the importance of raising cyber awareness and providing support to small businesses in enhancing their cybersecurity posture. Collaborative efforts between cybersecurity firms, governments and trade associations aimed to equip small enterprises with the necessary tools and knowledge to defend against cyber threats, empowering them to navigate the digital landscape with greater resilience and confidence.

The Weakest Link in the (Supply) Chain

According to the report, “supply chain attacks provide an indirect method for attackers to breach a target organization – by first compromising a supplier and subsequently exploiting their trusted relationships with downstream organizations, threat actors can entirely circumvent those organizations’ secure network perimeter, thus avoiding the need for direct action against a target network’s defenses. Many of the attacks we’ve seen in recent years have come via weak third and fourth parties with the methods used to provide remote access to these organizations found to be insecure. A [Gartner risk report](#) indicated that, “There were 100 times more supply chain attacks in 2022 than in 2020. This trend will only get worse – by 2025, 45% of global organizations will be impacted.”

This vulnerability has led to an increased emphasis on third-party risk management. Security audits of potential external vendors and partners are becoming standard fare in the vetting process. Companies that are unable to demonstrate a solid security approach are losing

business. As a result, many companies are prioritizing employee awareness and training programs. As the threat landscape continues to evolve, collaboration and information sharing within industries and regulatory bodies have become essential to stay ahead of cyber adversaries. “The future of supply chain cyber security lies in adaptability, resilience, and a proactive approach, ensuring that businesses can thrive in the face of the ever-changing cyber threat landscape.”

Cyber-fatigue emerged as a pressing concern within the technology and security communities with the unprecedented surge in cyber-attacks, data breaches and privacy violations.

Sleeping On Cybersecurity as A Result of Cyber-Fatigue

Cybercriminals continue to look for the easiest ways to access an organization’s network or systems – the quickest and cheapest path that allows them to stay hidden under the guise of an authorized employee. Grant Thornton saw continued growth in attacks perpetrated by social engineering, which contributed to fraud hitting all-time-high in Canada. In 2022, fraud cost Canadians at least \$530 million, a 40 per cent jump over the previous according to the Canadian Anti-Fraud Centre.

The report points out that, as the scope and number of attacks increased, cyber-fatigue emerged as a pressing concern within the technology and security communities with the unprecedented surge in cyber-attacks, data breaches, and privacy violations, led to a constant barrage of security alerts, updates, and notifications for individuals and organizations alike. Additionally, the spike in attacks has seen security teams impose an overwhelming number of precautions on workers: use extremely long and complex passwords, change them every six weeks, multi-factor everything, keep your systems updated, and never, ever use insecure Wi-Fi. “As a result, there was a noticeable sense of exhaustion among users (and security professionals). The continuous stream of cybersecurity news and incidents also contributed to a desensitization to the severity of the threats, making it challenging to distinguish genuine risks from noise.”

Cyber-fatigue manifests as decreased vigilance, complacency towards security measures, and a higher likelihood of falling victim to social engineering tactics. “Addressing cyber fatigue became a critical aspect of cybersecurity strategies, necessitating user-friendly security interfaces, clear communication of risks, and efforts to strike a balance between security measures and usability. In 2022, the industry recognized the importance of not only fortifying technological defenses but also fostering a cybersecurity culture that acknowledges the impact of fatigue and empowers individuals and organizations to remain vigilant and resilient in the face of evolving cyber threats.”

Overall, the past year has proved pivotal year for cybersecurity, emphasizing the necessity for constant innovation and adaptability to protect against emerging threats in an increasingly interconnected digital landscape.

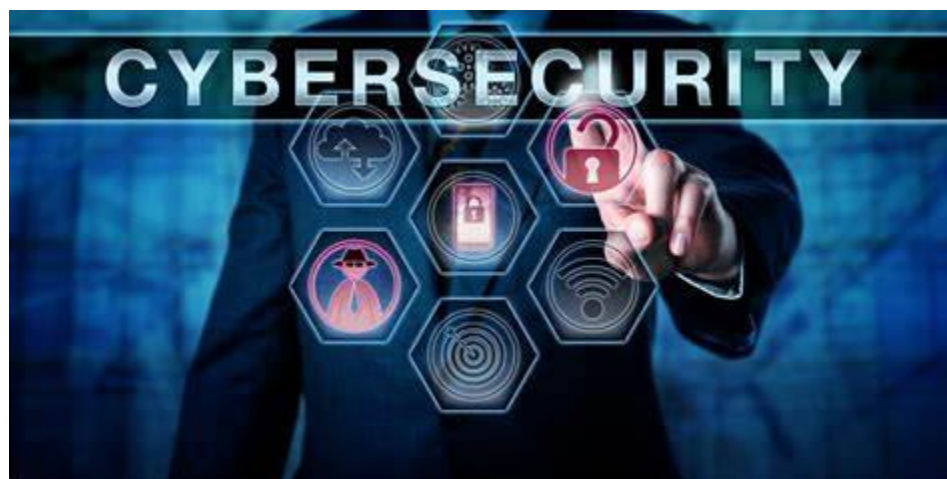
Trends On the Rise

Attacks on critical infrastructure

According to the report, cyber-attacks on critical infrastructure and Operational Technology (OT) systems are a growing concern due to their potential to cause severe disruptions and catastrophic consequences. As nations continue to digitalize and interconnect their essential services, attackers increasingly view critical infrastructure as attractive targets.

This trend has been consistently growing for years, the report says, but took on new urgency with the ongoing war in Ukraine. “Cyber warfare has emerged as a powerful tool used by state and non-state actors to achieve their strategic objectives. The conflict has witnessed an increase in sophisticated cyber-attacks targeting critical infrastructure, government institutions, and private organizations, both within Ukraine and beyond its borders. Canada is not immune to this. As a NATO member providing ongoing support for the Ukrainian government, we have been a target for attacks critical infrastructure such as our energy system. A recently published Communications Security Establishment (CSE) threat assessment noted that “...this activity is very likely to disrupt critical services for psychological impact, ultimately to weaken Canadian support for Ukraine. We assess that this activity will almost certainly continue for the duration of the war, and will likely increase as Russia's invasion efforts falter, or new support for Ukraine is announced.”

As the report points out, “the situation in Ukraine serves as an important reminder of the potential effects of cyber warfare on a global scale. It highlights the importance of enhancing cyber security measures not only for nations involved in armed conflicts but for the international community as a whole.”



Some key trends in cyber-attacks on critical infrastructure and OT in 2023 include:

- **Advanced Threats:** Cyber attackers are using more sophisticated tactics, techniques and procedures to target critical infrastructure. These attacks involve advanced malware, zero-

day exploits, and multi-stage campaigns that aim to evade detection and cause maximum damage.

- Ransomware Targeting Infrastructure: Ransomware attacks have evolved to specifically target critical infrastructure, such as power grids, water facilities, and transportation systems. The attackers' goal is not only to encrypt data but also to disrupt operations and extort large ransom payments.
- Supply Chain Attacks: Attackers may exploit vulnerabilities in the supply chain of critical infrastructure, compromising trusted vendors and suppliers to gain unauthorized access to critical systems and data.
- Convergence of IT and OT: As IT and OT systems converge to increase efficiency and connectivity, the attack surface for critical infrastructure expands, offering attackers more entry points into the industrial control systems.

Critical infrastructure operators are investing in state-of-the-art cybersecurity technologies, conducting regular risk assessments and prioritizing employee training to improve cyber awareness.

To counter these threats, the report says, “critical infrastructure operators are investing in state-of-the-art cybersecurity technologies, conducting regular risk assessments and prioritizing employee training to improve cyber awareness. Furthermore, comprehensive incident response plans and continuity strategies are being implemented to reduce downtime and mitigate the potential impact of successful cyber-attacks.”

Grant Thornton believes that, “as the world becomes increasingly reliant on interconnected systems, the focus on protecting critical infrastructure and OT from cyber threats will remain a top priority for both public and private sectors in 2023 and beyond.”

AI: the double-edged sword

The continued adoption of AI holds immense promise for various industries, but it also comes with significant cybersecurity implications. “AI's widespread integration in diverse applications, from autonomous vehicles and smart cities to healthcare and finance, enhances efficiency, decision-making, and user experience. However, this increased reliance on AI-driven systems opens up new attack vectors and potential risks that need to be addressed to ensure a secure digital landscape.”

The research for the report found that one major cybersecurity implication is the potential for AI-generated cyber-attacks. “As AI technologies advance, cybercriminals can leverage them to create more sophisticated and targeted attacks, such as AI-powered phishing campaigns, deepfake attacks and automated malware generation. These attacks can be difficult to detect and respond to, as they may mimic legitimate user behavior and exploit AI-based vulnerabilities in systems. Moreover, AI-driven cyber-attacks can lead to more significant and widespread

impacts. Automated and highly scalable attacks could potentially disrupt critical infrastructure, financial markets, or even influence political processes. The use of AI by malicious actors may also blur the lines between cyber warfare and cybercrime, creating complex challenges for attribution and response.”

Another cybersecurity challenge is related to the security of AI systems themselves. “As AI algorithms become increasingly complex and interdependent, they become vulnerable to adversarial attacks and data poisoning. If attackers can manipulate the training data or input to AI systems, they can lead to biased decisions, misclassification or unauthorized access to sensitive information.”

Additionally, the report points out that the current shortage of skilled cybersecurity professionals capable of effectively defending against AI-driven threats is a growing concern. “The demand for AI expertise in both offensive and defensive capabilities may outpace the availability of skilled personnel, leaving organizations vulnerable to emerging cyber threats.”

Collaboration between the cybersecurity community, policymakers and AI developers will be essential in order to establish ethical guidelines, standards and regulations to ensure the responsible and secure deployment of AI technologies in the years to come.

A change in the posture of cyber-insurance providers

A surge in online attacks has had a profound impact on the insurance landscape, sparking a reevaluation of business’ risk management strategies and prioritization of cyber insurance as a crucial component of their overall security posture.

Notes the report, “as cyber threats continue to diversify and become more sophisticated, cyber insurance policies will likely expand to cover a broader range of risks. This may include coverage for emerging threats like AI-driven attacks, supply chain vulnerabilities, and cyber-physical risks (e.g., attacks on IoT devices impacting physical infrastructure). It may also mean offering tailored and dynamic policies where insurers may offer more customized and dynamic cyber insurance policies tailored to specific industries, business sizes, and risk profiles. These policies may be designed to adjust their coverage and premiums based on real-time risk assessments and the insured entity's cybersecurity posture.”



As cyber-attacks became more disruptive and costly, insurance providers adapted their offerings to address the evolving threat landscape. But, the report points out, “the increased risk also led to a reevaluation of policy terms and premiums, with some insurers tightening their underwriting criteria to mitigate potential losses. The growing demand for cyber insurance led to an expansion of the market, with new insurers entering the arena and existing ones refining their coverage options. The year saw a greater emphasis on tailored policies, where businesses could customize coverage based on their specific needs and risk exposure. Additionally, the cyber insurance industry focused on providing proactive risk assessment and incident response services to help organizations bolster their cyber resilience.”

Cyber insurance is expected to undergo significant changes in response to the evolving cyber e. Overall, the future of cyber insurance is likely to be marked by innovation, greater risk awareness and a shift towards proactive risk management.

Even as insurance providers innovate to develop new risk mitigation products, Grant Thornton says, “organizations should also expect higher scrutiny over the maturity of their cybersecurity controls and requirements for more detailed cybersecurity risk assessments from policyholders to determine the level of coverage and premiums. Entities with stronger cybersecurity measures may receive more favorable premiums, while those with higher risk profiles may face increased costs. This could encourage businesses to improve their cybersecurity practices to qualify for better coverage terms.”

To mitigate both cybersecurity risk and the financial risk of high insurance premiums, “businesses must prioritize cybersecurity measures such as implementing robust security protocols, conducting regular security assessments, investing in employee training, and staying

informed about the latest threats and best practices in the industry. Collaboration with cybersecurity experts and leveraging advanced threat detection technologies can also help organizations fortify their defenses against the evolving cyber threat landscape.”

Zero Trust

The research found that, in 2023 and beyond, the concept of zero trust is becoming increasingly vital in the field of cybersecurity. “Traditional security approaches that relied on perimeter-based defenses are no longer sufficient to protect modern, dynamic digital environments. Zero trust architecture offers a paradigm shift by assuming that no entity, whether internal or external, should be trusted by default. Instead, it advocates verifying and validating every access request and transaction, regardless of the user's location or device.”

The importance of zero trust lies in its ability to address the evolving threat landscape. “With the rise of remote work, cloud computing, the attack surface has expanded, making it more challenging to establish a secure perimeter. Zero trust embraces the ‘never trust, always verify’ principle, reducing the risk of lateral movement for cyber attackers within a network. This model helps prevent data breaches and unauthorized access even if the attacker has already compromised one part of the system.”

Moreover, the zero-trust philosophy emphasizes data protection. “By adopting encryption and tokenization, data remains secure even if it falls into the wrong hands. This approach helps businesses comply with regulatory requirements and maintain customer trust.”

According to Grant Thornton, “as cyber threats continue to evolve, the concept of zero trust is poised to become a foundational pillar of cybersecurity strategies. Its adaptive, proactive, and context-aware nature makes it an essential approach to safeguard digital assets, privacy, and sensitive information in 2023 and beyond.”

The Need for Robust Cyber Defenses

As the cyber threat landscape continues to evolve with increasingly sophisticated attacks and emerging technologies, says Grant Thornton, “the need for robust cyber defenses has never been greater. Organizations and individuals alike must remain vigilant, proactive and adaptable to the dynamic nature of cyber threats. Embracing advanced technologies such as AI-driven security solutions and zero-trust architectures will become crucial in safeguarding digital assets and personal information. Collaboration between industry stakeholders, governments and cybersecurity experts will pave the way for more effective threat intelligence sharing and coordinated response efforts. Furthermore, a strong focus on cybersecurity awareness and education will empower individuals to protect themselves against cyber risks. Despite the complexity of the challenges ahead, the collective commitment to cybersecurity will lead to a safer digital landscape, where innovation and technology can thrive securely in 2023 and beyond.”



A Wealth Tax Proposal

By: Jason Fleming, CPA, CA, M.Acc



Jason is an associate professor teaching at York University's School of Administrative Studies and is the author of *CFE Tax*, 8th edition and *CFE Case Writing*, 2nd edition (Thomson Reuters)

This article proposes a new, administratively simple, wealth tax for Canada. The goals of this tax are to create income for the federal government and reduce the concentration of wealth. Most Canadians will *not* be subject to this tax and unlike current taxes it will be relatively easy to comply with.

Since Canada does not have a gift or estate tax, a new wealth tax, if properly designed and implemented, may be a good idea¹. Practical suggestions are given such as using cost to value private businesses in order to make compliance straightforward. The tax rate is 1%, with a \$20M exemption, to avoid discouraging hard work and success, and to keep wealthy individuals from leaving Canada.

Given the outrageous complexity of Canada's tax system, this wealth tax should only be implemented at the same time as Canada's income tax system is simplified.

Given the outrageous complexity of Canada's tax system, this wealth tax should only be implemented at the same time as Canada's income tax system is simplified and the payroll tax on employers is eliminated. For suggestions on how to simplify our tax system please see: *Tax Simplification Suggestions*, and see: *Tax Robots Not Payroll A Robot Tax Proposal* (Canadaone.com) for why we must eliminate employer payroll tax. Simplifying our tax system and removing payroll tax on employers, will also help keep wealthy Canadians from leaving Canada.²

Proposed Wealth Tax

¹ The OECD Tax Policy Studies summary No. 26, *The Role and Design of Net Wealth Taxes in the OECD*, says a wealth tax may be appropriate "...for countries that do not levy taxes on inheritances." Note: Canada has a deemed disposition of capital assets owned on death, but does *not* have an estate or inheritance tax.

² Canada's 10% federal luxury tax on certain: cars, trucks, aircraft and boats, that began in 2022, could also be eliminated. While the wealthy can afford to pay this luxury tax, it adds a major compliance burden (and tax risk) to car and boat dealerships. Note: when a rich person buys a multi-million-dollar painting, or other luxury items, they do *not* pay this luxury tax; since it only applies to certain vehicles. My proposed wealth tax will apply to all assets and hence the 10% luxury tax can be eliminated.



Individuals resident in Canada for income tax purposes, 18 and older, who own assets above \$20M, will pay an annual federal wealth tax equal to 1% of their wealth over \$20M. Worldwide assets beneficially owned on December 31st will be subject to this tax. Married couples (legal or common law) can report their assets, along with any assets of their minor children, on one return. Trusts will *not* need to file this return. See

Appendix I for a sample, one-page, wealth tax return.

The wealth tax return, and any wealth tax owing, will be due six months later, i.e., due June 30th of the following year. To reduce the compliance burden, only individuals with assets above \$15M will need to file the wealth tax return. With married couples, only couples with assets above \$30M will need to file.

Married people will each get the \$20M exemption, hence for married couples only assets above \$40M will be subject to this tax. Children under 18 will have their assets reported on their parent's (or caregiver's) return unless they are emancipated minors, who do not live with a parent (or caregiver), and who are not dependent upon their parent (or caregiver). Emancipated minors will have to file their own return (if *their* assets exceed \$15M).

Simplifying our tax system and removing payroll tax on employers, will help keep wealthy Canadians from leaving Canada.

Value of Assets

Assets include all assets beneficially owned, even tax-deferred assets like RRSPs (and TFSAs). Foreign denominated assets will be translated to Canadian dollars on December 31st.

Determining fair market value (FMV) can be challenging and, in order to make this tax administratively simple, the following rules should be enacted to determine asset values:

- Public company investments will be valued at FMV since market value is easily obtainable. The closest prior (monthly) investment statement provided by the financial institution can be used to determine the December 31st FMV. For example, if a bank's statement happens to be dated December 30 and the statement's FMVs are from December 28 closing share prices, then these values can be used as the December 31st FMVs (to simplify compliance). If foreign-denominated assets are translated into Canadian dollars on the financial institution's closest prior investment statement, then these values can be used; otherwise, foreign assets must be converted to Canadian dollars using the December 31st foreign exchange rate(s). Options and other derivatives on public securities, that are reported on investment statements at FMV will be valued at FMV, and included with public company investments.
- Private company investments will be valued at cost. Given the complexity of valuing private equity, and debt, cost will be used instead of FMV. Using cost is essential to make this

wealth tax easy to comply with and easy to audit. While this usually lowers an individual's asset values for a certain period of time, cost will eventually equal FMV. For example, any shares gifted or bequeathed to another person will have an adjusted cost base (ACB), i.e., tax cost, equal to FMV at the time of gift. Hence, the person receiving the shares now owns the asset with a higher cost (i.e., FMV at the time of the gift) and *they* will report this on their wealth tax return.

Options and other derivatives on private securities will be reported at cost, and included with private company investments. Note: employee stock options have no cost when granted, but will have a cost equal to FMV at the time the options are exercised.

- Real estate will be valued at the assessed value for property tax purposes at the most recent property tax bill prior to December 31st. Should a foreign jurisdiction not have property tax assessments, a valuation from a local real estate professional will need to be done.
- Cash, bonds, GICs, T-bills, and similar interest-bearing investments will be valued at cost. The closest prior (monthly) investment statements provided by the financial institution(s) can be used to determine the December 31st cost.
- Personally owned business assets, such as inventory, furniture and equipment used in a business are valued at cost. Internally generated goodwill does not have a cost (and hence will not be included).
- Life insurance policies with a cash surrender value (e.g., whole life, universal life) will be included as an asset at the cash surrender value as reported on the closest life insurance statement prior to December 31st. Term life insurance will *not* be included in the value of an individual's assets (unless it has a cash surrender value). This is due to the difficulty in valuing life insurance. Note: after death the cash paid out to the beneficiary will be included in the assets of that beneficiary and hence will be included in the beneficiary's future wealth tax returns.
- RRSP/RRIF/TFSA assets, and RCA (retirement compensation arrangements) assets will be included in assets (using the above rules, i.e., public company investments are included at FMV). Other pensions, such as arm's length work registered pension plans (RPPs) and the Canada Pension Plan and Old Age Security (or similar foreign pension plans) will *not* be included in the value of an individual's assets due to the complexity of determining FMV. Work RPP assets from a non-arm's length employer will need to be included in assets. The most recent actuaries' report or financial institution's investment statements, prior to December 31st, can be used to value the RCA or non-arm's length RPP (with public company investments included at FMV).
- A personal trust's/partnership's assets will be included in the beneficiaries'/partners' assets, based on their share, as per above (i.e., public company investments are included at FMV while private company investments are included at cost). With an RESP, the child's trust assets will be included in the parent's return when the child is 17 or younger (as discussed



above), and will be included in the child's return once the child turns 18 (if the child has more than \$15M in assets).

- Automobiles and listed personal property (such as art and jewelry) will be included in assets valued at cost. The value of most personal effects (such as home furniture, clothes, etc.) that are considered personal use property for income tax purposes will be ignored, i.e., will not be included in assets. Your home, and other real estate, is included in assets as per above.
- Some complexities are discussed in Appendix II.

Since only individuals with more than \$15M in assets need to file a wealth tax return, it should be relatively easy for the Canada Revenue Agency to audit the small number of returns.

Cost

Cost will be the higher of: (a) the actual cost paid by the taxpayer (in cash or assets); and (b) the deemed cost for income tax purposes. Cost will *not* be reduced by any capital cost allowance, depreciation or asset impairment(s). Since cost is readily available, using cost when FMV is difficult to ascertain is essential for reducing the compliance burden.

For example, if an individual transfers \$100M of public company stock to a private company using a tax-free rollover (e.g., section 85 of the Income Tax Act) and receives private company shares, and elects at a lower value of say \$20M, then the cost of the new private company shares, for wealth tax purposes, will be the higher of: (a) the actual cost paid (i.e., \$100M paid in public company shares); and (b) the deemed cost for income tax purposes (i.e., the \$20M elected amount). Hence in this example, the cost will be \$100M for wealth tax purposes.

Liabilities

Secured debts can be subtracted from the FMV of assets to determine the net assets subject to tax. Only debts owing by the taxpayer (or spouse or minor child) that are secured by assets that are included on his/her wealth tax return, can be subtracted when computing net assets subject to the wealth tax.

Other liabilities will *not* be subtracted from assets. The large exemption will help offset some of a wealthy individual's non-secured liabilities (which are not subtracted from assets).

Exemption (\$20M)

A large exemption, i.e., \$20M, is needed to have administrative simplicity, i.e., only the wealthy will need to pay this tax, and to avoid discouraging hard work and savings. Building up wealth is good and should be encouraged. However, money is needed to fund government programs and the wealthy can afford to help fund those programs. A 1% wealth tax, with a \$20M exemption, can bring about significant revenues (as discussed below).

Since only individuals with more than \$15M in assets need to file a return, it should be relatively easy for the Canada Revenue Agency (CRA) to audit the small number of returns to ensure compliance.

While annual indexing for inflation should not occur so round numbers can be used, approximately every 5 to 10 years the exemption should be increased to account for inflation. For example, in 5 to 10 years the \$20M exemption will likely need to be raised to \$25M.

The proposed wealth tax will raise billions of dollars of much needed revenue for the federal government each year and will be relatively easy to comply with and administer.

Tax Rate (1%)

While governments have a habit of increasing taxes when they want to increase spending, this new tax should clearly state that the rate will never rise above 1%. The wealth tax rate should never increase above 1% for the following reasons:

- One percent is not really a small number when you consider that this tax is paid every year. Hence, 1% of the FMV of assets, each year, can add up to significant tax.
- A higher rate will lead to more planning to reduce this tax, and may cause wealthy individuals to leave Canada taking their much-needed capital and job creating businesses with them.³

Administrative Matters

Any wealth tax paid will *not* be deductible for income tax purposes to ensure more funds for government and less concentration of wealth. No instalments will be required for this new wealth tax.

A late filing penalty of 5% of any wealth tax owing, plus 1% for each full month late will be owing (to a maximum of 12 months late), if the return is filed late. Hence, if one year's return is not filed at all, the penalty will equal 17% (i.e., 5% + 12% for each full month late).

Tax Planning

Some wealthy taxpayers will gift assets to reduce their annual wealth tax. Subject to the anti-avoidance rules (discussed in Appendix II), this is allowed, as it will reduce the concentration of wealth, which is one of the goals of this new tax. Note: gifting assets will lead to a deemed disposition at FMV for income tax purposes, which typically leads to income tax owing. Furthermore, the person who receives the gift will now include that asset in his/her annual wealth tax return (if they are an individual resident in Canada with assets above \$15M).

While this tax is designed to keep taxpayers in Canada, *if* an individual becomes a non resident of Canada, for income tax purposes, departure tax rules apply, which lead to a deemed disposition of capital assets at FMV (which typically leads to income tax owing).

Examples

³ See the Fraser Institute's "Wealth tax would make Canada's bad situation even worse" (appeared in the *Financial Post*, October 7, 2021) for arguments against a wealth tax.

A married couple with worldwide assets of \$50M (net of secured liabilities) would pay the 1% annual wealth tax on \$10M of assets (i.e., \$50M - \$20M - \$20M). Hence, this couple would owe \$100,000 (i.e., \$10M x 1%) of wealth tax for the year.

An individual with worldwide assets of \$1B (net of secured liabilities) would pay the 1% annual wealth tax on \$980M of assets (i.e., \$1B - \$20M). Hence, this person would owe \$9.8M (i.e., \$980M x 1%) of wealth tax for the year.

Tax Revenue Raised



As an approximation of the minimum annual federal revenue raised by this proposed new tax: according to Wikipedia Canada has 64 billionaire families with an average annual wealth of \$5B.⁴ Hence, each of these families would have, on average, assets of \$4.96B (i.e., \$5B - \$20M - \$20M exemptions, assuming they are all married). Each would then pay an annual wealth tax of \$49.6M (i.e., \$4.96B x 1%).

Just counting these 64 families, this wealth tax would raise annual revenue of \$3.2B (i.e., \$49.6M x 64). There are many more Canadians with a wealth above \$20M who would also pay this proposed annual wealth tax.⁵ Hence, significant annual revenue will result.

Deceased Taxpayers

Taxpayers who pass away in the period December 31st to June 30th will have their wealth tax return filing, and payment, deadline extended by six months (i.e., to December 31st). Taxpayers who die prior to December 31 will *not* owe any wealth tax (and will not need to file a wealth tax return) for that particular year.

Conclusion

This 1% proposed wealth tax will raise billions of dollars of much needed revenue for the federal government each year and will be relatively easy to comply with and administer. This tax will also reduce the concentration of wealth. Since only individuals with more than \$15M in assets (\$30M if married) will need to file, and only taxpayers with more than \$20M in assets (\$40M if married) will need to pay this new tax, it will *not* apply to the vast majority of Canadians.

The government should simplify the income tax system and remove the employer payroll tax prior to creating this (or any) new tax. The government should also clearly signal that the 1% wealth tax rate will *never* increase, and the \$20M exemption will never decrease, so as to avoid discouraging hard work and success, and to avoid encouraging wealthy Canadians to leave Canada.

⁴ From Wikipedia (October 25, 2023) (https://en.wikipedia.org/wiki/List_of_Canadians_by_net_worth). Data is originally from *Forbes Magazine* from 2021. I converted the U.S. figures to Canadian dollars using a 1.3731 exchange rate (which was the exchange rate on October 24, 2023).

⁵ A July 8, 2020 Parliamentary Budget Officer's report *Net Wealth Tax on Canadian Resident Economic Families*, estimates 13,800 Canadian economic families would pay a net wealth tax (on wealth above \$20M), and net revenue raised would be \$5.6B in 2020-2021.

Appendix I (Proposed 1-page Wealth Tax Return)

Year _____ **Wealth Tax Return**

Thank you for helping fund Canada's social programs. This return and any tax owing are due by June 30 of the following year. A late filing penalty of 5% of any tax owing, plus 1% for each full month late will be owing (to a maximum of 12 months), if filed late. Report using the closest: investment statements or real estate assessed values prior to December 31st. Cost is the *higher* of: (a) the actual cost paid; and (b) the deemed cost for income tax purposes. Cost will not be reduced by any capital cost allowance or depreciation. Personal effects (such as furniture, clothes, etc.) that are personal use property can be ignored. If your wealth (line 13) is \$15M or less (\$30M if married and filing 1 joint return) you do not need to file this return. Report amounts in Canadian dollars.

Name: _____ Address: _____

SIN: _____

Spouse's name (if married): _____ Spouse's SIN _____

Assets Owned on December 31st

Report world-wide assets beneficially owned by you, your spouse if married, and your minor children.

Public company investments (e.g., FMV of public: stocks, mutual funds, options and other derivatives, trust or partnership units)	_____ (1)
Private company investments (valued at cost)	_____ (2)
Real estate (including your home, valued at assessed value)	_____ (3)
Cash, bonds, GICs, T-bills, etc. (valued at cost)	_____ (4)
Personally owned business assets (e.g., inventory, equipment; valued at cost)	_____ (5)
Whole-life/Universal-life insurance (valued at cash surrender value)	_____ (6)
RRSP/RRIF/TFSA assets, and RCAs (public co. investments are valued at FMV)	_____ (7)
Personal Trust/Partnership assets (public co. investments are valued at FMV)	_____ (8)
Automobiles and LPP (such as art and jewelry; valued at cost)	_____ (9)
Other assets (Please list _____)	_____ (10)
Assets add lines 1 to 10	_____ (11)
Less: Secured debts (only report liabilities secured by an asset included above)	_____ (12)
Wealth (subtract line 12 from line 11)	_____ (13)
Exemption	_____ \$20M (14)
Less spouse's exemption (if married and filing jointly, enter \$20M)	_____ (15)
Wealth subject to tax (line 13 minus lines 14 and 15, if negative = \$0)	_____ (16)
Wealth tax (1% x line 16)	<input type="text"/> (17)

Appendix II (Some Complexities)

Trusts and Partnerships

The FMV of a personal trust's assets will be split equally with all the named (income or capital) beneficiaries of the trust, if the trust is discretionary. If the trust is not discretionary, each named (income or capital) beneficiary of the trust will include their share of the trust's assets as of December 31st. Future or potential beneficiaries (e.g., future children) will be ignored. Only specific beneficiaries known (i.e., named beneficiaries) as of December 31st will be included.

In the unlikely situation where there are no named beneficiaries, then the settlor (or settlors) will be deemed to own the assets of the trust (based on respective contributions to the trust).

To simplify reporting and to avoid double counting, a trust's income and capital beneficiaries' share of trust assets will be equal. For example, if a discretionary trust has 3 beneficiaries: A (income), B (capital), and C (both income and capital); then:

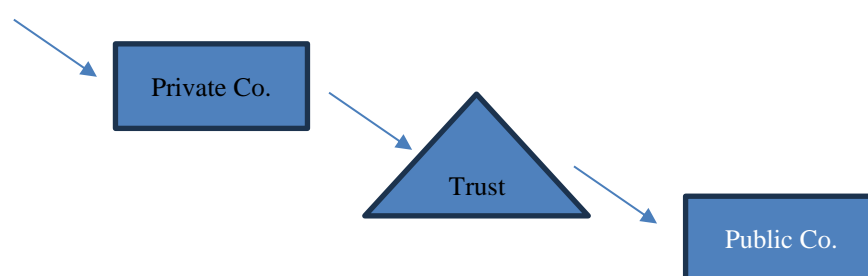
- person A will be deemed to own 50% (of the income) of 200% (i.e., 100% income + 100% capital) = 25% of the trust's assets
- person B will be deemed to own 50% (of the capital) of 200% (i.e., 100% income + 100% capital) = 25% of the trust's assets, and,
- person C will be deemed to own 100% (i.e., 50% income + 50% capital) of 200% (i.e., 100% income + 100% capital) = 50% of the trust's assets

Partnership assets will be deemed to be owned by the partners based on their respective share of the partnership assets (as per above; i.e., public company investments are included at FMV while private company investments are included at cost).

Flow-Through Rules

One complication will arise with complex structures, which are common. For example, Mr. X may own all the shares of a private company (with a low cost), which is a beneficiary of a trust that owns public company shares (with a large FMV), as can be seen in the diagram.

Mr. X



To ensure these structures cannot be used to avoid the wealth tax (by putting public company shares that are valued using FMV into a private company that is valued using cost), flow-through rules are needed.

A chain of any combination, of any number of: non-arm's length private investment holding companies, non-arm's length trusts and non-arm's length partnerships, will need to be looked through to determine the taxpayer's asset values on December 31st (using the rules above, i.e.,

public company investments are included at FMV, real estate is valued using assessed value, and private company investments are included at cost).

Assets will not flow through:

- arm’s length entities,
- public companies, or
- private corporations that are not investment holding companies.

An investment holding company will be defined as any private company with a FMV of public investment assets, or real estate investments, that is more than 50% of the company’s total assets on December 31st. A private company with 50% or more active business assets will *not* be considered an investment holding company. Hence, private company businesses will not be subject to this flow-through rule (unless their business assets are less than 50% of their total assets). The assets of a private company that is not an investment holding company will not flow through.

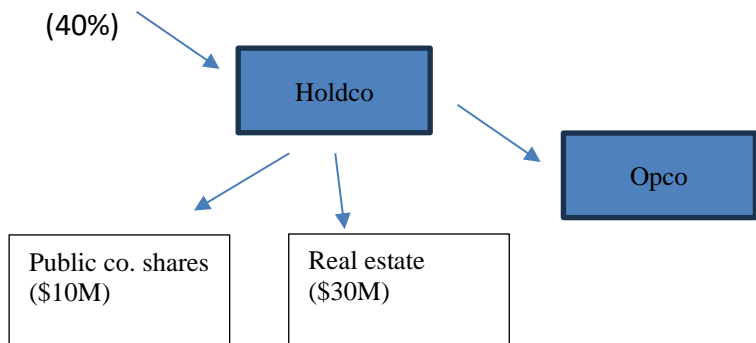
Examples of Flow-Through Rules

1) Mr. X’s only asset is 80% of the shares of a private company that is running an active business. The private company is also a beneficiary of a trust (or a partner in a partnership) that owns public company shares worth \$1B. As long as the FMV of the private company’s business assets are 50% (or more) of its total assets, on December 31st, Mr. X’s private company shares will be included in his wealth tax return at his cost of his private company shares. No complex flow through is required.

2) The facts are the same as in (1) except now the private company’s assets are mostly investment assets. Starting at the bottom of the diagram, the \$1B worth of public company shares owned by the trust would flow through to the private company as discussed above. Hence, if the private company is the sole beneficiary of the trust, it would be deemed to own all of the public company shares (owned by the trust). These public company shares would flow through the private company (for wealth tax purposes) and Mr. X will be deemed to own 80% of the public company shares (since he owns 80% of the private company). Hence, for Mr. X’s wealth tax for the year, he would report \$800M of public company investments, i.e., 80% of \$1B. Other investment assets of the trust, such as other private company investments owned by the trust will also be flowed through to Mr. X (at cost) in the same way.

3) Ms. Y’s only asset is 40% of the shares of an investment holding company (Holdco), with a low cost. Holdco owns three assets: (a) 100% of a private company that is running an active business, Opco (50% or more of the FMV of its assets are active business assets), with a cost of \$100 and a FMV of \$90M; (b) public company shares worth \$10M; and (c) real estate with an assessed value of \$30M, as can be seen in the diagram:

Ms. Y
(40%)



Since more than 50% of Holdco's assets are investment assets (all its assets are investment assets), its assets will flow through to Ms. Y for purposes of the wealth tax. Ms. Y's assets will consist of her share, i.e., 40% of: the \$100 cost of the Opco shares (cost is used since Opco is a private company that is not an investment holding company); the \$10M worth of public company shares; and the \$30M worth of real estate, which flow through to Ms. Y.

Hence Ms. Y's assets will be just over \$16M; i.e., \$40 (i.e., 40% of \$100) + \$4M (i.e., 40% x \$10M) + \$12M (i.e., 40% x \$30M). The assets of Opco do not flow through to Ms. Y since it is *not* an investment holding company.

When assets are flowed through, as in examples 2 and 3 above, the cost of the top private company shares will not need to be included in the individual's assets (to avoid double counting). Hence, in example 2 the cost of Mr. X's assets will not include his cost of his private company (Private Co.) shares. In example 3 the cost of Ms. Y's assets will not include her cost of her investment holding company (Holdco) shares.

Anti-avoidance Rules

None of the following transactions will be subject to the anti-avoidance rules:

- arm's length transactions,
- transactions at FMV,
- transactions that occurred prior to the enactment of this wealth tax.

To avoid this tax, some taxpayers will transfer assets to others to reduce the FMV of their assets. Actually, gifting assets to others is allowed and will *not* be subject to anti-avoidance rules. If, however, assets are gifted prior to December 31st and then gifted back to the taxpayer after December 31st, and one of the reasons for this gifting arrangement is to avoid the wealth tax, the asset will be deemed to be owned by both the taxpayer who initially gave the gift and the taxpayer who now legally owns the gift (i.e., double counting).

Any gifts that will revert back to the taxpayer will be deemed to be owned by both the taxpayer who initially gave the gift and the taxpayer who now legally owns the gift (i.e., double counting). For example, if a taxpayer gives assets to a trust, or private company, but has the right to get those assets back at any time in the future, then this anti-avoidance rule will apply.

Hence, real gifts are an acceptable way to reduce or avoid this wealth tax but "temporary" gifts are not.

Similarly, while most personal use property (PUP) is excluded, if an unreasonable amount of PUP is purchased prior to December 31st to lower the value of cash, or other assets, and then converted back into cash or other assets after December 31st, then *these* assets will be included in the taxpayer's assets at cost.

Finally, if a private company structure is used to own public company shares (perhaps through a chain of entities as discussed above), and if investment assets are sold shortly before December 31 and used to buy active business assets, and then the transaction is reversed shortly after December 31st, and one of the main reasons for these transactions is to ensure the private company meets the 50% test described above to avoid the flow-through rule, then the transaction will be ignored for wealth tax purposes and the flow-through rule will apply.

Corporate Reporting: Quo Vadis?

Paradigm Shifts Shaping the Future of Corporate Reporting: Purpose, Accountability, Value and Sustainability

By Alan Willis, FCPA, FCA



This is a unique new monograph by Alan Willis, notable authority on ESG and Sustainability Reporting, which of late is merging with traditional corporate reporting. It brings us up to date on the latest developments in Sustainability Corporate Reporting Standards and suggests future directions in the corporate reporting landscape. A must read for anyone interested in these areas.

"....who else could produce such a sweeping, incisive history of non-financial reporting spanning the last three decades? The publication offers a powerful reminder of how far we've come. Your narrative is accessible, engaging and authoritative."

- Dr. Allen White, Co-founder and former CEO, Global Reporting Initiative

Available on Amazon

at https://www.amazon.com/s?k=quo+vadis+coporate+reporting&rh=n%3A154821011&ref=nb_sb_noss

Or on our secure Shopify Store at

<https://thinktwenty20-magazine.myshopify.com/products/corporate-reporting-quo-vadis-by-alan-willis>

Price \$10.00

A person is shown from the chest up, sitting at a desk. They are wearing a dark jacket and are looking at a laptop screen. A tablet is also visible on the desk in front of them. The background is a solid dark purple color.

Certified Information Technology Professional

Upskill and earn this
AICPA Advisory
Services Credential

Twenty-First Century Corporate Reporting: Effective Use of Technology and the Internet

How and why do corporations use the internet for reporting to their stakeholders? How and why has corporate reporting extended beyond financial reporting to include environmental, social, and governance (ESG) reporting and even integrated reporting. The major drivers of modern reporting have changed, to include data driven decision making, big data, and advanced analytics, as well as the use of electronic representations of data with tools such as XBRL.

Here we explore the various vehicles for using the internet, including social media and blogs as well as corporate websites and the websites of regulators. And we delve into the impact of portable devices, like smartphones and tablets.

Corporate reporting on the internet is changing fast because of changes in technology and stakeholder expectations. Companies are having a hard time keeping up. This book offers a roadmap to follow—a roadmap to start on now. Most importantly, the book lays out a strong case for integrated reporting and shows how reporting on the internet is ideally suited to the creation of integrated reports.

This book is of interest to executives in charge of the reporting function for their companies, students of accounting and management, and to serious investors and others with a strong interest in corporate reporting and the direction in which it is headed.



Gerald Trites is a CPA with a history of writing and publishing and a unique background. He was a partner in KPMG for seventeen years, and a tenured professor of accounting and information systems for ten. He also served for twelve years as director of XBRL Canada. He has published twelve books and numerous articles and papers. He worked as a research associate for the Canadian Institute of Chartered Accountants and served as chair of the Auditing Standards Board. He currently serves as editor-in-chief of ThinkTWENTY20 magazine, a publication he started in 2019 with the objective of publishing well-researched articles of substance.

**Order your
copy now!**



www.businessexpertpress.com



1.800.632.0880



orders@aidcv.com