ISACA

The Promise and Peril of the AI Revolution: Managing Risk

Risk

CONTENTS

4 **When Corporate Wisdom Meets Artificial Intelligence**
4 **The Current State of Artificial Intelligence**
6 **To AI or Not to AI**
6 **Identifying AI Risk and Reward**
7 **Conducting an AI Benefit Analysis**
8 **Identifying AI Risk**
9 / Societal Risk
10 / IP Leakage and Invalidation
10 / Invalid Ownership
11 / Cybersecurity and Resiliency Impact
11 / Weak Internal Permission Structures
11 / Skill Gaps
12 / Overreactions
12 / Intended and Unintended Use
12 / Data Integrity
13 / Liability
14 **Adopting a Continuous Risk Management Approach**
14 / Step One: Identify Risk
14 / Step Two: Define Risk Appetite
15 / Step Three: Monitor and Manage Risk
15 **Building AI Security Programs: Eight Protocols and Practices**
15 / One: Trust but Verify
16 / Two: Design Acceptable Use Policies
16 / Three: Designate an AI Lead
16 / Four: Perform a Cost Analysis
17 / Five: Adapt and Create Cybersecurity Programs
17 / Six: Mandate Audits and Traceability
18 / Seven: Develop a Set of AI Ethics
18 / Eight: Societal Adaptation
19 **Prospering in an AI-Powered Future**
21 **Acknowledgments**

ABSTRACT

It is the premise of so many science fiction movies: technology surpasses human intelligence, wreaks havoc and ultimately takes over humankind. While that movie has not yet happened in real life, the recent release of ChatGPT felt like the opening credits–and that is just one of many generative artificial intelligence (AI) tools. Now high-profile tech leaders such as Apple co-founder Steve Wozniak and Tesla chief executive officer (CEO) Elon Musk are among those asking companies to hold back on "giant AI experiments"[1] while the industry conducts a risk assessment. Their open letter states that large-scale AI projects "can pose profound risks to society and humanity" without oversight and intelligent management and asked for a temporary pause on further development. The letter also stressed the need for governance systems and a new regulatory authority dedicated to AI.

Still, other industry leaders believe both the benefits and risks of generative AI have been exaggerated[2]–that we are dealing with limited technologies that aren't nearly as helpful as our biggest hopes or as powerful as our worst fears. But one conclusion is certain: AI is already sweeping through our businesses and our world, and the need for chief information security officers (CISOs), IT risk managers, executives and IT senior management to keep pace with the rapidly evolving risk landscape is urgent.

1 Futureoflife.org, "Pause Giant AI Experiments: An Open Letter," 22 March 2023, https://futureoflife.org/open-letter/pause-giant-ai-experiments/
2 Rundle, J.; "Cybersecurity Chiefs Navigate AI Risks and Potential Rewards," *The Wall Street Journal*, 25 May 2023, https://www.wsj.com/articles/cybersecurity-chiefs-navigate-ai-risks-and-potential-rewards-9138b76d

When Corporate Wisdom Meets Artificial Intelligence

Just months ago, it was hard to imagine that professionals from every industry would turn to one application to generate legal arguments and advice, computer code, Shakespearean-style sonnets and clinical treatment plans. Yet millions of users have quickly acclimated to the convenient new world of generative AI tools such as OpenAI's ChatGPT[3] and Google's Bard.[4] Despite its immense success and myriad of uses, most users are not familiar with the dangers of generative AI. Consequently, as companies leap into a white-hot race to design and utilize AI tools, many risk management efforts are falling behind.

The effort to establish and use emerging technology should not come at the expense of risk management. Unfortunately, this is a pattern common to most new technologies. Those who remember the advent of smartphones, 3D printing or the Internet of Things (IoT) may assume the emergence of AI is on par with those breakthroughs. But it is more akin to the creation of the automobile or the Internet: a blaze of innovation that will engulf every industry.

The effort to establish and use emerging technology should not come at the expense of risk management.

AI ushers in a foundational shift in how we engage with technology. The traditional guardrails and security protocols that have served us up to this point are now to a certain extent inadequate, as generative AI has only grown in popularity and influence. New territory includes new risk, and unlike previous quantum leaps in technology, businesses looking for a voice of authority are instead finding uncertainty about how to thoughtfully maximize AI value while deftly minimizing risk.

The Current State of Artificial Intelligence

Despite AI's ability to mimic human thought patterns and speech, none of it is sentient. Most of what is commonly referred to as AI is actually comprised of machine learning techniques or large language models (LLMs). For example, after being fed a dataset of 300 billion words,[5] ChatGPT consumed books, websites, Wikipedia and other sources and was trained using Reinforcement Learning from Human Feedback (RLHF), with the feedback improving its responses. Bard was trained in similar ways but also draws its information from the Internet. Megatron,[6] a joint venture between Microsoft and Nvidia, was trained through novel "parallelism" techniques and could soon surpass ChatGPT through a radical increase in capabilities. The techniques used to develop these tools raise questions about where the data used in LLMs is coming from and whether to trust this data to be used to train AI-enabled tools.

While a private company like ChatGPT has claimed the lion's share of the media spotlight, startups like ChatSonic, Jasper, Wordtune and others are helping users think of AI not as one tool but as a new type of

3 Openai.com, "Introducing ChatGPT," 30 November 2022, https://openai.com/blog/chatgpt
4 bard.google.com, "Try Bard, an AI experiment by Google,"https://bard.google.com/
5 Iyer, A.; "Behind ChatGPT's Wisdom: 300 Bn Words, 570 GB Data," Analytics India Magazine, 15 December 2022, https://analyticsindiamag.com/behind-chatgpts-wisdom-300-bn-words-570-gb-data/
6 Developer.nvidia.com, "Megatron-Turing Natural Language Generation," NVIDIA Developer, 3 October 2022, https://developer.nvidia.com/megatron-turing-natural-language-generation

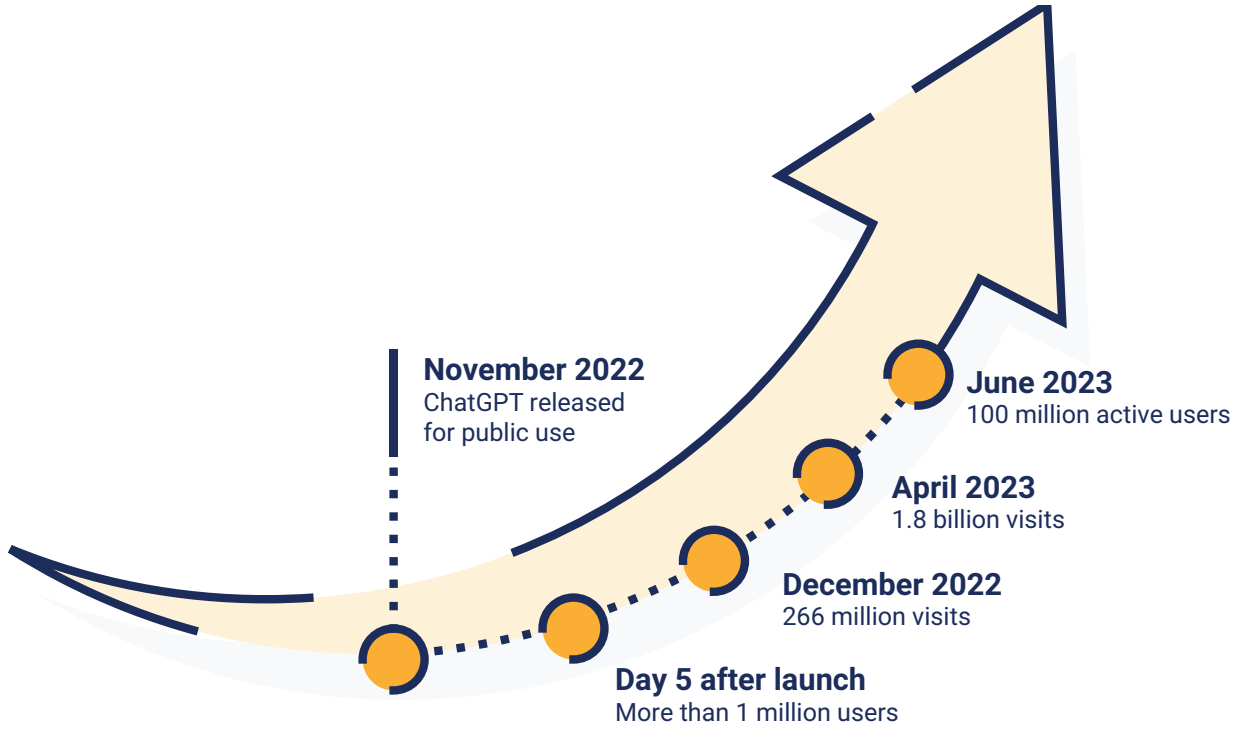
functional technology. This is in part through generative AI pre-training that uses information contributions from the private and public sectors. These companies are revolutionizing the way we interact with AI by providing a range of tools and services that cater to the diverse needs of users. In response to user feedback, creators are adding security controls, text classifiers and other features to become more competitive and useful.

For instance, Bard is designed to also work as a personal assistant and can complete tasks ranging from booking a holiday to creating a meal plan. ChatGPT is being integrated into Microsoft Office 365 as Microsoft 365 Copilot.[7] Soon, anyone using Microsoft Word, Excel or PowerPoint will be able to use Copilot to create a new presentation, develop go-to-market strategies or distill even the most complex financial data into a report.

The speed of AI evolution has dazzled even the most seasoned of tech veterans. Nearly every week brings a new pronouncement on AI's advantages, dangers, limitations or potential, with often contradictory conclusions. It is not a surprise that many business leaders have opted to wait for the AI dust to settle before designing a formal business strategy. But while this may seem like the safest path, a delay carries a risk of its own.

For this reason, no matter what shape the AI revolution takes, we know that AI is here to stay and that the safest and smartest path to security is to begin adapting now. Business leaders should assume that AI is already being used within the enterprise, as its popularity has only grown exponentially within the past couple of years. An example of the explosive growth[8] in the use of ChatGPT is shown in **figure 1**.

FIGURE 1: AI Use Breaks the Speed of Sound



7 Spataro, J.; "Introducing Microsoft 365 Copilot – your copilot for work," The Official Microsoft Blog,16 March 2023, https://blogs.microsoft.com/blog/2023/03/16/introducing-microsoft-365-copilot-your-copilot-for-work/

8 Ruby, D.; "30 + Detailed ChatGPT Statistics – Users & Facts," DemandSage, 7 July 2023, https://www.demandsage.com/chatgpt-statistics/

To AI or Not to AI

> The horse is here to stay, but the automobile is only a novelty—a fad.[9]
>
> —Advice from Michigan Savings Bank to Henry Ford's lawyer Horace Rackham

Some organizations, scared of the unknown, have taken to ignoring AI's growing influence. Others, afraid of another technological gimmick, dismiss AI promises as mere hype. But wielded well, AI tools can augment human ideas, complement business processes and distill complex information into digestible content, all of which can drive higher profit and performance.

From the wheel to the automobile, history shows that any technology that lets us do more with less effort has been wildly popular–as generative AI has proven. From automating mundane tasks to generating creative content, generative AI has demonstrated its potential to enhance productivity and unleash human creativity. Already, some workers view using AI as normal as checking email or purchasing goods online. It is only a matter of time before AI is enmeshed with our personal and professional lives.

Despite its infiltration into almost every facet of society and culture, some businesses have banned or restricted AI use. Stack Overflow, which offers a forum for coding questions and answers, temporarily banned ChatGPT[10] because of its tendency to give incorrect answers that sound confident and legitimate, leading users to be confused or mislead when looking for relevant answers to their questions. Samsung Electronics,[11] Apple,[12] JPMorgan Chase[13] and Verizon Communications[14] have heavily restricted the workplace use of generative AI over security fears.

While these restrictions make sense given the current ambiguity of AI capabilities and consequences, most business leaders realize decisions regarding the long-term AI landscape will be far more complex than a simple yes or no. If an enterprise bans AI completely, it could minimally risk its competitive advantage as some employees, partners, distributors and competitors may benefit from it. Even if AI-enabled tools are not used in the enterprise, ignoring this technology can leave an enterprise more vulnerable to risk (e.g., obsolescence, lower access to top talent, etc.).

From the wheel to the automobile, history shows that any technology that lets us do more with less effort has been wildly popular–as generative AI has proven.

For this reason, senior leaders, if they wish to utilize AI technologies, will need to ensure the right infrastructure and governance processes are in place at their organizations. To accurately understand the vulnerabilities and advantages AI carries, leaders must conduct a thorough risk impact analysis that accounts for the current uncertainty of the AI landscape and its future power.

Identifying AI Risk and Reward

AI is poised to permeate businesses in every industry. From supplying students with ready-made academic essays to writing scripts for Hollywood studios and analyzing the flaws in factory floor designs, AI offers benefits to nearly every team, field and organization. On a collective industry level (and individual business level),

9 Bushnell, S.T.; *The Truth About Henry Ford*, The Reilly & Lee Company, USA, 1992
10 meta.stackoverflow.com, "Temporary policy: ChatGPT is banned," https://meta.stackoverflow.com/questions/421831/temporary-policy-chatgpt-is-banned
11 Cawley, C.; "Samsung Restricts Generative AI Use After Code Leak," Tech.co, 8 May 2023, https://tech.co/news/samsung-restricts-generative-ai-use#:~:text=New%20Policy%20Bans%20Samsung%20Employeesz
12 Tilley, A.;M. Kruppa; "Apple Restricts Employee Use of ChatGPT, Joining Other Companies Wary of Leaks," *The Wall Street Journal*, 18 May 2023, https://www.wsj.com/articles/apple-restricts-use-of-chatgpt-joining-other-companies-wary-of-leaks-d44d7d34?mod=article_inline
13 Lukpat, A.; "JPMorgan Restricts Employees From Using ChatGPT," *The Wall Street Journal*, 22 February 2023, https://www.wsj.com/articles/jpmorgan-restricts-employees-from-using-chatgpt-2da5dc34?mod=article_inline
14 Moneylife.in, "JPMorgan Chase restricts workers from using ChatGPT," 23 February 2023, https://www.moneylife.in/article/jpmorgan-chase-restricts-workers-from-using-chatgpt/69948.html

leaders must take four important steps to maximize AI value while installing appropriate and effective guardrails:

1. Identify AI benefits.
2. Identify AI risk.
3. Adopt a continuous risk management approach.
4. Implement appropriate AI security protocols.

If business leaders are able to follow these steps, they are much more likely to strike a good balance of risk versus reward as AI-enabled tools and processes are leveraged in their enterprises.

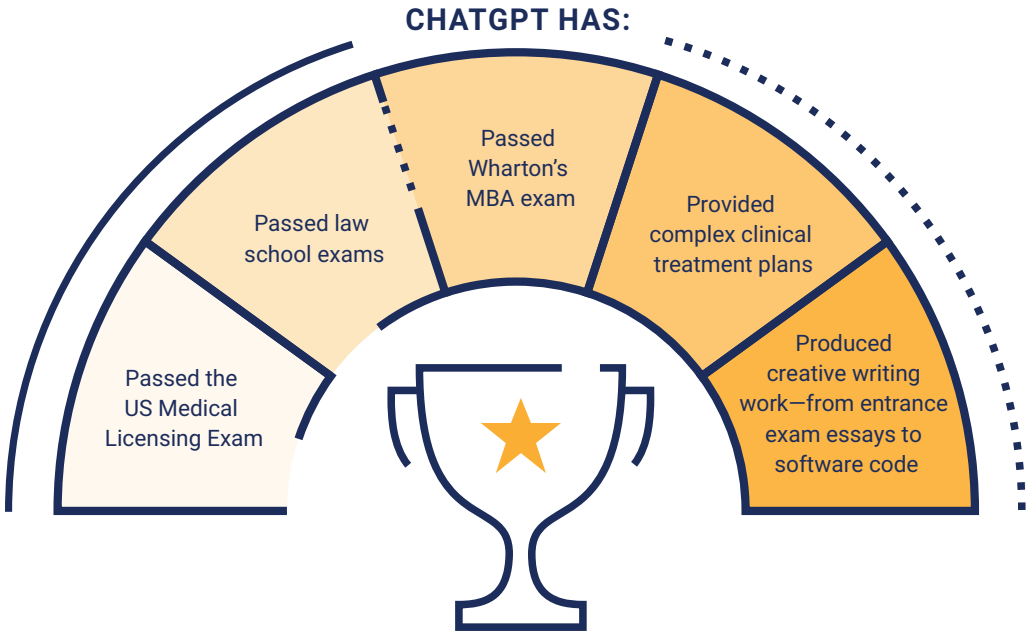
Conducting an AI Benefit Analysis

Leaders and philanthropists like Bill Gates foresee a cornucopia of AI benefits,[15] from bringing healthcare and education to the underserved to rectifying the impacts of climate change. For enterprises, potential advantages include better innovation, efficiency, productivity and workforce optimization. Companies are already looking to automate tasks with AI and reallocate staff to more value-driving work where they can, for example, focus on designing a remarkable new service line or developing more attentive client relationships.

Companies that wish to opt out of leveraging AI will most likely find themselves on a path to obsolescence. Just as AI programs captivated billions of users in mere weeks, the speed at which these programs will change markets and product capabilities could be staggering.

Enterprise titans may find that their AI-enabled competition is smarter, faster and more lethal than ever before. **Figure 2** contains some sample use cases.[16]

FIGURE 2: AI Insecurity Complex—Is AI Smarter Than We Are?



15 Gates, B.; "The Age of AI has begun," GatesNotes, 21 March 2023, https://www.gatesnotes.com/The-Age-of-AI-Has-Begun

16 Ault, A.; "AI Bot ChatGPT Passes US Medical Licensing Exams Without Cramming – Unlike Students," Medscape, 26 January 2023, https://www.medscape.com/viewarticle/987549; Sloan, K.; "ChatGPT passes law school exams despite 'mediocre' performance," Reuters, 25 January 2023, https://www.reuters.com/legal/transactional/chatgpt-passes-law-school-exams-despite-mediocre-performance-2023-01-25/; businesstoday.in, "'Next step for AI': ChatGPT clears US Medical Licensing Exam and Wharton's MBA exam," Business Today, 25 January 2023, https://www.businesstoday.in/technology/story/next-step-for-ai-chatgpt-clears-us-medical-licensing-exam-and-whartons-mba-exam-367569-2023-01-25;tribalhealth.com, "AI is Passing Med School Exams,"24 January 2023, https://tribalhealth.com/chatgpt/; Whitford, E.; "Here's How Forbes Got The ChatGPT AI To Write 2 College Essays In 20 Minutes," Forbes, 9 December 2022, https://www.forbes.com/sites/emmawhitford/2022/12/09/heres-how-forbes-got-the-chatgpt-ai-to-write-2-college-essays-in-20-minutes/?sh=313d2f3b56ad; Hutson, M.; "AI learns to write computer code in 'stunning' advance," Science, 8 December 2022, https://www.science.org/content/article/ai-learns-write-computer-code-stunning-advance

Use of AI Toughens Competition

Company A is an industry leader that has dominated its market for 10 years on the strength of one flagship product. The CEO feels secure in the company's position, as competitive intelligence assures her that no other company's research and development approaches the functionality of Company A's product.

Then an upstart named Company B uses AI to develop research, design a groundbreaking product, create pricing models and marketing plans, launch a new website and populate online sales channels–all within two weeks, with minimal workforce.

Within just two staff meetings, Company A's product becomes viewed as outdated, its customer base decamps for Company B and profits begin to plunge. Other upstarts begin to use AI to dethrone Company B. The market shifts radically within a few months, with Company A fighting and failing to remain relevant.

To conduct an exhaustive benefit analysis of any technology, leaders should look beyond simplistic advantages and revisit the foundational ethos of their companies. Some considerations include:

- What does the company do, and why do they do it?
- How do they do it?
- How are the company's competitors leveraging AI tools?
- What tools and talents do they rely on, and what are their metrics for success?
- How much will investment in AI cost, and how much return on investment does it deliver?
- How confident is the company that its security protocols and mechanisms will help ensure data quality, integrity and confidentiality (e.g., intellectual property, personal identifiable information, etc.)?
- How might the company's current strategy and objectives evolve when AI removes significant cost and talent barriers?
- What could staff and partners bring to the AI innovation table?

The answers to these questions will provide a roadmap that connects AI use cases to the company's mission and goals.

Identifying AI Risk

The potential risk associated with AI has been predominantly characterized as a future concern. However, proactively addressing this risk can help to ensure the safe and responsible development of AI technology for use in the business.

Dr. Geoffrey Hinton, commonly referred to as the "godfather" of AI, recently resigned from Google with a formal admission of regret about his work, calling some of the dangers "quite scary."[17] His work on neural networks and deep learning provided the foundation for what we now call AI programming; he has outlined ways future AI capabilities could exceed our understanding and therefore limit our ability to mobilize or institute effective safeguards.

Despite the importance of recognizing future risk, the present state of AI technology and our utilization patterns present immediate risk that must be addressed.

17 Vallance, B.; C. Vallance; "AI 'godfather' Geoffrey Hinton warns of dangers as he quits Google," BBC News, https://www.bbc.com/news/world-us-canada-65452940

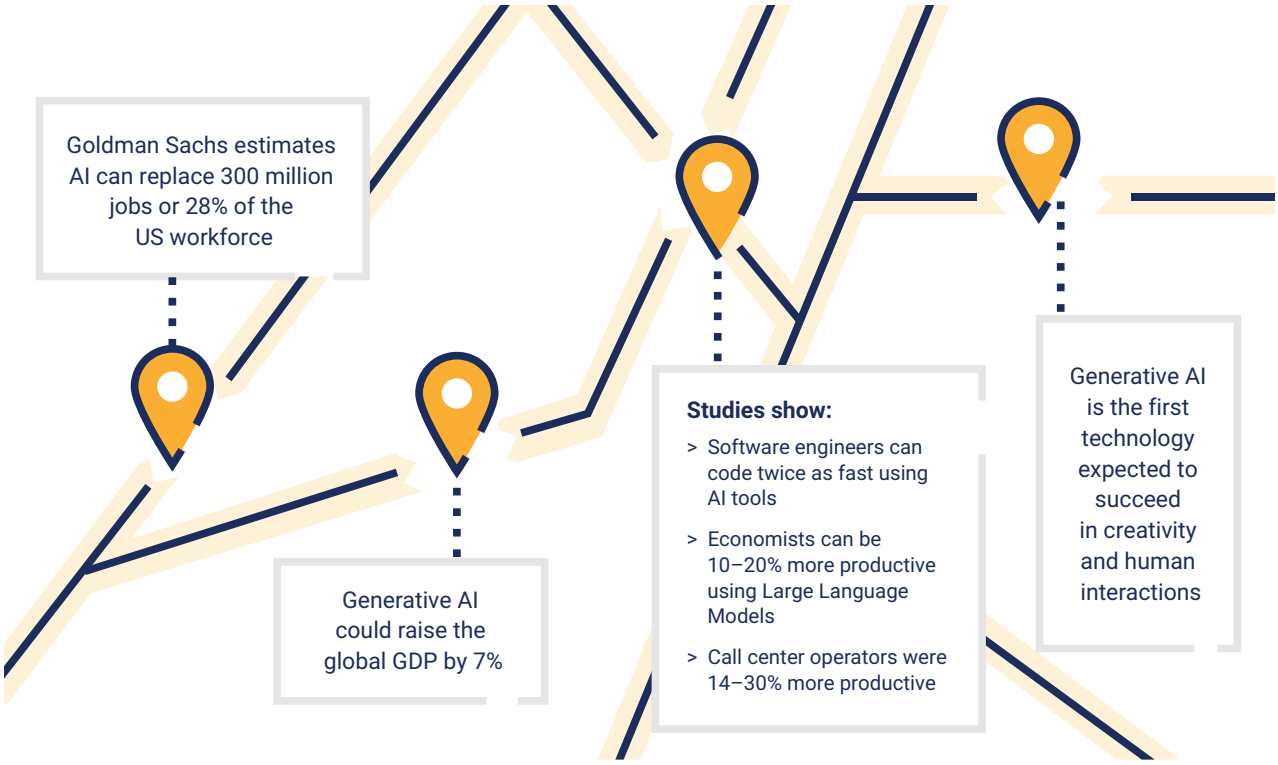
This risk can be broadly summed up: AI can exacerbate any existing issues, such as a lack of quality control or poor data integrity, and systems will be vulnerable to cyberattacks and may introduce new ones. From data breaches to CEO fraud, AI can quickly amplify a "controlled" risk to a chaotic level, potentially derailing an unprepared business. Some notable examples of how AI is changing business functions can be found in **figure 3**.[18]

However useful AI might be, it is not without inherent risk. Key aspects of AI risk are covered in the following sections.

Societal Risk

As AI continues to influence society, we must remain critical of its aims and potential harm. AI can be used to generate disinformation and manipulate populations and political demographics in a convincing and damaging way. AI has already been used in the execution of new types of cybercrime (e.g., deep fakes, sophisticated phishing emails, AI voice generators, etc.). For example, a fake image of an explosion at the Pentagon was widely circulated on Twitter, causing the stock market to react.[19] This incident illustrates how AI-generated

FIGURE 3: Disruption, Displacement and Discovery—How Much Will AI Change Business?



18 Jones, J.; "AI could automate 300 million jobs. Here's which are most (and least) at risk," ZDNET, 27 May 2023, https://www.zdnet.com/article/ai-could-automate-25-of-all-jobs-heres-which-are-most-and-least-at-risk/; Elder, B.; "Surrender your desk job to the AI productivity miracle, says Goldman Sachs," Financial Times, 27 March 2023, https://www.ft.com/content/50b15701-855a-4788-9a4b-5a0a9ee10561; Neil-Baily, M.; E. Brynjolfsson; A. Korinek; "Machines of mind: The case for an AI-powered productivity boom," Brookings, 10 May 2023, https://www.brookings.edu/research/machines-of-mind-the-case-for-an-ai-powered-productivity-boom/; Kalliamvakou, E.; "Research: quantifying GitHub Copilot's impact on developer productivity and happiness," The GitHub Blog, 7 September 2022, https://github.blog/2022-09-07-research-quantifying-github-copilots-impact-on-developer-productivity-and-happiness/; Korinek, A.; "Language Models and Cognitive Automation for Economic Research," National Bureau of Economic Research, https://doi.org/10.3386/w30957; Brynjolfsson, E.; D. Li; L. Raymond; "Generative AI at Work," National Bureau of Economic Research, https://doi.org/10.3386/w31161; Chui, M.; R. Roberts; L. Yee; "Generative AI is here: How tools like ChatGPT could change your business," McKinsey, 20 December 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/generative-ai-is-here-how-tools-like-chatgpt-could-change-your-business

19 Bond, S.; "Fake viral images of an explosion at the Pentagon were probably created by AI," NPR, 22 May 2023, https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai

misinformation can have far-reaching consequences, undermining the stability of financial markets and eroding trust in institutions. It is for this reason that mechanisms will need to be developed for companies and users to be able to weed out misinformation. It is also up to the users of AI tools to evaluate the information presented to them in order to mitigate its potential negative impacts. Furthermore, the potential for economic upheaval is directly linked to job displacement; it is predicted that over 300 million jobs[20] will be impacted by ChatGPT models, with unemployment affecting many industries and professions.

IP Leakage and Invalidation

Many AI users have thoughtlessly fed intellectual property (IP), trade secrets, competitor content and other data into AI models, which introduces a range of privacy risk. Recently, for instance, Samsung employees accidentally leaked proprietary company information by using ChatGPT.[21] Another example could involve a pricing and commodities company that wants to keep its wholesale prices confidential.

However, if they allow employees to utilize AI tools, that confidential information could become public if an employee copies and pastes it into an AI program. Additionally, the aforementioned Microsoft Copilot will scour internal company data on SharePoint, Excel spreadsheets, Slack, emails, Teams messages and OneDrive, potentially sharing private and sensitive data.

For this reason, some companies like Amazon have warned employees not to share sensitive information with ChatGPT.[22] Still, many more companies have no such policies or warnings, which should include a clear definition of what the company deems sensitive information. The policies should also ensure alignment with employees who may otherwise be oblivious to the copyrights, trademarks and sensitive information they are sharing with an enormous digital repository that can share it with others.

It should also be mentioned that disgruntled employees who realize the implicit harms of sharing this information may purposefully feed the AI tool data to potentially harm the company's reputation. Employees inserting information into AI applications could invalidate patents and other IP as IP protection is controlled by complex laws. For instance, if a company fails to protect its trade secrets adequately because of employee negligence, it may forfeit the legal protections afforded to the confidential information.

Invalid Ownership

Any company using AI to create output—such as a marketing tagline—must guarantee it is truly original IP and not a derivative of another person's work.[23] If not, these businesses may discover their ownership of the new assets is invalid. Further, the US Copyright Office has rejected copyrights for some AI-generated images,[24] depending on whether they were created from text prompts or if they reflect the creator's "own mental conception."

Invalid ownership could also occur if, for example, a writer copy and pastes a link to an admirable piece of competitor content as inspiration into an AI tool and is given back half-plagiarized content.[25] Invalid ownership claims regarding AI can ultimately lead to legal disputes and adversely impact an enterprise's reputation.

20 *Op cit* Jones
21 Maddison, L.; "Samsung workers made a major error by using ChatGPT," Techradar,4 April 2023, https://www.techradar.com/news/samsung-workers-leaked-company-secrets-by-using-chatgpt
22 Sengupta, A.; "Amazon warns employees about ChatGPT, says do not share sensitive info with chatbot," India Today,27 January 2023, https://www.indiatoday.in/technology/news/story/amazon-warns-employees-chatgpt-do-not-share-sensitive-info-with-chatbot-2327014-2023-01-27
23 McKendrick, J.; "Who Ultimately Owns Content Generated By ChatGPT And Other AI Platforms?", Forbes, 22 February 2023, https://www.forbes.com/sites/joemckendrick/2022/12/21/who-ultimately-owns-content-generated-by-chatgpt-and-other-ai-platforms/?sh=21cf97855423
24 Brittain, B.; "U.S. Copyright Office says some AI-assisted works may be copyrighted," Reuters,15 March 2023, https://www.reuters.com/world/us/us-copyright-office-says-some-ai-assisted-works-may-be-copyrighted-2023-03-15/
25 Duffy, J.; "Why Writers Know Using ChatGPT Is a Bad Idea," PCMAG, 25 January 2023, https://www.pcmag.com/opinions/why-writers-know-using-chatgpt-is-a-bad-idea

Cybersecurity and Resiliency Impact

From application programming interface (API) integration to the creation of increasingly persuasive phishing emails, AI opens the door to a much more sophisticated world of cybercrime. Bad actors are already using AI to write malware faster, generate hacking scripts, launch ransomware attacks and convincingly imitate CEO voices.[26]

The accessibility of AI is perhaps its greatest risk, as all that an attacker needs to do is insert a simple prompt into an AI tool. Little to no programming or specialized knowledge is necessary to launch an exploit. This has democratized the use of AI, allowing almost any individual to harness its power for harm.

AI opens the door to a much more sophisticated world of cybercrime.

AI offers would-be attackers who lack technical skills a ladder into cybercrime, as they can simply use an AI-powered penetration pre-testing tool like PentestGPT and a prompt such as, "Find me a security vulnerability for a specific piece of technology like Windows, Amazon Web Services or industrial control systems and write code to exploit it." Then, the attacker can paste in code from an email server, and the AI will write a script to exploit the vulnerability.

Backup and disaster recovery is another concern that should not be overlooked. AI must be factored into incident response and business continuity plans, both from the perspective of an AI-related incident and AI-driven response plan.

PentestGPT

- ChatGPT has been used to create an info stealer, encryption tools and dark web malware scripts.[27]
- Darktrace reported a 135-percent rise[28] in spam emails to clients between January and February featuring dramatically better English-language grammar and syntax. The company stated they believed hackers used generative AI applications to craft their campaigns and sound more convincingly American.[29]
- Video clips of Zscaler CEO Jay Chaudhry's voice were turned into a remarkably effective attempt at CEO fraud[30] through AI tools. The company also said AI was a factor in the 47 percent rise in phishing attacks[31] Zscaler saw in 2022.
- Fifty-one percent of IT professionals predict that we will witness a successful cyberattack done with the help of ChatGPT[32] by the end of this year, according to Blackberry Research.

Weak Internal Permission Structures

One of the first opportunities many business leaders identified in AI was the optimization of internal systems, like enterprise resource planning or pricing models and inventory systems. They did not foresee that after inputting information for these systems, employees were then able to ask the same tool for their colleagues' salaries and other sensitive information. While this risk may not seem specific to AI, consider how using tools such as PassGPT (an LLM used to guess and generate passwords)[33] significantly increases the likelihood of access exploits and other security breaches.

26 Menn, J.; "Cybersecurity faces a challenge from artificial intelligence's rise," The Washington Post, 11 May 2023, https://www.washingtonpost.com/technology/2023/05/11/hacking-ai-cybersecurity-future/

27 research.checkpoint.com, "OPWNAI: Cybercriminals Starting to Use ChatGPT," 6 January 2023, https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

28 darktrace.com, "Major Upgrade to Darktrace/Email™ Product Defends Organizations Against Evolving Cyber Threat Landscape, Including Generative AI Business Email Compromises and Novel Social Engineering Attacks," 3 April 2023, https://darktrace.com/news/darktrace-email-defends-organizations-against-evolving-cyber-threat-landscape

29 *Ibid*.

30 foxbusiness.com, "Zscaler's Jay Chaudhry gives chilling example of an AI deepfake," 2 June 2023, https://www.foxbusiness.com/video/6328691103112

31 Zscaler.com, "Zscaler ThreatLabz 2023 Phishing Report," https://info.zscaler.com/resources-industry-reports-threatlabz-phishing-report

32 Singh, S.; "IT Leaders Predict ChatGPT-Enabled Cyberattacks Are Imminent," Blackberry, 2 February 2023, https://blogs.blackberry.com/en/2023/02/it-leaders-predict-chatgpt-enabled-cyberattacks-are-imminent

33 Lanz, J. A.; "Meet PassGPT, the AI Trained on Millions of Leaked Passwords," Decrypt, 9 June 2023, https://decrypt.co/144004/meet-passgpt-aitrained-millions-leaked-passwords

Skill Gaps

In March 2023, the Biden-Harris administration announced a new National Cybersecurity Strategy.[34] Some of its more impactful changes include rebalancing the responsibility of security controls and asking software vendors to bear more accountability. To realistically implement these measures, IT staff will need advanced skillsets they may not currently have to defend the enterprise against highly skilled AI attacks. It also means potentially significant impacts on budgets to reskill existing employees and/or acquire the necessary talent.

Cyberexperts have also urged the creation of a nationwide digital identity framework[35] that will track citizen activity. Implementing and controlling these changes requires advanced technical skills that go beyond those of an average IT department.

Overreactions

IT professionals have long observed a pattern following ransomware attacks. Businesses that ignore their cybersecurity programs are attacked, after which they panic and overspend on security tools that do not always complement each other, which can increase their vulnerability to a second attack.

The same dynamic is likely to play out as businesses realize the scope of AI security gaps—or experience a disaster themselves—and act overzealously in their response.

While some enterprises will react in a way that excludes AI from business processes, others may move in the other direction, overreacting favorably toward AI and placing too much trust in unvalidated AI output. Staff may find themselves tasked with impossible workloads and resort to workarounds without testing their AI output. Those untested assumptions will exacerbate quality control issues and pose a reputational risk for the organization.

Intended and Unintended Use

Most AI applications currently have ethical limitations baked into their design to prevent the misuse of their knowledge. Because of the guardrails built into a tool like ChatGPT, for example, someone who asks AI how to commit a violent act may be advised to see a therapist. Unfortunately, users have found a way to utilize jailbreak[36] prompts or use tools such as WormGPT[37] to bypass those limits, resulting in increased sophistication of business email compromise (BEC) attacks for obtaining information on topics ranging from making weapons to carrying out widescale violence.

Data Integrity

ChatGPT, Bard and other programs tend to produce deeply flawed content that looks legitimate and sounds confident. This leads users to place too much confidence in the outputs generated. When AI generates misinformation or information not backed by real-world data, it is called a "hallucination."[38] Users have also noticed that different AI programs will offer different answers[39] to historical questions and provide information without citations.

ChatGPT creator and Open.AI CEO Sam Altman admitted on Twitter[40] that it is "a mistake to be relying on [AI tools] for anything important right now," adding, "We have lots of work to do on robustness and truthfulness."

34 Whitehouse.gov, "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy," 2 March 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

35 Macdonald, A.; "Biden urged to consider federal digital identity framework," Biometric Update, 18 April 2022, https://www.biometricupdate.com/202204/biden-urged-to-consider-federal-digital-identity-framework

36 Loynds, J.; "How to jailbreak ChatGPT: Best prompts & more," Dexerto, 1 August 2023, https://www.dexerto.com/tech/how-to-jailbreakchatgpt-2143442/

37 Kelley, D.; "WormGPT - The Generative AI Tool Cybercriminals Are Using to Launch BEC Attacks," | SlashNext, 13 July 2023, https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

38 en.wikipedia.org, "Hallucination (artificial intelligence)," https://en.wikipedia.org/wiki/Hallucination_(artificial_intelligence)#:~:text=For%20example%2C%20a%20hallucinating%20chatbot

39 McCracken, H.; "If ChatGPT doesn't get a better grasp of facts, nothing else matters," Fast Company, 11 January 2023, https://www.fastcompany.com/90833017/openai-chatgpt-accuracy-gpt-4

40 Altman, S.; "ChatGPT is incredibly limited, but good enough at some things to create a misleading impression of greatness. it's a mistake to be relying on it for anything important right now. it's a preview of progress; we have lots of work to do on robustness and truthfulness.", Twitter, 10 December 2022, https://twitter.com/sama/status/1601731295792414720?lang=en

As such, enterprises should consider ensuring human beings are the ultimate decision makers by implementing dual control over outputs used to make life-impacting decisions, such as medical treatments, criminal justice, surveillance, incarceration and more. In this scenario, the AI-enabled tool can make recommendations but is not responsible for the final decision.

Some users do not know how to use the right ChatGPT prompts, resulting in incomplete or incorrect data output from poor sources. In addition, users may not trust the corpus (i.e., data) used to train the AI model because of the lack of transparency and traceability. To this end, how can companies detect plagiarism, assess the authority and source of data or identify systemic bias built into the data or AI algorithm? This will be difficult to prove (and almost impossible to detect) when dealing with a volume of information too large for any human to sort through.

The reliability of data depends on its source. As of right now, AI-enabled tools cannot guarantee the integrity of data. This uncertainty makes it difficult for users to determine which information is trustworthy and which should be verified or disregarded. For example, an attorney working on a legal brief expected to take 50 to 55 hours may find that a generative AI tool completes the brief in under five minutes. However, without the time to review and assess the caliber of the work, the attorney can no longer verify its authenticity as the volume of information is simply too high. This situation presented itself in Manhattan federal court in May 2023.[41]

Without proper data integrity measures in place, employees using AI tools may produce incorrect or misleading results, which can have serious consequences for both the enterprise and its data quality.

Liability

When a person commits a crime or simply makes a catastrophic mistake on the job, there is no question about accountability and redress. But if, for example, an AI chatbot makes inappropriate remarks to minors, who is liable? Who will the lawsuits target? Is the engineer who helped design the AI an accessory to the crime? Who is responsible for making decisions regarding AI utilization and accountability? It is important to ask these questions and discuss their implications, as companies that leverage AI to pursue a viable commercial market could wind up responsible for unintended consequences with no grounds for redress.

This will become a prime consideration with job automation. A certain amount of trust and accountability is assigned to any human employee, but when that person is replaced by a machine, who is liable when it goes awry? A personal liability issue caused by an employee becomes a company liability issue when the AI does something wrong. In the past, it may have been possible to address transgressions by correcting an employee's behavior. However, when no human can be held accountable, who bears the responsibility?

A certain amount of trust and accountability is assigned to any human employee, but when that person is replaced by a machine, who is liable when it goes awry?

By the time AI risk information goes to press or is well-known, new risk will likely be uncovered. Practitioners are encouraged to keep close tabs on the latest developments in AI by following the latest in academia and regulations.

41 Weiser, B.; "Here's What Happens When Your Lawyer Uses Chat GPT," The New York Times, 27 May 2023, https://www.nytimes.com/2023/05/27/nyregion/avianca-airline-lawsuit-chatgpt.html

Adopting a Continuous Risk Management Approach

Adopting a framework may help teams that are new to developing a continuous risk assessment approach. For example, new frameworks such as the AI Risk Management Framework (AI RMF 1.0)[42] from the National Institute of Standards and Technology (NIST) are intended to guide businesses through uncharted AI territory.

It is important to remember that accepting some risk is healthy and advantageous, while complete risk aversion–particularly when it comes to benefiting from emerging technology–can carry an excessive cost. To strike the right balance, the journey to a continuous risk approach involves three steps:

1. Identify the company's overall AI risk.
2. Define the company's risk appetite.
3. Monitor and manage risk.

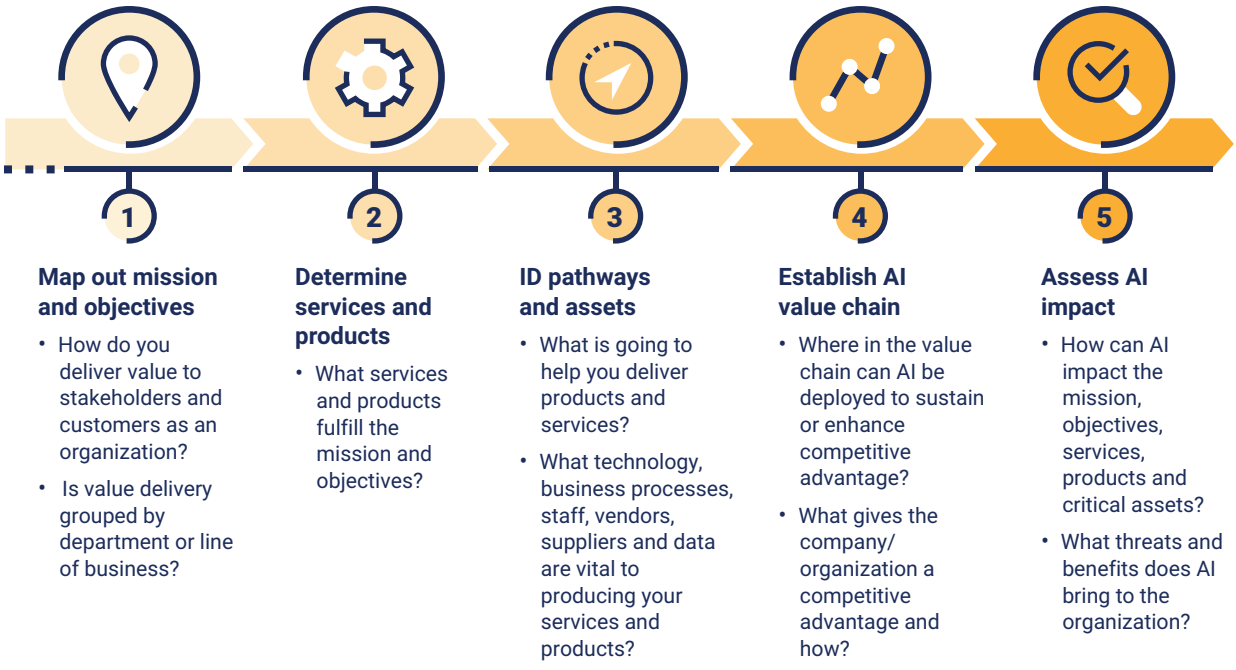
Step One: Identify Risk

To map out a tailored risk landscape, senior leadership and staff should work through possible loss-event scenarios and their impacts on organizational objectives. Use surveys, interviews, focus groups and brainstorming sessions to elucidate a full range of insights. An example risk identification process flow is shown in **figure 4**.

Step Two: Define Risk Appetite

Each risk should be evaluated and prioritized based on the severity of its potential impact and the likelihood of its occurrence. To help facilitate this, an AI exploration sub-committee can be established with responsibility to report findings and recommendations to enterprise risk management. This committee, comprised of key stakeholders, would be tasked with driving the work

FIGURE 4: Risk Identification Methodology



42 NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," January 2023, https://doi.org/10.6028/nist.ai.100-1

necessary to define which risk will fit within the enterprise's risk parameters versus which risk will require additional controls to be integrated into the enterprise's culture and objectives. Some risk will be assessed as carrying too high a potential cost.

Once the risk appetite is established, it should be documented and shared to ensure each team member understands their role in adhering to those limitations.

Step Three: Monitor and Manage Risk

To monitor and manage risk, leadership must recognize the potential impact of AI risk on their business, prioritize this risk in alignment with business objectives and take necessary measures to mitigate it while maximizing value. For this third step, an interdisciplinary oversight team of business and technology stakeholders (including legal, risk and compliance) should launch the risk management process. This process includes the following:

- Communicating the risk vision to all employees
- Prioritizing risk management activities
- Addressing all risk that requires action (such as new security controls) and instructing team members in addressing their area of risk
- Assigning ownership and personal accountability
- Identifying the frequency of risk monitoring

Once the risk management process runs smoothly, the risk oversight team should measure the success of their new security controls, track deviations from the risk program and continue assessing for new risk.

Just as AI is always evolving, risk management is always ongoing. For this reason, enterprises must adopt a continuous risk approach framework that tests assumptions with frequency and precision to ensure the quality of their AI output.

Building AI Security Programs: Eight Protocols and Practices

Effective cybersecurity has always required a proactive approach–and that is especially true with AI. After building a risk management foundation, enterprises must launch security policies and controls to mitigate the likelihood of data leakage and other AI misuse.

Smaller businesses may feel some of these controls and practices are beyond their scope. But in fact, AI can be an enormous security advantage for smaller organizations that may not have a CISO or dedicated cyber team on staff by automating process reviews or noncritical decisions that these human resources would be tasked with day to day. Alternatively, by engaging a managed service partner with specialized AI knowledge, these businesses can strengthen their security posture without increasing their headcount or exceeding their budget.

The eight practices discussed in this section may not account for AI developments and vulnerabilities down the road, but they can provide a thorough foundation of protection to any business beginning its AI journey.

One: Trust but Verify

In these early days of the AI revolution, law enforcement teams already use AI tools to predict crimes, and financial institutions use AI programs to predict loan defaults. It is clear that AI has the potential to improve efficiency, increase data-driven practices and expand capabilities for specific tasks and decisions, allowing for more informed and effective decision-making in law enforcement, finance and many other business sectors. Organizations utilizing AI most likely validate and blindly

follow the first AI-generated outputs. This is where organizations may develop misplaced trust in AI accuracy, just as we trust a calculator's math is correct and no longer bother to check.

However, it is important to remember that AI is not a calculator; it is a perpetually evolving and complicated tool, drawing from a sea of obscure data sources. Due to its iterative nature, AI platforms will be upgraded and also hacked and infiltrated. This is something we have already seen come to light when, in May 2023, OpenAI confirmed a data breach in its system.[43] Security researchers, technologists and hobbyists have taken to creating "jailbreaks" that work around the rules of the AI[44] to either produce unwanted content or even place malware into the AI model itself. Because of this, all output must be perpetually validated. This potentially burdensome task requires teams to develop mechanisms to assess and approve all AI-generated work.

Two: Design Acceptable Use Policies

Right now, most employees can use AI to design a banner ad, write an annual report or check the competitiveness of a sales model. This use of AI presents several concerns, including the sharing of proprietary company data and access to information not commensurate with their job responsibilities. Policy leaders must develop procedures and rules to enforce safe and ethical AI use. They must also collaborate with a diverse set of stakeholders and subject matter experts to design and pressure test these policies against unintended bias and discrimination. Policies should be augmented or modified to ensure they are consistent with evolving external requirements in the jurisdictions in which they operate (e.g., European Union AI Act). Additionally, employees should receive training on the appropriate and inappropriate uses of these tools to reduce risk. Another way to reduce risk is to implement approval chains and review processes, which can help prevent insider threats.

Three: Designate an AI Lead

Many enterprise C suites will likely have a Chief of Artificial Intelligence one day. That may be premature now–but organizations should consider appointing an analyst or project manager to track AI evolution and create a dedicated plan that documents the company's evolving relationship with AI tools. It is important that the AI lead collaborates with a cross-functional and diverse group of stakeholders which minimally includes representation from cybersecurity, data privacy, confidentiality, legal, procurement, risk and audit departments.

As we have seen, corporate use of AI has evolved at lightning speed in just months. To better navigate the path toward intelligent AI use, enterprises should begin documenting their history of using AI to track mistakes, misspent efforts and overlooked opportunities. Keeping track of this history will also help ensure AI-driven decisions can be explained because the steps to implement will be repeatable, thereby facilitating transparency.

Four: Perform a Cost Analysis

Similar to implementing cybersecurity measures, utilizing AI can place a financial burden on an organization. Conducting a thorough cost-benefit analysis for AI (e.g., evaluation on whether to build or buy AI tools) will be a critical first step–and these decisions will evolve as the level of cost prohibition lowers. Recently, a team of Stanford students built an AI platform called Alpaca for a mere $600,[45] proving that cost-effective AI solutions can be implemented. Organizations will need to calculate not only the cost-effectiveness of AI as a tool but also the price tag of security controls and the possible productivity gains and workforce optimization.

43 Poremba, S.; "ChatGPT Confirms Data Breach, Raising Security Concerns," Security Intelligence, https://securityintelligence.com/articles/chatgpt confirms-data-breach/

44 Burgess, M.; "The Hacking of ChatGPT Is Just Getting Started," Wired, 13 April 2023, https://www.wired.com/story/chatgpt-jailbreak-generative-ai-hacking/

45 Wodecki, B.; "Meet Alpaca: The Open Source ChatGPT Made for Less Than $600," AI Business, 20 March 2023, https://aibusiness.com/nlp/meet-alpaca-the-open-source-chatgpt-made-for-less-than-600

Five: Adapt and Create Cybersecurity Programs

CISOs and their security teams have two imperatives to follow in protecting the enterprise: adapting their current cyber programs and creating new AI-centric security practices across the organization (e.g., security by design). This process should begin as soon as possible, before any investment in AI strategies.

By using previous risk assessment work, enterprises can implement controls regarding the use of AI. This will help protect them from inevitable security events that occur in other less prepared organizations.

Ensuring AI-related risk considerations and security solutions are not an afterthought can reduce expensive rework or redesign of technology solutions.

AI-centric Security Practices

Eighty-two percent of IT professionals[46] would consider investing in cybersecurity to defend their organizations against AI-augmented cyberattacks in the next two years, with 48 percent considering it this year.

Ninety-five percent of participating professionals believe governments have some responsibility to regulate these types of technologies, with 85 percent rating that level of responsibility as either "moderate" or "significant."

When creating an AI cybersecurity program, a few areas to consider include:

- **IP Leakage**: Security and privacy teams should have the proper skillsets and controls to prevent IP leakage. Organizations can use permission-based access, visibility tools and firewall and application controls to determine where and how employees are using AI tools. These measures can prevent the unauthorized transfer of valuable company data and limit potential damage. For instance, when appropriate role-based access controls are established regarding data, the HR manager might be able to ask the AI tool about salaries from the LLM but only the company attorney can inquire about open HR cases. In addition, digital filters can block users from visiting private internal repositories. Training and policy commitments can also make employees understand the serious consequences of sharing sensitive information with AI tools.
- **Disaster Recovery and Incident Response**: AI can assist with business continuity and incident response planning in several ways. By analyzing operational data, AI tools can identify threats to business continuity, help devise response strategies and test them in simulated scenarios. When an unexpected disruption strikes, AI can automate certain phases of the business recovery plan, such as optimizing resource allocation to keep critical operations running.
- **Continuity**: AI use within an organization creates unique challenges for business continuity. Organizations that rely heavily on AI for business processes and functions can find themselves unable to operate if the AI tools stop functioning. For this reason, special consideration must be given to business continuity when crafting AI plans and strategies.
- **Threat Intelligence**: While many threat intelligence and cybermonitoring tools on the market already incorporate machine learning in some way, the latest generative AI tools can provide new insights regarding outputs and even detect threat alerts that were previously missed. Google released Google Cloud Security AI Workbench[47] in April, which can analyze code, perimeter security and networks for vulnerabilities. The platform creates a personalized threat profile to help teams proactively tighten their defenses through actionable intelligence and visibility across data sources. Organizations that implement tools like this may benefit from an increase in efficiency regarding threat awareness and remediation.

Six: Mandate Audits and Traceability

Enterprises will need better auditing and traceability capabilities around the AI model to understand where an AI tool is pulling its data and how it arrives at its decisions. Where did the source data come from? Has that data been manipulated by the AI or the human interacting with it? Is systemic bias a factor? These questions are integral in evaluating the trustworthiness of AI tools. The need for more trustworthy AI tools could become a competitive factor between AI models, with platforms offering transparency around how their model makes decisions.

46 Singh, S.; "IT Leaders Predict ChatGPT-Enabled Cyberattacks Are Imminent," BlackBerry, 2 February 2023, https://blogs.blackberry.com/en/2023/02/it-leaders-predict-chatgpt-enabled-cyberattacks-are-imminent

47 Potti, S.; "How Google Cloud plans to supercharge security with generative AI," Google Cloud Blog, 14 April 2023, https://cloud.google.com/blog/products/identity-security/rsa-google-cloud-security-ai-workbench-generative-ai

Seven: Develop a Set of AI Ethics

Many professionals have found that AI can help them deliver a service or product in a fraction of the time it took without it. However, if they are billing by the hour, they must reassess their pricing models and client contracts. They will also need to heed Microsoft's requirement to disclose AI interaction (e.g., ChatGPT-created work).[48]

Many people will likely ignore that directive. If a graphic designer is billing their client by the hour and quoted a project at 15 hours of work, they are required to disclose the use of AI. But that might reveal they spent one hour on the project, not 15. Thus, the use of AI presents a number of potential challenges in terms of the ethical use of AI tools. New software can detect AI creativity–just as academic integrity software detects cheating and plagiarism–but it may not catch everything. AI ethics must be addressed in each organization and industry as a serious standard of business operations.

Work is already being done to spotlight the ethical dimensions of AI in our daily lives. The United Nations Educational, Scientific and Cultural Organization (UNESCO), which has worked to create and enforce ethical guardrails in many scientific and technological areas, published its recommendation on the ethics of AI[49] in November 2021. Organizations like IBM[50] and the US Department of Defense[51] have adopted AI ethical principles, but we need to collectively work together to agree upon guidelines and ensure they are consistently enforced.

> In no other field is the ethical compass more relevant than in artificial intelligence….AI technology brings major benefits in many areas, but without the ethical guardrails, it risks reproducing real world biases and discrimination, fueling divisions and threatening fundamental human rights and freedoms.[52]
>
> –Gabriela Ramos, Assistant Director-General for Social and Human Sciences of UNESCO

Eight: Societal Adaptation

The decisions of many organizations will have a significant influence on the impact of AI on the economy. An organization facing widescale job displacement in their workforce with the introduction of AI-enabled tools can choose to help their employees train and transition into different jobs that offer new revenue streams.

Academics, from middle school teachers to medical school students, may have to change their assessment methodologies, while workplaces may need to rethink their performance review criteria. Both children and adults will need to be educated in the reality of deep fakes, AI errors and disinformation campaigns, just as we currently strive to educate citizens about Internet scams.

In addition, AI-based assessment tools used in the employee selection and placement process could result in the onboarding of unqualified candidates to an organization. As a result, these processes will need to be reevaluated to mitigate risk associated with using AI.

48 Microsoft Responsible AI Standard, v2 GENERAL REQUIREMENTS FOR EXTERNAL RELEASE. (2022). https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5cmFI

49 unesco.org, "Ethics of Artificial Intelligence," https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

50 ibm.com, "What are AI Ethics," https://www.ibm.com/topics/ai-ethics

51 defense.gov, "DOD Adopts Ethical Principles for Artificial Intelligence," 24 February 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

52 UNESCO, "UNESCO's Recommendation on the Ethics of Artificial Intelligence: **Key facts** ," 2023, https://www.unesco.org/en/articles/unescos-recommendation-ethics-artificial-intelligence-key-facts

Prospering in an AI-Powered Future

In *The Republic*, Plato said, "The beginning is the most important part of the work." How we begin our organizational response to AI will determine our long-term success in reaping its advantages and weathering its storms. As a society, now is the time to step back, reflect and map out the risk and repercussions of the AI revolution. The breakneck pace of the market–and the calls for regulation–may convince leaders to pause before official AI adoption or strategy work. But as with so many technologies, users have already surged ahead, creating a movement that demands action now. Analysis and action cannot wait, and the organizations that act fast will create the strongest foundation and prosper the most from this new era of artificial intelligence.

Acknowledgments

Lead Developer

Ryan Cloutier
CISSP
President, Security Studio, USA

Expert Reviewers

Urs Fischer
CISA, CRISC, CIA, CPA (Swiss)
Director, Tech Cyber Security Specialist, UBS Business Solutions AG, Switzerland

Larisa Gabudeanu
CDPSE, CIPM, CIPP/E
Researcher, Babes Bolyai University, Romania

Maria Koslunova
CIPM, CIPP, FIP
Data Privacy Educator, York University, UK

David Kuo
CISA, CIPT
Distinguished Fellow, Ponemon Institute, USA

Carol Lee
CISM, CRISC, CDPSE, CCISO, CCSP, CEH, Certified Change Management Practitioner, CIPM, CSSLP
Head of Cyber Security & Risk Management, Hang Lung Properties Ltd, China

Nsuhoridem Ndeokwelu
CGEIT, CRISC, CDPSE
IT Risk and Compliance Lead, Central Bank of Nigeria, Nigeria

Dina Nu'man
CRISC, ISACA COBIT Lead Assessor, ITIL
Head of Advanced Governance & Management, Scanwave, Jordan

Dilek Ozdemirci
CMMI Instructor, CMMI Lead Appraiser, CSM, PMP, SAFe PC, ITIL
Process Improvement Consultant, Dora Process Consulting Inc., Canada

ShanShan Pa
CISA, CISM, CDPSE, CIPM, CIPP/E, CIPP/US, CIPT, FIP
Managing Director, Alpha Technology Risk Management, State Street, USA

Max Shanahan
CISA, CGEIT, FCPA, MACS (senior), MIIA (Aust)
Governance and Assurance Consultant, Self Employed, Australia

Greg Shields
CISA, CRISC, CDPSE, CIPM, CIPT, CISSP
Senior Manager, Confidentiality and Privacy, Deloitte, USA

Alok Tuteja
CGEIT, CRISC
Global Head of Governance Risk and Compliance, Agthia PJSC, UAE

Patricia Voight
CISA, CISM, CGEIT, CRISC, CDSPE
Managing Director, FSO Consulting–Technology Risk, Ernst & Young LLP, USA

Board of Directors

John De Santis, Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Brennan P. Baybeck, Vice-Chair
CISA, CISM, CRISC, CISSP
Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Stephen Gilfus
Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP, NACD.DC
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, France

Gabriela Hernandez-Cardoso
NACD.DC
Independent Board Member, Mexico

Jason Lau
CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP
Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo
Independent Director, Former Chief Executive Officer and Executive Director, VADS Berhad Telekom, Malaysia

Maureen O'Connell
NACD.DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Erik Prusch
Chief Executive Officer, ISACA, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

Pamela Nigro
ISACA Board Chair 2022-2023
CISA, CGEIT, CRISC, CDPSE, CRMA Vice President, Security, Medecision, USA

Gregory Touhill
ISACA Board Chair 2021-2022
CISM, CISSP
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

About ISACA

ISACA® (https://www.isaca.org/) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *The Promise and Peril of the AI Revolution: Managing Risk* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/