WHAT IS CHATGPT?

Dave Hatter, CISSP, CISA, CISM,CCSP, CSSLP, Security +, Network+, PMP, ITIL V3

Director of Business Growth

Intrust IT

linkedin.com/in/davehatter

twitter.com/davehatter

www.youtube.com/user/davidlhatter

My goals for today

- Educate you
- Motivate you
- Provide actionable advice
- Engage and collaborate

"Machine intelligence is the last invention that humanity will ever need to make." - Nick Bostrom

"Within a few decades, machine intelligence will surpass human intelligence, leading to The Singularity — technological change so rapid and profound it represents a rupture in the fabric of human history." - Ray Kurzweil

Intelligence

"The capacity for abstraction, logic, understanding, self-awareness, learning, emotional knowledge, reasoning, planning, creativity, critical thinking, and problem-solving. More generally, it can be described as the ability to perceive or infer information, and to retain it as knowledge to be applied towards adaptive behaviors within an environment or context." - Wikipedia

Artificial Intelligence (AI)

"perceiving, synthesizing, and inferring information—demonstrated by machines, as opposed to intelligence displayed by humans or by other animals. Example tasks in which this is done include speech recognition, computer vision, translation between (natural) languages, as well as other mappings of inputs." - Wikipedia

Artificial General Intelligence (AGI)

"a type of hypothetical intelligent agent. The AGI concept is that it can learn to accomplish any intellectual task that human beings or other animals can perform. Alternatively, AGI has been defined as an autonomous system that surpasses human capabilities in the majority of economically valuable tasks." - Wikipedia
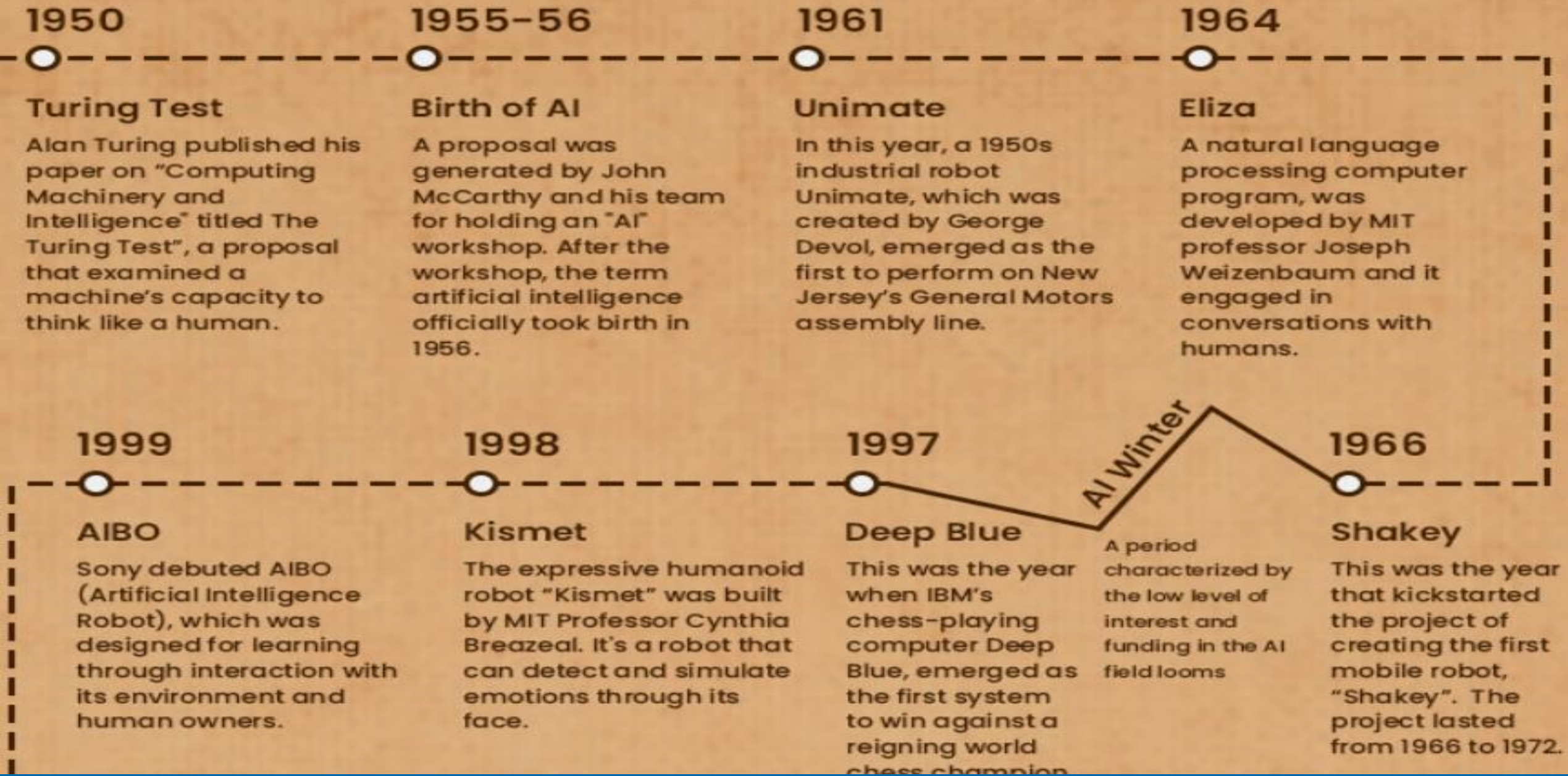
Superintelligence

"a hypothetical agent that possesses intelligence far surpassing that of the brightest and most gifted human minds. "Superintelligence" may also refer to a property of problem-solving systems (e.g., superintelligent language translators or engineering assistants) whether or not these high-level intellectual competencies are embodied in agents that act in the world." - Wikipedia

Timeline

1950

Turing Test

Alan Turing published his paper on "Computing Machinery and Intelligence" titled The Turing Test", a proposal that examined a machine's capacity to think like a human.

1955-56

Birth of AI

A proposal was generated by John McCarthy and his team for holding an "AI" workshop. After the workshop, the term artificial intelligence officially took birth in 1956.

1961

Unimate

In this year, a 1950s industrial robot Unimate, which was created by George Devol, emerged as the first to perform on New Jersey's General Motors assembly line.

1964

Eliza

A natural language processing computer program, was developed by MIT professor Joseph Weizenbaum and it engaged in conversations with humans.

1999

AIBO

Sony debuted AIBO (Artificial Intelligence Robot), which was designed for learning through interaction with its environment and human owners.

1998

Kismet

The expressive humanoid robot "Kismet" was built by MIT Professor Cynthia Breazeal. It's a robot that can detect and simulate emotions through its face.

1997

Deep Blue

This was the year when IBM's chess-playing computer Deep Blue, emerged as the first system to win against a reigning world chess champion

AI Winter

A period characterized by the low level of interest and funding in the AI field looms

1966

Shakey

This was the year that kickstarted the project of creating the first mobile robot, "Shakey". The project lasted from 1966 to 1972.

Timeline

2002

Roomba

The popular Roomba was released by i-Robot, which was an autonomous robot vacuum cleaner that cleans while dodging hurdles.

2011

Watson

Two former Jeopardy! Champions Ken Jenning and Brad Rutter lost to IBM's Watson, a natural language question-answering computer in a televised game.

2011

Siri

Apple released Siri, a built-in, voice-controlled personal assistant, available for Apple users.

2014

Eugene

A computer algorithm claiming to be a 13-year-old boy called Eugene Goostman passed the Turing test, managing to convince 33% of the human judges at a Royal Society event that it was a human.

2018

BERT

Google developed BERT (Bidirectional Encoder Representations from Transformers). This technology allows anyone to train their own state-of-the-art question answering system.

2017

Dialog agents

Two "dialog agents" (chatbots) get trained by the Facebook AI Research lab (chatbots) to negotiate via machine learning, inventing their own communication language.

2016

Sophia

Hanson Robotics developed the humanoid robot Sophia pegged to be the first "robot citizen".

2014

Alexa

The legendary Alexa was released by Amazon, which is a home assistant that develops into smart speakers, functioning as a personal assistant.

Timeline

2020

Open AI GPT-3

Open AI's GPT 3 was first introduced in May 2020 and was in beta testing in June 2020. This language model generates text by adopting algorithms that are pre-trained.

AI Benefits

- **Productivity gains**
- **New capabilities**
- **Better customer service**
- **Improved monitoring**
- **Reduction in human error**
- **Industry specific improvements**

AI Dangers

A.I. will cause 'significant labor-market disruption' over next 5 years, says World Economic Forum

Google's Sundar Pichai thinks A.I. will spur 'big societal labor market disruptions' but also make professions better

Brace Yourself for the 2024 Deepfake Election

AI could replace equivalent of 300 million jobs - report

NSA Cybersecurity Director Says 'Buckle Up' for Generative AI

AI Dangers

The Verge / Tech / Reviews /

ARTIFICIAL INTELLIGENCE / TECH

Elon Musk and top AI researchers call for pause on 'giant AI experiments'

TIME

The New AI-Powered Bing Is Threatening Users. That's No Laughing Matter

CNN BUSINESS Markets Tech Media Calculators Videos

AI pioneer quits Google to warn about the technology's 'dangers'

Forbes

Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find

The Guardian

'We are a little bit scared': OpenAI CEO warns of risks of artificial intelligence

Sam Altman stresses need to guard against negative consequences of technology, as company releases new version GPT-4

NEW YORK POST

MAY 23, 2023

Ex-Google exec Mo Gawdat warns AI will view humans as 'scum,' could create 'killing machines'

9abc CINCINNATI WCPO

Listen how AI can clone your voice, use it in phishing scams

Reporter's words recorded, then turned into the "Grandparent scam"

AI Dangers

- **Job loss**
- **Disinformation**
- **Propaganda**
- **Bias**
- **Cybercrime**
- **Copyright**
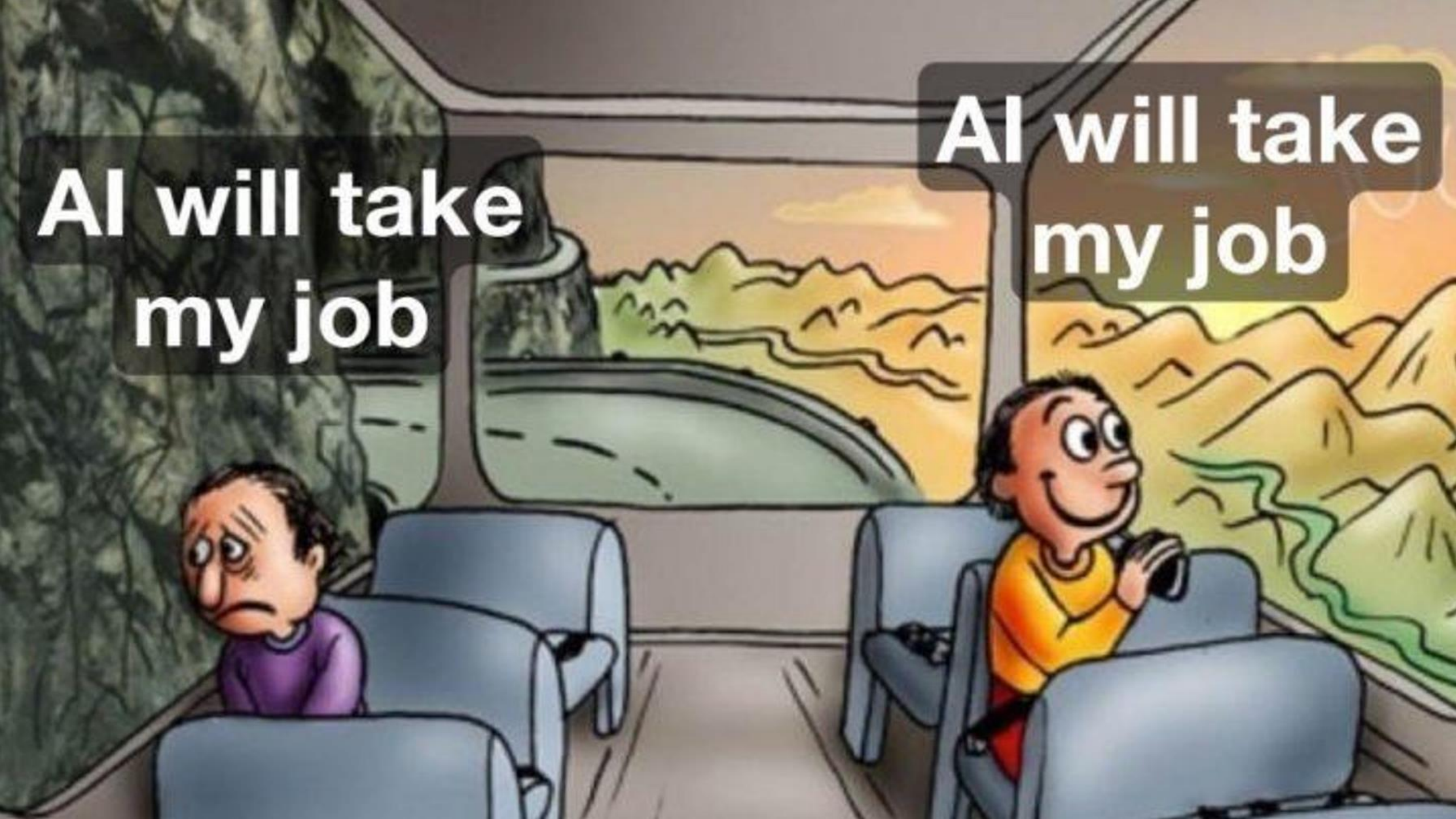
Generative AI

"is a type of artificial intelligence (AI) system capable of generating text, images, or other media in response to prompts Generative AI models learn the patterns and structure of their input training data, and then generate new data that has similar characteristics." - Wikipedia

Generative AI

"Notable generative AI systems include ChatGPT (and its variant Bing Chat), a chatbot built by OpenAI using their GPT-3 and GPT-4 foundational large language models, and Bard, a chatbot built by Google using their LaMDA foundation model. Other generative AI models include artificial intelligence art systems such as Stable Diffusion, Midjourney, and DALL-E."

Large Language Model

"A large language model (LLM) is a type of artificial intelligence (AI) algorithm that uses deep learning techniques and massively large data sets to understand, summarize, generate and predict new content. The term generative AI also is closely connected with LLMs, which are, in fact, a type of generative AI that has been specifically architected to help generate text-based content." – WhatIs.com

Large Language Model

"A large language model (LLM) is a type of artificial intelligence (AI) algorithm that uses deep learning techniques and massively large data sets to understand, summarize, generate and predict new content. The term generative AI also is closely connected with LLMs, which are, in fact, a type of generative AI that has been specifically architected to help generate text-based content." – WhatIs.com

LLM Training

How it works

"For example, you could type into an LLM prompt window "For lunch today I ate…." The LLM could come back with "cereal," or "rice," or "steak tartare." There's no 100% right answer, but there is a probability based on the data already ingested in the model. The answer "cereal" might be the most probable answer based on existing data, so the LLM could complete the sentence with that word. But, because the LLM is a probability engine, it assigns a percentage to each possible answer. Cereal might occur 50% of the time, "rice" could be the answer 20% of the time, steak tartare .005% of the time." – ComputerWorld

It is a "Black Box"

INPUT
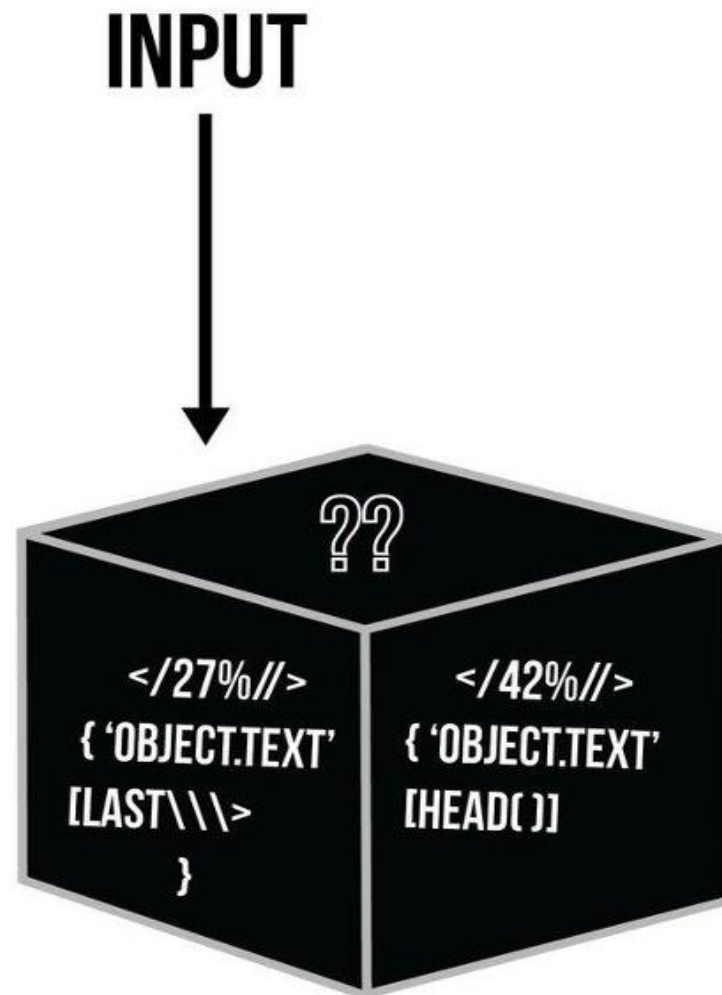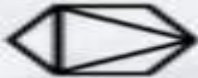
BLACK BOX

THE BLACK BOX IS AN ALGORITHIM THAT TAKES DATA AND TURNS IT INTO SOMETHING. THE ISSUE IS THAT BLACK BOXES OFTEN FIND PATTERNS WITHOUT BEING ABLE TO EXPAIN THEIR METHODOLOGY.

??

</27%//>
{ 'OBJECT.TEXT'
[LAST\\\>
}

</42%//>
{ 'OBJECT.TEXT'
[HEAD( )]

OUTPUT

General Generative AI Types

- **Text**
- **Audio**
- **Video**
- **Photo**

Generative AI Types

Video	◇ Muse AI	▶ Visla AI	▶ Topaz AI
Text	⬢ ChatGPT	N Notion AI	◉ Compose
Images	⛵ Midjourney	◉ Magic Studio	☁ Pebblely
Design	◆ Viesus	🐷 Piggy AI	✦ Galileo
Coding	🦫 Bugasura	N CodeGPT	⧉ Replit Ghostwriter
Audio	💬 FineShare	🎤 Boomy AI	Playlist AI
Productivity	🍃 Briefly AI	▲ Socra AI	🎧 Leexi AI

AI Chat and Search

- <u>ChatGPT</u>: Conversational AI trained on a large set of text from 2021 and earlier. Free, but costs $20 per month to speed up responses and use during peak demand.
- <u>The new Bing</u>: ChatGPT-based conversations and search results inside Bing. Limited beta requires joining a waitlist.
- <u>Perplexity.ai</u>: Ask questions and follow-ups, get direct responses with citations. Free to use with no limitations.
- <u>YouChat</u>: Ask questions and follow-ups, and engage in ChatGPT-style conversations. Free; sign-in required.
- <u>NeevaAI</u>: Get direct, AI-generated responses with citations, followed by standard search results. Free; sign-in required.
- <u>Poe</u>: Conversational AI from Quora that includes multiple assistants with differing strengths. Free; currently iPhone only.
- <u>Google Bard</u>: Conversational AI trained on a large set of text. Free; sign-in required

AI Art Generators

- **Stable Diffusion Online: Free Stable Diffusion artwork generator; no login required.**

- **El Pintador: Free Stable Diffusion artwork generator for iOS with a "Learn" section that provides prompt crafting advice.**

- **DiffusionBee: Stable Diffusion artwork generator for MacOS, works offline with no usage limits.**

- **Craiyon: Online artwork generator that uses the Dall-E Mini model. Removing watermarks requires a $5-per-month subscription.**

- **Dall-E: Create up to 15 free images per month with OpenAI's image-generation tool.**

- **Nvidia Canvas: Windows software that turns brushstrokes into artwork. Requires an Nvidia RTX graphics card.**

- **Playform: Online app that turns sketches into artwork. Free to try, but requires paid credits to download watermark-free images.**

AI Writing Tools

- **<u>PicsArt AI Writer</u>: Generate marketing copy, slogans, product descriptions, LinkedIn headlines, Instagram captions, and more. Free.**

- **<u>NotionAI</u>: Use prompts to create text inside any Notion document, activated by pressing Space on a new line. Free for up to 20 prompts, then $10 per month.**

- **Chatbot tools like ChatGPT, YouChat, and Poe can be used to generate copy as well.**

AI Content Summarizers

- <u>Eightify</u>: Create text summaries of YouTube videos, with highlights you can click on to jump to the relevant video section. Up to three free summaries per week (on videos less than an hour and with more than 30,000 views), then pay as you go.

- <u>Summarize.tech</u>: Another YouTube summarizer. Less in-depth than Eightify, but with no usage limits.

- <u>Gimme Summary</u>: Chrome extension for summarizing web articles, seemingly works by asking ChatGPT to condense the article content. Free to use, but slow.

- <u>SkimIt.ai</u>: Email an article link to go@skimit.ai, get a summary in 10 minutes.

- <u>WordTune Read</u>: View article and PDF summaries next to the full text, with excerpts highlighted. Three free summaries per month, then $120 per year.

- <u>OtterPilot</u>: Feature of the Otter meeting assistant that transcribes and summarizes video calls. Free for up to 30 minutes per call and 300 transcription minutes per month, then $17 per month.

- <u>Sonoteller.ai</u>: Paste a link to a song on YouTube, get an analysis of its lyrical content, instrumentation, genres, and moods. Free to use.

AI Speech To Text Transcribers

- <u>Whisper</u>: Online transcription of audio files using language models from OpenAI. Free.

- <u>Buzz</u>: Offline version of Whisper for Windows, free unlimited use.

- <u>MacWhisper</u>: Offline version of Whisper for Mac. Pay what you want, or $14 for larger language models and translation.

AI Visual and Audio Tools

- **AI VISUAL EDITORS**
    - <u>Runway</u>: Photo and video editor with an array of AI tools, including green screen, image expansion, and 3D texture creation. Free with limitations on export resolution and AI tool use, then $15 per month.
    - <u>Genmo</u>: Turn still images into animations using text prompts. Free with usage limits.
- **AI AUDIO TOOLS**
    - <u>Eleven Labs</u>: Generate speech from text, free for up to 10,000 characters of text per month. A $5-per-month subscription lets users clone an existing voice.
    - <u>Riffusion</u>: Generate music from text descriptions using Stable Diffusion. Free.
    - <u>Boomy</u>: Generate music tracks by specifying the genre, instruments, and production values. Free.
    - <u>Beatoven</u>: Create music by specifying the genre and mood. Free to use with up to 15 minutes of monthly downloads, then $20 per month.

ChatGPT

- **GPT = Generative Pre-trained Transformer**
- **2015: Founded as a non-profit with $1Billion pledged**
  - CEO: Sam Altman
  - Notable investors include Elon Musk, Peter Thiel, and Amazon Web Services
- **2018: Musk resigned from the board, but remained a donor**
- **2019: Transitioned to a "capped" for-profit to attract/retain talent**
  - Microsoft invested $1Billion
  - Announced its intention to commercially license its technologies
  - The non-profit entity is the sole controlling shareholder of the for-profit entity
- **2020: Announced GPT-3 and the API**
- **2021: Introduced DALL-E, an image generating AI**
- **November 2022: Launched free preview of ChatGPT 3.5**
  - Achieved over a million sign ups in the first 5 days
- **January 2023: Microsoft announced commitment of $10 Billion**
  - Estimated 100 million daily users
  - Investment valued the company at $29 Billion
  - Forecast $200M in revenue in 2023, $1B+ in 2024
- **February 2023: Microsoft announces it's building ChatGPT into its product**
- **ChatGPT 4 released March 14th, 2023**

Comparison

Exam results (ordered by GPT-3.5 performance)

Estimated percentile lower bound (among test takers)

Legend: gpt-4 (dark green), gpt-4 (no vision) (light green), gpt3.5 (blue)

What can you do with ChatGPT?

- **Generate ideas**

- **Understand complex topics**

- **Write copy**

- **Summarize research**

- **Get coding assistance**

- **Translate text**

- **Write a book**

- **Advance in your career**

- **Find data sets**

Ways to use ChatGPT

- **UI**

- **Apps**

- **Plugins**

  - ChatGPT Plus users can now access 70+ plugins

- **Application Programming Interface (API)**

How Intrust Uses AI

- **Writing**

- **Idea Generation**

- **Automation**

  - Code generation

  - Autoresponder

  - Intrust Man

  - Call resolution

  - Augment Robotic Process Automation (RPA)

Remember:

- Use for general research and non-proprietary ideation
- Do not provide personal information of customers or employees
- Do not provide any proprietary data
- It can "hallucinate"
- It may confidently provide wrong answers
- To vet third-parties

C.R.E.A.T.E. Process

- **Context: Give ChatGPT clear and concise context**

- **Result: Tell it what you want it to produce for you**

- **Explain: Give it more details**

- **Audience: Tell it who you are making the content for**

- **Tone: If necessary, add a speaking tone to spice up the output**

- **Expand: Expand, elaborate and edit**

ChatGPT Demos

- **Context: Give ChatGPT clear and concise context**
- **Result: Tell it what you want it to produce for you**
- **Explain: Give it more details**
- **Audience: Tell it who you are making the content for**
- **Tone: If necessary, add a speaking tone to spice up the output**
- **Expand: Expand, elaborate and edit**

Voice Cloning

- **Example**

Additional Resources

- https://openai.com/

- https://bard.google.com/

- https://www.zdnet.com/article/best-ai-chatbot/

- https://www.forbes.com/sites/bernardmarr/2023/02/28/beyond-chatgpt-14-mind-blowing-ai-tools-everyone-should-be-trying-out-now/?sh=1451240e7a1b

- https://www.techradar.com/news/what-is-ai-everything-you-need-to-know

- https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai

- https://news.yahoo.com/superintelligence-ai-could-replace-humans-084735136.html

- https://www.pcmag.com/how-to/ai-on-the-go-how-to-use-chatgpt-from-your-mobile-device

- https://www.pcmag.com/news/chatgpt-adding-bing-as-its-default-search-experience

- https://www.amazon.com/Superintelligence-Dangers-Strategies-Nick-Bostrom/dp/1501227742/ref=asc_df_1501227742

Q & A

"Success in creating effective AI, could be the biggest event in the history of our civilization. Or the worst. We just don't know. So, we cannot know if we will be infinitely helped by AI, or ignored by it and side-lined, or conceivably destroyed by it." - Dr. Stephen Hawking

THANK YOU!

Dave Hatter, CISSP, CISA, CISM, CCSP, CCSLP, Security +, Network+, PMP, ITIL V3

Intrust IT
linkedin.com/in/davehatter
twitter.com/davehatter

Get our checklist:
https://www.intrust-it.com/cyber-security/cyber-essentials-checklist/

Catch Tech Friday live on 55KRC at 6:30 AM every Friday on 550 AM or http://55krc.iheart.com

Catch Cyber Monday live on WTVG at 6:30 AM every Monday on 13 ABC or https://www.13abc.com/