What business fears about AI — and how to trust it

Artificial intelligence (AI) is no longer seen as a side project or science experiment, according to 1,000 US executives surveyed for PwC's 2019 **AI Predictions report**. At the same time, they are concerned about AI risks that could undermine investments. Here's what worries business and tech leaders, and what they — and you — can do about it.

20% said their companies will deploy AI across their businesses in 2019

Tomorrow's fears …

Over the next five years, executives are concerned about the following threats:

43% New privacy threats

1,027 data breaches, exposing 57,667,911 records, have occurred in 2018 through October.[1]

41% New cyberthreats

Malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016.[2]

34% New legal liabilities and reputational risk

In 2018, just 48% of people said they trust US businesses, a decline of 10% from the prior year.[3]

33% Too complex to understand or control

200% increase in DARPA XAI funding from 2017 to 2019.[4]

31% Unable to meet demand for AI skills

32% year-over-year growth of AI-related job postings.[5]

31% US falling behind other countries in AI innovation

6X, the number of deep learning patent publications by China, compared with the US.[6]

1. Identity Theft Resource Center, Data Breach Reports, October 31, 2018.
2. Council of Economic Advisors, The Cost of Malicious Cyber Activity to the U.S. Economy, February 2018.
3. 2018 Edelman Trust Barometer.
4. Department of Defense Fiscal Year (FY) 2019 Budget Estimates.
5. Indeed Hiring Lab, Demand for AI Talent on the Rise, March 2018.
6. CB Insights, Artificial Intelligence Trends To Watch In 2018.

Source: PwC 2019 AI Predictions
Base: 1,001
Q: Which of the following scenarios around AI do you perceive as a real threat in the next 5 years?

Top-ranked AI threat by industry

Consumer Markets	**Energy, Utilities, Mining**	**Financial Services**	**Health**	**Industrial Products**	**Tech, Media, Telecommunications**
New privacy threats	Unable to meet demand for AI skills	New privacy threats	New privacy threats	AI is too complex to understand or control	New cyberthreats
45%	41%	49%	51%	39%	43%

Source: PwC 2019 AI Predictions
Bases: Consumer Markets, 132; Energy/Utilities/Mining, 46; Financial Services, 187; Health, 110; Industrial Products, 208; Tech/ Media/Telecom, 208; Other, 110.
Q: Which of the following scenarios around AI do you perceive as a real threat in the next 5 years?

… call for action today

Despite finding themselves in uncharted territory, executives surveyed said trust tops the AI agenda. And they're taking steps to manage that, including using AI itself to address risks like cyberthreats.

37% of executives said ensuring AI systems were trustworthy was their top priority

	All	Consumer Markets	Energy, Utilities, Mining	Financial Services	Health	Industrial Products	Tech, Media, Telecom
Boost AI security with validation, monitoring, verification	64%	70%	72%	60%	58%	63%	70%
Create **transparent, explainable, provable** AI models	61%	58%	67%	64%	56%	60%	63%
Create **ethical, legal, understandable** AI systems	55%	52%	57%	53%	56%	53%	58%
Improve governance with AI operating models, processes	52%	55%	63%	54%	36%	51%	60%
Test for bias in data, models, human use of algorithms	47%	50%	43%	48%	48%	48%	50%
Use **AI to manage risk, fraud, cybersecurity** threats	46%	47%	41%	52%	55%	34%	49%

Source: PwC 2019 AI Predictions
Bases: Total, 1,001; Consumer Markets, 132; Energy/Utilities/Mining, 46; Financial Services, 187; Health, 110; Industrial Products, 208; Tech/ Media/Telecom, 208; Other, 110.
Qs: What steps will your organization take in 2019 to develop and deploy AI systems that are trustworthy, fair, and stable? Which AI applications will be most important to your organization in 2019?

The ultimate goal: Responsible AI

To build trust in AI, address these five areas:

Fairness

Are we minimizing bias in our data and AI models? Are we addressing bias when we use AI?

Interpretability

Can we explain how an AI model made a decision? Can we ensure the decision is accurate?

Robustness and security

Can we rely on AI system performance? Are our AI systems vulnerable to attack?

Governance

Who is accountable for AI systems? Do we have the proper controls in place?

System ethics

Do our AI systems comply with regulations? How will AI impact our employees and customers?

pwc.com/AI2019