Artificial intelligence (AI) is either the greatest thing to ever happen to human work or the dread of our existence. Like most polarizing topics, the truth typically resides somewhere in the middle.

Yes, the “robots” are here and more are coming. All types of work will be changed in good ways and not so good ways. For professionals in finance and accounting, robotic process automation (RPA) is being used to perform rote, repetitive tasks, reducing the need for technical accountants who did this work previously. But RPA, which mimics human behavior, is not AI, which uses machine learning to draw inferences and conclusions, thinking like humans.

What will work be like if and when AI truly takes off? It depends on whom you ask. Studies by well-regarded...
research organizations generally are either utopian or dystopian in their projections, with not much gray in between.

Gartner predicts that AI will create more jobs than it eliminates by 2020. “Starting in 2020, AI-related job creation will cross into positive territory, reaching two million net-new jobs in 2025,” Gartner said in late 2017.

Oxford University’s Carl Benedikt Frey and Michael A. Osborne estimated in a 2013 research paper that nearly half (47%) of all jobs in the United States were at high risk of seeing unemployment through automation in the next 10 to 20 years (see The Future of Employment: How Susceptible Are Jobs to Computerisation? available at tinyurl.com/y9mcxlep). To be fair, Oxford’s researchers lump together RPA with AI in reading the tea leaves.

The more important point is that AI will change the nature of work and therefore the jobs built around these activities. We reached out to a mix of thought leaders, data scientists, financial software providers, and consultants to posit the future of work at midsize and smaller businesses, with an emphasis on finance and accounting jobs. We learned that the likely impact of AI on small and midsize businesses is somewhat unclear as much of the current transformation is happening in larger businesses.

WHAT’S IN A NAME?
“Many people often think AI is actually predictive data analytics and RPA,” said data architect Sapna Nagarat, director of Big Data and Machine Learning at financial and accounting automation software provider BlackLine. “There’s a lot of confusion over the meaning of these different technologies. But true AI, where a machine thinks like a human being, is still in its infancy.”

AI at its simplest is a computer that simulates human thought processes. By understanding how the brain works, the computer performs the same functions. Our brains rummage through our memories to instinctively make a thoughtful decision. AI does the same, albeit its “brain” combs through a vast amount of data at high speed.

Whereas predictive data analytics relies on algorithms to identify specific words and phrases in a volume of data for analytical purposes, the algorithms in AI are vastly more sophisticated, capable of interpreting the meaning of these words and phrases to make deeper inferences and draw more robust conclusions.

“AI duplicates the cognitive computation of what the human mind does in terms of thinking through a problem, but does it exponentially faster,” said data scientist Henna Karna, Ph.D., chief data officer at XL Catlin, a Bermuda-based property and casualty reinsurer. “Where it comes into play, much like RPA and predictive data analytics, is its use of complex algorithms to perform high-velocity computations involving massive volumes and types of data. The difference with AI is that it has equal or greater intelligence than people, easily beating the world’s greatest chess masters in games of chess.”

This extraordinary capability fuels the alarmist view of AI. A computer that can make faster and more accurate work-related decisions than humans is an easy sell. But the truth is more nuanced.

Some providers of financial and accounting automated software products have embedded RPA into their products to better capture, segment, and analyze transactional data. The tools free accountants and other finance and accounting staff members from many of the time-consuming tasks associated with closing the books.

From a business standpoint, fewer people may be needed to execute these tasks. The professionals who remain may be freed from some work activities and able to take on other value-added responsibilities — like figuring out what the numbers may mean in terms of the organization’s vision, strategy, and tactics.

In other words, what’s changing the nature of work is not AI — not yet — but RPA and predictive data analytics. “For years we keep hearing that AI will replace this job and that one, fueling fears across the workplace,” said Stan Sterna, vice president of risk consulting firm Aon Affinity, the national administrator and insurance broker for the AICPA insurance program. “And yet to my knowledge — and I spend a lot of time with accounting firms in my job — this is just not the case. The idea that robots will completely replace CPAs is overblown.”

R2-D2 AND C-3PO
Many smart people predict AI for the foreseeable future will play an assistive role for humans, which is how robots have been portrayed in popular literature and films for decades, from Robby the Robot in the 1956 film Forbidden Planet to R2-D2 and C-3PO in the Star Wars movies. “The notion of a world run by robots with humans in a constant state of relaxation is absurd,” said Karna. “Rather, what we will see are remarkable human-machine partnerships balancing human creativity and art with the machine’s computational services.”

This vision of AI goes by the same acronym — “augmented intelligence.” Today’s bots using natural language and text processing technologies are an early manifestation of augmented intelligence in a consumer context.
An example is Amazon Echo, the cylindrical table adornment that serves as a personal assistant named Alexa. Amazon Lex, the technology that powers Alexa, recently was made available to any developer to build sophisticated conversational robots. Business applications are likely and imminent.

Nagaraj imagined how an accountant might use a voice-enabled bot. “Instead of digging out reports in a computer to determine what the balance might look like a couple months from now, you’d simply query the bot, ‘What’s my balance in two months?’” she said. “The question is answered without booting up the computer.”

The challenge for developers — not a big one — is to translate commonly used accounting terms into conversational language. “Today, people in different disciplines generally use specific terminologies understood only by their peers,” said Nagaraj.

As these more human-assistive AI tools are refined, tomorrow’s finance and accounting professionals will have more time to provide more strategically oriented services. Some of the more tedious tasks that accountants do will disappear, “and that’s a good thing,” said workplace transformation thought leader Spiros Margaris, founder of Margaris Advisory.

“If you’re an accountant at a midsize company and you spend most of the day going through reams of documents to analyze the data, those types of jobs will be curtailed,” said Sterna.

Margaris concurred. Humans can’t compete on computational tasks with the “speed and accuracy of a machine,” he said. “It’s not a pretty picture for everyone, I know. But there is still plenty of time to train technical accountants to be the analytical accountants that will be needed in the future.”

COMPETENCE IMPLICATIONS

Margaris is not alone in making this forecast. “The technical knowledge that an accountant has today will be less important in the future because this knowledge will be accessed instantly by auditors using a machine,” said Karen Hochrein, consulting firm EY’s global assurance talent leader. “But other skills will have increased importance.”

Chief among them is an analytical mindset. Accountants will be called upon to analyze numbers in diverse ways, from unearthing evidence of mistakes and fraud to posting where resources can be reallocated to achieve a better return on investments.

Hochrein sees a role for more analytical accountants and finance staff in implementing new forms of automation. “As routine tasks continue to be replaced by machines, it makes sense to have someone define if a computing technology is needed, does it address business needs, and which providers are best positioned to provide the tools,” she said. “An accountant with domain knowledge, broad business acumen, and critical-thinking skills can ensure a tight fit.”

Sterna noted another skill likely to be in high demand. “There’s an ongoing need for accountants with deep knowledge of the regulatory and legal environment, particularly as it relates to cybersecurity,” he said.

Lastly, there will be a role for those accountants able to communicate dense, comprehensive information succinctly, compellingly, and empathically. “Analytical people who are strong communicators can explain why a particular decision is good for the business and how it will affect people, helping colleagues embrace change instead of fearing it,” Hochrein said.

Margaris agreed: “There will always be a need for people who can understand and analyze complex matters and put them in a context for others to understand.”

ALL PROFESSIONS WILL CHANGE

Accountants are not alone in confronting the realities of an “AI-powered” future, to borrow the marketers’ catchphrase. A case in point is radiologists.

In the very near future, machines powered by AI may interpret complex clinical images much faster and more accurately than an experienced radiologist. In doing this work, the machines also would analyze the findings of previous imaging exams and the patient’s medical history to draw conclusions superior to human thinking alone. Unlike a human radiologist, the robot version would perform these tasks every minute of the day with no fatigue, distractions, or boredom.

Rather than fear the march of the robots into their clinical examination rooms, many radiologists are welcoming AI as an opportunity to do more of what they do better.

Given the skyrocketing growth in the anticipated number of imaging examinations conducted annually worldwide, this help is needed. “Radiologists will always be needed to do more than look at an X-ray for anomalies,” Margaris said. “Only an experienced radiologist has the expertise and instincts to determine if a patient needs an X-ray, the type of imaging that needs to be done, and when and how the exam should be performed. And only a human being can provide the conclusions in human terms. A machine can’t do any of that.”

Perhaps that’s the bottom line on AI’s effect on the workplace. Some tasks will be displaced, but new jobs will materialize. As Karna put it, “People have a tendency to view every new iteration in technology with alarm. Then they use it and wonder what all the fuss was about.”

Russ Banham is a Pulitzer-nominated business journalist and author who writes frequently about the intersection of finance and technology.
Smart speakers raise privacy and security concerns
By Lea Hart

If you’re considering a voice-activated smart speaker for your office, the first question you may want to ask it is, “How secure are you?”

Amazon, Google, Microsoft, and others offer an array of these smart speaker devices for use at home. These devices are activated by the user’s voice and connect to the internet upon activation to play music, adjust the home’s temperature, and answer questions, among other features.

Companies are already advertising the benefits of these devices to businesses, where they could serve as a sort of virtual assistant. Amazon, for example, has launched Alexa for Business, suggesting the Alexa voice-activated devices can be used for everything from managing calendars to coordinating conference calls.

However, the use of these devices in an office setting raises both privacy and security concerns. Symantec recently published a white paper, A Guide to the Security of Voice-Activated Smart Speakers (a summary and a link to the full white paper are available at tinyurl.com/yd8ko5e3), that details the risks that come with these devices — from the intentional, where the device is hacked, to the unintentional, where a voice from another room wakes the device without meaning to do so.

Candid Wueest, principal threat researcher at Symantec and the author of that white paper, said the biggest concern revolves around privacy and potential interference — whether it’s intentional or not. “Because these devices are always listening, there is the risk that confidential information may be recorded and sent to the cloud back end once a keyword is recognized,” Wueest said.

Anurag Sharma, principal of WithumSmith+Brown’s cybersecurity consulting and System and Organization Controls (SOC) practices, believes the risk currently outweighs the convenience of these devices. He said the devices make easy targets for hackers. For example, a hacker might be able to turn a device on without the necessary voice command, such as “OK, Google,” for Google Home. Once the hacker has done so, the device would allow him or her to record a conversation that was not intended to be recorded, he said.

“Now you’ve made it easier for someone to target you by giving them a way in,” Sharma said.

It might not require a malignant actor to cause problems with devices that are always listening for voice commands. “There’s also the potential of undesired triggering of voice assistants by websites, work conversations, or an office neighbor,” Wueest said. “This could accidentally disrupt conference calls, add unwanted events to calendars, or impact any physical office functions it’s tied to, such as turning off the lights during a meeting.”

Considering one of these devices for your office? Wueest and Sharma offered a few tips and advice to strengthen security:

**Consider the consequences first**
If you’re thinking about employing one of these devices in your office, Sharma said to ask yourself first, “If it were to be compromised and someone were able to listen to the conversation in that space, how comfortable are you with that fact?”

“Use that as a basis for where and when you want to deploy that device,” he said. “If it were to get compromised, what is the risk of that to your business?”

If sensitive conversations happen in a conference room, for example, consider putting the device somewhere else where confidential information isn’t being shared.

**Lock down your device**
Each device arrives with default settings, Sharma said. These can be configured to an individual’s needs, and this includes security configurations, he said.

“If you do not need specific services like online purchasing, drop-in calls, or calendar entries, then disable them or restrict them where applicable,” Wueest said. “This includes locking the voice assistant down to your personal voice pattern. If the device is not in use, turn it off or mute it.”

**Protect your network**
Since these devices require access to a Wi-Fi connection to operate, hacking a smart speaker device can provide a way into the company’s Wi-Fi network. Because of this, Wueest said it’s important to protect the office Wi-Fi through the use of WPA2 encryption and a strong password, and ensure all Wi-Fi devices are updated regularly.

“Offices with voice assistants should consider setting up a guest network for clients and visitors that is separate from the one connected to smart devices,” he said. “This prevents an outside device from attacking or infecting other devices in the voice assistant’s network and vice versa.”

— Lea Hart is a freelance writer based in Durham, N.C.