AI Reworks IT
Why CIOs Are Extending AI to IT Operations
Why CIOs Are Extending AI to IT Operations. The following industry perspective explains how AI can empower the IT workforce, relieve stress, and improve results today. A future-looking perspective from an academic researcher discusses AI advances that may one day transform one of IT’s biggest headaches: cybersecurity defenses.

**EXECUTIVE:** Technology has become so deeply entwined in our personal and work lives that we have come to expect omnipresence and availability from a huge breadth of information and services. No one feels the pressure of this demand more than enterprise IT professionals, who must keep up with constantly evolving digital technologies. As much as 25% to 30% of the typical IT environment changes annually; companies update and upgrade systems, decommission others, apply software patches, move to new platforms, add entirely new technologies, and certify new applications. It’s little wonder that IT has been one of the earliest and most enthusiastic adopters of artificial intelligence.

**IT Workers Face Endless, Repetitive Labor — Like Sisyphus**

In today’s complex, dynamic systems environments, hundreds of thousands of incidents can occur in just minutes of business uptime, generating overwhelming amounts of data about operations. IT workers have to cut through this deluge to find and address problems like a credit card transaction mistakenly declined or a network crash that throws a crucial system offline. It’s become nearly impossible for even the best IT teams to respond quickly and effectively.

It’s absolutely necessary to resolve IT issues, but such firefighting does not contribute to the growth of the organization. Worse, an IT worker can start to feel like the mythical Sisyphus, pushing a stone up the hill to solve one problem only to see it roll down again when another ticket opens. Such an environment can drive even the brightest, most capable IT people to suffer burnout and leave.

Even as IT departments try to prevent revenue losses caused by unexpected downtime, they must also improve IT efficiency and continually transform customer experience. Doing so requires that IT workers engage in log analysis, performance optimizing, capacity planning, and infrastructure scaling. While IT infrastructure is dynamic, its problems are well defined. These tasks demand finding patterns in massive data sets and are often dull and repetitive. They are perfect, then, for AI automation. AI tools can enhance both the speed and accuracy of such work, reducing stress on IT employees.

**Using AI to Improve IT Performance and Efficiency**

Of course, there have been previous waves of automation in IT and business processes, and these have traditionally not scaled well in dynamic enterprise environments. Today’s AI-based automation is different. IT departments using off-the-shelf AI tools are already reducing unscheduled downtime of revenue-generating systems. In fact, AI tools are helping IT operations resolve problems within minutes instead of hours, and transforming customer experience for IT and the business overall.

We are seeing that AI is adaptive, scalable, and autonomous. It is capable of using multiple kinds of intelligence. As a recognition intelligence, it can find patterns in immense quantities of data. As a reasoning intelligence, it can tell what those patterns mean: Are they reflecting deviations in normal
While IT infrastructure is dynamic, its problems are well defined. These tasks demand finding patterns in massive data sets and are often dull and repetitive. They are perfect, then, for AI automation.

enterprise systems behavior that mean a system breakdown is looming or an attack from malicious sources is imminent? And as an operating intelligence, it can help manage the problem — both making recommendations for how to fix it as well as invoking automated, prescribed actions to fix it.

AI also improves how IT people see the connection between technology and the business. The IT environment features distinct towers of expertise: There’s the database, middleware, operating systems, storage, network, and so on. Each tower is staffed by people who know its area intimately but may have a limited view across the overall enterprise. AI can be a contextual engine that cuts across all of IT’s siloed towers; it is better able to pinpoint the source of a problem than any individual in the organization. Experience shows us that the most difficult part of fixing IT issues is identifying the source of the problem.

Considerations for Implementing AI in IT

New technologies can be idealized in ways that create difficult-to-meet expectations, and AI is no different. Indeed, AI’s prominence in popular culture has created a variety of perceptions about what it can do, from panacea to paranoia. It is crucial for CIOs to have a clear sense of how and why AI is going to be applied in IT. CIOs who do not carefully define how AI will be applied risk losing control of business expectations for the technology.

There are multiple ways for CIOs to bring AI into IT. The highest dollar value comes from using it for business assurance, keeping revenue-generating systems running and fixing whatever problems do occur more quickly. Another effective way to get buy-in for and payoff from AI is to apply it to specific issues such as improving customer experience issues or driving IT agility.

One plus for IT is that companies may not have to try to find and attract scarce AI talent. It doesn’t hurt to have IT staff with AI skills, but vendors are building intelligence into their systems, and IT-oriented AI-as-a-service offerings are available. From an enterprise perspective, IT AI should mean significantly less time putting out IT fires. That means CIOs can begin to redeploy their human capital, focusing their team more on the growth and transformation of the enterprise instead of keeping the lights on. Ultimately, that means AI will help the CIO be much more aligned to business needs.

Over the longer term, AI will develop in its ability to handle higher-level, more complex problems. As it does so, IT’s role in the enterprise and its ability to respond to business needs will change markedly. AI could usher us into a golden age for IT.

Akhilesh Tripathi is global head of Digitate, a Tata Consultancy Services venture founded in 2015. His 23-year career with TCS has included roles as head of TCS Canada and head of Enterprise Solutions and Technology Practices for TCS North America.
SCHOLAR INTERVIEW: How AI May Help IT With Cybersecurity in the Future

Erik Hemberg is a research scientist at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) and a member of the ALFA Group, where his work focuses on developing simulation autonomous, proactive cyber defenses that are anticipatory and adapt to counterattacks. He recently spoke with MIT SMR Connections about his work; what follows is an edited and condensed version of that conversation.

Q. What makes cybersecurity an interesting problem for artificial intelligence?

Hemberg: The ALFA Group approaches network cybersecurity from a different angle than you might expect. We originally investigated tax avoidance. There, the regulator wants to enforce tax law, and tax avoiders are trying to avoid or minimize their tax. The conflicting objectives set up an arms race. One side sets up structures and the other finds loopholes. The regulators know there are loopholes, and they're interested in how to patch them and what way the avoider will move next. Cybersecurity is the same sort of adversarial situation. You have competing actors in a system, and they're trying to learn and best each other.

Artificial intelligence helps you anticipate future possibilities. Given a domain structure, you want to consider what sorts of attacks are likely to happen. If you have data about prior incidents, you can build models around it. If you don’t have data, you can use AI to simulate a system based on how it works, the rules of it, and how it’s governed. And accurate modeling can get quite close to what actually could happen.

Q. Do you see this as the attacker evolving new techniques in response to defense tactics or as systems are upgraded?

Hemberg: Yes, attackers are evolving based on what behaviors are effective in the environment, and the defenders are asking how they could defeat these behaviors. We call this coevolution. There are two adversaries, and they react to each other, they form a coupled system. The hacker needs to react to the environment when the environment reacts to the hacker’s action or when something else, such as a system upgrade, occurs.

“AI agents will become the high frequency traders of finance in cyber systems. There will be autonomous attacks and autonomous defense deployments.”
Q. Are there aspects of cybersecurity where AI is most effective?

Cyber systems are very, very complicated. AI is useful when you need to adapt your system continuously and also when you have a lot of data you want to filter and classify. In our research, if you have or think you have a zero-day exploit — a vulnerability you don’t know about that is within your system — or if you’re concerned an attacker will get in your system some unknown way, say through social engineering, then AI can provide insights. It’s a given [that] you always need to be vigilant because there’s no guarantee that your perimeter will block an adversary.

Q. What about the unglamorous task of just patching software holes? Does AI help with that?

**Hemberg:** The ALFA Group is interested in the automatic comprehension and modification of software. Could AI help with patches? It’s hard engineering to do the patches. Can AI help with the logistical operational procedure of when should I patch what? How should I roll out my patches? If I have a legacy system that’s impossible to patch because I have to run it and I can’t replace the equipment, can the AI system help me set up at least my defensive perimeter? We think AI can help with all of that.

AI could help with patching despite it being a very challenging engineering task. It can aid in the logistics of finding bugs and automatic vulnerability repair. It can help decide when to roll out a patch. In a legacy system that’s impossible to patch, it could help improve the defensive perimeter.

Q. You’ve talked about cybersecurity as an arms race. How does that look in an AI-driven cybersecurity battlefield?

**Hemberg:** When you have autonomous systems, they are faster and handle more volume of activity than humans. Humans are a bottleneck; it isn’t feasible for us to handle the order of magnitude and speed of transactions. So we’re forced to use AI because of the need for speedier responses.

AI agents will become the high-frequency traders of finance in cyber systems. There will be autonomous attacks and autonomous defense deployments. Humans have general intelligence and supervisory powers that we haven’t yet achieved with AI agents, so they will play a key role.