ActualTech
MEDIA

Your Logo
GOES HERE

AI for IT Pros

Job Destroyer or Status Quo?

BY SCOTT LOWE

> “All of this has happened before. All of this will happen again.”
>
> – Number Six, Battlestar Galactica

It’s over. Pack it up. Update your resume. AI is coming for your IT job ...

... but that’s not necessarily a bad thing. In fact, it may be a good thing—if you allow it to be—so don’t update that resume quite yet.

If you’ve worked in IT for any significant amount of time, you’re aware that the only real constant in this industry is change. The 70s were defined by mainframe; the 80s ushered in the era of the personal computer; the 90s brought the local network and internet to the mainstream; the early 2000s pushed computing into the cloud.

Big, disruptive change has happened before. Big, disruptive change will happen again.

With each passing era, the technologists of the time were forced to adapt or die. Such is the case with every kind of evolution, from that of species to that of career. If you fail to keep pace with change, you often become easily replaceable by something with more capability and resilience.

We’re at yet another crossroads for valiant IT heroes, many of whom have successfully crossed evolutionary chasms from era to era to land where they are now. Today, of course, as often happens whenever something potentially disruptive enters the mainstream, many are looking nervously at their job descriptions, wondering what horrors may lie ahead should they fail to adapt to the AI wave currently crashing on the shores of every organization on the planet.

The reality is that AI tools have spent years infiltrating the IT market. From AIOps tools to tools that leverage machine learning to automate security event correlation and more, many such tools—even those with bright yellow “New and Improved with Even More AI!” slathered across the front of the box—were just fancy algorithms without what would be considered “real” AI under the hood. However, with the onslaught of generative AI tools, even these previous algorithms-in-AI-clothing tools can now access the incredible potential that generative AI brings to bear.

In this article, I’m sharing some of my thoughts on how I see modern AI impacting IT jobs in three very common areas—IT infrastructure, IT operations and support, and information security. More importantly, I’ll provide you with some insights on how you might overcome the potential concerns you may have about what AI—from basic “pseudo AI” algorithms to generative AI—may mean for your career.

> **We’re at yet another crossroads for valiant IT heroes, many of whom have successfully crossed evolutionary chasms from era to era to land where they are now.**

But, Wait … What About My Job?

I'm going to start with answering the question that everyone wants to know: Will AI impact my job if I focus on IT infrastructure, including data centers, networking, storage, and servers?

The answer is an emphatic ***yes***.

However, before you become too concerned, your job has probably been impacted by changes that came before. What happened when the era of cloud computing came on the scene? Did your job change? Almost certainly. Back in 2009, you probably had Exchange servers littering your data centers. Today, you probably have Microsoft 365 or Google to handle your email. Even if you were the hardest of hardcore Exchange engineers back in 2009, you probably still have opportunity as the resident Microsoft 365 expert.

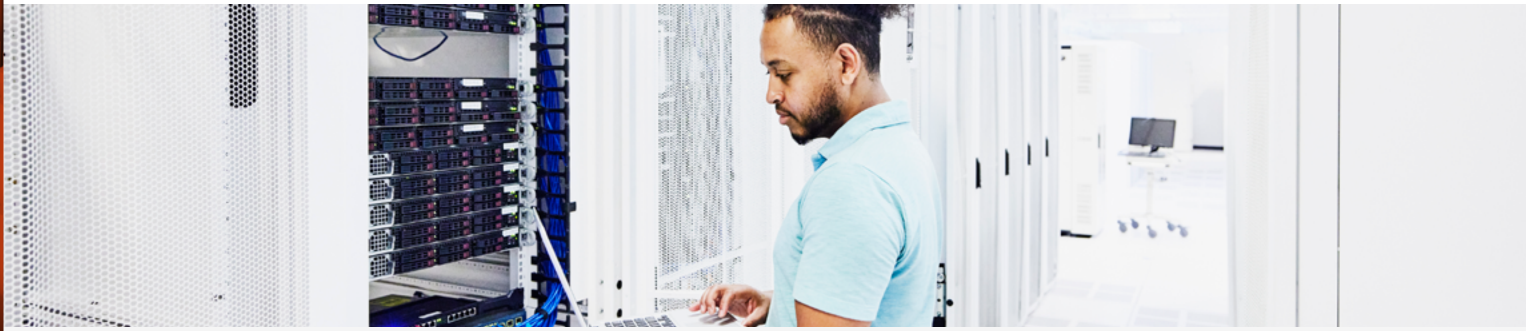
For those that see IT for what it is—an ever-changing landscape of new solutions—although your world may shift, you're going to be fine.

Why is that? Simply put, the fundamentals that matter didn't change. You still need someone that understands mail flow, distribution groups, security, and all the things that really matter to users of the system. Further, as Microsoft, for example, has extended the 365 offering over the years, as the newly minted "365 expert" you had to learn things like Microsoft Teams and all the other capabilities that Microsoft has piled into the service.

And you're still here! And the reason is simple: you adapted.

This is how I see things happening with AI as well. While it will certainly negatively impact those that have roles that simply cannot evolve or those that choose to stay static, for those that see IT for what it is—an ever-changing landscape of new solutions—although your world may shift, you're going to be fine.

At the very end of this article, I provide a series of ways that you can stay ahead of the potentially job-crushing AI wave.



IT Infrastructure, IT Operations, and Support

The range of modern IT infrastructure is vast, from the edge to the cloud, but, for each individual organization, the spectrum may be narrower, depending on the breadth of that organization. Some organizations may still have heavy reliance on local data centers while consuming Software-as-a-Service (SaaS) products, while others may have presence at every point in the spectrum.

Regardless of the full scope of supported services, the complexity inherent in today's IT infrastructure is far higher than that of past IT environments. There's also an expectation of more dynamic reaction/proactivity than was expected of yesterday's more static environments. Some of this is due to evolving business requirements and expectations and some of this is in response to fast-moving security threats that can bring down environments with administrators that can't respond quickly enough to a breach.

> **The complexity inherent in today's IT infrastructure is far higher than that of past IT environments.**

In this section, I'm not going to focus much on the security side of infrastructure—although there will be some overlap—as that's covered later, but I will be discussing how AI impacts, augments, and disrupts some of the operational services that were often previously managed manually by IT staff.

With that out of the way, here are some of the big areas where I see AI having the most impact.

SERVER PROVISIONING AND CONFIGURATION

Setting up new servers used to be hard work. The act of racking, connecting, installing, and configuring took hours, if not days. Virtual machines made this process much easier, but there was still the installing and configuring part to deal with. Containers made it even easier, but there was still a big caveat.

As we marched into a time of infrastructure that adapts to current workload demands, we couldn't rely on an error-prone system and manual intervention every time we needed new services.

Manually setting up servers, virtual machines, and containers is a repetitive and time-consuming process. AI tools can learn your configuration patterns and automatically provision resources based on demand policies you define. This ensures faster deployments and consistent configurations across environments, freeing up admins from manual setup work.

> **Automation done right can help organizations avoid catastrophe and can also reduce security risks.**

The constructs themselves—servers, virtual machines, and containers—are just one part of the discussion. The resources inside those constructs—RAM, CPU, storage—are the second part. Allowing an AI tool to granularly adjust these resources based on real-time telemetry from the environment and on user demand means that we get an IT environment that quickly adapts so that the business can operate at whatever speed it needs.

SOFTWARE PATCHES AND UPDATES

Keeping systems updated with the latest patches is really important but can be tedious work. AI-based tools can schedule and apply patches off-hours, test updates in virtual environments, and even predict which patches are high-priority.

AI excels at handling routine, rules-based tasks. Little is more routine and rules-based than dealing with software patches! Part of the beauty of automation, besides efficiency, is the reduced potential for human error, the most common element in IT failures. Automation done right can help organizations avoid catastrophe and can also reduce security risks. Of course, if you're not careful and you can use AI to make mistakes faster. You still need a human to review what an AI is planning to do to make sure you're focused on positive outcomes.

NETWORK MONITORING

Automated network monitoring is aging a bit as we've had tools to help with it for a while, but with generative AI having become mainstream, there's a lot more capability on the horizon. Prior to the advent of such tools, monitoring network traffic for performance and faults generally required admins to sift through logs and alerts. Doing that for one system was mind-numbing. Doing that across systems and attempting to correlate events was like doing a puzzle from five different sets, a combined 20,000 pieces, and no pictures to use as a reference.

AI tools are really good at real-time pattern recognition, so they can watch network flows and flag anomalies or optimize routing far faster than us mere humans. Networks and the systems on those networks generate massive volumes of data. The reality is that there is so much data generated by systems today that humans simply don't have the capability to do this work manually.

Automating this task means issues like congestion, packet loss, or device failures are detected and addressed immediately, often before users notice. Finally, we can rest easy knowing that the problem is not, in fact, the network.

> **AI tools are really good at real-time pattern recognition, so they can watch network flows and flag anomalies or optimize routing far faster than us mere humans.**

PREDICTIVE MAINTENANCE

Back in the day, we practiced IT by waiting for people to scream. Example: “Hey, Scott! The file server crashed!” could be screamed across the office as users noticed that a critical resource suddenly disappeared. In those days, we reacted to hardware failures or capacity issues after the fact. It wasn’t ideal.

With AI tools, you can get ahead of problems through predictive maintenance by analyzing sensor data, logs, and performance trends to predict problems before they occur. Tasks like checking disk health in servers and storage systems, monitoring hardware temperatures, or tracking error rates can be handled by AI models that alert teams of impending doom.

Why is this process so suitable for IT? Like network monitoring, there are logs from everywhere that are correlated to determine a failure is imminent. By allowing a data-slurping AI monster to digest these logs in real-time, administrators enable a proactive approach that minimizes unplanned downtime by analyzing data at a scale beyond (most) human capabilities.

> **With AI tools, you can get ahead of problems through predictive maintenance by analyzing sensor data, logs, and performance trends to predict problems before they occur.**

IT Operations & Support

So much of our IT infrastructure operates on runbooks and standard operating procedures. These are exactly the kinds of tasks that AI lives for. We already use tools to automate user account lifecycle management, to provision computer systems for users, to deploy software to workstations, and manage endpoint patching. Adding a bit of AI to the mix to enhance the user experience, streamline operations, and reduce human error is a natural evolution for these services.

THE SERVICE DESK CHATBOT

I'm not always a fan of chatbots, personally, but if they're done well, they can be incredible assets in your IT support arsenal.

A significant portion of IT administration involves handling user requests and routine support tickets such as password resets, access requests, software requisitioning, and general questions. AI-powered assistants, often referred to as chatbots or virtual agents, can automate these tasks by understanding user requests and executing workflows that you design in advance.

> **So much of our IT infrastructure operates on runbooks and standard operating procedures. These are exactly the kinds of tasks that AI lives for.**

The key phrase in the last sentence is "you design." Anyone can follow a series of checkboxes to resolve user requests. If that's all you do, your job is at risk of automation.

As I've said before, anything defined and repeatable is well-suited for AI. Repetitive level 1 support tasks definitely fall into that category and, even better, can be available 24/7, handle high volumes without fatigue, and never get annoyed by the phone ringing off the hook.

If, however, you truly understand the process and its intended outcomes, you hold a far different value in terms of institutional knowledge. This is key in the AI era. Those with process and outcomes knowledge are critical to ensure that the AI tools that are brought into the environment are doing what they're intended to do.

AI-driven software deployment and automated access provisioning

This item may be considered an extension of the previous one in some cases as the workflows you define there may address software deployment and access provisioning. That said, this is another key area in which AI may prove useful and somewhat disruptive to the IT status quo.

Again with the repeatable, rules-based service stuff! Software deployment and access provisioning are services that typically rely on rules created by crafty IT pros. In a manual world, managing user software installations, access requests, and provisioning is traditionally time-consuming, requiring you to manually approve and deploy applications or grant permissions. AI can automate access approvals based on behavior analysis, security policies, and organizational roles, so that users get the software and access they need without business-impacting delays or human error.

> **That spark of what makes us human with the ability to make intuition-based leaps of logic is something that an AI can't yet replicate.**

Self-Healing Endpoints and Automated IT Issue Resolution

Imagine, if you will, a user contacting the service desk about slow performance, and an AI tool jumps in action to diagnose and maybe even resolve the problem.

End users frequently encounter minor IT issues—slow performance, application crashes, connectivity problems—that typically require helpdesk intervention. AI-powered self-healing IT systems proactively detect, diagnose, and resolve common endpoint and application issues without user involvement. This reduces downtime, improves user experience, and allows IT teams to focus on more complex problems.

Again, process knowledge is critical. Only armed with information can a human bring an AI to bear on a particular challenge. Think about the trillions of data points in which modern AI tools have been trained. What is the genesis of that knowledge? Human ingenuity. That spark of what makes us human with the ability to make intuition-based leaps of logic is something that an AI can't yet replicate.

Security

I'll be blunt. If you're an old-school security pro circa 2010 and you haven't stayed current on anything except threats, AI will replace you. Why? The threat landscape is simply too big and there is far too much complexity in even modest environments for a mere human to be able to stay on top of everything that can go wrong.

I suspect that the *vast* majority of security people have done much more than tread water, although, sadly, I've met some that haven't.

The amount of data that has to be gathered, correlated, and analyzed is simply too much for a human to process in time for action to be taken against threats. That fact forms the basis for most of the items in discussion in this section.

Yesterday's signature-based tools are no longer sufficient given the sophistication of the modern hacker.

THREAT AND ANOMALY DETECTION

Security used to consist of watching logs and networks for things that had already happened. Today, nothing could be further from the truth. Security pros need to maintain to stop criminals from executing their nefarious plans. Along with that has emerged the need to monitor disparate systems and correlate their log data streams in real-time. Simply put, humans can't do this without an assist. Yesterday's signature-based tools are no longer sufficient given the sophistication of the modern hacker.

Security pros need to maintain constant vigilance and monitor for signs of cyber threats criminals attempting to execute their nefarious plans. Sometimes, a tiny anomaly harkens the start of a major cyberattack. But not every anomaly is created equal. One might be a perfectly safe variance while another is a sign of trouble brewing.

This needle-in-a-haystack problem is well-suited to AI. AI-powered threat detection systems analyze network traffic, user behavior, and system logs from across the entire organization to identify suspicious activity in real time. Unlike signature-based tools, AI-based tools can detect unknown or advanced threats by recognizing anomalies that deviate from normal behavior. Given the huge volume of security data, AI is essential for automating this task and catching threats that humans ~~might~~ will miss. (note: the strikethrough was intentional)

VULNERABILITY MANAGEMENT AND PRIORITIZATION

Threat detection and vulnerability management are two sides of the same coin. Threat detection is a little more reactive, responding in real-time to something happening right now. Vulnerability management is intended to be proactive, helping to obviate the need for threat detection systems to jump into action in the first place.

If you've ever looked at a vulnerability report, you've seen a lot of items that cause high concern followed by a seemingly unending number of pages devoted to minutiae. The reality is that your organization may have thousands of known vulnerabilities across its systems, but not all pose equal risk.

The process of manually analyzing the aforementioned reports to decide which bugs to fix first can be overwhelming. An AI tool can help you by combining vulnerability scan data with threat intelligence and predictive models to help you prioritize remediation efforts. AI-driven models can predict which vulnerabilities are most likely to be exploited or cause damage, helping your teams to focus on those rather than trying to eat an elephant all at once.

Another item that falls into the vulnerability management bucket is maintaining security policy compliance. Failure to do so brings systems into a potential state of vulnerability, so it's important to stay on top of this. This can include a wide range of activities, such as not storing PII and sensitive (such as social security numbers and credit card numbers) in the wrong place, or checking other systems to maintain compliance with GDPR rules.

This can be a really labor-heavy process, but like most rules-based processes AI can continuously audit configurations and settings across the environment, flagging violations or risky misconfigurations. It can also classify sensitive data to help with compliance, including finding personal data in logs or cloud storage. These tasks involve checking systems across a number of silos and comparing them against defined patterns. This kind of repetitive job is one that AI can do much faster and with less error than humans.

IDENTITY AND ACCESS MANAGEMENT

Managing user access – provisioning accounts, assigning roles, detecting misuse – has traditionally been a manual administrative task. AI can streamline these processes by analyzing usage patterns to find places where an admin may have forgotten to remove someone's access or granted risky access and automate access decisions. For example, AI might detect if an account's behavior strays from expected norms and flag or suspend it. These kinds of deviations can possibly be an insider threat or someone using stolen credentials.

It can also learn if a user's access is over-provisioned or if an access request is unusual. These tasks involve analyzing large amounts of identity data and permissions – something AI does well – to improve security and compliance without constant human review.

Evolving Your IT Skills in the AI Age

As AI takes over routine tasks, IT professionals must adapt to stay relevant. The good news is that while AI automates mundane work, it also opens up new opportunities for people that have maintained an understanding for the "why" behind what they do.

Here are some ways that you can evolve your skills to jump the chasm to the promised-land of the AI-driven enterprise:

UPLEVEL YOUR SKILLS

You can never have too much knowledge about what you do. Continue developing your core expertise, whether it's in networking, systems, security, or something else) while learning how AI and automation tools can augment what you do and help you go faster. For example, a network engineer can upskill in AI-driven network management tools, and a security analyst can learn to fine-tune machine learning models for threat detection. By understanding AI's role, you become the expert who can supervise and improve those AI systems.

Most importantly, do what an AI can't and focus on more complex problem-solving. Let AI handle basic tasks while you focus more on higher-level thinking. Sharpen your ability to analyze complex problems and design creative solutions. Modern IT roles place a lot more importance on these kinds of things as opposed to repetitive work.

> **Do what an AI can't and focus on more complex problem-solving. Let AI handle basic tasks while you focus more on higher-level thinking.**

By the way, this whole "skill upleveling" thing never ends... you have to maintain a focus on continuing education throughout your career in order to remain relevant.

Regardless, never forget that soft skills reign supreme outside the data center, so if these are skills that you haven't honed, start figuring them out. The ability to clearly and concisely communicate will help you as you advance your career beyond IT technical work and move into more company-wide activities, management, and leadership.

GET COMFORTABLE WITH DATA

In the world of our new AI overlords, the ability to analyze data will separate teams. It will be a crucial skill. Learn it! If you haven't done it before, start doing some of your own light scripting, learn querying languages, and get comfortable with dashboards and reports from AI systems. Building the ability to bridge the gap between raw AI output and business decisions are highly valuable.

CHANGE JOBS

I'm not suggesting you give up IT to go become a coal miner but that you take a look around the career landscape and find potentially adjacent roles you might slide into. For example, if you've been a server jockey for a decade, you might be able to add some scripting skills to your arsenal and move into an SRE-type role with a focus on helping organizations automate their AI-managed infrastructure.

Or, you might jump ship altogether and go hardcore into AI and build skills necessary to get a job in data science or some other AI-specific discipline.

Summary

Yes, AI is coming for your job. No, it doesn't necessarily spell doom for your career, as long as you take steps to stay ahead of the wave. You've probably done it before and you'll probably do it again.

I hope that sharing in this article some of the ways that AI may impact and benefit common processes has helped to assuage immediate concerns while also providing you with some ideas on ways you may be able to adapt your current skill set to become even more important to your organization than you are today.

> **You've probably done it before and you'll probably do it again.**

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future B2B company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

Stay on top of AI and IT with ActualTech Webinars

ActualTech MEDIA