5 Reasons Why IT Operations Will Cost More in 2022

LeapFROG®

5 Reasons Why IT OperationsWill Cost More in 2022

This coming year is unlike any other when it comes to IT budgeting.

Not that any two years are identical, but IT budgets for 2022 will look decidedly different because of the pandemic. COVID-19 forced companies to change the way they do business and they used technology to do it. The rush to work from home (WFH) and digital transformation not only transformed business but further enticed cybercriminals who were already trying out new and more sophisticated cyberattack strategies. Meanwhile, supply-chain and tech-talent shortages continue and technical debt keeps growing.

These combined, simultaneous events point to 2022 being a one-off year with a bigger bottom line.

In 2022, the most surprising change will be additional costs in your Run budget. Operating IT will require a bigger piece of your overall IT-budget pie — the overwhelming trend is a 20% to 25% increase.

Successful IT budgets strike the right balance between the three separate portions of your overall IT budget — Run, Grow, and Transform. Your Run budget covers the cost of IT operations, your Grow budget covers the cost of scaling, and your Transform budget covers the cost of innovations.

In 2022, the most surprising change will be additional costs in your Run budget. Operating IT will require a bigger piece of your overall IT-budget pie — the overwhelming trend is a 20% to 25% increase.

This increase will likely trigger some eye pops and a lot of discussion at your company. Leadership may be focused on keeping digital transformation on the fast track — understandably so. However, after this year, many 2022 IT operational increases should level out then return to a higher baseline than pre-pandemic if your IT operational scope has expanded.

A closer look at the five reasons why IT operations will be more expensive next year can help your company make the best decisions for 2022 and beyond.

Reason #1: There's more IT to manage

Now that you've leveraged technology to do things you used to do in person, your IT environment is more complex. Tools for WFH — collaboration, communication, e-commerce, VoIP, others — need to be configured, integrated, monitored, and secured. More tools mean more management.

And instead of being under one roof, your infrastructure is now under many roofs. The devices and power supplies at each employee location are now part of your infrastructure. So are the internet connections and security controls — the scope of your IT environment is much wider and more distributed now. Problems under one roof can impact productivity company-wide, and when events like storms can cause outages in dozens or hundreds of remote workplaces simultaneously, the back-up plan for your office location doesn't apply. Your IT team may need to travel to individual homes to replace or repair fried computers or troubleshoot other problems. Investing in uninterruptable power sources (UPS) helps, as does paying for faster internet service, better modems and routers, and security software for employee homes. Maintaining these items to help ensure productivity are additional IT operations expenses.

Maintaining a high-performing, secure IT environment for a distributed workforce requires more money and IT staff unless your company already had a fully distributed workforce before the pandemic began. If you must adhere to compliance standards, the investment required is even larger.

Reason #2: IT environments need to be made more secure

When your company was in emergency mode, you weren't focused on securing your systems. You needed to stay in business. Now it's time to go implement the proper security controls because you're in a race with the cybercriminals.

Cybercriminals are having tremendous success with new strategies and tactics, and the pandemic-driven mass migration to WFH and digital transformation has been a gift to them. Highly targeted ransomware, malicious code embedded in enterprise software, cloud attacks, and attacks that go after supply chains deliver them a much higher ROI with very little added risk. Even companies with solid security protocols must improve their posture to keep up.

With relentless attacks on cloud platforms and services, every company needs to budget for securing not only their owned infrastructure but everything they migrated to the cloud and all of their digital transformation initiatives.

With relentless attacks on cloud platforms and services, every company needs to budget for securing not only their owned infrastructure but everything they migrated to the cloud and all of their digital transformation initiatives. This includes new security tools, the resources it takes to write new processes and procedures, and the staff if takes to follow and manage them.

Investing in securing your IT environment does more than help protect your company — it improves your risk profile when applying for cyber insurance. Cybercrime claims have skyrocketed, driving up premiums by 20-50% for those who can still qualify.

Reason #3: The IT resources you need are scarce

It might take another year for the supply chain to return to normal and some predict it will take until 2024. The pandemic revealed existing supply-chain weaknesses, plus COVID-19 related lockdowns, worker shortages, raw materials shortages, transportation interruptions, and other disruptions create bottlenecks that drive up prices.

Starting March 1, 2022, pricing for Office 365 and Microsoft 365 will cost more per user after a decade of flat pricing. Countless other cloud platforms and services are increasing prices, too.

The semiconductor shortage is just one example felt across many industries, including technology. Factories are maxed out and items are backordered, despite higher prices due to inflation. Even if the equipment you need has been produced, what will it cost to get it? Scarce resources make finding deals and promotions all but impossible. With overseas ports struggling with the COVID-19 delta variant and the persistent and growing truck driver shortage, count on paying higher shipping and delivery prices on top of higher product prices. This can impact your IT operations budget in significant ways, especially if you've been postponing lifecycle-management activities during the pandemic — you're now facing higher prices for your 2020, 2021, and 2022 equipment replacements.

Human resources for IT are also in short supply, as usual, and the shortage won't resolve away any time soon. For software developers alone, the U.S. is graduating less than a third of the number of developers annually (400K) than the current open developer positions (1.4M). Budgeting to pay your IT team more and give them bonuses when they do a good job will help, as will investing in more automation.

Reason #4: Cloud services are becoming more expensive

One study found 90% of companies have accelerated cloud adoption. Demand is high, so cloud pricing is responding.

Starting March 1, 2022, pricing for Office 365 and Microsoft 365 will cost more per user after a decade of flat pricing. Countless other cloud platforms and services are increasing prices, too. While you can still find basic service levels at a low cost, keep in mind you now need to add all of the security components, given the cybercrime environment. What was once $8 per user may now be $12 or $20 per user to perform basically the same function but do it more securely.

Public cloud pricing varies by region and is cheaper with reserved capacity commitments but it can be difficult to forecast your cloud spend even if you've been using cloud computing for many years. Private cloud prices are also increasing and present similar budgeting challenges. Waste is common and often accounts for 30% to 35% of cloud spending and cloud spending for the year often ends up over budget. Cloud optimization to reduce cost is a high priority for most companies and can help offset cloud price increases. Low-end competitors offer pricing at a fraction of what you pay for the big three (AWS, Google, and Azure), but there are also caveats with low-cost providers.

For 2022, budget for cloud platforms and services to cost more and for the research required to continually forecast your needs, cut waste, and, possibly, migrate to more cost-effective clouds.

Reason #5: Technical debt is coming due

Technical debt is the cost of correct technologies in your IT environment that were either rushed into production or put on the back-burner. Every organization has some technical debt. And it makes sense that technical debt has exploded during the pandemic — the focus has been on transforming business quickly to meet short timelines. But the more technical debt you accrue each month, the less resilient your networks and the higher the cost of running your IT.

Technical debt is the cost of correct technologies in your IT environment that were either rushed into production or put on the back burner. Every organization has some technical debt. And it makes sense that technical debt has exploded during the pandemic — the focus has been on transforming business quickly to meet short timelines. But the more

technical debt you accrue each month, the less resilient your networks and the higher the cost of running your IT.

Now is the time to budget for correcting your technology in a planned, controlled way that does not negatively impact productivity so you don't keep digging a deeper hole. Examples of activities that pay technical debt include software updates and bug fixes, standardization, asset replacement, process documentation, and physical infrastructure hardening.

If you're hesitant to invest in reworking systems to reduce technical debt, an option is to invest in technology that automates as many IT operations as possible. Leapfrogging to automation can also help alleviate resource shortages and reduce human error.

None of the five reasons your IT will cost more to run in 2022 is avoidable. Each is directly related to the pandemic. Budgeting to address them in the coming year puts your organization in the best position to stay nimble, productive, secure, and ready for whatever comes next — including bold new opportunities. For comprehensive guidance on IT budgeting, download our IT Budgeting Guide for 2022.

Leapfrog Services is an IT Security, Network, and Infrastructure Managed Service Provider (MSP/MSSP) that's been helping organizations meet their business goals and protect their data since 1998. Our team designs and operates outsourced solutions based on our proven methodology that includes matching your level of threat protection to your business needs and adhering to the highest cybersecurity standards (we are SSAE 18 SOC 2 compliant). Guarding against risks systematically and consistently reduces the likelihood your organization will be attacked and helps you to remain productive and successful.

You can reach us at 404-870-2122 or leapfrogservices.com.