the ame group

IT SERVICES TO INCLUDE IN YOUR ANNUAL BUDGET

As a small business owner, you have to make the most of your resources. Just like any other business, it's important to manage budgets effectively, practically and thoroughly. Instead of hoping you'll have the budget for tech needs, be proactive and incorporate the most common IT needs into your annual budget planning to experience fewer surprises throughout the year.

Ongoing IT Services You Need to Plan for

It's critical to budget for realistic IT expenses, including regular maintenance, system replacement expenses, license and warranty fees, and even unforeseen system failures. Taking stock of your previous year's IT budget and improving it can be useful for guiding your organization's technology spending and for planning and communicating.

Listed below are a few key areas you should allocate a sufficient budget for:

- [ ] **Management:** Do you have a certain budget set aside for hiring internal staff members or collaborating with IT service providers? Your annual IT budget must accommodate salaries, bonuses and benefits paid to IT staff. Also, make sure you have a dedicated budget for hiring new resources and providing IT training to the workforce.

  Partnering with an IT service provider is cost-effective, and they can support you beyond the routine monitoring and maintenance of systems.

- [ ] **Comprehensive cybersecurity:** Given the current rise in cyberattacks, cybersecurity should be your top priority when preparing your IT budget. Your business needs a cybersecurity strategy that offers a more comprehensive and team-based approach to thwart threats, especially considering the industry's persistent shortage of experienced cybersecurity experts.

  What if you could catch new vulnerabilities on your IT network before cybercriminals could exploit them? Imagine having a solution that can notify you in real time if sensitive company data goes up for sale on the dark web? This is why you need a comprehensive solution suite that offers best-in-class security.

- [ ] **Physical security:** You don't just need protection from the bad guys online — you need to consider physical security threats you might become victim to, such as break-ins, employee safety and on-site accidents, while planning your security budget. You can allocate funds for access-control systems, insurance, surveillance devices and commercial door locks as part of your security budget.

- [ ] **Compliance:** Failure to comply with industry regulations may lead to severe fines, work stoppages, legal action or even the closure of your company. Being compliant is not a choice, it is mandatory.

  Before you invest in any tool, assess your current compliance needs first and create a roadmap of your long-term needs. It's better to go with a tool that can suit both your present and future needs when estimating the cost of your compliance and risk management solution.

- [ ] **Backup:** Imagine receiving a late-night email from a cybercriminal demanding a significant ransom. Panicked, you log into your company's network only to find that your systems have been encrypted by hackers, and you haven't backed up any data in months. How will you cope with this crisis? It's not just about downtime or revenue loss, you couldn't protect customer data and might lose their trust forever.

  Knowing how much money you'll need to invest to keep your business operating in the event of a disaster is one of the most crucial components of your data backup strategy. A cloud backup solution ensures your business will continue to provide excellent service, regardless of a ransomware attack, natural disaster or hardware failure. Depending on your company's unique needs, the price of the systems and solutions that support backup, disaster recovery and business continuity may vary.

- [ ] **Security training:** Keeping employees up to date about how to protect themselves and your organization from threats is a crucial component of a healthy security strategy. Your staff should receive regular cybersecurity training so they are aware of good cyber hygiene, the security risks associated with their actions and how to spot cyberattacks they could come across via email and the web. An IT service provider can help with security awareness training services if your organization lacks internal security resources and expertise.