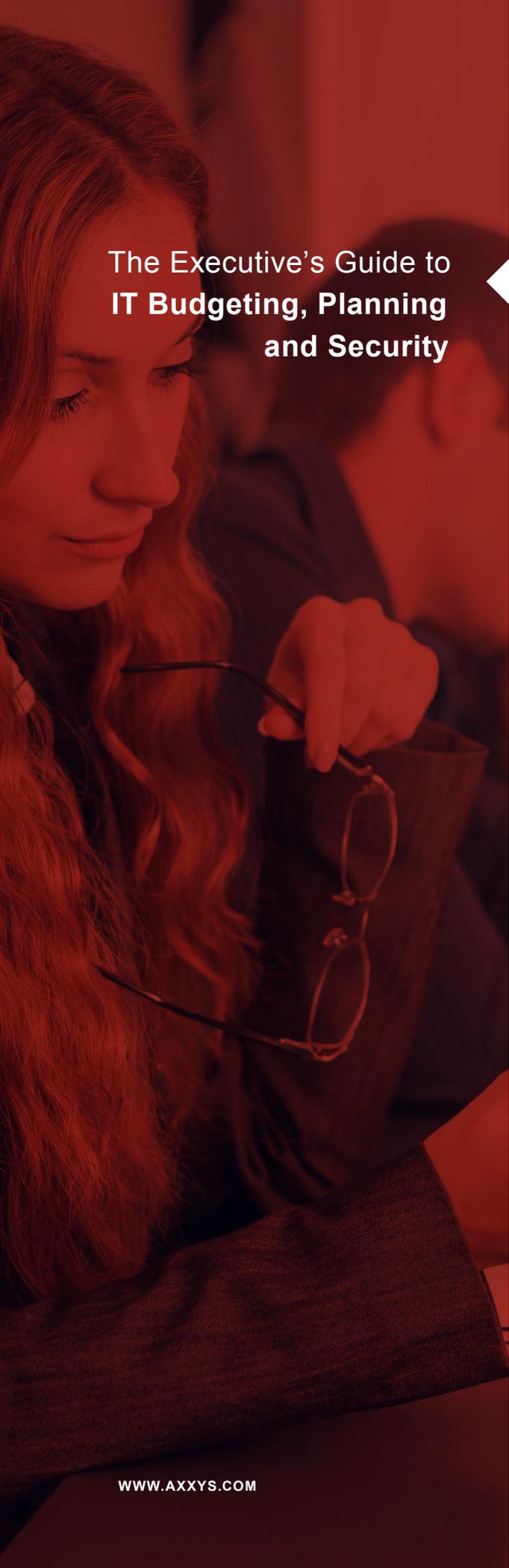


— THE EXECUTIVE'S GUIDE TO —

IT BUDGETING, PLANNING AND SECURITY



5850 GRANITE PARKWAY, SUITE 700 | PLANO, TX 75024 | 214.297.21000 | WWW.AXXYS.COM | INFO@AXXYS.COM



The Executive's Guide to IT Budgeting, Planning and Security

In the past two decades, IT has secured a permanent and ever-growing foothold in the boardroom. What was once regarded as little more than a simple budget line item has become a topic dominating C-suite conversations on everything from investment and strategy to risk and security. Business technology has outgrown the dark, back room full of servers and circuits managed by a singular resident “computer guy” and snowballed into one of the most integral pieces of your company’s success.

Today, it requires a team of highly skilled professionals to ensure your technology needs are satisfied. **From keeping your employees efficient and productive to keeping your clients happy**, technology is essential to every facet of your business. What’s more, technology isn’t going anywhere—each year, our dependency on reliable tech grows exponentially. Regardless of industry, IT helps us all become better-connected and more innovative.

But if ensuring your IT is handled appropriately—and that you’re making the right choices—keeps you up at night, you’re not alone. As a successful leader, you know the most important decisions are rarely the easiest. To help you properly budget, plan and protect your technology assets, we’ve put together a comprehensive guide. Read on to discover expert secrets to ensure your continued technology success.



Part 1: Finances & Budgeting

Regardless of business model, management style, background or education, every executive shares one common goal: Improve the bottom line. This is often easier said than done as technology evolves at breakneck speeds.

Whether you've been a business leader for three decades or three years, you've likely noticed a trend: **every quarter, technology consumes a larger portion of your budget.** From workstations to phone systems, data storage to security systems, the technology filling just one corner of your office space is enough to make you feel like you're running NASA instead of a business.

Even if you forego investing in the latest and greatest devices for your employees, simply maintaining an efficient and secure network and keeping up with basic software updates and licensing is a costly endeavor. And like most business investments, the less you spend the thinner your returns. In many cases, cutting back isn't an option. While dependable IT doesn't come cheap, you can make certain modifications to ward off budget vampires and achieve a healthier bottom line.

THE TOP THREE BUDGET DRAINS

Out-of-Date Technology

Even your most brilliant team members are only as capable as the tools you provide. While outfitting every employee with a new smartphone every year may not fit within your budget, some technology updates are critical to increasing output.

Old technology can weigh down your workforce, threatening efficiency and frustrating your team. A sluggish 5-year-old laptop or spotty WiFi connection can prevent an otherwise highly competent employee from performing at full-capacity which, in turn, negatively affects ROI.

SOLUTION:

Keep a running inventory of each and every asset. Document the age and performance of each device, and replace as necessary.

Inefficient Systems

Technology doesn't just have to be outdated to affect your company's ability to meet objectives. To foster success, your technology also needs to be efficient. For example, your engineering team probably can't function at their highest level on the same caliber of computer provided to your administrative staff. In some cases, efficiencies may go undetected until reported by an employee.

SOLUTION:

Set up 24/7 monitoring and support. Picking up on inefficient trends, such as an overloaded network at certain times of day, can help you streamline processes and make way for better usage.

In-House IT Professionals

The more important technology becomes to businesses, the more valuable the skills of highly trained IT specialists. Often, however, the technology you need to run your business exceeds the availability of in-house personnel. Hiring more assistance often means paying additional salaries, or paying for third-party contractors. Either way, the expense is astronomical and you're still likely not entirely covered.

SOLUTION:

Invest in an experienced managed services provider (MSP) who can expertly meet your needs while also taking a proactive approach to your business technology.

In addition to the above modifications, there are a few things you will need to consider as you prepare your next IT budget.



THE TOP THREE BUDGET CONSIDERATIONS

How Often Do I Need to Replace Various Assets?

One of the most difficult parts of technology budget planning is determining which pieces of technology need to be replaced. Waiting too long can mean forcing employees to amble along on inefficient devices, but replacing too soon can mean unnecessary expenditures.

As mentioned above, the best solution is to keep an updated inventory of every asset. While [Stanford University IT](#) recommends a three- to four-year replacement schedule, hardware should be assessed on a case-by-case basis. Consider investing in an asset management tool so you know when each item needs to be updated or upgraded.

Cost of Updates, Tech Support and Potential Repairs

One of the worst mistakes executives make when planning their IT budget is only accounting for the cost of hardware and software. While these two pieces make up a significant portion of technology expenses, you also need to factor in the cost of updates, tech support and repairs. From glitches and network outages to accidents and user error, it's often the unexpected issues that cost businesses the most.

Data Security

Although many business leaders agree that data is among their most valuable assets, it often takes a breach—or, at least, an attempted breach—to convince executives to beef up data protection. As we've seen over the past few years, no one is safe from attempted cyber crimes. In other words, every budget must include data security.

We'll talk more about cybersecurity in a later section.

Part 2: Devices

Twenty years ago, the average office worker carried a briefcase with little more than a few files and an ink pen. Today, employees arrive to work armed with a plethora of company-issued and personal devices. From smartphones and laptops to tablets and wearables, [Sophos](#) estimates the average user carries about three devices. While this level of connectivity allows for greater mobility, it's not without its challenges—namely, controlling device usage and determining which devices your company should purchase.

THE BYOD CONUNDRUM

Only a short time ago, whipping out your personal cell phone at work was considered taboo and, in some environments, grounds for termination. Now you'd be hard-pressed to attend a meeting without seeing a smartphone within arm's reach of every employee. Thanks to [remote work](#), mobility and the Internet of Everything, **BYOD (bring your own device) is nearly unavoidable.**

In many cases, allowing your employees to bring their own technology means you don't have to supply them with expensive equipment. Unfortunately, this also means each device presents another vulnerability—another point through which hackers can access your network and sensitive data.

To reduce these risks, many businesses are implementing a BYOD policy. A thorough policy includes:

- **Detailed requirements for each device connected to the company's network**
- **Company-wide ban on unauthorized applications**
- **Limit on activities performed on devices while connected to the company's network**
- **Installation of encryption software on each device**
- **Regular IT audits of each device**

By exercising greater control over devices and device usage, you can allow BYOD without opening up your business to dangerous security risks.

CHOOSING THE RIGHT DEVICES FOR YOUR BUSINESS

As we discussed previously, an investment in up-to-date, highly efficient technology, will help you reach business goals. But, how do you know which pieces of hardware will be most beneficial to your work environment? To help determine the best investment, ask yourself the following questions:

- **Do your employees work remotely or only in one fixed location?**
- **If employees work remotely, will they be traveling with the device?**
- **Do your employees utilize software that uses a great deal of memory and hardware space?**
- **Will employees be sharing workstations or does each team member need their own equipment?**
- **How important is visual display, responsiveness or audio to job role?**
- **Will employees use devices for creation or solely as a mode of communication?**
- **Will clients or customers ever come into contact with the device?**

Keep in mind that not all employees need the same devices. To ensure you're spending wisely, consider each department independently.



Part 3: Cybersecurity and Disaster Recovery

In 1979, a hacker ring dared a 16-year-old boy to infiltrate the computer system of Digital Equipment Corp. The feat, as it turned out, was nearly effortless. The teenager quickly researched the name of the company's lead developer, Anton Chernoff. He called DEC and, armed with just enough information to believably pose as Chernoff, told a system admin he was unable to log into his account. The admin created a new account for Chernoff, unknowingly providing the credentials to the amateur hacker.

The teenager was Kevin Mitnick, who eventually became known as the world's "most wanted" hacker. This particular breach, however, required no sophisticated knowledge of computer networking, no late nights spent poring over complex code and no physical breaking and entering. Mitnick easily accessed the entire system armed with little more than the name of an employee and rudimentary acting skills.

SOCIAL ENGINEERING & YOUR SECURITY'S WEAKEST LINK

Social engineering, a method of hacking that relies on deception rather than technical skill, is nothing new. But in an age where you can discover almost anything you need to know about someone by browsing their social media profile, it's becoming even easier.

"There are free databases that aggregate people's entire life—where they were born, where they live, their birth dates, the last four digits of their Social Security number, their parents' names, their maiden names," says Rob Kleeger, founder and managing director of Digital4nx Group Ltd. "When we do ethical hacking assessments, we leverage all the information that's publicly available and then leverage it to spoof an email."

In other words, what Kevin Mitnick accomplished in 1979 would, arguably, be even easier today. Criminals don't need a great deal of technical finesse to get their hands on sensitive data—they just have to be decent detectives. Then they have to find the weak spot in your business.

Which, as Kleeger points out, may not be what you think.

“It’s not a matter of protecting hackers from getting access to your network,” Kleegeer says.

“Generally it’s the people who are the weakest link, and often mistakenly contribute to incidents that can lead to a data breach—such as using a personal cloud based file sharing account, unsecured BYOD or a lost USB device that contains sensitive data.”

So what can you do to protect your business? Here are Kleegeer’s top three tips.

How to Avoid Social Engineering Attacks

Offer Education

It’s never a good idea to assume your employees know how to identify a phishing email or who is authorized to access various databases. Offer regular training sessions or, at the very least, send out correspondences with explicit instructions and examples of what not to do.

Understand Data Sources

Even if you have ethical and well-trained employees, mistakes happen. For example, a harmless email that contains confidential or sensitive information sent via an unauthorized personal device connected to your network can put your entire business at risk.

Be Proactive

From penetration testing to ethical hacking, third-party businesses can help you identify your vulnerabilities. Then, your managed services provider can help you monitor your network and offer support in the event of a breach. Locating the weak spots and remedying them (instead of simply reacting to vulnerabilities after a breach occurs) can help you save time, money and your reputation.



DISASTER RECOVERY

Of course, cyber attacks aren't the only threats to your company. Just ask the hundreds of businesses that were forced to shut down in 2012 as Hurricane Sandy ripped through the Northeast United States—especially those that never reopened. From physical property (office space and equipment) to digital assets such as data, the loss from an unexpected disaster can destroy a company.

No business leader wants to imagine their hard work washing away in a flood or burning to ash in a fire, but these things can happen at any time. Whether it's the largest storm in a decade or a small overnight pipe burst, some events can't be stopped. Luckily, you can take a few steps to prepare your business for whatever you may face.

Here are the five components of a [successful disaster recovery plan \(DRP\)](#):

- **Contact Lists:** A hard copy that includes employees and key vendors.
- **Contact Plan:** What to do if phones and Internet are down.
- **Alternate work location:** Where to temporarily move business in the event of a disaster.
- **Accounting:** Who will pay bills and/or employees, and how?
- **Update process:** Make sure to schedule time to review the plan twice a year.

Here are three additional elements to consider as you build your DRP:

Financials.

Just because your business has suffered a disaster doesn't mean you can stop paying your bills or your employees. Make sure your accounting can stay up and running.

Communication.

Your IT systems play a big role in being able to [communicate internally](#) and with clients, but what do you do if you can't recover the information you need quickly enough? Always maintain hard copies of your most important contacts.

Location.

If a disaster renders your office unusable, what's your backup plan? Make sure you have somewhere else to do business, along with all the components of moving offices.

Be sure to revisit your DRP often and make sure the heads of each department understand their responsibility in the event of a disaster.

The better you and your team are prepared, the more likely your business is to survive a disaster—and the easier you'll sleep at night.

Part 4: Technology for Success

Properly investing in and planning and protecting your business technology is critical to success in any field, but it's about more than achieving higher levels of productivity. Technology can help you create a more [innovative company culture](#) with opportunities for employees to advance their skills, de-silo departments and harness the data you need to take educated risks. Technology is the catalyst you need to launch your business beyond your competitors and become an industry leader.

To help you position technology for ongoing success, let's take a look at how to use technology to create a more forward-thinking, modern, employee-friendly environment.

HOW TO EFFECTIVELY LEVERAGE YOUR TECHNOLOGY

As an executive, there are four things you can do to amplify success through technology:

Know what today's employees want and expect.

Nobody loves substandard technology, but did you know it can be the sole reason an employee leaves your company? According to a [study by Dell](#), one in four employees would consider switching jobs for better technology. And according to a survey conducted by [Premiere Global Services Inc.](#), better technology is the third most important thing employees wanted from their jobs in 2015.

Seek opportunities for mobility and constant-connectivity.

In the United States, 3.7 million employees work from home at least half the time, according to [Global Workplace Analytics](#). Americans aren't just working from home, though. They're working from coffee shops, airport terminals and subway trains, too. Cloud technology and mobile devices lift restraints and allow your team to work nearly anywhere at any time.

Set boundaries to prevent overuse and burnout.

Of course, just because you can work 24/7 doesn't mean you should—and neither should your employees. Overuse of technology leads to burnout, which can suffocate productivity and destroy employee satisfaction. To keep your team happy and energized, establish boundaries. For example, implement a “no communication on vacation” rule to keep employees from checking in on days off.

Encourage technology skill-building.

When your employees become more adept with technology, not only are there fewer calls to tech support, but they also feel empowered and confident. Call in software vendors to provide on-site demos, encourage webinar attendance and set aside an hour or two of educational time each week. When you provide your employees the opportunity to improve, you'll enjoy the benefit of a more nimble workforce.

CONCLUSION

To say that “technology is everything” may sound melodramatic, but it’s true. Your business needs technology to become more prosperous, and it relies on IT for its most basic processes. Without reliable technology, businesses often flounder and fail. On the flip side, investing in, integrating and securing valuable technology positions your business to exceed its goals, foster client and employee satisfaction and grow at a rapid pace. [Making the right IT decisions](#) means transforming your business into your industry’s most powerful and innovative force.

By using the above tips and guidelines to better plan your IT budget, select the right devices, develop secure and sustainable processes, educate your team and prepare your business for the future, you can ignite unstoppable success.

**Are you ready to position your business
for your most lucrative year yet?**

Contact us today and we’ll begin building a strategy to help you achieve your technology goals fast.

GET STARTED