Top 5 Mistakes that Business Owners Make with Technology

A Business Services Provider Executive Report

Y3K IT SERVICES

928.388.6058
info@y3kitservices.com

Top 5 Mistakes that Business Owners Make with Technology

As I help companies navigate the complex and confusing world of technology, I see a lot of things…and some things you can't un-see, like the horrors of a Business losing everything.

Business Owners are busy with day-to-day activities, and there's generally more work to do than employees to help, so, things get overlooked and missed.

Technology is a forever-changing animal and can become obsolete within months. We lack expertise and experience, plus we have budget restraints preventing us from hiring full-time experts.

Nobody wants to read about the 25 mistakes they and everyone else is making. We say to ourselves: "How do I deal with all of this Technology? How do I avoid poor technology planning and mistakes? I don't want my business losing time and money."

I'm here to help. I want to point you in the right direction, offer some real help, and provide some guidance for what you can do. So, I'm going to give you (2) Business Focused Technology Mistakes and (3) Specific Technology Mistakes. These will cover a more over-arching view of things. I also include some action steps that you can take today.

Business Focused Technology Mistakes

As the Business Owner, your primary Focus is on Growing the Business...getting more Revenue and Profits. You're focused on Increasing Efficiencies, getting more Customers, providing Customer Service, Hiring and Keeping great employees, building a Terrific Culture, watching for Risk, Diversifying, having an eye on the Competition, keeping a Pulse on the Industry, and hugely important, performing a massive amount of Marketing and Sales.

#1 Failure to: Engage with a Technology Strategist

What it is:

A Business Growth Strategist is a Technology Expert who collaborates with you on your Business Goals and the Creation a Strategic Roadmap concerning your Technology. They offer Valuable Insights and Foresights, then can Orchestrate all Aspects of your Technology Puzzle.

Why it matters:

If you're busy running the business, and trying to keep your eye on the ball, you really don't have the bandwidth or the time to figure out all the Technology on your own. Rule #1...off-load what you're not best at and what isn't the most productive use of your time. Technology over-whelm, and where do I begin, should not be on your plate. Focusing on growing your Business, is what should be on your plate. A Technology Expert can help you turn Tech from being a 'Cost-Center' to a 'Profit-Center' and increase your revenues.

What you can do:
Don't lose focus on your responsibilities. Partner with a Business Growth Strategist, who not only takes care of your Technology Strategy, but is focused on helping your company succeed and grow, far beyond what you could do, by yourself. When you partner with a Tech Strategist, your Business Goals are the focus. You get where you want to go, and growth is accelerated.

#2 Lack of: Proper Maintenance and Support

What it is:
Support involves: Monitoring & Maintaining the Technology...Protecting & Securing it... Performing Preventive and all Reactive work…along with Supporting all Users in your Business.

Why it matters:
[1] This is Phase #2 of above...after things are implemented, they need to be maintained. Things left to themselves always degrade. People are always in need of assistance. "Set it & Forget it" is an unwise Business decision. Technology is a tool that you use to grow your Business. It's important to Maintain your Systems' integrity and optimal levels of performance. When employees are unproductive…Profits shrink, Moral decreases due to frustrations, and Customers aren't being serviced like they should. On and on.
[2] Additionally, if you have under-qualified people doing the support, it can really add to the problems. When they don't really understand the complexities of a Network, aren't an expert in Best Practices, etc., the harm caused by bad decisions can leave the Network in shambles.

What you can do:
[1] Depending on your company size, you have (2) choices.
{A} Create your own IT Department…DIY or by hiring qualified full-time Technicians, or
{B} Engage with an Outsourced IT Department that provides all of that for you...which can be half the cost of a Highly qualified full-time employee. They already have the systems and procedures in place, you would have to figure out. They assist with user training & awareness. *Both A/B scenarios are better than believing in "As-Needed" random help, calling the 911 Technician for every emergency...which in all cases, is a time-bomb. Like believing a AAA Card is the answer when traveling, because you don't check your Oil, Water or Tires on the car.

[2] Establish a maximum 5-year lifecycle policy on your throughput is slower, they lack new advances that have come along, and induce a huge amount of Risk to your Business.

[3] Standardize on Hardware components and Software applications. When you have a mishmash of components, that complicates deployment, troubleshooting & repair. It also requires companies to support a variety of programs with different license terms and renewal dates.

Specific Technology Mistakes

While focusing on the (2) Business Mistakes addresses most issues head-on, you do need to be aware of (3) Tech areas that must be in place, for you not to be a statistic. Remember, this conversation is about business growth and you achieving your dreams. We don't want to allow your dreams to be hi-jacked, due to negligence in these (3) following areas.

#3 Failure to: Implement a Complete Backup Solution

What it is:

A Complete Backup Solution is one that protects not only your Data, but also the Applications and Systems that you have in place. Data only is an incomplete Backup.

Why it matters:

Losing your Data can cost you Time, Money, Customers, and possible fines due to Regulations. It could even cost you the Business itself. When there's an event or disaster, you may not only lose data, but your Business Operations are halted. No payroll, accounts payable, accounts receivable, etc. They stop. What if the event caused you to lose all of this and your records? When Systems go down, it could be as much as two to three weeks before they are back online. It takes time to order a new server, get it configured, get all applications installed and then finally restore the data. A big percentage of companies that lose all or part of their data, eventually shut down or file for bankruptcy. Bottom line…Downtime is Money. Latest averages are an hour of downtime costs $8,000 for a small company, $74,000 for a medium company and $700,000 for a large enterprise. This is absolutely the 1st thing you should verify (or implement) immediately.

What you can do:

[1] Ensure all Data Files are being backed up…and nothing is being missed.
[2] Verify the Applications and the Servers themselves are also protected.
[3] Ensure the Backups are going to Reliable media (tape drives are the least reliable).
[4] Enable off-site secondary backups. A second copy is necessary due to any local failure, theft, flood, or corruption that could compromise or destroy your onsite backup.
[5] Verify the Backup is functioning and hasn't stalled, or some cable has come loose.
[6] Finally, perform periodic test restores to verify there isn't backup corruption and the program is working correctly.

#4 Not Serious about: Cyber-Security

What it is:

Backups can be considered the 'Last Line' of defense...Security can be considered the 'Front-Line' of defense. Cyber-Security involves Protecting the Network; the Devices; and the Users in your environment from Malicious people, Hackers, and Nation States - that Delete, Corrupt and Steal your Data.

Why it matters:

Cyberattacks, data breaches, spy-ware, malware, viruses, online scams, vulnerabilities in Software, User Logins, Password compromises, and Email scams...can completely sideline your business. These 'Bad Actors' are infecting and exploiting businesses mostly for profit. It’s a big business for them. Something as simple as an infection can require two-and-a-half days to resolve and cost small and medium-size businesses $1000’s every year. This doesn't factor in lost revenue that was a result of this.

What you can do:
[1] Don't skimp on Security. Never ignore it. Implement Current, 'Up-to-Date' tools & practices to address the (4) Cyber-Security areas...your Network, your Devices, your Apps and your Users.
[2] Research the following Cyber-Security areas: a Modern Firewall; End-Point Malware protection; Advanced Security software; regular Updates and Patches; Remove/Disable unused user accounts; Multi-factor authentication password enhancements; File-sharing software restrictions; Email usage guidelines; Company Policies and Procedures; VPN's; Encryption; Web surfing filters; DNS filtering; a Monitoring and Resolution Service, etc.
[3] Suggestion: start with these (2) following items...

{A} a **Security Assessment** scan of your environment, to get a current state.
{B} Also, have all users go through **Security Awareness Training**, which could yield your biggest bang for the buck...as user activity is the weakest link.

[4] Consider outsourcing these activities to an IT Organization that provides these services.

#5 Buying: Cheap Equipment

What it is:
Using Lower-Cost Home-use equipment (or even Discounted Off-Brand Equipment), in a Business setting, vs. acquiring 'Business-Class' hardware.

Why it matters:
With low cost 'Home-use' mass-market devices, you always pay the difference on the back end…due to sacrificing Reliability, Security and Performance.
People don't realize that the cost of installing improper equipment is much higher, when you consider repair costs, shorter lifespan, data corruption, security issues, tech support time, and downtime. Cheap equipment simply will not perform as reliably, lacks business class features, are susceptible to security breaches, and the need to replace it is sooner than you want exists, because it wasn't built well. What may work for someone at home, is not what's suitable for a Business environment.
Business-class devices have high performance designs and are built for continuous multi-user activities. They allow for software upgrades, bug fixes and enhancements – a regulatory requirement. Necessary support, along with warranty replacements is also provided.
The point here is: a business needs dependable & reliable equipment for operations to stay up and running, in a stable environment so Business Operations can continue making money.

What you can do:
[1] Purchase and Use 'Business-Class' hardware…to keep your Business activities online, with a faster performing, secure experience.
[2] Resist the Distraction of dedicating your time to discover what's quality hardware and what's not. Is it Secure, What Model is correct, What vendor has the Support I need, etc. It's not the best use of your time to research, investigate, and demo products to figure this out.
[3] Contact a Technology consultant who has done that already and can help you with the correct hardware right away. Plus, if you need installation and maintenance services, they can provide that support as well.
[4] If you need multiple similar devices, standardize - as discussed in Mistake #1

We Hope this Report has Provided you with some Valuable Insights that you can use and act on right away.

Y3K IT Services is a 'Business Services Provider' that Assists Businesses with all Areas Covered in this Report. We can Provide Help and Support with your Technology or Collaborate with you on a Strategic Roadmap that aligns with your Business Goals.

To Answer any Questions or to Point you in the Right Direction, Feel Free to Reach Out to us for a Chat.

To Schedule a Chat:

Click the Link and Choose a Time that works for you
https://calendly.com/y3k-it/lets-chat