

Stop Failures!

9 Ways to prevent Disaster.

1. Spam Emails: Secure your email
Most attacks happen through Email.
2. Passwords: Apply Security Policies.
3. Computer Updates: Keep Microsoft, Adobe and JAVA products updated.
4. Training: Train your users – Often! Teach them about data security, Email attacks, policies and procedures.
5. Advance Security: Move beyond outdated antivirus tools of the past.
6. Firewall: Turn on Intrusion Detection & Intrusion prevention features.
7. Encryption: Whenever possible, the goal is to encrypt files at rest and in motion.
8. Two factor Authentication.
9. The Most important is Backup: Local (BDR Appliance) & to the cloud, test your backups often.

If you need help to implement anything of these, call us today!

June 2018



This monthly publication provided courtesy of **SHAN DHOLARIA**, CTO of PCPlus Networks.

"As a business owner, you don't have time to waste on technical and operational issues plus security is a BIG concern too.. That's where we shine! Call us and put an end to your IT problems finally and forever!"



3 Deadly Mistakes You're Making By Being Cheap With Technology

Today's small and midsize businesses (SMBs) have an uneasy relationship with technology – even if they don't realize it yet. As the marketplace reaches new heights of complexity and speed, and consumers migrate to cyberspace en masse to make their buying decisions, SMBs are responding in turn. Today's savvy business owners utilize ever-evolving technologies to capture their customers' interest and imagination, make conversions and manage their day-to-day operations with unprecedented ease and clarity. Certainly, the Internet age is a thrilling time to be in business. Each business is equipped with wildly powerful tech that has transformed the landscape of commerce forever.

But there's an uncomfortable truth that goes hand in hand with this increased dependence on technology. At its best, IT allows us to do incredible things we never would have imagined were possible even 10 years ago. At its worst,

IT is an unreliable, finicky and potentially hazardous scaffolding upon which we built our loftiest hopes and dreams. Even the best IT requires wrangling to shape it to our needs and keep it on track and safe from intruders.

Despite this reliance on technology, the vast majority of business owners consider it an extra expense rather than a foundational element of their company. As a result, they skimp on technology spending. But being cheap comes with a cost – one much bigger and more dangerous than you probably realize. Here are three mistakes you're making by underspending on this key part of your business.

- 1. You're spending on technology based on an unrealistic, poorly planned budget rather than building your technology budget around your actual needs.**

Continued on pg.2

Continued from pg.1

When you're an SMB with limited resources, it's easy to see any money saved on software and hardware as a success, leading businesses to opt for cheap, clunky and outdated solutions. But in a world where the lion's share of your day-to-day operations is dictated by the digital equipment you and your team use, where small businesses exist under constant threat of cyber-attack and data is a precious commodity that could disappear at the speed of a failed backup, cutting corners is unwise. Updating your digital approach and tightening your cyber security may not result in obvious, immediate returns on your investment. But adequate technology spending is just that – an investment. When you invest in the latest technology, you're investing in the long-term productivity and security of your business.

2. You're opening yourself up to disaster.

It's one thing to have an employee's computer unexpectedly fail or for an Internet connection to have a momentary hiccup. But if you're skimping on technology, you're leaving your business vulnerable to catastrophes that could cost you thousands. One of the most prominent and overlooked of these threats is cybercrime.

"When you invest in the latest technology, you're investing in the long-term *productivity* and *security* of your business."



According to the 2016 State of Cyber Security in Small and Medium-Sized Businesses report, half of all U.S. small businesses fell victim to a cyber-attack in 2015 – a number that has only continued to climb. The majority of these attacks are ransomware, in which entire systems are locked out of vital data and forced to shell out enormous sums to recover it. Even if you assume you're secure (and you probably aren't), there are other risks to contend with. Server failures, backup loss and system downtime can shutter businesses just as easily as a vicious hacker.

3. You're letting the competition get ahead.

Outsmarting your competitors takes more than just mimicking whatever latest strategy the thought leaders of your industry are championing at the moment. It requires anticipating future trends and acting on them. And in business, there's one universal truth you can count on: The future of your industry lies in technology. Cloud services, new and constantly updating software, CRMs and a staggering array of productivity-enhancing tools are just a few of the advances your competitors are considering (if they haven't snatched them up already). If you neglect the future, your company is destined to become a thing of the past.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now



At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To Get Started And Claim Your Free Assessment Now

Call Our Office at 678-523-5599

Services We Offer

PCPlus Networks connects you to maximum return on your IT investment with top notch business continuity solutions. As your partner we'll deliver speed, value, and quality from start to finish - using expert Engineers & project managers to keep everything running smoothly. We work with you every step of the way, from consulting to design, project management, installation and ongoing support. We even back it all up with a long lasting warranty.

IT Services includes:

- Managed Cyber Security
- IT Infrastructure Management.
- Network Support
- Managed IT Services
- Cloud Integration
- IT Consulting.
- Hardware/Software
- Backup & Disaster Recovery
- Network Storage Solutions
- VOIP / Virtualization
- Wireless / Wi-Fi Solutions
- Virus/Malware Protection
- Email / Spam Protection.
- Business Continuity Solutions
- IP Video Surveillance.
- Network Wiring/Cabling

**Give us a call today at
(678) 523-5599 to
discuss your needs.**

3 Questions No Leader Should Ever Ask

At ghSMART, we advise board members and CEOs of large companies on their most important leadership issues. One of the most important skills we discuss is making sure they are consulting on the right questions.

I think of a "right" question as one that matters - a question that will cut to the heart of an issue, produce an answer on which the leader can act and provide the highest value to the leader in terms of results.

But the "right" question then becomes, "What are the wrong questions?"

There are three categories of "wrong" questions that I've heard time and time again over the years. Merely asking these questions can lead you down the wrong path when you're seeking to achieve your career's full potential.

1. If you have to ask an ethical question, just don't do the thing you were considering.

The wisest, most successful leaders I have served or worked alongside all seem to lead according to this rule regarding ethical questions: "If you have to ask, then don't." In other words, if there is something you're considering that's in a moral gray area or might be misinterpreted as unethical, then just don't do it. At ghSMART, we call this "having 110% integrity." We do things that are not only 100% ethical, but we give an extra 10% safety margin to avoid things that could be misinterpreted.

2. If you have to question whether someone is underperforming in their job, they are.

There's a common cycle of "facing reality" I often see my clients go through. They have a bold vision and a goal to achieve something great. And when they realize that they don't have the team to make it happen, they start to fantasize and think, "I wonder if Fred or Amy is going to rise to the occasion and display strengths we've not yet seen to achieve these results." Great leaders know who they can count on. They don't expect a subordinate to suddenly start performing well in a role that does not appear to fit their talents and interests.

3. If you wonder whether you can trust your boss, you can't.

There is a saying: "People don't quit companies; they quit bad bosses." So if you find yourself wondering whether you can trust your boss or not, you likely can't. Instead, go find a boss you can trust. Find a boss who will hold your interests in high regard and care about your career goals as much as you do, giving you coaching and feedback to help accelerate your learning. These bosses will have your back during bonus time. Rarely do you see great leaders who wonder about the trustworthiness of their boss staying at that particular job very long.

~ Geoff Smart is chairman and founder of ghSMART.



IT Security Tip: Don't download **ANYTHING** you're not authorized to download

So you have a big file you need to get over to your printer **YESTERDAY** and you can't get it to "send" via e-mail because the file is too big. What should you do? The right thing to do is contact your IT department (us!) so we can assist by installing a secure, commercial-grade file-sharing application. What you shouldn't do is download a free copy of Dropbox or some other file-sharing software without telling us. Dropbox and other free apps come with a price: **SECURITY**. These applications are known for security vulnerabilities and hacks. Plus, if we don't know about it, we can't manage it or secure it; so the golden rule is this: **NEVER** download any software or application without checking with your IT department first!



2775 Cruse Rd. Suite 2203
Lawrenceville, GA 30044

Inside This Issue

3 Deadly Mistakes You're Making By Being Cheap With Technology - 1

3 Questions No Leader Should Ever Ask - 3

How To Quickly And Easily Make Your Business More Profitable

Early in any small business, it's extremely difficult to turn a profit. Even after you gain a little traction, it's easy to get caught up in the never-ending details. This means you have no time left for the things that will actually increase your revenue. But there are a few things you can do right now to raise your bottom line.

Perhaps the most important action item on your list should be to calculate the exact costs of your business. In order to know where you're starting, you need to look beyond general expenses and pinpoint just how much your activities are worth to the company. Then you can start cutting out tasks that are measurably low in value,

automating them wherever possible. If you can do that for both you and your team, you have a great place from which to start.

*SmallBizTrends.com,
March 26, 2018.*

Top Ways To Stay Secure In The Social-Media World

Social media allows millions of people to reconnect and stay up-to-date with family members, friends, acquaintances and even former in-laws. But as social media reshapes the way we communicate with one another, it's important to keep a couple of things in mind to protect yourself and your data.

Remember that there's no "delete" button on the Internet. Even if something seems temporary, a simple screenshot or check through

the archives can make it permanent. Even if you keep your social media completely private, relationships change, and what was private yesterday may suddenly become public record. The question you need to ask is whether you'll be comfortable in 10 years with what you're posting today.

In the same vein, if you post in online forums or on message boards, consider using a pseudonym. Never share names of real businesses, clients, friends or family. If a bank manager wouldn't allow a picture of all the money in the vault to be shared on the web, you shouldn't allow a picture containing confidential, financial, legal or other protected documents and items to be shared either. A good social-media policy in the office now can save headaches down the road.