2021 TECHNOLOGY BYTES

Insider Tips to Make Your Business Run Faster, Easier & Be More Profitable

Exclusive For CEOs

New Year's Resolutions To Boost Your Cyber Security

Know More On Page: 2

What's Inside

Finally Shed The Old This Year, It's Costing You Much More Than You Think

New year, new technology! If your business is still relying on older and aging technology, it's time to think about updating it. As it ages, the effort to keep it running comes with many hidden costs. While it may seem financially savvy to keep older hardware and software running, you may be setting yourself up for major costs down the road.

It's understandable why many small businesses shy away from investing in new equipment and software. They do the math and see a number that keeps rising. While the upfront costs of new technology, hardware or software can be high (or higher than you would like), you have to consider what you would be paying for versus the cost of keeping aging technology running.

Let's start by looking at some of the "hidden" costs that come with using older or outdated technology. First, consider **the cost of productivity.** The older technology gets, the less efficiently it runs. This applies to hardware and software. Hardware has a tendency to lag, even if it's well-maintained. Devices simply wear out with use. This cannot be avoided.

But the productivity issues that come with aging hardware only get worse when you bring aging software into the mix. Over time, you will start to lose support from developers, and this comes with all sorts of problems. Here are three examples;

Loss Of Integration Older apps lose stable integration with companion apps. At one point, your CRM software may have worked perfectly with your billing software. As developers focus on newer versions of their apps, they stop updating past versions. The end result is more hiccups or errors. You risk losing data.
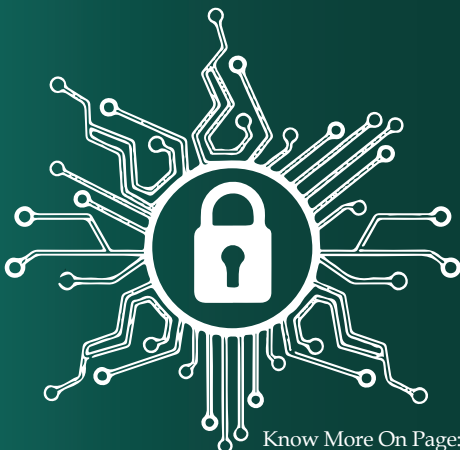
Loss Of Compatibility Older apps aren't always compatible with newer apps. What should you do when still using an old software and your vendors or customers use the up-to-date version? It can result in a lot of aggravation on everyone's part, and you can end up losing customers. One Microsoft survey showed a vast majority of consumers "91%" would walk away from a business if that business was using older technology.

Loss Of Time And Money Factoring in slow equipment and a loss of integration and compatibility, aging tech makes it harder for your team to do their jobs.

CYBERTRUST IT SOLUTIONS
WE PUT IT TO WORK

A recent study by Currys PC World found that employees lose an average of 46 minutes **every day** due to aging technology. That adds up to about 24 days per year and an average loss of about $3,500 per employee, though that number can vary wildly from industry to industry. You can be sure the cost in time and money has a ripple effect throughout the entire business.

While productivity takes a hit, there's another major issue that comes up when your business relies on aging technology: **security.**

As your tech ages, and as developers end support, this means you'll see fewer security patches. Eventually, there will be zero security patches, leaving you vulnerable. Developers may stop supporting older products, but hackers and cybercriminals will keep on trying to break into those products. They know small businesses tend to update their systems at a slower pace, and this gives criminals an advantage.

If you get caught using outdated software and a hacker is able to break into your network, the costs associated with

> **"One Microsoft survey showed a vast majority of consumers "91%" would walk away from a business if that business was using older technology."**

this kind of a data breach can put a business under. It's devastating. The problem is made worse if you had limited IT security in place (or none at all) and weren't backing up your data. It's like handing your business over to the criminals! The importance of IT security cannot be overstated, and if you are working on older computers with outdated software, risks are greater.

So, What Can You Do? As we said before, many small businesses assume that keeping their technology up-to-date is cost prohibitive. They don't want to deal with the upfront cost that comes with investing in new hardware and software. While it can be costly, there are ways to mitigate your costs, depending on your needs.

One great example is through a Hardware-as-a-Service (HaaS) and Software-as-a-Service (SaaS) company or program. These allow small businesses to stay current without having to drop a tidy sum in order to make it all happen. These services are often offered through managed service providers (MSPs) that are dedicated to helping small businesses with all of their IT needs, including keeping their technology updated and their network secure from outside intruders.

When you factor in the loss of productivity (and the frustration that comes with that) along with the costs that come with data breaches, malware infections or cyber-attacks, it can easily be worth it to kick your old tech to the curb and embrace the new!

5 New Year's Resolutions To Boost Your Cyber Security

2021 is here! As we get back on the job this year, here are some thoughts for resolutions to make, to help keep you cyber safe in 2021.

1. Make Strong Passwords To make your passwords strong, do not include easy-to-guess personal info such as names and birthdays. The minimum recommended password length is 8 characters. Along with letters, make your password diverse; use uppercase letters, lowercase letters, numbers, and symbols. Ex. Str0ngPa$$w@rd3

2. Use MFA Wherever Possible To avoid identity theft and other malpractices, it's always better to confirm the user's identity to add that extra layer of protection. Multi-Factor Authentication (MFA) is often described as "something you have and something you know." It requires you to enter two or more authentication forms, and it can be any combination of a password, smart card, token or even a fingerprint or voice pattern.

3. Block Suspicious Websites Clear guidelines must be given to employees not to access an unknown website. Apart from the necessary, other websites must be blocked. Those who are not aware of distinguishing a malicious site from a good one must be taught immediately.

4. Regular Update Of Technologies When it comes to cybersecurity, software plays a major share in protecting user data or saving any company from cyber-attacks. Bots, viruses, and attacks are evolving as we speak. So regular updates of the technologies used in protecting your company must also be updated regularly.

5. Expand Tools And Services Digital security dangers are expanding in seriousness and recurrence, which is stressing the IT-associations in numerous organizations. Many tools have extended their administration portfolio with down-to-earth digital security administrations to help the organizations in their voyage to better digital security.

Developing your organization's capacity to identify interruptions rapidly and react speedily will be of the most considerable significance in 2021 and the near-future future.

For more information, visit: www.CyberTrust-IT.com Or Call: (949) 396 1100

Shiny New Gadget Of The Month:

NexOptic DoubleTake Binoculars

You might not realize it, but binocular technology has come a long way in the past 10 years. It's all thanks to advances in other areas of technology, including high-resolution cameras and high-resolution displays. Bring these technologies together along with some serious image processing, and you are left with NexOptic's DoubleTake Binoculars!

This pair of binocs is slightly smaller than a good pair of traditional lenses, but it comes with so much more, including a 12-megapixel sensor capable of shooting 4K video. It's GPS and WiFi enabled and has a Micro SD card port so you can easily save your photos and video. It's like a supercharged camera, but it has something your average phone camera does not: 10X digital zoom. It's great for travel or hobbies like birdwatching. Learn more at NexOptic.com/doubletake

6 Time Management Tips For The Busy Entrepreneur

Face it, there will never be enough hours in the day to accomplish everything you need to do. But, if you methodically review how you spend your days and instill focus and discipline while completing daily priorities, you will soon find more time to work on the long-term success of your business. Here are six ways to do it.

1. Conduct A Time Audit.

Sit down and review three months of activity. The data from the analysis will show where you spent your time (which projects, tasks and priorities demanded your attention) and with whom you collaborated to get the work done. The audit will also shed light on areas where you were distracted, where you were the most productive and which tasks/projects took more (or less) time than anticipated.

2. Eliminate Time Drains.

These are the kinds of things that sneak up on you and steal time that can be put to better use growing your business. Look for these time drains: not delegating tasks, not managing meetings efficiently (tip: always have an agenda!) and spending too much time writing/responding to e-mails. If you've done your job as a leader, members of your team can handle a majority of meetings and e-mails. You hired great people. Now let them do their jobs.

3. Take Control Of Your Calendar.

Remember, you drive your schedule; don't let others drive it. Block time throughout your day and guard against changing your schedule to work on tasks that are not important or urgent. The way you allocate your time has a direct correlation to your effectiveness as a leader and, ultimately, the performance of your business. Prudent calendar management will also send a strong signal to your team that you should take this seriously.

4. Plan Your Day.

When you know your priorities for the day, you will be better prepared to reset your work schedule if the unexpected comes your way. Once your schedule is set, block off chunks

of time to work on your priorities. I recommend 90-minute blocks so you can concentrate on big-picture items or work on a group of related tasks. Stay disciplined and don't allow yourself to go over that allotted time.

5. Limit Interruptions.

Now comes the hard part. Once you start working on each priority, you need to remain focused. Close the door and don't answer the phone unless it's a critical issue. Avoid checking your e-mail. Don't let distractions slow you down.

6. Hold Yourself Accountable.

Share your tasks, priorities and deadlines with a colleague. Meet with that person at least monthly to review how well you managed your time. The probability of success increases when you have someone watching your progress and coaching you until you the cross the finish line.

Cyber Security Tip

Remember Phones Aren't Immune To Cyber Security Threats

■ 4 Ways To Make Sure Your Business Is Ready For What 2021 May Bring

As you prep for the coming year, here are four things you need, to give your business a serious edge.

1) Head To The Cloud. Back up your data to secure cloud storage. This makes it a breeze for you and your team to access. Should anything be disrupted on-site, you have a backup you can turn to.

2) Update, Update, Update! Patch all of your security solutions, apps, programs, you name it. You don't want to accidentally leave yourself open to security exploits because you're four months behind on the latest security patch.

3) Dive Into Software-As-A-Service (SaaS). One great way to stay ahead of the curve on software is to pair with a SaaS for your various needs, such as marketing, project management or billing. It's easier to keep updated and integrated with the latest and most reliable software on the market.

4) Call Your MSP. Talk to your managed service provider to make sure all of your current needs are being met. Do you need additional protection? Do you need to back up data more frequently? Do your employees need more IT security training? Look for gaps and work together to fill them.

■ The "Human Firewall" - What is it and why you should be freaked out by it

Social engineering is a scary thing, and we're all vulnerable. It starts when scammers try to build trust with their victims. They trick their victims into handing over e-mail addresses, physical addresses, phone numbers and passwords.

Scammers often use phishing e-mails (and sometimes phone calls) posing as legitimate sources to get this information. They might tell you they're a representative at your bank or your favorite online store. They may even pose as one of your colleagues. They prey on your desire to help or fix a problem.

Social engineering works because scammers know how to break through the "human firewall," or the people in your organization.

Did You Know?

81% Of Hacking-Related Breaches Leveraged Either Stolen And/or Weak Passwords.

You can have all the malware protection in the world, but hackers can still break in by **exploiting your employees.**

How can you protect yourself and ensure your human firewall isn't breached? While no method can stop social engineering completely, **ongoing cyber security training can go a long way in patching that firewall.** When your team knows what to look for and how to deal with it, they can stop the scammers in their tracks.

HAPPY NEW YEAR 2021