TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON
CONSULTING & SOLUTIONS

Inside This Issue

January 2021

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

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 that technology. 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Let's start by looking at some of the "hidden" costs that come with using older or outdated technology.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

Continued on pg.2

Continued from pg.1

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 were 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. 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.

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

If you get caught using outdated software and a hacker is able to break into your network, the costs associated with 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, depending on your needs, there are ways to mitigate those costs.

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 Critical Facts Every Business Owner Must Know Before Moving Their Computer Network To The Cloud

INTRO TO CLOUD COMPUTING

"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud"

Discover What Most IT Consultants Don't Know Or Won't Tell You About Moving Your Company's Network To The Cloud

If you need to upgrade your current computer network and are considering cloud computing to save money and simplify IT, the insights provided in this report will arm you with the right information and questions to ask to avoid getting "sold" a solution that doesn't work for you.

To Gain Instant Access To Our Free Report visit:
www.hodgsonconsulting.com/moving-to-cloud/

INTRODUCING: A NEW And Superior Approach To I.T. Support

Co-managed I.T., also called Co-MITs, is a customized set of ongoing I.T. services, support and tools we offer to companies with I.T. departments to help "co-manage" all aspects of I.T. support. Not only does this save your organization money, but it also enables your I.T. team to be more effective and efficient, giving you greater peace of mind, better I.T. support and protections against downtime, cybercrime, ransomware and I.T.-related compliance violations.

It is NOT about taking over your I.T. leader's job or replacing your entire I.T. department.

It is NOT a one-off project-based relationship where an I.T. company would limit their support to an "event" and then leave your team behind to try and support I.T.

It's also NOT just monitoring your network for alarms and problems, which still leaves your I.T. department to scramble and fix the problems.

It IS a flexible partnership, where we customize a set of ongoing services and software tools specific to the needs of your I.T. person or department that fills in the gaps, supports their specific needs and gives you far superior I.T. support and services at a much lower cost.

Here are just a few of the reasons why growing companies are moving to a co-managed I.T. approach:

- A significant reduction in I.T.-related problems, faster support and greater productivity for everyone. We don't replace your I.T. staff; we make them BETTER by filling in the support gaps, giving them professional-grade tools, and training and assisting them where they need help. That means your entire office sees a significant reduction in I.T. issues, making everyone more productive.
- You don't have to add to your head count. Finding, hiring and retaining TOP talent is brutally difficult and expensive. With co-managed I.T., you don't have the cost, overhead or difficulty in staffing a large I.T. team. We don't take vacations or sick leave. You won't lose us to maternity leave or an illness, or because we have to relocate with our spouse or we've found a better job. You can flex the support you need as your company's needs change.
- Your I.T. team gets instant access to the *same* powerful I.T. automation and management tools we use to make them more efficient. These tools will enable them to prioritize and resolve your employees' problems faster, improve communication and make your I.T. department FAR more effective and efficient. These are software tools your company could not reasonably afford on its own, but they are *included* with our co-managed I.T. program.
- You have instant access to "9-1-1" on-site I.T. support. In the unexpected event your I.T. leader was unable to perform their job OR if a disaster were to strike, we could instantly step up to provide support and prevent the wheels from falling off.
- You get a TEAM of smart, experienced I.T. pros. No one I.T. person can know it all. Because you're a co-managed I.T. client, your I.T. lead will have access to a deep bench of expertise to figure out the best solution to a problem, to get advice on a situation or error they've never encountered before and to help decide what technologies are most appropriate for you (without having to do the work of investigating them ALL).
- You'll stop worrying (or worry less!) about falling victim to ransomware, a cyber-attack, outage or data-erasing event. We can assist your I.T. leader in implementing next-gen cyber security protections to prevent or significantly mitigate the damages of a ransomware attack or security breach. We can also assist in providing end-user awareness training and help you initiate controls to prevent employees from doing things that would compromise the security and integrity of your network and data. Critical proactive maintenance will actually get done!

Think Co-Managed I.T. Is Right For You? Our 10-Minute Discovery Call Will Give You The Answer 847-906-5005

If you want to see if co-managed I.T. is right for you, we'd like to offer a free 10 Minute Discovery call to answer your questions. At the end of this call you'll know the pros and cons of co-managed, the implementation process and timeframe, cost analysis, productivity measures and more.

Get your no obligation 10–minute Discovery Call 847-906-5005

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.

Nearly **48%** of employees are now working remotely. **70%** project at least **1/3** of their employees will remain remote for at least another **18** months.

Source: Gartner, Skybox Security

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. 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.