Cybersecurity TECHNOLOGY

NEWSLETTER

NETWORK PROVIDERS, INC.
MAY 2023

How Co-Managed IT Could Save Your Company From Financial Disaster

BY JAY HILL
President & CEO

ADVICE FROM THE SHARKS

In April, I spent time with the Shark Tank judges. I presented to them what I have done to strengthen my business. They asked questions and gave great business strategies. I wanted to share a few of them.

First: Security/Compliance.

This is a HUGE issue. It cannot be stressed enough how important this area of technology is to everyone. The Sharks said it is vital that every business asks questions about their system and think about what they are willing to do for security/compliance. We are already ahead of the game, so rest assured we are protecting you, but things are changing fast.

We will contact you with more options for your protection.

Second: Love What You Do!

If you don't love what you do, you'll put off what needs to be done. Love will turn ideas into action. Action is success.

I will share more next newsletter.

Happy Mother's Day and Have a Wonderful Memorial Holiday!

When you consider the investments in your business that you can make as a CEO, you probably think to yourself, "Which investments will give my company the best ROI?" With that in mind, would you think of making a significant investment in bolstering your IT department?

Many CEOs are understandably hesitant to throw a lot of money into their IT department because the ROI is more difficult to estimate. That said, though, consistently updating your company's IT services is becoming increasingly crucial to the continued success, and indeed safety, of your company. Ransomware and other cyber-attacks that steal company data are becoming more frequent and more costly, while IT departments continually get the short end of the budgetary stick.

While that all undoubtedly sounds horrible, you might be wondering just what you can do about it. After all, you only have so much money you can invest back into your company's IT department, and it might not be sufficient for keeping your IT staff from getting burned out, disgruntled or making costly mistakes – even when they're performing their responsibilities to the best of their abilities.

What if there were a way that you could have access to the most up-to-date IT knowledge and software while also not having to shell out the funds necessary to update your systems and hire more knowledgeable employees? Well, that's where co-managed IT can be your company's life preserver.

Co-managed IT is a flexible system for keeping data for your company, employees and clients safe from cyber-attacks as well as assisting in your daily operations where needed. Think of it as "filling in the gaps" that your current IT department (try as they might) struggle to fill.

For instance, say your current IT department is great at taking care of the day-to-day fires that inevitably come up in a normal workday, but they struggle to get to the "important but not urgent" task of updating your company's cyber security and creating data backups. Maybe it's the other way around, where your IT department is very focused on security, but they struggle to find time to assist employees with password resets and buggy programs. Maybe neither of these cases describes your IT department, but they still need better access to the tools and software that would allow them to reach their full potential in protecting the company's sensitive information. Or maybe your company is going through a period of rapid expansion, and you just don't have time to build the kind of IT infrastructure that would best serve your needs.

@networkprovidersinc.com

110 W 13775 S | STE 3 | Draper, UT 84020 | (801) 849-0521

Continued from pg. 1

Regardless of what your IT department's current needs are, co-managed IT is the solution. We're here to do the tasks and provide the tools that your current IT department just can't provide. Make no mistake, however: our intent is not to replace your current IT leader or team. In fact, we rely on the expertise that your IT department has about your systems. That's what makes up the "co" in "co-managed IT."

In order for co-managed IT to work, your company's IT department will need to see us as an ally in doing their job, not as an adversary. At the same time, they'll also need to be open to new ways of doing things. The world of cyber security is constantly changing, and if your IT department is set in their ways and unwilling to budge, your company will be left with an antiquated system, chock-full of valuable data that hackers and cybercriminals can easily exploit.

Finally, however, in order for co-managed IT to work, your company still must be willing to invest in its IT department. We know that the ROI might not be as clear as it is for some other investments, but trust us, the

consequences of not having up-to-date IT services if (or when) hackers steal your sensitive data could financially devastate your company – or even end it altogether.

So, with that in mind, we hope you'll consider the benefits of co-managed IT and how it can make your company safe from cyber-attacks and bring you peace of mind.

If you wish to learn more about Co-Managed IT Services, speak to our Business Technology Strategist, Chris Adams, at (801) 849-0521 ext. 116 or email him directly at chris@networkprovidersinc.com. We are here to help and find solutions to your IT concerns.

How Recessions Benefit Great Companies

By Geoff Smart

Recessions are bad for most people, and I won't make light of how horrible these times can be for the vast majority of companies and their employees. It's true that for most companies, recessions mean increased stress at work, stalled career progression or even layoffs, uncertainty, raised board and shareholder pressure, increased financial strain and extreme anxiety. It's no fun to wake up to that every day! But for great companies, people can turn things around and make recessions awesome.

So, what are great companies? They're the ones that make great products or deliver exceptional services to customers. They provide a wonderful work culture that attracts and retains talented people. And because they take good care of their customers and employees, great companies don't have a dangerous debt burden. They are profitable, can pay their bills to suppliers and deliver an attractive return to investors in dividends and equity appreciation.

Recessions are awesome for certain companies for the following reasons.

Losing The Cobwebs Of Complacency

"Success breeds complacency." Andy Grove, the legendary CEO of Intel, wrote that. And while I'm not here to suggest everybody embrace full-on "paranoia" in the workplace, I am suggesting that successful companies must keep hustling to stay on top. A recession provides an opportunity for a wake-up call to companies that may otherwise start coasting. Now is the time for them to get back on track.

Taking Customers And Colleagues From Undeserving Companies

I'm not sure why customers buy products or services from lesser companies. And I'm not sure why talented people work at lesser companies. Maybe it's due to convenience, connections or just habit. In any case, as lesser companies stumble during a recession (e.g., shutting locations, letting service and quality drop, highlighting dysfunction in the culture, etc.), it's the perfect time for great companies to pick up more of these customers and talented people.

Increasing The Rate Of Learning For Your Leaders

I don't know about you, but time seems to move more quickly for me during harder times than when things seem easy. This can enhance the learning curve of your up-and-coming leaders. Just remember not to make too many decisions for them that will stunt their growth. Allow your leaders to come to you with problems and solutions so you can aptly coach and support them. Let them test and learn various approaches to leading through uncertain times.

If you buy from a lesser company or work at one, the next recession is likely to be a bummer for a couple of years. But if you work at a great company, fear not. This will be an awesome opportunity to shake loose some cobwebs of complacency, take customers and colleagues away from lesser companies and increase the rate of learning of your leaders.

5 Seemingly Innocent Download Habits Your Employees Must STOP Now To Avoid a Ransomware Attack

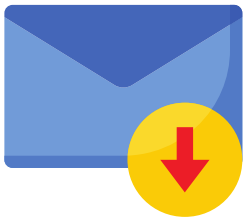
Once upon a time, you could install antivirus software and go about your merry way online and in your inbox, opening, clicking and downloading files without a care.

Today, antivirus alone cannot and will not protect you, especially if you INVITE the hack by downloading a file that is infected with a piece of code designed to circumvent your security protocols. Whether it's a personal computer, phone or a laptop you use for business, here are 5 things you need to STOP doing now to ensure you don't get hacked.

STOP downloading apps from unknown sources.
There are thousands of free apps available online that are very tempting to download. Hackers are masters at curiosity and "clickbait" designed to nail you in a moment of weakness. To prevent rogue apps and programs from installing, configure your devices to disallow the installation of programs from unauthorized sources. On your phone, ONLY download apps from your device's respective app store that are tested and forced to meet the store's security and privacy requirements.

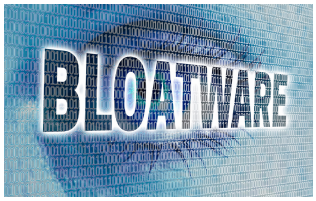
Business owners: while I'm sure all of your employees are trusting souls, it IS possible (and recommended) to have business machines locked down, preventing your employees from downloading any applications (or files) that could harm you and compromise your security.

STOP surfing the web unprotected, particularly when accessing downloads.
This is particularly true if you are on public WiFi. Starbucks is not going to guarantee your Internet connection is safe, nor is any other business, restaurant or location offering free Internet access. Talk to your IT company (that's US!) about installing more than just antivirus, but endpoint protection solutions, like a VPN, that will "hide" you from cybercriminals and filter out nefarious websites and attacks so you CAN use public WiFi without the fear of inviting a hack.



STOP opening and downloading files e-mailed to you without extreme caution.
Phishing attacks via e-mail are still the #1 way hackers gain access to a network. It's very common for an attacker to hack into someone's e-mail and get their list of friends, colleagues, coworkers and their boss to send e-mails that appear legitimate on "their" behalf, even using their actual e-mail – these are are highly sophisticated phishing attacks. So, before you open or download ANY file e-mailed to you, make sure it was one you were expecting. It's far safer to use IT-managed file sharing like OnDrive, SharePoint or Citrix ShareFile to send attachements. But bottom line, if ANY file "feels" wrong or suspicious about a file download, including a weird extension or suspicious file name, CALL the person who sent it to verify. If it's important, they can send it again.

STOP downloading "bloatware."
It's common for legitimate, reputable apps to sneak in other applications or toolbars you don't need. They sell this as a sponsorship to make more money every time one of their users downloads an app. The best way to spot these is to look for checkboxes when installing that automatically opt you into services by default. So, before you hit "Next" and keep rolling to get your app installed, take a second to really read and review what you're agreeing to when installing that new app.



STOP downloading music, software, games, movies and the like from websites like BitTorrent, RARBG, 1337x and similar peer-to-peer file-sharing sites.
It's very common for file-sharing networks to be breeding grounds for hackers who post files infected with malicious software for people to download. Some of the ads on these sites are malicious as well. Don't feel "safe" just because you have antivirus – because you're not.

Business owners: after showing this to your team for both their work and personal devices, contact us to find out how we can implement security systems that will give you stronger protections against hackers and against employees who accidentally click on or download a malicious file.

Ask us about our cybersecurity trainings for employees.

Employee Spotlight

DAVID BARNETT
Consultant of the Quarter

At Network Providers, Inc. we recognize employees who show us their best work performance for each quarter.

David Barnett has been with us since the dawn of time. He has been a very valuable employee to Network Providers, Inc. He has taken on the firewall configurations and excels at that and many other abilities. David has demonstrated a real growth in the past year. He takes on challenges that have a very high difficulty level, gets them done on time and makes it seem easy in the process. David has a great bond with his clients and has a eye for them and their success. Thank you David for being an example to all and keeping our clients happy. We at NPI, appreciate all you do!

Let's congratulate David Barnett for being the best employee of the Quarter!

One of today's biggest phishing risks is email spoofing. This form of phishing involves cybercriminals mimicking official corporate communications to lure unsuspecting employees into interacting with them. In this scheme, emails purporting to be from large firms, such as Amazon, Microsoft or DHL, are malicious. Discerning what is real versus what is fake can help your organization prevent costly cybersecurity breaches.

Check the Sender's Email Address
Legitimate companies send emails from their official domain, like "microsoft.com," and not variants like "microsoft.business.com." If a domain looks odd, check the address on the company's website.

Pay Attention to the Header and Footer for Clue
If the header or footer is inconsistent with other messages from that brand or has missing information or is just slapdash, it's likely the message is a phishing attempt.

Look at the Subject Line and Preheader
Does the subject line or preheader of a message seem a little "off" to you? Are there odd phrases, emojis or unusual things in the subject line and/or preheader? If yes, it indicates phishing.

Analyze the Content and Implied Urgency
Claiming an action is urgent, offering a special that's too good to be true or insisting a company must make a payment before services are cut off are all hallmarks of phishing.

Beware of Formatting Red Flags
This is where many of us catch phishing attempts. If the message has strange formatting, spelling mistakes or bad grammar, or the colors, logos and fonts are "off," it's probably phishing.

Be Wary of Unexpected Attachments like PDFs or Word docs
If you aren't expecting an attachment or that looks suspicious because it has a strange name, it might be malware or ransomware, which are frequently deployed through phishing. We have the right training solution for your business. Contact us to learn more.

Use Caution if a Message asks you to Log in through a New Link
Consider the links that a message asks you to click to see if they go to the company's actual domain or log in on their site directly. Fraudulent password reset requests are a staple of phishing.

Better safe than sorry when it comes to email management. Phishing is one of the most common attack vectors employees encounter. The good news, however, is that regular security awareness training empowers employees to spot and stop bogus messages, such as fake branded emails, and reduces your company's chance of experiencing a damaging cyberattack.

Choose a training platform/learning management system that allows you to design training courses and then upload/deploy them to team members. The solution must host a wide range of training courses including employee safety, conduct (anti-harassment), orientation/employee onboarding, cybersecurity, policy changes and more.

We have the right training solution for your business. Contact us to learn more.