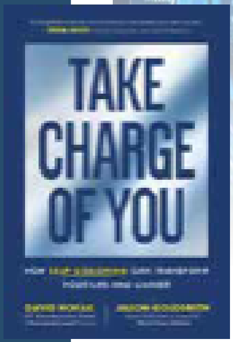
WCI Technology Insider

Insider Tech Tips - Written For Humans, Not Geeks

Take Charge of You by David Novak & Jason Goldsmith



Many business books will tell you that one of the keys to success is finding a strong mentor and learning from them, but, in reality, finding a mentor is easier said than done. Wouldn't it be easier if you could simply coach yourself? *Take Charge of You,* provides readers with the tools to coach themselves. With extensive coaching backgrounds in the worlds of professional sports and business, the authors are well equipped to teach others how to coach themselves. If you're looking for a thought-provoking read that will provide you with a road map for growth, this is the book you've been waiting for.

September 2022

Bill Wright Founder & CEO

Our Mission:
Technology systems that anchor your business and protect what you have built, from a company inspired to make the world better.

It's Time For a Refresh!

4 Cybersecurity Trainings to do With All Employees

Students are returning to the classroom now that back-to-school season is officially underway. During the first few weeks, teachers will be reteaching their students the topics they learned in the previous school year to help them regain knowledge they may have forgotten during the summer break. But students aren't the only ones in need of a refresher every year. Your employees also need to be refreshed on company policies, values and, most importantly, cybersecurity practices.

Did you know that human error accounts for 95% of all successful cyber-attacks? When a cybercriminal is planning an attack, they look for weak points within a company's cyber-security plan. The easiest spot for hackers to exploit is a company's employees. New cyberthreats are created on a consistent basis, and it's important that your employees know what to do when they encounter a potential threat. If your employees are not routinely participating in cybersecurity trainings, your business could be at serious risk, regardless of size.

Every single one of your employees should be familiar with your cybersecurity practices. When they're hired on, they should go through an initial training that lays out all of your practices, and they should also participate in refresher trainings throughout the year to ensure that the entire team is on the same page with cybersecurity. At the very least, you should host at least one security training annually. If you've never put together a cyber-

Continued on Page 2 ...

... Continued from Cover

security training, you may be wondering what topics you need to cover with your team. Below, you will find four of the most important topics to cover.

Responsibility for Company Data

This is your opportunity to explain to your employees why cybersecurity is so important. They need to understand why cybercriminals are interested in your company's data, and what they could potentially do with it. Everyone on your team has a legal and regulatory obligation to protect the privacy of your company's information. When discussing this topic with your team, it's imperative that they know the ramifications of falling victim to a cybersecurity threat.

Internet Usage

Does your company have restrictions on what websites your employees can use while at work? If not, that's something you should look in to. Every device that's used by your employees should have safe browsing software downloaded onto it to prevent them from stumbling upon dangerous sites that could put your company's data at risk. Your employees should know what sites are acceptable to use and that they should not be accessing their personal accounts while connected to your company's network. They should never click on links that are sent from an anonymous source or are found on an unapproved website.

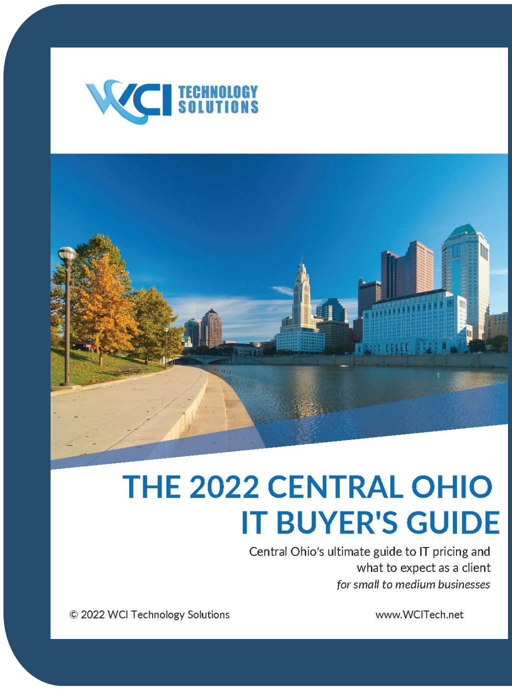
Email

If your employees utilize email while at work, it's important that they know which emails are safe to open. Employees should not respond to email that are from people they aren't familiar with, as that could be a cybercriminal attempting to gain access to your company's data. Employees should only accept and open emails that they are expecting or that come from a familiar email address.

Protecting Their Computers

If your employees have their own personal computers, they should be doing everything in their power to keep them protected. Whenever they walk away from their computer, they should make sure it's locked; they should also never leave their computer in an insecure location. Also, ensure that your employees are backing up their data routinely and have downloaded necessary antivirus software.

It's of the utmost importance that your team has been fully trained in your cybersecurity practices. If they haven't, they could open your business up to all sorts of cyberattacks that will damage your company's reputation from a customer perspective. Your business will also no longer be compliant, and insurance companies may not cover your claims if your team is not participating in regular training.


WCI TECHNOLOGY SOLUTIONS
THE 2022 CENTRAL OHIO IT BUYER'S GUIDE
Central Ohio's ultimate guide to IT pricing and what to expect as a client
for small to medium businesses
© 2022 WCI Technology Solutions
www.WCITech.net

The 2022 Central Ohio IT Buyer's Guide

If you're actively looking for new IT support options, or know that you will be soon, head over to our website and check out this year's edition of the IT Buyer's Guide. As a trusted MSSP and IT expert in Central Ohio, you can rest assured that this eBook is packed full of all the information that you need to make the right decision for your company's IT needs. Check it out today at

www.WCITech.net/2022ITBuyersGuide

TECH FACTS

#1

Nearly three quarters of execs believe AI will be a business advantage in the future

#3

20% of Google searches are now done by voice

#2

A typical person spends an average of 6 hours and 55 minutes online, daily

Bill's Favorite Business Gadget of the Month

Using more than one monitor can help make you more productive. But it's not always convenient if you work on a laptop from multiple locations. Enter the Trio from Mobile Pixels, Inc.

It's a portable monitor that attaches to the back of your laptop, giving you another screen. Add two Trios and you have a three screen setup you can use anywhere.

Bill

Inspirational Quote of the Month:

"Just because something doesn't do what you planned it to do, doesn't mean it's useless."

- Thomas Edison, Inventor

September's Featured Everyday Gadget:

Logitech Litra Glow

Zoom calls have become a part of our daily routine regardless of whether you work remotely, in the office, or a combination of the two. If you'll be on camera every day, don't you want to look your best? That's exactly how you'll look with the Logitech Litra Glow Light. The Litra Glow uses innovative geometry and is frameless to provide more light to the areas within your camera's view. It uses soft and diffused light that's easy on your eyes in case you have to be on the call for an extended period of time. Whether you're on Zoom calls, shooting marketing videos or doing anything else webcam-related, the Litra Glow provides you with perfect light for any situation.

3 Questions No Leader Should Ever Ask

Over the years, I have advised many board members and CEOs of large companies on their most important leadership issues. In life, people like to think that there aren't inherently right and wrong questions to ask, but I think that's a misconception - especially in the world of business. "Right" questions are the ones that matter. They cut to the heart of the issue and produce an answer that a leader can act on. The "right" questions help leaders get results.

On the other hand, you have "wrong" questions. The mere act of asking these questions can lead you down the wrong path and prevent you from achieving your full potential in your career. Over the years, I've heard the "wrong" questions asked a multitude of times, and they can usually be grouped into three distinct categories.

Ethical Questions

The wisest, most successful leaders I have 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 something feels to you as if it is in gray area, or that taking an action might even be misinterpreted as unethical, then just don't do it. I've never seen a leader regret having held back from taking an action when they had an ethical question. "How unethical would it be if..." is a question no leader should ever ask.

Questions Regarding Under-performance

There is a cycle of "facing reality" that my clients sometimes go through. They have a bold vision: 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 will rise to the occasion and suddenly display strengths or show a burst of energy we have not seen to achieve these results." Subordinates typically follow a very predictable pattern of performance. Great leaders know who they can count on to do what. So you rarely see great leaders asking themselves, "I wonder if my subordinate will suddenly perform well in a role that does not appear to fit their talents and interests."

Questions About Trusting Your Boss

There is a saying that 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. Go find a boss you can trust, one who will hold your interests in high regard. Rarely do you see great leaders staying in roles where they ask themselves, "I wonder if I can trust my boss."

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple *New York Times* best sellers. He stays active in his community and has advised many government officials.

Here's why you need to automate more, now

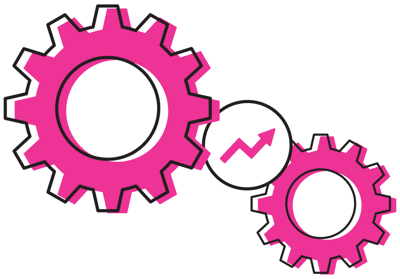
Most staff love automation.

Because it's about creating a set of rules that software can follow automatically, so humans don't need to do boring and repetitive tasks.

Who in your business would be against this?!

As well as saving you and your employees valuable time, automation has loads of other benefits for a business.

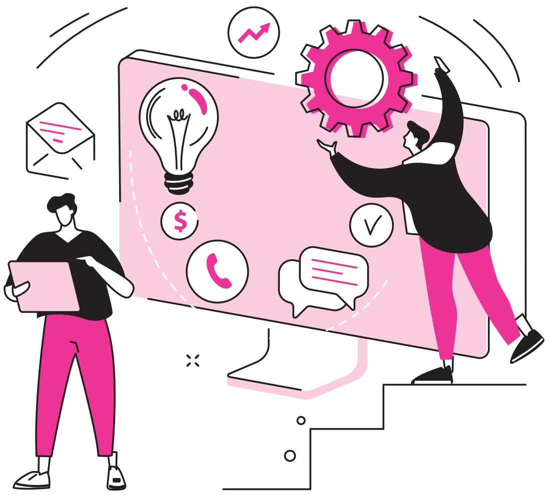
You should see a productivity boost as people can get more done in the same amount of time. It can also produce a leap in motivation and job satisfaction. That's because your people are spending longer enjoying the work they do.



They'll feel more listened to as you've made their jobs better, and will reward that with increased loyalty. Recruitment might be easier as your reputation gets a boost.

Another benefit of automating tasks is for your customers. Perhaps they can get a response to a question a lot faster. Or maybe they can have a smoother experience when they deal with you.

So which tasks in your business could be automated? Even the simplest automations can have a really big impact on the way your business works.



Did You Know

your executives might be your weakest link?

When it comes to cybersecurity, your executive-level managers might be the least vigilant members of your team.

A recent report showed that a huge 49% of execs had requested to bypass security measure on at least one occasion over the past 12 months.

If you're already in the practice of regularly training your people in cybersecurity, are you including everyone in the business, from the top down? It's one of the best ways to make sure all your people are aware of the risks of skipping vital security steps.

New to Windows 365

Managing your Outlook signature in one place

You know when you set an email signature in Outlook on one device, but when you use Outlook on the web, the signature isn't there?

It's a frustration that's been around for years. Traditionally the solution has been to use independent software to manage your signatures.

But Microsoft is hard at work changing the way it stores signature settings. It is moving them to the cloud, so you get a consistent experience, wherever you use Outlook.

It's due to go into testing this month, and be available next month... although it's been delayed for a couple of years up to this point, so... watch this space.

Who's to blame for a cybersecurity breach?

We all know what a huge danger a cybersecurity breach can be for a business. And just how many businesses are being breached right now?

In truth, we hate having to write this. We don't want to fell like we're scaring you, or being all doom and gloom! But it's really important that you're fully aware of the risk to your business if you suffer a breach.

Last year, the number of reported data breaches rose 68% compared to 2020.

And while it's a good idea to implement the right cybersecurity tools to help reduce the risk of an attack, it's practically impossible (or definitely unworkable) to give your business 100% protection from attack, just using software tools.

Because according to research, 85% of data breaches are caused by human error.

If that happens, who's to blame for your cybersecurity breach? Your employee? Or you, the business owner/manager?

It's a difficult question. Sure, your employee is likely the one to have clicked the link or downloaded a bad file that turned out to be malware. They may even have disabled security feature to try to speed up their work.

However, as the business owner or manager, it should be your responsibility to reduce the risk of that happening in the first place.

It all starts with training your people regularly to make sure they understand the risks and how to avoid them. But you should also have the right policies in place to remind your employees of best practice, and what happens if they fail to comply.

Employees are your first line of defense against security breaches. They can only ever be as good as your cybersecurity strategy. Get that in place and everyone knows what's expected of them, how to avoid risk, and what to do if things go wrong.

We say don't worry about who's to blame - just get your ducks in a row, starting with your cybersecurity strategy. If we can help, get in touch!

Technology Update

Home and small office routers are being targeted by cybercriminals in an attempt to steal sensitive data.

This is a smart move by the bad guys, as these routers exist outside of your business's usual security protection. It means they may have additional weaknesses to exploit.

So, how do you protect your data?

If you have remote or hybrid workers, you need to make sure they have the right firewalls installed so that incoming and outgoing traffic can be monitored.

Insisting they use company devices for business work is a good idea. You can also give them encrypted connections when they're working away from the office.

It's time for another monthly tech quiz!

Winner gets bragging rights for 30 days

1. **How many generations of computer have been invented (so far)?**
2. **What does CPU stand for?**
3. **Which company designed the first CPU?**
4. **What's the name of the information storage used to store short-term running programs and data in a computer?**
5. **Which company invented the USB port?**

The answers are on page 8.

Question

I just closed an Office file without saving it. Please tell me I can get it back?

ANSWER

You should be able to recover your file, with a bit of luck. If you saved the document once, Autosave may have done its job. Otherwise, try using AutoRecover or check your temporary files.

Question

I can't open an email attachment.

ANSWER

First make sure this is a genuine file - phone the sender to check. Then, it's possible you don't have the software the file was created with. Right click the document and select "Open With" to see if there's another option.

Question

I've had an email telling me an account needs updating. Is it genuine?

ANSWER

Don't click any links in the email. If you're even slightly unsure, the safest thing to do is to visit the website by typing the URL into your web browser.

QUIZ Answers

1. FIVE. THE FIRST GENERATION STARTED IN 1940 WITH THE VACUUM TUBE. OUR CURRENT GENERATION IS STARTING TO USE AI
2. CENTRAL PROCESSING UNIT
3. INTEL
4. RAM (RANDOM ACCESS MEMORY)
5. IT'S INTEL, AGAIN. THE FIRST USB-COMPATIBLE PRODUCT WAS A MAC IN 1998, FOLLOWED BY USB SUPPORT FOR WINDOWS 98 A YEAR LATER. THE REST IS HISTORY

WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech

These Marketing Trends Didn't Go Out of Style

When people think about trends, they often imagine what's in style at that current moment. We like to imagine that trends come and go, but the opposite is sometimes true. In fact, the greatest trends become a part of our culture. At one time, people thought cellphones, texting and computers were just a phase, but, decades later, they're still here because they made our lives better! Trends in marketing are the same way. Sometimes, a fresh marketing strategy will pop up, but, if it works, it will become a mainstay.

As you continue to plan your marketing strategy for the next few months and the upcoming year, you can look at previous statistics to ensure your methods are successful. Below, you will find three marketing strategies that have proven successful in the past. If these strategies are properly utilized by your company in today's climate, you will quickly see results.

Using Influencers
People love to use their smartphones and social media. During the pandemic, many businesses started to advertise on Instagram and TikTok through the use of social media influencers. A TopRank Marketing survey found most B2B marketers believe this strategy changes minds, improves the brand experience, and yields better campaign results.

Advertising on Podcasts
There are podcasts available that discuss every topic imaginable, and over 30% of Americans listen to a podcast on a monthly basis. That percentage rises when you look at younger demographics. Advertising on podcasts is a great way to reach a younger audience.

Leveraging Ai
The importance of artificial intelligence (AI) for B2B marketing became crystal clear recently, when a Salesforce study reported that 80% of business buyers expect the companies they reach out to will talk to them "in real time", regardless of the hour. This statistic highlights how important chatbots and other AI solutions are for customer conversion.

If you've seen success with certain marketing trends in the past, you don't have to get rid of them when you develop a new marketing strategy.