

TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS



HODGSON
CONSULTING & SOLUTIONS

Inside This Issue

Make 2023 A Great Year For Business With 3 Tech Resolutions | 1

FREE Report Download: The Cyber Security Threat Crisis | 2

Your Credentials Have Been Compromised – What Are Your Next Steps? | 3

2 Ways To Refine Work Relationships With Young Employees | 4

Improve Your Sales Team And Grow Your Business | 4

January 2023



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.



Make 2023 A Great Year For Business With 3 Tech Resolutions

The new year is upon us, and many business owners will use this opportunity to create plans to ensure that 2023 is as profitable as possible. You can devise all kinds of business resolutions you want to focus on during the year, but most of the time, business owners think about key performance indicators like sales opportunities, customer loyalty, or referrals. Still, while these are vital, it's just as important to include resolutions relating to new technological advancements.

You can see growth in many different areas when you improve the technology within your business. Some improvements will help you make each experience better for your customers, while others will allow you to save time and money. If you're unsure of what tech resolutions to make, don't panic; we're here to help!

Here are three tech resolutions to think about in 2023 – they will help you both improve and protect your business.

Improve Your Cybersecurity Practices

It's no secret that technology is constantly evolving, but many people fail to realize that cybercriminals are also evolving. Every business, regardless of size, needs to be aware of the risks and take the necessary precautions to avoid having a cyberattack. If you don't have cyber security practices in place – or it's been some time since you last considered this – you should review your current needs and make any necessary updates.

One of the best ways to improve your cyber security practices is to run your team through annual or semiannual cyber security training.

Continued on pg.2

Continued from pg.1

According to Verizon's 2022 Data Breaches Investigations Report, 82% of data breaches involved a human element. If your team is well-trained in cyber security and has bought into a cyber secure culture, your business will be less at risk. Make sure they know the importance of password security, the different types of cyber-attacks and how to protect sensitive business and customer information.

Utilize A Managed Services Provider (MSP)

There was once a time when businesses used in-house IT teams to take care of all of their technology needs, but this is no longer the most efficient or affordable way to do things. Now, businesses use MSPs to handle most of their technological affairs. MSPs are well-known for their ability to help with any technological needs since their teams are usually full of well-informed experts. They can take care of everything on the technology side of your business, so you can focus more on boosting sales and pleasing customers.

If your business experiences power outages or natural disasters, MSPs will work around the clock to get you back up and running. They even ensure your data is backed up in case disaster does strike. If you're worried about cyberattacks, there's no better way to protect

“According to Verizon's 2022 Data Breaches Investigations Report, 82% of data breaches involved a human element.”

your business and its data than by hiring an MSP. They monitor your network security and keep patches up-to-date to prevent hackers from accessing your information.

Hiring an MSP may be the best thing you can do to protect your business.

Implement Artificial Intelligence Into Your Business

Prepare yourself for the AI boom in 2023. Throughout the past few years, many businesses have utilized AI to boost their profits and customer satisfaction scores, but the uses and benefits of AI will grow significantly this year. In fact, you'll soon notice AI being used in new and beneficial ways in the health care and automotive industries.

If you aren't using any form of AI in your business, you should immediately look into it. You can implement an AI chatbot on your website to provide personalized conversation and help your customers with their questions or needs. Some AI software will even track customers as they peruse your website and offer them product suggestions, which can help improve your sales scores.

The New Year is the perfect time to reset, reevaluate, and plan to ensure 2023 is a successful year for you and your business. If you are unsure about where to start, try implementing some of the tech resolutions listed here. They'll quickly help you grow your business and keep it protected from cybersecurity risks.



Free Report Download: THE CYBER SECURITY THREAT CRISIS

Download This Free Report To Learn:

- The top 5 ways your company can be severely damaged by cybercrime and what you can do NOW to protect your business.
- The #1 threat to your business that even the BEST firewalls and anti-virus software can't protect against (and what you need to do now to remedy it).
- A common misconception about business bank fraud that will shock you - and simple things you can do to protect your bank account.
- NEW protections to put in place now including tools available to monitor cybercrime websites and data for YOUR specific credentials being sold or traded.

Claim your FREE copy today at www.hodgsonconsulting.com/cyberreport or call our office at (847) 906-5005

YOUR CREDENTIALS HAVE BEEN COMPROMISED WHAT ARE YOUR NEXT STEPS?

You've just discovered compromised employee credentials and other sensitive data of your company exposed and available on the dark web. The reality is that, once exposed on the dark web, your information cannot ever be completely removed or hidden.

You cannot file a complaint or contact a support line to demand your data be removed. Your company should immediately start taking appropriate steps and measures to correct or minimize the risks and potential damages associated with this exposed data.

Identify, understand, and learn from past mistakes or failures and adopt a more proactive and preventative cybersecurity strategy moving forward.



WHAT CAN YOU DO TO MINIMIZE THE RISK OF THIS HAPPENING AGAIN?



Implement Multifactor Authentication

Even the strongest and most complex passwords won't protect you if they have been compromised and exposed on the dark web. Requiring users to verify who they say they are via two or more unique security factors will virtually eliminate more than half the threats and risks associated with exposed user credentials.



Consider A Password Management Solution

A password management platform will enable your entire workforce to adapt and thrive in a security-first environment while reducing password frustration and fatigue for users and empowering increased productivity.



Ongoing Security Awareness Training For Users

Users continue to be the weakest link in security for businesses worldwide. This is often due to genuine ignorance regarding security best practices and a lack of knowledge or awareness of common threats and risks. Establish ongoing security awareness training for all users and turn your weakest link into your most robust security defense.



Perform Regular Risk Assessments

A comprehensive audit of your business infrastructure and systems will inevitably reveal vulnerabilities and security gaps within your network, applications, or on your devices. Regular assessments will keep you informed and enable you to achieve and maintain a more preventative approach to security, often preventing issues or problems from arising in the first place.



Proactively Monitor For Breaches And Cyberthreats

Cyberthreats continue to increase and evolve, and hardware and software vulnerabilities are discovered regularly, exposing your business to a steady barrage of security risks. To adopt a proactive and preventative approach to cybersecurity, your business must have visibility and insight into internal and external activities, trends and threats to your organization's network and data.



Back Up Everything

You must ensure your business and customer data is protected and secured against any incident or disaster, such as system failure, human error, hackers, ransomware, and everything in between. In addition, make sure you explore the importance of accessibility and consider investing in business continuity as part of your backup strategies.



Invest In Cyber Liability Insurance

Sometimes things don't work out, no matter how much effort you put into them. As a business, you must do everything right. However, a hacker only needs a single gap or weak point in your security systems to slip past your defenses like a trojan horse. Every business in operation today needs cyber liability insurance to protect itself when all else fails.

REMEDATION TIPS FOR EXPOSED LOGINS

- Replace exposed login passwords** with new, unique passwords.
- Change/refresh** any passwords older than six months.
- If the source of the **breach** is "**not disclosed**," change the passwords of any accounts you know you used the same or similar password for.
- If you can't remember the passwords for all your accounts, change them all. **If you want to be safe, you'll need to update all of your passwords.** We know it's inconvenient, but it's the only way to ensure your online accounts are secure.
- Password awareness:** Many people use the same username and password on multiple websites. If you use the same credentials or a variation of the same password across numerous sites, ensure that the passwords are changed to make them unique.
- Adding \$, ! or any other special characters** or numbers to a password does not make it unique.
- Don't use passwords that are easy to guess**, such as your pet's name, spouse's name or favorite sports team.
- Watch out for phishing emails.** We've seen a significant increase in phishing attacks against emails that have been discovered on the dark web.
- We recommend **keeping an eye on any suspicious activity** on your online accounts if the reported compromise does not include a password. Check for suspicious or otherwise questionable emails on a regular basis.
- To keep track of your passwords, **consider using a password manager.**
- Close unused accounts.** If a previous employee's credential was compromised, double-check if all third-party sites they had access to were turned off.

2 Ways To Refine Work Relationships With Young Employees

The workforce gets younger every day, which can make things more challenging for business owners. Many have recently adapted to meet the needs of new millennial employees, but now even younger generations have started to work. This has required business owners to learn how to build meaningful relationships with these new employees. Here are a few ways you can do this, too.

Setting Standards Early

One of the most significant concerns for business owners, especially in regard to young employees, revolves around values. It can be hard if values don't align. To avoid this situation, dive deep into this topic during the hiring process so you are well aware ahead of time.

Giving Young Employees Responsibility

Young employees want their work to matter and their voices to be heard. Once you get them through



onboarding and you're comfortable with their skills, give them a chance to prove themselves.

Improve Your Sales Team And Grow Your Business

It's no secret that sales can make or break any business. Without a strong sales plan and team in place, it's difficult to bring in any profit or move your products. If your business has struggled to reach its sales goals, you must reevaluate your sales process and make any necessary adjustments. Check out the

following three pieces of advice to help you get started.

Discover Your Company's Vision

Where do you want your business to be in five to 10 years? How will you get there? You need to figure this out and get your sales team to buy into your vision so they can help your business reach its goals.

Hire The Right Team

Evaluate your current team members and see if there's anyone who is not meeting expectations. Have a discussion and try to inspire them – but if there's no improvement, find a more suitable option.

Create A Pleasant Company Culture

Your team members will put forth their best effort if your business is somewhere they want to work. Create a culture where everyone is recognized, heard, and has the opportunity to grow, and you'll soon notice many benefits, including sales growth.

