IT² TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

Why Choose IT²?

Technology can work in one of two ways: It can give rise to a more profitable, efficient and successful organization, or it can exhaust and frustrate your team, result in downtime and be a big hassle. For this reason, countless companies rely on IT² for the security and support of the technology that powers their business. Our Team brings the C-level leadership, experience, skills and toolset to allow you to focus on your business. IT & Telecom is our business.

To learn more about how IT² can support your business, give us a call today at **937.428.5880** or e-mail **AskIT2@it2resource.com**, subject line: <u>learn more</u>.

Summer 2022

IT Squared Resource, Inc.
1201 Commerce Center Dr.
Franklin, OH 45005

IT Squared Resource, Inc.
Delivering Exceptional Results

Your Technology Managed Service & Security Resource since 1999.

<u>Our Philosophy:</u> TO ADD VALUE TO ALL THOSE WE SERVE. To our clients as a trusted advisor and resource delivering exceptional results. To our employees, through continuous growth, opportunity and flexibility. To our partners and community as active contributors and involved supporters.

Do I Need A Compliance And Cyber Security Plan?

We talk a lot about cyber security and how incorporating the right practices can help fully protect your company from cyber-attacks, but there's another term that's often referenced when discussing cyber security that's just as important: compliance. While it's incredibly important for businesses to focus on maintaining the highest cyber security standards, they also need to ensure protocol meets compliance standards.

In regard to cyber security, compliance means creating a process to help protect the confidentiality and accessibility of information that's stored, processed or transferred. There is not an overarching standard for compliance when it comes to this. Instead, there are different guidelines and requirements for every industry, so it's important to be aware of your company's needs. If you're not, you could be subject to fines and penalties

in addition to being at greater risk for cyber-attacks.

Though they're related, there are still some glaring differences between cyber security and compliance. Cyber security is practiced for the company's own sake instead of to satisfy the needs of a third party. It's also present to protect a business from the risk of constant threats and needs to be continually managed and updated. IT compliance, however, is completed to satisfy external requirements and is driven by what the business needs more than anything else. Unlike cyber security, compliance is finished when the third party is satisfied with your process.

Compliance and cyber security work best when they're aligned, so it's extremely important that your business has a plan for compliance and cyber security. On its own, compliance is incredibly important

Continued from pg.1

for various reasons. The first is probably the most obvious since you can be fined or penalized if you fail to comply with industry standards. Having the proper compliance program will prevent your company from being fined. Additionally, your compliance plan needs to include continuous monitoring and assessment of networks, devices and systems that your company uses in order to align with regulatory cyber security requirements. It also sets up an action plan if your business is ever breached, since you need to communicate news of the breach to any parties that could've been impacted.

Every business, regardless of size, is susceptible to data breaches. It's only with strong cyber security and IT compliance plans that you can hope to plug every hole hackers may look to exploit. Compliance is an important part of risk management,
and it's essential for the future success of any business.

A compliance plan alone is a great start, but having cyber security measures in place as well will help you be prepared if you're ever audited by a third party.

Whether you have teams or individuals who oversee security protocols, they all need to know the

> **"Compliance and cyber security work best when they're aligned, so it's incredibly important that your business has a plan for compliance and cyber security."**

requirements for cyber security compliance and exactly how protected the company is. If your company utilizes a firewall, which it absolutely should, your teams need to know exactly how protective that firewall is. They also need the evidence to back up their claims so they can prove the information they provide is accurate. Auditors want to see a handful of different documents, so make sure your team is prepared for any questions or requests.
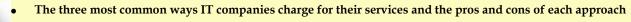
Once you have the basics of your plans taken care of, you can focus on accurately documenting each step. From meeting notes to the list of items that an auditor may need, your entire team needs to document anything they do or see regarding cyber security.

There is another, much easier option to ensure your business stays compliant and is protected from cyber-attacks. You can hire a managed IT services provider. With a managed IT provider, you will have a dedicated team that ensures your company's sensitive information is protected and all of your cyber security holes are filled. They'll also ensure your business stays compliant with any third-party regulating bodies in the process.

Though technology is ever-advancing, you shouldn't have to worry about cyber-attacks on a daily basis. With strong security protocol, or with the help of a trusted managed IT services provider, you can rest easy knowing your company's information is as secure as possible.

4 Benefits of Proactive Managed IT

Let's face it, your business technology running smoothly is VITAL to operational efficiency. Taking a proactive versus reactive approach to your technology management can help prevent most disasters and problems. Here are four great reasons why a proactive approach makes sense.

1. Less Downtime
2. More Productivity
3. More Predictability
4. Less Frustration

"An ounce of prevention is worth a pound of cure."
- Benjamin Franklin

8 Tips To Reach The Top Of Your Field

I've been consulting business leaders for well over 20 years now, and in that time, I've worked with some of the brightest minds across various industries. At ghSMART, we have helped many people reach the top of their field, and you may be wondering how we helped them. A professor taught me a tactic years ago that has helped me reach the top of my field. Now, I enjoy sharing this information with our clients.

Essentially, there are three roles in every profession – rainmakers, doers and trackers. The trackers are those who track other people's work. They play an important role but will rarely leave a lasting impact on their field. Most people are doers, since they do the work that is provided to them by someone else. They're also important, but they probably won't reach the top of the field. Then there are the rainmakers. These are the people who are proactive and go above and beyond to achieve results. Rainmakers always push to reach their goals and often reach the top of their field in the process.

Just being a rainmaker is not enough to leave an impact, though. If you follow these eight tips, you'll be well on your way toward success.

- Go to the best schools you can while achieving the highest grades possible and establish your technical skills. You don't necessarily have to attend the best school possible, but it does help.

- Spend 20% of your time building relationships. Try to spend a day each week learning what concerns are affecting customers in your industry and work toward solutions.

- Keep a list of your 50 most important relationships and rank them in order of importance.

- Don't do tasks or offer advice if it is outside of your area of expertise. If you don't deliver great results, you will push your clientele away.

- Improve your public speaking skills. On average, 95% of professionals are not confident when speaking in public, so the 5% who are confident usually shine on a regular basis.

- Learn how to hire and delegate. You can't do everything on your own, so you need to surround yourself with a team you can trust.

- Price yourself high, but don't get greedy. You know how much your work is worth and you know how much the competition charges. For desired results, clients don't mind paying a little extra for good work.

- Mentor others to become rainmakers. Your team will only grow stronger.

As a caring and courageous rainmaker, you will rise to the top of your field – while your peers who rest entirely on their technical skills will not.

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.*

■ The Future Of Leadership

The pandemic completely changed the way many people view work. If there's one thing for certain, it's that remote work will continue once the pandemic ends. If your business has switched over to a remote or hybrid environment, you may need to reevaluate your leaders to ensure their skills align with the new work environment. Strong remote leaders possess traits that are essential for success.

In fact, if you want your business to prosper in the future, you must ensure your leaders are good communicators since they might not be working in the same location as their employees. They also need to possess collaboration skills to ensure each facet of every

project is covered. Additionally, your leaders should be able to align their values with those of your staff and customers. Empathetic and understanding leaders are the future, and you need to have a leader who will look out for their team while also taking care of any customer needs.

If you interview a candidate who possesses these great characteristics, they should be a top contender for your leadership positions.

■ 4 Ways To Better Protect Your Personal Information

Most people keep their personal information as secure as possible. They don't post their passwords on social media or share Social Security numbers with untrustworthy sources. These practices seem obvious, but there are smaller things we can do to provide better protection. You'll find four of those tactics here.

Dangers Of Unsecured WiFi – Hackers can use this connection to download malware on your devices.

Password Manager – You shouldn't use the same password between multiple accounts. Utilizing a password manager will help you keep track of different passwords.

Breached Companies – When a company's security is compromised, all of its customers' personal information can be exposed. Avoid working with these companies until they've offered improved security.

Think Before Posting – Be careful about what you share on social media. Revealing too much personal information can leave you vulnerable to a cyber-attack.