June 2021

TechTidbit.com

brought to you by Tech Experts

Do You Have A Business IT Strategy?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

As a business owner, you already know the importance of strategy and planning.

Without it, you have no aim, no goals, and really, no direction.

While you probably spend a lot of time working on your strategy every month, quarter, or year, how much of that time is spent on your business's IT strategy?

If the answer is "not very much", it's time to change that.

Your business's IT is one of your most powerful, crucial tools in growing your business, keeping your team productive, and giving your customers a great impression of your company.

It makes sense that you have a plan for how:

- It will work for you now and in the future
- You will need it to grow with your business
- It can help take your business to the next level, faster

If you've never created an IT strategy before, or it's been a while, here are a few of the key elements you need to include…

Your business goals

Your IT infrastructure is there to work seamlessly alongside your business. It should complement everything you do, or plan to do, and make reaching your business goals a little easier.

Will you need additional tools to help your sales pipeline? Will it accommodate any future partnerships or acquisitions you plan to make? What about the different departments within your business; do their needs differ?

People and time considerations

Who in your business is responsible for delivering your IT strategy? Will it be created and driven in-house, or will you outsource it to external experts? Internally, who needs to be involved, whether that's liaising with external experts, or overseeing elements of your plan?

And how long do you want to take to make these changes? As with any business plan, you need to take both long and short-term goals into account. Do your plans rely on reaching a new level of turnover, or will they be based on your people adapting to the changes?

Your current infrastructure

How's it working for you right now? What would you change? What can't you manage without? It's a great idea to speak to people in different departments about this, because what works for one team may be totally unhelpful for another. You can tailor your infrastructure to work well for everyone and keep all of your departments feeling happy and motivated.

A technology roadmap

This step may be a little more difficult that the others, but it is really worthwhile.

Think about your whole IT architecture here. Your hardware, software, and any other tools that you'll want to utilize. If you need assistance here, a good IT support partner will be able to make recommendations on the best of everything to fit your needs.

Break your roadmap down into departments and include everything that each will need. This will allow you to see how everything fits together.

New metrics

While your infrastructure needs to be functional, it also has to be cost effective. What's the point in making all of these changes if it's not bringing a financial benefit to you?

Look at your current KPIs and forecast how these should improve with the changes you're making. Make sure they're realistic - change won't happen immediately.

Allow some time for your people to adapt to the new tools. You can not only measure performance, but your KPIs should also help you to identify issues before your end users are affected.

Your business's IT is one of your most powerful, crucial tools in growing your business, keeping your team productive, and giving your customers a great impression of your company.

Human Error: The Reason Why Cybercriminals Love Email

"It is important that you and your staff – the end users who do the clicking – still do your part and remain vigilant. Attackers send such a high percentage of attacks through email because of that human element. It works."

Mark Funchion is a network technician at Tech Experts.

Defending your data network against viruses, malware, ransomware, and other threats is a never-ending battle. Some attacks can be very sophisticated, using extremely complex techniques to try and exploit even the most secure networks. However, the vast majority of threats to your network – over 80% – are delivered through a very basic method: email.

Email is a common tool that many of us use constantly at work. Oftentimes, we use it without giving much thought to what we're doing or what we're opening.

It's normal for coworkers, clients, or new prospects to communicate and share files with us via email. The file can be a document, spreadsheet, PDF, etc., but the fact is that it's common and repetitive to us.

Like anything we do frequently, we can develop muscle memory. Think about the program guide on your TV – you probably navigate the menus without thinking. After an update or a provider switch, those menus can change and you might click the wrong buttons out of habit. No harm there.

But consider making the same mistake when a document is sent to you. The message arrives, and you briefly glance at who it's from. Maybe you recognize them, maybe you don't. You see an attachment, and you open it out of habit. The file is infected, and in less than a second, the damage has begun.

Like it or not, the people who are attacking your systems are running a business. Like any business, they are concerned with the return on their investment. Developing high-end, sophisticated attacks takes time and skill, which is expensive to do.

However, minimal skill is required to send an email – and that process

can be replicated to hundreds of thousands of users with a simple click of a button. And almost everyone working today might accidentally open an email with little to no thought.

For small businesses, having a firewall, an email filter, and anti-virus software is a must. We can help install and maintain that infrastructure. Unfortunately, the methods that attackers use to slip under your defenses are always changing.

It is important that you and your staff – the end users who do the clicking – still do your part and remain vigilant. Attackers send such a high percentage of attacks through email because of that human element. It works.

It's essential that you fight your muscle memory and treat email like physical mail. Look at what is being sent, who it is from, and if there is anything attached. If anything seems off, do not open it. Always err on the side of caution.

Also, if you do open something you shouldn't, it's better to notify your IT department or provider of a potential issue so they can look at what you were sent.

Often, I have observed someone get a suspicious message, open it, notice something is not right, then forward it to a co-worker for help. By sending the message on, there is a potential to increase the scope of damage done.

Those looking to do harm and steal information will always try the path of least resistance. All the security in the world can't stop an intruder if you open the door for them.

The same caution you take at home when an unexpected knock is heard should be how you handle all email. Consider the source and content, and if you have doubts, don't open the message. Delete it.

Malware will never be fully eradicated – cybercriminals will make sure of that – but you can do your part to make sure you do not infect your PC or business.

Think You're Covered For Ransomware? Best To Double Check

On May 9, European insurance giant AXA announced it will no longer provide support for ransom payments made to hackers.

While AXA appears to be the first insurer to deny ransom payments, the move could signal an impending shift in ransomware insurance coverage.

The AXA announcement comes as ransomware attacks prove an increasingly lucrative business model.

For instance, victims paid an estimated $350 million in ransom payments in 2020, over 300 percent more than in 2019. In recent high-profile cases, Colonial Pipeline paid attackers $4.4 million, and CNA Financial Corporation paid a whopping $40 million.

Meanwhile, cyber criminals continue to attack organizations across critical sectors. While the FBI and other security experts warn against paying ransoms, companies face devastating losses and even interruptions to critical care.

Cybersecurity best practices, combined with following recommended steps when an attack does occur, may provide the best protection.

Ransomware insurance coverage

Cyber insurance has become a hot topic as organizations scramble to protect themselves against losses resulting from cyber-attacks. In addition to ransom negotiations and payments, typical policies also cover legal costs, as well as costs for forensic analysis, data restoration and communications related to the breach.

However, even before the AXA announcement, many cyber insurance companies had begun to ask more from the companies they insure.

For instance, some insurers require policy holders to complete certain basic security steps. Others have begun to charge a coinsurance or limit payment to a percentage of the loss incurred.

To pay or not to pay

This evolution in cyber insurance reflects more than a move by insurers to manage their own risk. The FBI and other government agencies, as well as many cybersecurity experts, warn against paying ransoms. Researchers at cybersecurity provider Kaspersky explain that paying a ransom provides no guarantee that organizations will recover their data intact.

More importantly, paying the ransom encourages attackers to carry out more attacks. And some experts suggest that carrying cyber insurance actually makes organizations more attractive targets. Clearly, companies cannot depend on insurers to continue to shoulder the bulk of the cyber risk.

Best practices to protect against ransomware attacks

While cyber insurance still provides significant benefits, organizations must focus on cybersecurity best practices to defend against ransomware. Some of those best practices include:

Regular backups – Conduct regular data backups, including system images. Keep multiple copies of the backups, including a copy not connected to the network. And make sure to test the backups.

Keep systems and software up to date – Apply security updates to software, firmware and operating systems when they become available. This includes antivirus and other security solutions.

Develop and review an incident response plan – Having a detailed plan in place before a security incident occurs greatly increases the chance of a successful outcome.

Conduct regular cybersecurity training – While organizations can, and should, implement technology solutions, employees remain a key line of defense against cyber-attacks. Make sure users know how to recognize phishing attempts, share files safely and secure home offices.

Address third party risks – Look into the security practices of the vendors with which you do business to ensure they do not put your company at further risk.

Carefully regulate access controls – Give users only the access they need to the services and data necessary to perform their jobs. This proves even more important in a remote work environment.

"More importantly, paying the ransom encourages attackers to carry out more attacks. And some experts suggest that carrying cyber insurance actually makes organizations more attractive targets. Clearly, companies cannot depend on insurers to continue to shoulder the bulk of the cyber risk."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

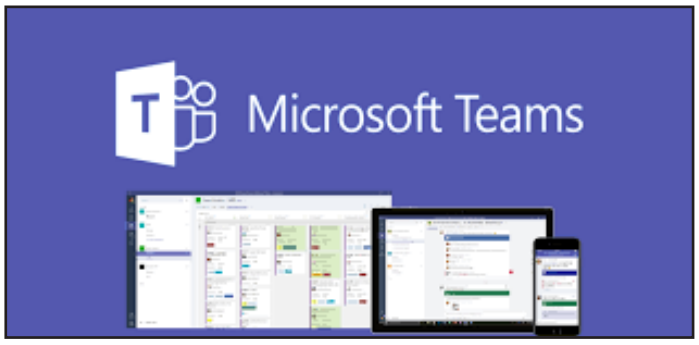
Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

A Love Letter To Microsoft Teams



We're massive fans of Microsoft Teams, and believe it has huge advantages for most of the businesses that we support.

We all know that successful businesses have great teamwork. And with everything that's happened over the last year, Teams has been the number one app to keep everyone working together.

Microsoft brought it out almost four years ago, in 2017. It was their answer to alternative platforms such as Slack that let you collaborate and communicate more effectively.

However, because Teams integrates with the rest of the Microsoft 365 platform, it has a real edge over Slack (the deep integration is AWESOME!).

If you're using Slack, it also means you can cut down on yet another monthly expense and take advantage of the enterprise level security features Teams has. Here are the three things we most love about it:

Project management

Teams allows you to focus in on just the project you're curently working on.

Information is partitioned into separate channels, so you can view messages, documents and meetings just related to a specific project.

That removes the hassle of wading through an inbox full of noise and clutter. And it's surprising how productive that kind of focus can make you.

Easy communication

No need just to rely on email anymore. With Teams, you can post messages in channels, again with the context of the project you're working on. It's easy to get the attention of any colleague by giving them a @Mention. You can also arrange one to one or group video calls easily.

The interface makes it easy

Microsoft has done a really good job here. It's intuitive and easy to use. It's so easy to find the information you are looking for and to move between different projects. Even if you've never used Teams before, the interface is so intuitive you'll pick it up right away.

If you're not using Microsoft Teams in your business and you'd like to learn more about how it can help you better communicate internally with your team (and externally with your clients), give us a call at (734) 457-5000, or email us at info@mytechexperts.com.

Did You Know… Alexa Doubles Up As A PA?

Alexa is great for many things. She always reminds us when it's time to take the dinner out of the oven. She gives an accurate weather forecast. And she definitely has a good grasp of our music tastes.

But did you know she can be even more useful than that? She can help with your work life and make you more productive.

If you give Alexa access to your contacts and calendar, she can make it faster to call colleagues, schedule meetings, and find someone's contact details and email address.

She can also give you reminders for appointments and meetings, which is perfect when your head is down and you're losing track of time.

You can also use a great service called Zapier to connect your Alexa to hundreds of other apps - some of which you may use for work already.

What are you waiting for?

Whether you're working from home or the office, making Alexa work harder for you will make your life easier.