April 2020

TechTidbit.com

brought to you by Tech Experts

Working From Home? Probably The "New Normal"

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

I hope that you and your family (and pets) are safe and sound and doing as well as can be expected. This is an extraordinary time for all of us, and the very embodiment of the ancient Chinese aphorism "may you live in interesting times." We surely do.

Our team is mixed between working in the office and working from home, and everyone is doing a great job. We initially saw a huge increase in our ticket volume as our client's teams prepared to work from home but that's tapered off in the last week to a pretty normal level of activity.

If you had to wait for help, please accept my personal apology for the inconvenience – while we have plans to handle client disasters, I never anticipated something as far-reaching as the current pandemic.

The "new normal"

If the politicians and experts are to be believed, many of the changes we've had to make to slow the spread of this virus are going to be around for quite a while, at least until we have an effective vaccine for COVID-19. From an IT perspective, that means more of your team will probably be working remotely. And that presents a new kind and new level of security exposure for your company.

The majority of our clients have their team members working from home by remoting into their desktops at the office, and that works fine. We have a great solution to enable this functionality (please email us at support@mytechexperts.com if you have team members who need to be set up for remote work).

However, if one of your team member's work location changes permanently to their home that solution no longer works. We'd need to deploy a VPN (virtual private network) to connect their home computer to your corporate network, which opens up a can of worms for sure.

Some of the considerations for permanent work from home team members include:

Securing the home computer – just like a computer at the office, a home computer being connected to your corporate network will need anti-virus, monitoring and management software and advanced threat protection.

Blacklisted applications – there are some software applications we don't install on office computers for security or data privacy reasons. When your team members are working from home, these same restrictions should be in place.

Threat management – on your corporate network we use tools to prevent team members from connecting to harmful or time-wasting sites. The security risk is the same regardless of the employee's location so we'd need to implement similar restrictions.

While we haven't worked through all of the details and requirements, our best guidance right now is that permanent work from home employees will need a computer dedicated to your business. The restrictions and security requirements necessary to protect your network would be very difficult to implement on a home computer.

By all means, please reach out if you have questions or would like to discuss transitioning some of your team members to permanently work from home.

Conferencing and web meetings

If you need audio conferencing to gather your team virtually, please let us know. We can assign you a dial-in conference line with unlimited users at no charge. Your team would simply dial your conference line, enter a four-digit PIN, and be connected. Email support@mytechexperts.com to have a dial-in conference line configured for your company.

Clients who use our 3cx phone system have web-conferencing

Continued on page 4

If the politicians and experts are to be believed, many of the changes we've had to make to slow the spread of this virus are going to be around for quite a while, at least until we have an effective vaccine for COVID-19. From an IT perspective, that means more of your team will probably be working remotely. And that presents a new kind and new level of security exposure for your company.

Designing A Comprehensive S

After years of being in the industry and watching the evolution of cyberattacks, we feel that there are 13 critical pieces to any cybersecurity plan that we, as your managed service provider, should implement. They are:

Two-factor/Multi-factor authentication

Two-factor authentication is probably the most widely misunderstood security solution, but a critical and effective part of every cybersecurity strategy.

Two-factor authentication is just how it sounds: two separate layers of security. The first is a typical username and password log-in with the addition of a secondary level that looks for something you know, something you have, or something on your body (e.g., fingerprint).

Here are some stats you should know that describe the critical need for two-factor authentication:

- 90% of passwords can be cracked in less than six hours.
- Two-thirds of people use the same password everywhere.
- Sophisticated cyberattackers have the power to test billions of passwords every second.

This sobering reality is why we require two-factor or multi-factor authentication for all of our employees and users of our system, and we highly recommend that you do too.

Password management

The main reason people use the same password everywhere is because it's impossible to keep track of hundreds of usernames and passwords across various devices and systems.

A secure password is a unique, hard-to-guess one, so it's understandable why users resort to the use of the same password for each site. This is why we have a password management program built into our procedures. The password manager program generates unique, complex passwords for each site or program then securely stores them in the management program.

When one of our staff needs credentials, they use the master password to open their database of passwords and obtain the login information they need, making it easy to "remember" a complex password and significantly reduce the risk of a breach.

Security risk assessment

A security risk assessment involves reviewing your technology and how you use it, followed by the implementation of security improvements and preventive measures.

The assessment should be performed at a minimum of one time per year, if not more. A full security assessment includes the following pieces:

Identification - When performing a security risk assessment, we first need to take inventory of all of your critical information technology equipment, then determine what sensitive data is created, stored, or transmitted through these devices and create a risk profile for each.

Assessment - This step takes identification to the next level. To complete the assessment step, we need to identify the security risks to each critical asset and determine the most effective and efficient way to allocate time and resources to mitigation.

Mitigation – This is where we solve problems. We have specifically defined a mitigation approach for each potential risk in our network and what security controls will be initiated in case of a breach.

Prevention - We have specific tools and processes to minimize the risk of threats against us and our network in order to help keep you safe.

Information security plan

There is a significant need to safeguard any information that is collected, transmitted, used, and stored within information systems, so the development of an information security plan is crucial. We take this very seriously. We have taken steps to document a plan and designed systems to secure our and our clients' sensitive business data.

A security program is essentially about risk management, including identifying, quantifying and mitigating risks to computers and data. There are some essential basic steps to risk management:

Identify the Assets - Beyond generating a list of all the hardware and software within the infrastructure, assets also include any data that is processed and stored on these devices.

Assign value - Every asset, including data, has a value and there are two approaches that can be taken to develop the value: qualitative and quantitative. "Quantitative" assigns a financial value to each asset and compares it to the cost of the counter-measure. "Qualitative" places the threats and security measures of the assets and sets a rank by use of a scoring system.

Identify risks and threats to each asset - Threats to the system go beyond malicious actors attempting to access your data and extend to any event that has the potential to harm the asset. Events like lightning strikes, tornados, hurricanes, floods, human error, or terrorist attacks should also be examined as potential risks.

Estimate potential loss and frequency of attack of those assets - This step depends on the location of the asset. For those operating in the Midwest, the risk of a hurricane causing damage is extremely low while the risk of a tornado would be high.

Recommend countermeasures or other remedial activities - By the end of the above steps, the items that need improvement should become fairly obvious. At this point, you can develop security policies and procedures.

Policies and procedures (internal & external) - A

ecurity Plan For Your Company

crucial part of an effective cybersecurity plan is the policies and procedures, both for internal assets and external assets. You can't have one without the other.

A general description can be thought of as this: a policy is the "rule" and a procedure is the "how." With this in mind, a policy would be to effectively secure corporate data with strong passwords. The procedure would be to use multi-factor authentication.

Cybersecurity insurance and data breach financial liability - CyberInsureOne defines cybersecurity insurance as "a product that is offered to individuals and businesses in order to protect them from the effects and consequences of online attacks."

Cybersecurity insurance can help your business recover in the event of a cyberattack, providing such services as public relations support and funds to draw against to cover any financial losses. It's something that your MSP should carry as well as your own business.

And just like business liability and auto liability insurance, it is paramount that your business (as well as your MSP) covers themselves with data breach financial liability insurance to cover any event that may be attributed to their activities causing a breach.

Data access management - Access management is determining who is and who isn't allowed access to certain assets and information, such as administrative accounts.

This is critical for your business as it enables control over who has access to your corporate data, especially during times of employee turnover. Other benefits include increased regulatory compliance, reduced operating costs, and reduced information security risks.

Security awareness training (with phishing training) - Phishing is the number one attack vector today with over 90,000 new attacks launched every month. If your provider is not actively participating in security and phishing awareness training, they will be unable to keep you up on the latest trends in how these malicious actors are attempting to gain access to your businesses data.

Data encryption - At its basic level, data encryption translates data into a different form, making it readable only by the starting and ending points and only with the appropriate password. Encryption is currently considered one of the most effective security measures in use as it is nearly impossible for an outside force to crack.

Next Gen antivirus and firewall - Antivirus is software designed to detect and neutralize any infection that does attempt to access the device and should be on every endpoint.

Many providers are marketing their software as "next generation," but true next generation antivirus includes features such as exploit techniques (blocking a process that is exploiting or using a typical method of bypassing a normal operation), application whitelisting (a process for validating and controlling everything a program is allowed to do), micro-virtualization (blocks direct execution of a process, essentially operating the program in its own virtual operating system), artificial intelligence (blocking or detecting viruses the same way as a human user could), and EDR/Forensics (using a large data set from endpoint logs, packets, and processes to find out what happened after the fact).

Next generation firewalls also include additional capabilities above the traditional firewall, including intrusion protection, deep packet inspection, SSL-Encrypted traffic termination, and sandboxing.

Business continuity plan – This is a process surrounding the development of a system to manage prevention and recovery from potential threats to a business. A solid business continuity plan includes the following:

- Policy, purpose, and scope
- Goals
- Assumptions
- Key roles responsibilities
- A business impact analysis
- Plans for risk mitigation
- Data and storage requirements that are offsite
- Business recovery strategies
- Alternate operating plans
- Evaluation of outside vendors' readiness
- Response and plan activation
- Communication plan
- Drills and practice sessions
- Regular re-evaluation of the current plan

Your MSP should be able to provide you with a copy of what is included in their plan and how it will affect your business if they do encounter a business continuity event, as well as their backup plan to maintain your critical business infrastructure.

Email security layers - In short, layers limit risk. Email security layers include tactics such as two-factor authentication and spam filters at the basic level (which give your employees time to evaluate a potential threat by removing the words "urgent" or "do right now" from internal subject lines).

As your managed service provider, we are dedicated to helping you maintain effective cybersecurity through these advanced tactics, as well as through a consultative, trusted advisor relationship. You are more than just a number to us and we will do everything in our power to help keep your business safe and running smoothly.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

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

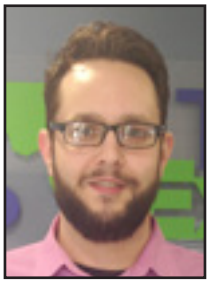
Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

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

Working Remotely: Changes Amid The Outbreak



Jason Cooley is Support Services Manager at Tech Experts.

It was early March when Microsoft decided to mandate its employees work remotely. Over a month since then, the world has not yet "bounced" back.

It's still looking like we haven't seen the worst of things to come. Many industries are closed altogether. Others are running with reduced staff. More people than we can count are out of work and seeking unemployment.

Unless your position called for travel, working remotely wasn't something many people would consider. However, there is no normal right now, and many people find themselves working from home for the first time.

Not all industries can manage it. There are front liners that have to work. Sure, you can likely do a video appointment with your doctor, but doctors are still seeing patients.

Food service, gas station, and grocery store employees are all critical and in-person jobs that are going to work on a daily basis.

Insurance companies and accounting offices? Their employees are probably very important to a lot of people right now. Their jobs are unlikely to be reliant on a central location.

A computer with web access can be enough to get you through in some situations, and other times, you need access to resources on your corporate network. Different people have different needs. In some cases, people are learning what they need and how to get it as they go.

As someone working in the IT industry, a fair portion of my normal work is done remotely. The only difference is my physical location. I can make calls, remotely assist clients, resolve issues, and carry on like a typical day at the office.

Many are not so lucky. The world doesn't stop running, and being under quarantine is creating some unique situations. People who have never worked from home suddenly are.

Non-critical business is on hold, but the justice system isn't on complete shutdown. Different cities and states are still working with its judges to get things done. There are certainly some instances of cities where they have the infrastructure in place to do telecourt appearances. There are others that are trying to put systems in place to be able to operate and hear cases.

While it is likely that some criminal cases will be put on hold, other court matters, like custody cases, can't always wait indefinitely.

With such uncertainty, some judges are doing Zoom meetings just to make sure that the world does keep moving around us.

Meeting apps like Zoom are being used more and more frequently as people attempt to find ways to host meetings. Skype, Discord, and just about anything else have been used in a pinch to try to make ends meet. Technology can be daunting, especially when new concepts like virtual meetings or VPNs are introduced.

People trying to use a webcam and mic or remote connection for the first time can get frustrated; it can be hard enough when we're not facing a global pandemic. Having a technology partner like Tech Experts can ease the transition (and your mind) in these trying times.

There are many things to be learned from this entire situation, though, and many things are sure to change. One thing is for sure: we will all likely be a little more comfortable with the idea of working from home in the future, should we need to.

Working From Home? Probably The "New Normal" - continued

licensing built in. You can read more about the system here: https://www.3cx.com/user-manual/webmeeting/

We're happy to assist with usage or configuration questions.

Increased threat from phishing emails and viruses

Sadly, cybercrooks love a crisis because it gives them a believable reason to contact you with a phishing scam. We've seen an alarming uptick in phishing emails and other virus delivery methods since a majority of our client's team has shifted to working from home. Be on high alert.

What can we do for you?

The lockdown and abrupt change to working from home is disorienting, and I think we're all still trying to get used to it. Please reach out if there is anything we can do for you or your business to make things easier.