7 Urgent Security Protections Every Business Should Have In Place Now

Cybercrime is so widespread that it's practically inevitable that your business – large OR small – will be attacked. However, a few small preventative measures CAN PREPARE YOU and minimize (or outright eliminate) any reputational damages, losses, litigation, embarrassment and costs.

InTech SOLUTIONS

Leia T. Shilobod
IT Princess of Power
CEO & President of InTech Solutions, Inc.

From the Desk of:
Leia Shilobod | President & CEO, InTech Solutions, Inc.

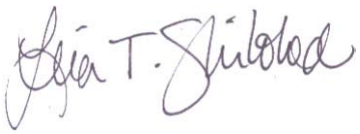
Dear Colleague,

If you are the decision maker in a business in the Greater Pittsburgh area that is currently looking to outsource some or all of the IT support for your manufacturing company, law firm, or CPA firm, this report contains important information that will be extremely valuable to you as you search for a competent firm you can trust.

My name is Leia Shilobod, CEO of InTech Solutions and author of "The 3 Indisputable Rules Every Manufacturer Must Know Before Purchasing Any IT Product Or Service. We've been providing IT services to businesses in the Greater Pittsburgh Area for over 11 years now. You may not have heard of us before, but I'm sure you're familiar with one or more of the other businesses who are clients of ours. A few of their comments are enclosed.

In the end, my purpose is to help you make the most informed decision possible about the security of your firm so what you worked so hard to build is protected.

Dedicated to serving you,



One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**

About The Author

Leia Shilobod is the CEO and President of InTech Solutions, Inc. She founded InTech in 2006 because she wanted to build a company that delivered fast and effective IT services to raving fan clients and provided an engaging and fun work environment to knowledgeable staff.

She believes in continuous improvement and is constantly reading business and technology best practices to deliver stellar service and solutions.

But she doesn't stop there.... She's interviewed dozens of manufacturers and industry CEO's, toured plants, talked to vendors, network with security professionals across the country.... anything that can help her learn more about businesses, security, and the specific IT needs of manufacturers.

This drive for learning prompted her to write her first book "The 3 Indisputable Rules Every Manufacturer Must Know Before Purchasing Any IT Product Or Service" and to develop EDP IT: the first IT Support and Administrative service EXCLUSIVELY for manufacturers (www.intechit.net/edpit).

Leia is a member of the FBI's Infragard, Board of Trustees of Westmoreland College, Chapter Advisor of Alpha Sigma Alpha at IUP, Sunday School Teacher, and also known as the IT Princess of Power.

When she's not saving the IT World, you'll find Leia consulting with clients, managing projects, or hosting one of many webinars and seminars.

Contact Leia directly at Leia@intechit.net or by calling the office at 724.235.8750.

When You Fall Victim To A Cyber-Attack Through No Fault Of Your Own, Will They Call You Stupid… Or Just Irresponsible?

It's EXTREMELY unfair, isn't it? Victims of all other crimes – burglary, rape, mugging, carjacking, theft – get sympathy from others. They are called "victims," and assistance and support comes flooding in.

But if your business is the victim of a cybercrime attack where client or patient data is compromised, you will NOT get such sympathy. You will be instantly labeled as stupid or irresponsible. You will be investigated and questioned about what you did to prevent this from happening – and if the answer is not adequate, you can be found liable, facing serious fines and lawsuits. You will be required by law to tell your clients and/or patients that YOU exposed their private records, financials and data to a criminal. Your competition will have a heyday over this, and clients will leave in droves once they discover you've been compromised. Your bank will NOT come to your rescue either, and unless you have a very specific type of crime insurance, any financial losses will not be covered.

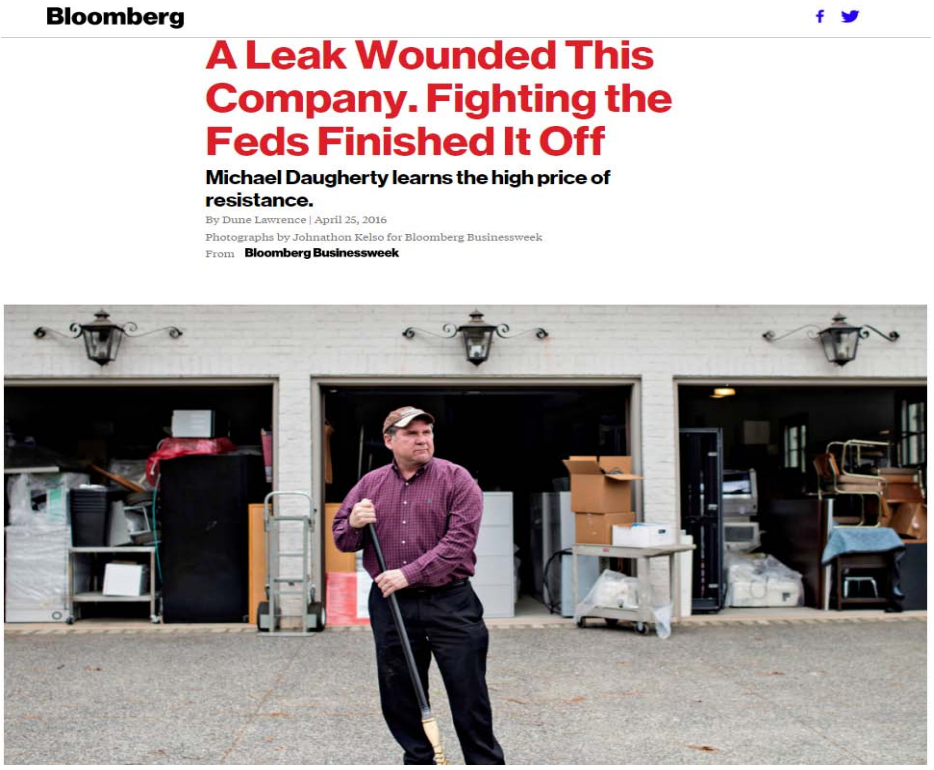
Here's The Ugly Truth:

You already know that cybercrime is a very real threat to you – but it's very possible that you're underestimating the potential damage, OR you are being ill-advised and underserved by the employees and/or vendors you hired to protect your business from these threats.

ONE cyber-attack…one slipup from even a smart, tenured employee clicking on the wrong e-mail…can open the door to ABSOLUTE FINANCIAL DEVASTATION, and undo everything you've worked so hard to achieve. **Take the story of Michael Daugherty, former CEO of LabMD**. His $4 million Atlanta-based company tested blood, urine and tissue samples for urologists – a business that was required to comply with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA.

He HAD an IT team in place that he **believed** was protecting them from a data breach – yet the manager of his billing department was able to download a file-sharing program to the company's network to listen to music, and unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network. This allowed an unscrupulous IT services company to hack in and gain access to the file and use it against them for extortion. When Daugherty refused to pay them for their "services," the company reported him to the Federal Trade Commission, who then came knocking. After filing some 5,000 pages of documents to Washington, he was told the information he had shared on the situation was "inadequate," and the FTC requested in-person testimony from the staff regarding the breach, and more details on what training manuals he had provided to his employees regarding cybersecurity, documentation on firewalls and penetration testing.

Long story short, his employees blamed HIM and left. Sales steeply declined as clients took their business elsewhere. His insurance providers refused to renew their policies. The emotional strain on him – not to mention the financial burden of having to pay attorneys – took its toll, and eventually he closed the doors to his business, jamming medical equipment into his garage where it remains today (image below).


Bloomberg

A Leak Wounded This Company. Fighting the Feds Finished It Off

Michael Daugherty learns the high price of resistance.

By Dune Lawrence | April 25, 2016

Photographs by Johnathon Kelso for Bloomberg Businessweek

From Bloomberg Businessweek

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? Think again. 160,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment - but make no mistake: small businesses are being compromised daily, and the smug ignorance of "that won't happen to me" is an absolute surefire way to leave yourself wide open to these attacks.

In fact, the National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last year** – and that number is growing rapidly as more businesses utilize cloud computing and mobile devices and store more information online.

You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these seven security measures in place.**

But I Have An IT Guy I Can Trust….

One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**

Many business owners are shocked when they get compromised because they BELIEVED their IT company or guy had it "handled." However, there is a virtual army of thousands of hackers and very sophisticated crime rings that work around the clock to overcome known protections – and you can't stop a brand-new threat that was invented yesterday with a security system that was designed six months to a year ago. It requires special expertise to stay on top of all of this, which is why many don't.

To that end, here's your quick, 7-step checklist. If YOUR company isn't actually implementing ALL of these protocols – OR if you don't know if you are – WHY NOT? What hasn't your current IT Company told you about all of this?

1. The #1 Security Threat To Any Business Is... YOU! Like it or not, almost all security breaches in business are due to an employee clicking, downloading or opening a file that's infected, either on a website or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (an e-mail cleverly designed to look like a legitimate e-mail from a website or vendor you trust) are still a very common occurrence – and spam filtering and antivirus cannot protect your network if an employee is clicking on and downloading the virus. That's why it's CRITICAL that you educate all of your employees in how to spot an infected e-mail or online scam. Cybercriminals are EXTREMELY clever and can dupe even sophisticated computer users. All it takes is one slipup, so constantly reminding and educating your employees is critical.

   On that same theme, the next precaution is implementing an Acceptable Use Policy. An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employees access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

   Having this type of policy is particularly important if your employees are using their own personal devices and home computers to access company e-mail and data. With so many applications in the cloud, an employee can access a critical app from any device with a browser, which exposes you considerably.

   If an employee is logging in to critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter YOUR network – which is why we don't recommend you allow employees to work remote or from home via their own personal devices.

Second, if that employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete al of that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?
Further, if the data in your organization is highly sensitive, such as patient records, credit card

One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**

information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

2. Require STRONG passwords and passcodes to lock mobile devices. Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

3. Keep Your Network and all devices Patched and Up-To-Date. New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office, Java, Adobe, and Chrome; therefore, it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

4. Have A Business-Class Image Backup BOTH on-Premise And In The Cloud. This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored 24/7; the worst time to test your backup is when you desperately need it to work!

5. Don't allow employees to download unauthorized software or files. The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is a known username and password. Employees are now even asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything.

   But this trend has DRASTICALLY increased the complexity of keeping a network – and your company data – secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility); the biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud application.

   So if you ARE going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

   But here's the rub: most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what

you'll need to do to protect your company. Our suggestion is that you allow employees to access work-related files, cloud applications and e-mail only via company-owned and monitored devices, and never allow employees to access these items on personal devices or public WiFi.

6. Don't Scrimp On A Good Firewall. A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company.

7. Protect Your Bank Account. Did you know your COMPANY'S bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account!) Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

   So here are three things you can do to protect your bank account. First, set up e-mail alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the DAY it happens can be stopped. If you discover it even 24 hours later, you may be out of luck. That's why it's critical that you monitor it daily and contact the bank IMMEDIATELY if you see any suspicious activity.

   Second, if you do online banking, dedicate ONE computer to that activity and never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc., with that PC. Remove all bloatware (free programs like QuickTime, Adobe, etc.) and make sure that machine is monitored and maintained behind a strong firewall with up-to-date antivirus software.

   And finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account. All of these things will greatly improve the security of your accounts.

Are You REALLY Willing To Be Complacent About This?

Look, I know all of this appears to be a giant distraction and cost that interferes with REAL work. You and I both realize that implementing proper security protocols won't win you the "employer of the year" award or deliver an ROI – in fact, we HOPE by doing OUR job, it never has to deliver one.

BUT if you foolishly choose to turn a blind eye and be arrogant, complacent or careless, cybercriminals WILL take advantage of you. You WILL pay the ransom...NOT YOUR FAILING IT COMPANY that was SUPPOSED TO PROTECT YOU. This tsunami of pain will land directly on YOUR desk to deal with, everyone pointing the blame at YOU. YOUR bank account. YOUR business. You will be faced with significant losses, costs and an emotional drain on you and your team as you deal with a breach.

One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**

Mark Twain Once Said, "Supposing Is Good, But KNOWING Is Better"

If you want to know for SURE that your current IT company (or IT person) is truly doing everything they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other threats, problems and costs that come with a data breach, then you need to call us for a FREE Security And Backup Audit.

At no cost or obligation, we'll send one of our security consultants and a senior, certified technician to your office to conduct a free Security And Backup Audit of your company's overall network health to review and validate as many as 29 different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?
- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).
- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?
- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines.
- Is your firewall and antivirus configured properly and up-to-date?
- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the over 100 businesses we've audited over the years.

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you

One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**

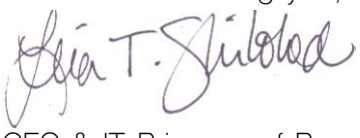
You Are Under No Obligation To Do Or Buy

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security And Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at 724.235.8750 or you can e-mail me personally at Leia@intechit.net.

Dedicated to serving you,



CEO & IT Princess of Power
InTech Solutions, Inc.
724.325.8750
www.AwesomeITGuys.com

Read On to Hear What Our Clients Have to Say

"Outclasses the competition with responsiveness to our 100+ Employees"

InTech has, in a short amount of time, greatly outclassed our prior IT provider. Leia and her team have shown a high level of responsiveness, organization, and pleasantness in dealing with our 100+ employees spread across the country (offices in PA & FL + 25% home office workers). They are capable of handling any problem, as evidenced by their recent successful troubleshooting for a 15-year-old ColdFusion app our company uses. I couldn't be more pleased with InTech and wholeheartedly recommend them for any business!

Jason Jason Kelley, Corporate System Administrator, Learning Sciences International

"Not only do we find a cost savings, but we find competence in all areas."

"As a mid-sized company it doesn't make sense to have in-house IT. We need to be cost-effective. With InTech, not only do we find that cost-savings, but we find competence in all areas. It is almost impossible to get that from just one in-house guy. Quality and accessibility is the key benefit from choosing InTech."

Lutz Heidrich, Plant Manager, Hennecke USA, Polymers Manufacturer

"They Blew Me Away With Their Knowledge of IT & Computer Networking!"

"I first met InTech back in 2007 when I joined a local networking group. They blew me away with their knowledge of IT & Computer Networking! I have worked with InTech since then, and they have done a great job each time! They are honest, dependable, and an asset to our business community. I would highly recommend them to anyone!"

Rita Violette, Owner, Business Partner, One Stop Business Marketing

"No more side-tracking from IT Nuisance – Now we can focus on our core business!"

Leia and the InTech team have provided first rate support, and more than that, they are a true partner. They have provided us an honest assessment of our IT infrastructure and enhanced our ability to focus on our core function as a business, rather than being side-tracked by IT "nuisances". I'd highly recommend Leia and her team to be IT support provider for any business, regardless of size.=

Randy Hutzler, Manager – Enterprise Solutions, Learning Sciences International, Educational Consulting

One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**

"You got our network problems resolved – fast!"

"I wanted to thank you again for your hard work in getting our networking resolved. You all did a great job. Not only that, your crew worked hard to not displace us during our work day."

Bill Utzman, *Vice President*, Morris Knowles & Associates, Engineering Service

"My Only Regret Was Not Making The Change Sooner."

"I was very concerned about the downtime we might experience in our email migration, and am both surprised and pleased with how smoothly everything went. I have a ton of emails, and was very concerned about losing them. The down time was minimal, and I really didn't miss a beat. The new email is working great, it is soooooooo much faster than the old email we had. We have probably been using our cheapest option in the past, and as you said, you get what you pay for. My only regret is not making the change sooner."

Maryann White-Helfferich, Owner, Kelly Sparber White PC, CPA Firm

"The Solutions They Recommend Help Me Do Business From Anywhere."

"InTech has proven to be a truly professional company in every sense of the word. They are committed to my satisfaction. The services provided are always done correct and on time. They follow up to make sure that we are happy and that they are no re-occurring problems. They give me continued advice and provide solutions for managing my information and helping me to do business from anywhere. I would highly recommend them to any one in need of computer services."

R. Tyler Courtney, RTC Financial Services, Securities/Employee Benefits / Corporate Lending

"They blew me away with their knowledge of IT & Computer Networking!"

"I first met InTech back in 2007 when I joined a local networking group. They blew me away with their knowledge of IT & Computer Networking! I have worked with InTech since then, and they have done a great job each time! They are honest, dependable, and an asset to our business community. I would highly recommend them to anyone!"

Rita Violette, Owner, Business Partner, One Stop Business Marketing

One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**

"The Only Thing They Could Do Better Is Move In Here!"

"We have worked with InTech for 8 years and we will continue to because of their reliability, knowledge, and flexibility. They have everything covered for us and we know we can always count on them to give us the best advice for our network. They only they could do better is move in here!"

Carmen Irwin, Purchasing, Uptegraff Manufacturing, Transformer Manufacturer

"We Saved Tens Of Thousands Of Dollars."

"We used to pay an in-house tech $70K-$80K a year. We wanted to lower our technology costs, but we still needed a go-to person who could deal with any issues. We put all of our trust in InTech, and they really did a great job. They helped us purchase a server and put in place the back-up we needed. They seemed to be one step ahead of the 'corporate' techs."

Diane Shar
Assistant Controller Hennecke, Inc.

"I'm So Happy We Decided to Go to the Cloud."

"I wanted to thank you guys for bringing us into the 21st century. Your company always does a bang up job, and your staff has been a huge help."

Cindy Bankosh
Independent Settlements, Inc.

"They Quickly Solved An Issue We Were Having With Our Email For 4 Years!"

"After meeting with InTech the first time we were knew they were the perfect fit for us. Since beginning our relationship with them, we have experienced far less problems. They even solved an issue with our email that we had been dealing with for 4 years! Employees no longer have to deal with disruptions from computer problems, and InTech's work has definitely improved the internal functioning of our business. They always treat our problems with a sense of urgency and importance."

Sharon Roup
Controller, MedTech Rehabilitation, Medical Rehab

One Northgate Square, Ste. 202 | Greensburg, PA 15601
724.235.8750 | **www.AwesomeITGuys.com**