5-Step System

To Make Sure Your Business Technology Runs Like A Ferrari Instead Of A Fiat

Provided as an educational service by:
Stefanie Groot, President
Windstar Technologies
451 James Madison Hwy. Suite 108, Culpeper, VA 22701
540-317-1200 | www.WindstarTech.com

5-Step System

To Make Sure Your Business Technology Runs Like A Ferrari Instead Of A Fiat

How many of you are tired of hearing bad news?

The world is full of bad news. Every day we hear stories about pandemics, inflation, recessions, wars, and cyberattacks. So I thought that maybe you could use some good news.

We've all been taught that bad news is popular and profitable, and we definitely hear a lot more bad news than good news every day. But, sometimes, good news can be even more useful and valuable.

The media loves to spread FUD: fear, uncertainty, and doubt. This is even a sales technique that many companies use to scare people into buying their product or services. But I want to do the opposite with this report today. Instead of making you feel fearful, uncertain, and doubtful, I'd like to help you feel confident, certain, and courageous.

A great example of this is called "*Some Good News*".

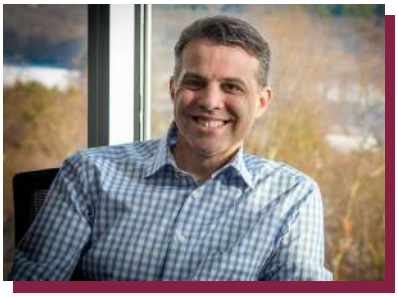
Some Good News was a YouTube series created and hosted by the actor **John Krasinski**, which premiered on March 29, 2020. John is best known for playing Jim on *The Office*. He funded and produced the show and filmed each episode remotely from his home in Brooklyn during the pandemic.

After eight episodes, and a live-streamed prom for high school seniors who were on lockdown, the show was sold to Viacom CBS.

Since the first season concluded, *Some Good News* has raised over $2 million for various charities through their *Some Good Merch* store. Donations have gone to Direct Relief, Boys & Girls Clubs of America, Trauma Free World, World Central Kitchen, the NAACP Legal Defense and Education Fund, Toys For Tots, and the Restaurant Employee Relief Fund. *Some Good News* turned into something good for John and something even better for a lot of charities.

So what is the good news when it comes to your small business and the technology you use every day?

Well, it's important to acknowledge a truth spoken by former FBI counter-terrorism and counterintelligence operative, **Eric O'Neill**.



> It's scary out there and small businesses are definitely the targets of an increasing number of cyberattacks. In fact, 43% of all cyberattacks are directed towards small businesses.

Some small business owners mistakenly believe that they're too small to get hacked. They think cybercriminals aren't interested in their companies. But that's not true.

As **Justin Weller**, with Blackpoint Cyber, a Managed Detection & Response Company, explains:

"You're not too small. You're just too small to be on the news."

That's bad news BUT there is some good news. . .

First, not all cyberattacks are malicious. In fact, some are hilarious.

For example, hackers regularly take over unsecured road construction signs in cities throughout the country to share ridiculous messages with drivers who are stuck in traffic.

In San Francisco, commuters were warned that Godzilla was running rampant in the city. Other hackers also use this same theme, their signs warned people to watch out for Zombies and dangerous Rogue Pandas on the rampage. Another sends out a cry for help from someone "trapped in a sign factory."

These silly and rude hacks aren't new. I did some research to find out about the first cyberattack in history… Can you guess when it happened? It's probably earlier than you think.

The first cyberattack actually occurred in 1903. That is almost 120 years ago and 40 years before the first electronic digital computer was even created.

Guglielmo Marconi was the inventor of the first wireless telegraph. He told the public that his wireless messages could be sent privately over great distances. Marconi claimed, "I can tune my instruments so that no other instrument can tap my messages." But when he attempted a demonstration at the Royal Institution in England, an unexpected source began beaming powerful wireless pulses into the theater.

It was spelling one word, over and over: "Rats." Then it got more personal, mocking Marconi: "There was a young fellow of Italy, who diddled the public quite prettily." And it wasn't over. Further rude language followed.

The demo continued, but the damage was done. If somebody could intrude on the wireless frequency in such a way, it was clearly nowhere near as secure as Marconi claimed. And it was likely that they could eavesdrop on supposed private messages too.

Four days later a gleeful letter confessing to the hack was printed by *The Times*.
Its author was Nevil Maskelyne, a 39-year-old British music hall magician. Maskelyne was interested in wireless technology, and in 1900, Maskelyne sent wireless messages between a ground station and a balloon 10 miles away. But his ambitions were frustrated by Marconi's broad patents, leaving him frustrated and angry. Maskelyne hacked Marconi's demonstration to fight back. AND that leads us to more good news . . .

Hacking isn't new, so we've had time to learn how to protect our technology systems. In other words, we are getting better at fighting back against hackers. For example, after the Colonial Pipeline ransomware attack, the FBI was able to recover $2 million in bitcoin from the hackers' accounts.

And the good guys are even becoming hackers. They are using cyberattacks to fight the bad guys. The British intelligence service, MI6, the same one that James Bond works for, took over a radical Muslim preacher's online magazine and replaced an article on how to manufacture pipe bombs, with a collection of...cupcake recipes.

Additionally, when US and Israeli coders unleashed a computer worm on Iranian nuclear facilities, they decided to upload AC/DC's 'Thunderstruck' to the main PA system. At random intervals, the iconic rock song would blast throughout their nuclear complex. Na na nana na nana na na...

And we're not done yet. Here is the best news of all...

Cyber security doesn't have to be complex and confusing...
Just treat your computer the same way you'd treat your dream car.

I'm serious. If you want to understand how to manage information technology, just follow the same principles you use to manage your vehicles. The evolution of automobiles and the automobile industry is very similar to the evolution of computers and the information technology industry.

Let's start with cars.

What is your dream car? I want you to imagine it.

I'm not talking about a nice car that you want and could probably afford in a couple of years. I'm talking about your dream car. One that is probably out of reach but that you would love to have if you won the lottery or if you sold your business for a premium price. Are you picturing it?

Okay. Now think about what you want that car to do for you and what you are going to do for that car.

The first thing we want is for our cars to be **safe & reliable**. We don't want them to break down, and we don't want to get in an accident.

There are more than seven million car accidents in the United States each year. And almost 50,000 people die in those collisions annually.

So cars come with an incredible number of safety features:

- Seat belts
- Anti-lock brakes
- Crash sensors
- Air bags
- Roll cages
- Safety glass
- Lane change warnings
- Tire pressure sensors
- Mirrors
- Brake lights
- Accident monitoring
- Adaptive cruise control will slow you down if you get too close to the car in front of you
- Your wipers will come on automatically if it starts to rain
- Your lights will come on automatically when it gets dark

If you think about it, most of the features of a car are actually safety features.

And even with all those safety features, you'd still buckle up and you'd still drive carefully so that nothing bad happens to your sweet new ride.

Like **Robin Robins**, the founder of TMT, says,

"Nobody believes they will be in a car wreck when they leave the house in the morning, but you still put your seatbelt on. You don't expect a life-threatening crash, but you still buckle up."

But what about **reliability**?

If your dream car breaks down, are you going to watch a YouTube video and try to fix it yourself? Are you going to go to AutoZone and pick up the cheapest replacement part you can find? Are you going to take classes to become a certified mechanic so you can take care of your dream car?

Probably not.

You're going to go to a certified mechanic who specializes in this particular type of car. You're going to get all the oil changes. You're going to check the tire pressure and rotate the tires and get them aligned. You're going to change the filters and the fluids on a regular basis.

If a warning light comes on, you're not going to ignore it. You're going to immediately schedule an appointment to get it checked out. You're going to constantly get it detailed and washed inside and out. You're going to make sure that nothing goes wrong with your dream car. Your spouse is definitely going to get jealous because you treat your car better than you treat them.

But you care about more than just safety and reliability. You want your car to run smoothly, but you also want to make sure that it doesn't get stolen.

You care about **security.**

In the United States, a car is stolen every 41 seconds. That means that 65 cars will be stolen while you read this report. Almost a million cars are stolen each year.

The worst cities for car theft are Bakersfield, California and Denver, Colorado. And the most commonly stolen vehicles are Honda Civics and Ford F-150 trucks.

So, if you want to protect your dream car, make sure it's not a Honda Civic or Ford F-150. And move out of Bakersfield and Denver. Make your new home in Harrisonburg, Virginia and State College, Pennsylvania. These are the two safest cities for vehicles in the United States.

But, if you want to keep your dream car away from thieves, you will also make sure you have every possible anti-theft device:

- Alarms
- GPS tracker
- Auto-locking doors
- Remote immobilizer
- You might even buy "The Club" to lock the steering wheel

When you park the car, you'll always:

- Roll up the windows
- Lock the doors
- Take the keys with you
- Set the alarm
- Hide valuable items inside the car
- At night you'd make sure to park in a well-lit area
- At home you park it in the garage and set your home alarm

And you'd never leave your car in a bad neighborhood. You're going to be vigilant, not complacent. You don't want anything to happen to your dream car.

If you're really serious about security, you could even get the bulletproof Mercedes-Benz GL550 by TAC (Texas Armoring Corporation).

As automotive journalist **Joe Santos** explains, good vehicle security has many layers.

"Ultimately, if you want to keep your car safe, there isn't any one solution that will keep a thief from stealing it. If a thief wants your car, they will find a way to get it. In that case, it could be better to add multiple layers of security (lock your car, car alarm, steering wheel lock, a GPS device, etc.) in order to keep your car sitting right where you parked it. A steering wheel lock could work in some situations, but it's far better when combined with other anti-theft devices."

But even with all of these safety and security features, you know that it's still possible that you might be in an accident. There are a lot of bad drivers on the road, and you can't control every variable. You also know that, if someone really wants to steal your car, they probably can.

If Vin Diesel and Ludacris from *The Fast and the Furious* come after your car, there's nothing you can do to stop them. So you're going to want to have really good **insurance.**

Insurance to replace your car if it's stolen. Insurance to repair your car if it's damaged in an accident.

But you know that your biggest financial risk is medical costs, not property damage. So you want insurance to protect you from the liability of hurting someone on the road. Collision insurance and liability insurance. The good stuff. Not some cheap policy from an unknown insurance company.

They'll pay for a tow truck if your car breaks down or you get a flat tire. They'll pay for a rental car while your car is getting repaired.

And then there's **compliance.**

You probably aren't thinking about this when you get your dream car. It's almost invisible. But it starts right away.

You can't even buy your dream car without paying tax, title, license, and registration fees. The law requires you to have car insurance as well.

There are thousands of local, state, and federal rules and regulations related to owning and driving your car:

- Speed limits
- Seat belt laws
- Traffic lights
- Emissions tests
- Annual state inspections

You have to pass a test and get a driver's license. You have to regularly renew that license by waiting for hours at the DMV. The list goes on and on forever.

If you ignore those laws, you have to pay big fines. Or you could even lose your dream car. If you get in too many accidents or get too many traffic tickets, then you might lose your insurance or it might become so expensive that you can't afford to drive your dream car anymore.

Compliance is something that we don't think about, but it's everywhere and it affects every aspect of our life on the roads and highways.

- Safety & Reliability	- Security	- Insurance	- Compliance

These **four layers** are crucial to owning, driving, and enjoying your dream car. And these same four elements are crucial to managing your business technology.

Remember . . .

Cyber security doesn't have to be complex and confusing...
Just treat your computer the same way you'd treat your dream car.

Safety & Reliability

You want your computers to run smoothly. You want your email system to be reliable. You don't want downtime on your servers. Just like with your car, you don't want your systems to crash.

So you hire a competent and trustworthy Managed Service Provider. Just like you would take your car to a certified mechanic.

Hiring a company to manage your IT can be a difficult decision. A nonprofit in Virginia was hesitant to invest in a backup system for their data. It just seemed too expensive and maybe unnecessary. But then the organization's executive director saw their friend's business get hacked and realized the importance of backing up their information. They worked with an MSP to create and put proper backups into place. Very soon after that, they lost a server to a power outage related to a severe storm. Because they had backups in place, they were able to quickly recover everything they lost.

Online and offline backup systems are crucial layers for ensuring the safety and reliability of your technology.

Another example of this is a CPA firm in Missouri. They had a vendor installing software on their system. The tech was new and was completing the installation for the first time. During the process, he accidentally eliminated thousands of records from their database. The tech was embarrassed and frustrated because this loss could have been very costly and time consuming to fix.

Fortunately, the company had invested in a backup system with their MSP. When they noticed the lost data, they were able to work together to quickly restore it via the backup systems.

But you want more than just safety and reliability. You want security.

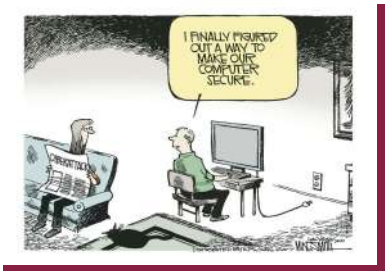
Because you can't guarantee your safety on the roads, even if you drive safely, when other people are driving recklessly.

As Fred Langa, tech editor and author of *Windows Secrets*, says

"Just as drivers who share the road must also share responsibility for safety, we all now share the same global network, and must regard computer security as a necessary social responsibility."

Security

You want your technology to be secure. You don't want to get hacked. You don't want to pay a ransom to regain access to your company's data. You don't want malware or viruses. You don't want your website to disappear. You don't want to lose your reputation because you revealed sensitive customer data.



There is a simple solution. Just shut everything off and disconnect it from the internet.

Dan Farmer, a computer security researcher, explains it this way...

"If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders."

But going off the grid isn't an option for your business. You need a safe and reliable system that you can operate securely.

So you hire a competent and trustworthy Managed Service Provider who also has experience and expertise in cyber security.

There's an interesting connection between car theft and cyberattacks.

I shared earlier that a car is stolen every 41 seconds. When I was researching the frequency of cyberattacks, I found that they occur at almost the exact same rate, every 39 seconds.

Cyber security advocate **Paul Herbka** makes a similar connection. He says that . . .

"Security in IT is like locking your car – it doesn't stop the bad guys, but if it's good enough they may move on to an easier target."

You don't need to make it impossible for hackers to breach your systems. You just need to make it as inconvenient as possible. And that isn't as hard as it might seem.

There are so many cyber security success stories, and we usually don't hear them in the barrage of bad news. So I wanted to share a couple with you.

As we saw in the story of the Virginia nonprofit, a good backup system is important for safety & reliability. But backups are also a crucial part of cyber security.

In 2019, the office manager for a chemical and ink manufacturer in Southern California called their MSP and explained that they couldn't access some of their files. After logging into their system and looking, it was clear that they had been hit with a ransomware attack. Within an hour, their MSP had them up and running on their backup server, fully functional, with no data loss. The best part is the MSP's security expert was able to do all this remotely from a hotel room in Vegas where they were attending a conference.

And this isn't an isolated incident. Success stories like this happen all the time. Every day, companies avoid disaster because they take security seriously and invest in systems that reduce the probability that they will be attacked or that attacks will be successful.

This is important. Companies that avoid disaster invest in systems. They don't just rely on a single system for protection. They have multiple systems. They have multiple layers of protection.

If they can't prevent an attack, they can still prevent damage from the attack.
And if damage occurs, they can help you recover whatever was lost.

James Scott advises the US Government on cyber warfare and cyber security. He argues that...

"There's no silver bullet solution with cyber security, a layered defense is the only viable defense."

So why are layers so important?

As **Doug Theis**, director of national strategy at Expedient, explains...

"A security system with several layers is difficult to hack. So, even if your data is targeted, getting through the many tiers of security will be a hassle. The simplest of programs, such as free online email accounts, have multi-layered security. Even if accessing your accounts takes a few extra steps, it is still worth the effort, certainly better than losing your data. Using a firewall, making sure your antivirus software is updated, running antivirus checks frequently and updating your programs regularly are all part of maintaining your personal data security."

Cyber security education and training for employees is another crucial layer.

For example, in Virginia, there was another small chemical manufacturer made up of mostly older employees in a rural part of the state. The company's owner was George, and he was 67.

George was smart enough to partner with an MSP and invest in cyber security, but he was skeptical. He didn't think he could really understand all the complicated technological concepts. In one training session, he actually shouted out, ***"I can't learn this. I'm a dinosaur!"***

But he did learn it.

One day he got an email from his company's health insurance provider. It looked suspicious, just like the emails from his MSP's cyber security training. So he called the insurance company and let them know that they might have been hacked. He also recommended that they work with his MSP to resolve the problem. The MSP researched the issue, changed passwords, turned on Multi-Factor Authentication, and resolved this issue, which was isolated to a single email account.

What George experienced is known as a phishing attack. The hacker sends a malicious link via email with the goal of infecting the receiver's computer system. Some estimates say that 90% of cyberattacks start with phishing.

If an old guy out in the country in the middle of Virginia can identify and stop a cyberattack at someone else's company, so can you. You just need to treat your computer like you'd treat your dream car. Focus on safety and reliability and invest in security. And get a good insurance policy.

Insurance

You're trying to do everything right, but you know that no one can completely eliminate the possibility of a cyberattack. Just like professional car thieves, professional hackers can access almost anything. Just like Vin Diesel deciding to steal your car, there are some criminals that you aren't going to stop.

You know that you can reduce the probability of an attack. You can make yourself less of a target. But you can't guarantee your company's safety.

As **Gene Spafford**, a computer science professor at Purdue, sarcastically explains,

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards."

But you can't run your business that way. **So you hire a competent and trustworthy Managed Service Provider, who also has experience and expertise in cyber security, and you work with them to choose a good cyber insurance policy.**

Smart business owners understand the importance of insurance. Currently, 32% of companies have purchased cyber liability coverage.

As **Rusty Goodwin** from The Mid-State Group explains...

"A mature risk posture is achieved with security, insurance, and compliance."

All three layers are crucial. You want multiple layers of security, but you also need other layers of protection in addition to security. You also need insurance and compliance.

So how can cyber insurance help you? Let's look at an example from Texas.

A local pizza restaurant had a disgruntled employee. Can you relate? How many of us have had unhappy employees over the years?

The employee used access to the company's email system to create a new fake employee with their outside payroll service provider. Then they authorized a very large check to be deposited into their account. However, the payroll provider had procedures in place to prevent this exact type of attack.

When a new employee was added to the system, the first check wouldn't be directly deposited into the employee's account. A paper check would be created, reviewed, and then mailed. During the review process, the fake account was discovered, and the payment was never sent.

Dr. Larry Ponemon found that this type of internal attack is becoming even more common.

"We discovered in our research that insider threats are not viewed as seriously as external threats, like a cyberattack. But when companies had an insider threat, in general, they were much more costly than external incidents. This was largely because the insider that is smart has the skills to hide the crime, for months, for years, sometimes forever."

But that's not the end of the story.

When the pizza place found out about the hack, they sued their payroll provider for mismanagement. In order to defend themselves from the lawsuit, the payroll company paid almost $50,000 for a forensic audit to demonstrate that they had done nothing wrong, had followed proper procedures, and had avoided a potential loss for the pizza restaurant. The audit also revealed that the pizza restaurant had been negligent and had insufficient cyber security processes that allowed the employee to access the payroll system.

The cost of the audit was paid for by the payroll company's insurance provider. This process was important to protect the company's reputation. If customers believed that the payroll company was unreliable, then they wouldn't be able to continue to build their business and they would rapidly lose their existing customers.

And this is not just about protecting your reputation with customers. Protecting your reputation with investors or potential buyers is also important.

Malcolm Marshall, Global Head of Cyber Security at KPMG, warns that...

"Investors see data breaches as a threat to a company's material value and feel discouraged in investing in a business that has had its sensitive information compromised."

Compliance

You know that the only way to get affordable insurance coverage is to create, audit, and enforce cyber security processes and procedures. You also know that your insurance might not pay your claim unless you can demonstrate that you were following your written policies and procedures.

But UK Information Commissioner **Elizabeth Denham** worries that ...

"When it comes to data protection, small businesses tend to be less well prepared. They have less to invest in getting it right. They don't have compliance teams or data protection officers. But small organizations often process a lot of personal data, and the reputation and liability risks are just as real."

You understand these risks, **so you hire a competent and trustworthy Managed Service Provider who also has experience and expertise in cyber security. You work with them to choose a good cyber insurance policy and then you work together to train your employees and monitor compliance.**

The last example about the pizza restaurant and the payroll provider illustrated the connection between insurance and compliance. Both layers are crucial. But compliance is also important on its own, regardless of insurance. In fact, it might even keep you from needing to use your insurance.

An internal IT employee for a rural hospital shut off Multi-Factor Authentication for the CEO's email during a software installation. There is nothing inherently wrong with this, but, unfortunately, they forgot to turn it back on when they were done. Shortly after this, the CEO's email got hacked. The hacker created a fake invoice and sent it to accounts payable using the CEO's email account. However, the hospital has an internal process that requires invoices to be sent to accounts payable with a copy to the CFO. The hacker couldn't have known this and so they didn't copy the CFO on their invoice email. This mistake allowed the hospital to catch the fraud and the invoice was never paid.

All of this was discovered by their MSP, who then went in and reset the compromised accounts and reactivated Multi-Factor Authentication.

Similarly, an electrical parts company signed up for cyber security services after experiencing a scare.

While setting up the new security system, the MSP discovered a router that needed to be patched. The internal IT employee kept offering to do it, but never actually did. Fortunately, the MSP's cyber security services included a SOC, Security Operations Center, which does constant monitoring of the company's systems. The SOC noticed an active cyberattack and shut down the power to the router, which stopped the attack. They then completed the necessary patch, installed relevant updates, and verified that the attack hadn't harmed any of the company's assets.

Compliance is important and is becoming even more important.

Michael Vatis, former director of the FBI cyber crime protection program, believes that

"In the very near future, cyber security exercises are going to be absolutely expected of all companies by regulators."

Robert Herjavec from *Shark Tank* agrees, predicting that ...

"America should get ready. Cyber security regulations will soon be coming to the United States — and that's actually a good thing... I firmly believe that the US will pass similar regulations (like GDPR in Europe) over the next two years."

Schedule a **FREE Cyber Security Risk Analysis** at:
www.WindstarTech.com/discoverycall
Or call us at: 540-317-1200

- Safety & Reliability	- Security	- Insurance	- Compliance

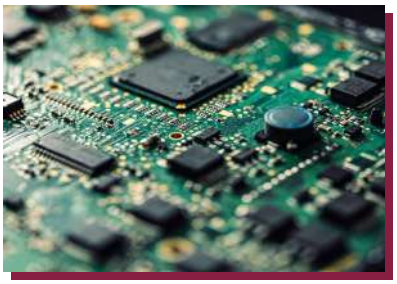
Four crucial layers.

It doesn't have to be confusing or overwhelming.

It can seem complex but it's just four simple steps.
You just treat your computer the same way you'd treat your dream car.

And now it's time to take this analogy a little farther. Because cars are actually turning into computers. And cars and businesses are both becoming more automated. Understanding these two new realities can help you prepare for the future of your business and your industry. . .

First, you don't have to treat your computers LIKE a car anymore because cars have essentially become mobile computers.



For example, a car mechanic isn't usually called a mechanic anymore. They're called a service technician. They're a tech, just like the person who fixes your computers. They aren't up to their elbows in grease and oil most of the time. They use digital diagnostic tools that tell them what is wrong with the car and recommend the proper repairs. Very often, that repair is related to microchips and electronics, not the mechanical parts of the car.

This transition has happened slowly. But you can see it clearly in the microchip shortage that began during the pandemic. A shortage of chips led to a shortage of cars.

Additionally, think about your car key. It's probably not a metal key that you turn in a lock. It's a key fob with remote start. Your key is a mini-computer. In fact, I recently drove a rental car with a key that limited both the vehicle's speed and the audio system's volume.

Similarly, computers run on electricity and now many cars run on electricity as well.

Because cars are becoming computers, it won't be too long until car thieves will be hackers. It's not Vin Diesel from *The Fast and the Furious* that you'll have to worry about. It's Sheldon Cooper from *Big Bang Theory*.

Teslas are the best example of a car becoming a computer. They also take automation to another level.

Schedule a **FREE Cyber Security Risk Analysis** at:
www.WindstarTech.com/discoverycall
Or call us at: 540-317-1200

Teslas don't have a model year like traditional cars. They can be updated regularly and automatically overnight while charging in the garage. Just like your phone can add new features with updated software, a Tesla that was built in 2019 can add new features that were developed in 2022. Tesla is the most computerized car and the most automated car, with a fully autonomous feature coming very soon.

And that takes us to the last similarity between cars, computers, and businesses.

Automation is becoming essential for both businesses and vehicles, and that automation is driven by computers and technology.

For example, most of the safety features that we discussed earlier are automated. They protect drivers from their own mistakes.

They also help drivers accomplish more than they could ever do on their own so they can focus on driving safely:

- Anti-lock brakes engage and disengage very quickly and automatically
- Crash sensors automatically detect potential accidents
- Air bags automatically deploy during a crash
- Lane change warnings automatically detect other vehicles around the car
- Tire pressure sensors automatically provide warnings
- Brake lights automatically come on when the brake pedal is pressed
- Accident monitoring automatically recognizes when the vehicle crashes
- Adaptive cruise control automatically adjusts the speed of the vehicle
- Windshield wipers come on automatically if it starts to rain
- Headlights come on automatically when it gets dark or when the wipers come on

Think about an automatic transmission. If you've ever driven a manual transmission (stick shift), then you don't have to imagine what it is like to do all of the shifting yourself. Power steering is another great example. It doesn't steer for you, but it makes the steering much easier.

Your car is even built by robots and designed on computer-aided software. You can make a service appointment for your car online. You can buy your car online using an app. Scheduling the car's delivery is also automated. And it won't be long until a Tesla will be able to deliver itself.

There are so many examples of this for small businesses as well:

- Automated ordering
- Automated email notifications
- Automated tracking
- Automated updates
- Automated delivery confirmations
- Automated calendar notifications

Chatbots can handle routine customer inquiries and search databases to provide common responses to common questions. Efficiency, reliability, and availability are all advantages of automation for small businesses.

Cyber security software is a form of automation, and the beauty of automation is that it is always on. Always working. Always protecting. It never sleeps and never goes home.

For example, an electrical company was looking for new employees. Because of this, their human resources department was receiving a lot of resumes. One of these resumes included an infected link to ransomware. An employee opened the infected link, but the ransomware was blocked by antivirus software and kept it from infecting the company's servers. The employee's email was damaged but was restored from the backup.

Then the same employee opened another infected link in the same way that same week. The antivirus protected the company again, and their email was restored from backup. Then the same employee did the same thing again for the third time in the same week. And the antivirus protected the company for the third time in the same week. Automatically.

It's common to worry that technology will replace people. However, technology doesn't just replace people. It also assists them. This is important because when it comes to cyber security, people are your biggest asset AND your biggest liability.

Bob was the owner of a farm equipment company in the Midwest that had about 100 employees. His MSP was getting alerts that someone inside of the company was trying to breach the firewall by clicking on a link to a malicious website. The firewall prevented the employee from going to the hacker's website, but then the employee tried again on a different computer. They were stopped again by the firewall. And then they tried again on a different computer. And they were stopped again.

At this point, the MSP called Bob to let him know that one of his employees was trying really hard to circumvent the company's cyber security processes. That is when Bob sheepishly told them that he was the one trying to click on the link. He thought the link would allow him to order a special part that he needed for a customer. When the link didn't work on the first computer, he tried it on a different computer. When it didn't work on that computer, he went to another one. If it wasn't for the firewall, the owner of the company would have helped hackers get inside his own computer system.

This illustrates the importance of proper training and having the right tools installed on your systems. Both are crucial. It's not just one or the other. Because employees can also be the last line of defense when hackers do actually breach your system.

Eric O'Neill tells the story of an attempted hack of a water treatment plant in Florida.

An employee at the plant noticed the cursor on their computer moving around on its own. Then he watched while the hacker increased the level of sodium hydroxide in the water supply to 100 times higher than normal. Sodium hydroxide is the main ingredient in liquid drain cleaners. It is used to control acidity and remove metals from drinking water in treatment plants. Ingesting too much of it can cause burns, vomiting, severe pain and bleeding.

After the hacker exited the computer, the operator immediately reduced the sodium hydroxide back to its normal level and then notified his supervisor.

Even if it hadn't been quickly reversed, the system has safeguards and the water would have been checked before it was released, so the public was never at risk.

This is a great illustration of the importance of employee training and compliance as well.

Like power steering or automatic transmission, automation doesn't always eliminate the need for people. It just gives them better tools.

For example, a $20 million marketing company in upstate New York worked with companies that required compliance, but they were unable to verify their compliance internally. Additionally, a vulnerability scan showed them that they had major weaknesses in their cyber security so they hired an MSP to help them increase both their security and compliance.

Part of their new cyber security system was a SOC, Security Operations Center. Within the first three days, the SOC team responded to more than 100 alerts on the CFO's machine. The SOC cleaned up the existing issues and since then has stopped 18 new attacks, including ransomware, on the company's systems.

This example illustrates the importance of security and compliance. But maybe more importantly, it demonstrates the value of people and technology working together.

It isn't one or the other. Both are crucial.

For example, in July of 2021, a healthcare provider with over 100 employees had their email system compromised. Their MSP detected the breach very quickly and resolved the problem in a few hours. They also prevented the hackers from accessing sensitive data.

Quick detection and quick recovery are crucial.

As **Ted Schlein**, the CEO of Fortify Software, explains,

"Most people are starting to realize that there are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it."

An **MSP owner** in California says that it is very common for companies to be unaware that their systems have been compromised.

"When we onboard new clients and install our tools, we find a myriad of things our new clients never knew about. Our security tools have detected hacker footholds on workstations, vulnerabilities the previous MSP never patched and recently, a new client had an employee who had installed a remote access software on their workstation to get tech support from a 'friend' and the owner had no idea about it."

Schlein goes on to suggest that ...

"Prevention is not sufficient and you're going to have to invest in detection because you're going to want to know what system has been breached as fast as humanly possible so that you can contain and remediate."

Research supports this. Companies that can detect a breach in 30 days or less can reduce potential losses by more than one million dollars.

One way to ensure both quick detection and response is with an MDR (Managed Detection and Response).

A small city government in Massachusetts had recently hired an MSP who implemented cyber security systems and training. Unfortunately, an employee still forwarded a malicious link which then initiated a ransomware attack.

The attack was noticed over the weekend by technicians with the MDR and they fought back and forth with the Russians until Monday, when they finally won the battle and saved the city millions of dollars in ransom.

If automation is becoming integral to running a business effectively, then managed service providers aren't just service providers anymore. They are an indispensable partner as you try to grow and manage your increasingly automated and technological business.

Kevin O'Leary, also known as "Mr. Wonderful" from *Shark Tank*, argues that technology is THE link between the business and the customer. This means that making sure your technology is safe, reliable, secured, insured, and compliant is also becoming more and more important. It is absolutely essential.

Just like cars are becoming computers, your business is no longer separate from technology, your business IS your technology.

- Safety & Reliability **- Security** **- Insurance** **- Compliance**

Four crucial layers.

It doesn't have to be confusing or overwhelming.

It can seem complex but it's just four simple steps.
You just treat your computer the same way you'd treat your dream car.

Partner with a competent and trustworthy Managed Service Provider who also has experience and expertise in cyber security. They can help train your employees and monitor compliance. Work with them to choose a good cyber insurance policy.

Would You Like To Set Up A Free Call With Us?

If you have any questions about what you read today, we'd like to answer them. On this call we can discuss your unique situation, any concerns you have and of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our **FREE Cyber Security Risk Analysis**.

This Analysis can be conducted 100% remotely with or without your current IT company or department knowing (we can give you the full details on our initial consultation call).

Visit:
www.WindstarTech.com/discoverycall
Or call us at: **540-317-1200**

See What Other Business Owners Are Saying:

Consistency, Value And Trust

Windstar takes their customer's experience seriously. The Windstar leadership does an excellent job of reviewing the company's overall technology needs and offers an array of services to support them. Their judgement on these needs has been very valuable to our organization. Over our long relationship our needs have fluctuated, but Windstar has been there as a partner to help identify solutions that address them.

System monitoring is a critical part of a technology solution. It is always best to be proactive in protecting data and systems from loss or severe damage. Trying to recover from an incident is more expensive and stressful than paying for service up front that will protect against them.

Windstar does not always have the lowest price available but the adage "you get what you pay for" comes to mind. We are confident in the superior level of service that Windstar has provided us over the years. Windstar does not oversell services, they offer what they think is best for the company. They have consistently delivered on their promised services.

– DS, IT Director

Our IT Staff Can Be More Productive

The single biggest benefit of doing partnering with Windstar Technologies is the call center and troubleshooting capability at the Help Desk. Windstar's commitment to documenting and developing processes continuously improves day to day support. All of this allows our limited IT staff to be more productive in our respective roles. If you aren't sure if you need additional IT support, I recommend starting small; quickly you will realize the benefits and find just the right balance for your team and your new IT partner. Our relationship is excellent!

– GM, IT Manager

Never Pay The Ransom

Our Dental office had an experience with ransomware infecting our software dental program which caused all our files to be lost. With the Data Back-up Solution Windstar had put in place they were able to recover our entire program and we were back up and running in less than a day.

– DR, Office Manager

See What Other Business Owners Are Saying:

I Now Have Peace Of Mind

Since we started working with Windstar Technologies, I now have peace of mind! I can reach out to Windstar whenever there is a tech issue, or when I want to discuss implementing a new solution. The responsiveness of the help desk is better than other IT firms we have worked with. I would recommend Windstar to other businesses looking for IT services.

– DS, Owner

Our Company Is Secure, Productive, And Growing

A lot of businesses struggled to stay connected during the Covid-19 pandemic. We didn't.

What set the pace for us was our relationship with Windstar Technologies. The team at Windstar prepared us with Microsoft Teams, and **our staff stayed connected** no matter where we worked. At our homes, in the office— Windstar taught us how to use all the options available with Teams. Now, our staff has more flexibility than ever before.

Everyone at the Windstar team is on top of new security and tech developments; that's been our experience. They take the time to know our organization inside and out. When Windstar shows us new products or services, we trust they will make sense for us. They aren't just knowledgeable; they're also responsive. It's an **unbeatable combination** that means we can count on them anytime.

Windstar is a terrific team that kept our business interconnected during a difficult time and keeps us on track with the latest security trends. Thanks to Windstar, we're confident **our company is secure, productive, and growing.**

– DH, MSW, LCSW, ACSW

We Have A Knowledgeable Team To Rely On

Several weeks ago, I was devastated to find that I had lost all my work emails. The friendly and patient staff at Windstar retrieved them quickly and got me back in business! Not only that, but they helped us get our QuickBooks and other files backed up consistently. Windstar set us up with Microsoft 365 and now I trust that everything is recoverable if needed.

As a Church, we previously relied on volunteers to help with our IT. Now that we have established a working relationship with Windstar Technologies, it is a blessing to know that we have a receptive and knowledgeable team to rely on at a moment's notice who address our concerns and are responsive to any issues that arise during our workday. Our relationship with Windstar is beneficial to our staff and the entire congregation; we couldn't be more grateful!

– BJ, Business Manager

To Schedule A

FREE
Cyber Security Risk Analysis

Visit:
www.WindstarTech.com/discoverycall
Or call us at: 540-317-1200