What Every Dealership Owner or Manager Must Know About Protecting And Preserving Their Critical Data And Computer Systems

If You Depend On Your Computer Network To Run Your Dealership, This Is One Report You DON'T Want To Overlook!

This report will outline in plain, non-technical English common mistakes that many dealerships make with their computer network that cost them thousands in lost sales, productivity, and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration of these oversights.

You'll Discover:

- The single most expensive mistake most dealership owners and managers make when it comes to protecting their company data.
- The universal misconception owners and managers have about their computer networks, and how it can end up costing between $9,000 to as much as $60,000 in damages.
- 6 critical security measures every dealership should have in place.
- How to greatly reduce – or even completely eliminate – frustrating crashes, slow performance, and other annoying computer problems.
- How to avoid expensive computer repair bills and get all the computer support you need for a low, fixed monthly rate.

From the Desk of: Timothy D. Ricketts
President
T. Daniels Consulting

Dear Colleague,

Have you ever lost an hour of work on your computer?

Now imagine if you lost days or weeks of work – or imagine losing your client database, financial records, and all of the work files your dealership has ever produced or compiled.

Imagine what would happen if your network went down for days, where you could not access service records or financial information. How frustrating would that be?

Or, what if a major storm, flood, or fire destroyed your dealership and all of your files? Or if a virus wiped out or ransomware encrypted your server…do you have an emergency recovery plan in place that you feel confident in?

How quickly do you think you could recover, if at all?

Many dealership owners and managers tend to ignore or forget about taking steps to secure their company's network from these types of catastrophes until disaster strikes. By then it is too late, and the damage is done.

But That Could Never Happen To Me!

(And Other Lies Dealership Owners And Managers Like To Believe About Their Businesses…)

After working with businesses, including many dealerships, across the country, we found that 6 out of 10 them will experience some type of major network or technology disaster that will end up costing them between $9,000 and $60,000 in repairs and restoration costs *on average*.

That does not even include lost productivity, sales, and customer goodwill that can be damaged when a dealership cannot operate or fulfill on its promises due to technical problems.

While it may be difficult to determine the actual financial impact computer problems have on your dealership, you cannot deny the fact that they do have a negative effect. If you have ever had your dealership grind to a screeching halt because your server crashed, you must have some idea of the frustration and financial loss to your business even if you have not put a pencil to figuring out the exact cost.

Most Computer Problems Are Hidden And Strike Without Warning, And At The Most Inconvenient Times

Hardware failure, viruses, ransomware, and other problems usually are not detectable until they strike by causing a server to go down, data to be lost, or some other catastrophe. Viruses and spyware are particularly sneaky because they are designed to hide themselves while they do their damage. For example, spyware can secretly transmit information about you and your company to an outsider without being visible to you.

Even if your network was recently audited by a computer consultant, viruses, spyware, and hackers are constantly attacking your network (that is why we constantly monitor our clients' networks because you never know when a new virus is going to strike).

Unfortunately, most computer consultants only offer "break-fix" services. That basically means when something breaks or stops working, they come in and fix it. While this may seem like a good setup for you, it actually leaves you wide open to a number of threats, problems, and other disasters because it is *reactive* rather than *proactive* maintenance.

Take a look at these statistics:

- Companies experience an average of 501 hours of network downtime every year, and the overall downtime costs an average of 3.6% of annual revenue. *(Source: The Costs of Enterprise Downtime, Infonetics Research)*

- 93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. *(Source: National Archives & Records Administration in Washington.)*

- 20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. *(Source: Richmond House Group)*

- Nearly 72% of small and mid-sized businesses, nonprofits and local government entities experience cyber-attacks and half do not know how to protect their companies. (Source: Ponemon Institute's 2019 State of Cybersecurity in Small and Medium Size Businesses.)

- Of those companies participating in ITIC's latest 2020 Global Server Hardware, Server OS Reliability Survey: 98% said each hour of downtime would cost their companies up to $100,000, 86% said each hour would cost $300,00 or more, and 34% said it would cost their companies more than $1million per hour. *(Source: Cost of Downtime Survey Results, 2020.)*

What These Failures Are REALLY Costing Your Dealership

Even if you do not factor in the soft costs of lost productivity, there is a hard cost of repairing and restoring your network. Most major network repairs will require a minimum of four to eight hours on average to get the network back up and running. Plus, most consultants cannot get on-site to resolve the problem for 24 to 48 hours. That means your network could be down for one to two days.

Since the average computer consultant charges over $100 per hour plus a trip fee and a surcharge if it is an emergency, the average cost of these repairs is $600 to $1,000; and that does not even include any software or hardware costs that may also be required. Over a year, this results in $1,800 to $3,000 in costs without even considering hardware and software costs, or other soft costs of lost sales and work hours. Of course, those numbers quickly multiply with larger, more complex networks.

What is most exasperating about this situation is that 100% of these disasters and restoration costs could have been completely avoided or greatly mitigated easily and inexpensively with a little planning and proactive maintenance.

Why Dealerships Are Especially Vulnerable To These Disasters

With the constant changes to technology and the daily development of new threats, it takes a highly-trained technician to maintain even a simple 3 to 5 person network; however, the cost of hiring a full-time, experienced technician is just not feasible for most dealerships.

In an attempt to save money, most try to do their own in-house IT support and designate the person with the most technical expertise as the part-time IT manager. This never works out because this makeshift IT person has another full-time job to do and is usually not skilled enough to properly support an entire computer network anyway.

This inevitably results in a network that is ill-maintained and unstable. It also means that the backups, virus updates, and security patches are not getting timely updates, giving a false sense of security.

It is only a matter of time before the network crashes. If you are lucky, it will only cost you a little downtime; but there is always a chance you could end up like one of these companies:

Auto Body Shop Shells Out $20,000 To Clean Up A Virus

> A local auto body shop with multiple locations discovered the importance of preventative maintenance the hard way. Without warning, a virus was downloaded to their server and started replicating and attaching itself to files. This virus corrupted

their data, impaired their customer management system, and immediately brought down their Exchange server (no e-mail could come in or go out).

Preventing this disaster would have only cost them 1/25th of the cost ($800 per month) AND they would have experienced better performance and fewer problems with their network. Instead, they were forced to spend a whopping $20,000 to remove the virus and restore their network. Even then, this huge, enormous fee only got them back up and running; their systems were still not optimized, secured, and updated, as they should have been.

Two Failed Hard Drives Cost Health Products Company $40,000 and 9 Days of Downtime

The back office of a health products company had two hard drives fail at the same time, causing them to lose a large number of critical customer files.

When they contacted us to recover the data from the system backups, we found the backups were not functioning properly. Even though they appeared to be backing up all of this company's data, they were in fact worthless. In the end, recovering the data off of these failed drives took a team of disaster recovery specialists 9 days and $15,000. In addition to the recovery costs, they also incurred $25,000 in other services to get their network stabilized.

Had they been properly monitoring their network, they would have been able to see that these hard drives were failing and that the backups were not performing properly. This would have prevented the crash, the downtime, and the $40,000 in costs to get them back up and running, not to mention the 9 days of lost productivity while their network was down.

Property Management Company Spends $9,000 And Weeks Of Downtime For A Simple Inexpensive Repair

A 10-user property management company was not monitoring or maintaining their server. Due to the overuse and lack of maintenance, it started to degenerate and eventually shut down under the load. This caused their entire network to be down for two full days and cost them $3,000 in support fees to get them back up and running. Naturally the costs were much higher when you factored in the lost productivity of their ten employees during that time.

This client did not want to implement a preventative maintenance program so the same problem happened again two months later, costing them another $3,000 and two days of downtime.

Six months later it happened yet another time bringing their total to $9,000 in hard

costs plus tens of thousands in productivity costs for a problem that could have quickly been detected and prevented from happening.

Six Things You Must Do At A Minimum To Protect Your Dealership From These Types Of Disasters:

While it is impossible to plan for every potential computer problem or emergency, a little proactive monitoring and maintenance of your network will help you avoid or greatly reduce the impact of the vast majority of computer disasters you could experience.

Unfortunately, I have found that most dealerships are NOT conducting any type of proactive monitoring or maintaining their network, which leaves them completely vulnerable to the types of disasters you just read about. This is primarily for three reasons:

#1. They do not understand the importance of regular maintenance.

#2. Even if they DID understand its importance, they simply do not know what maintenance is required or how to do it.

#3. They are already swamped with more immediate day-to-day fires demanding their attention. If their network is working fine today, it goes to the bottom of the pile of things to worry about. That means no one is watching to make sure the backups are working properly, the virus protection is up-to-date, that critical security patches are being applied, or that the network is "healthy" overall.

While there are numerous critical checks and maintenance tasks that need to be performed on a daily, weekly, and monthly basis, I am going to share with you the **6** that are most important for protecting your company.

Step#1: Make Sure You Are Backing Up Your Files Every Day

It just amazes me how many dealerships never back up their computer network. Imagine this: you write the most important piece of information you could ever write on a chalkboard and I come along and erase it. How are you going to get it back? You are not. Unless you can remember it, or if YOU MADE A COPY OF IT, you cannot recover the data. It is gone. That is why it is so important to back up your network. There are a number of things that could cause you to lose data files. If the information on the disk is important to you, make sure you have more than one copy of it.

Step #2: Check Your Backups On A Regular Basis To Make Sure They Are Working Properly

This is another big mistake I see. Many dealerships set up some type of backup system, but then never check to make sure it is working properly. It is not uncommon for a system to APPEAR to be backing up when in reality, it's not. There are dozens of things that can go wrong and cause your backup to become corrupt and useless. That is why it is not enough to simply back up your system; you have to check it on a regular basis to make sure the data is recoverable in the event of an emergency. Remember the Health Products Company that shelled out $40,000 to recover data they THOUGHT they backed up? Do not let that happen to you.

Step #3: Keep An Offsite Copy Of Your Backups

What happens if a fire or flood destroys your server AND the backup tapes or drive? What happens if your office gets robbed and they take EVERYTHING? Having an offsite backup is simply a smart way to make sure you can get your dealership back up and running in a relatively short period of time.

Step #4: Make Sure Your Virus Protection Is ALWAYS On AND Up-To- Date

You would have to be living under a rock to not know how devastating a virus can be to your network. With virus attacks coming from spam, downloaded data and music files, instant messages, web sites, and e-mails from friends and clients, you cannot afford to be without up-to-date virus protection.

Not only can a virus corrupt your files and bring down your network, but it can also hurt your reputation. If you or one of your employees unknowingly spreads a virus to a client or vendor, or if the virus hijacks your e-mail address book, you are going to make a lot of people very angry.

Step #5: Set Up A Firewall

Dealership owners and managers tend to think that because they are "just a small business", no one would waste time trying to hack into their network, when nothing could be further from the truth. I have conducted experiments where I connected a single computer to the Internet with no firewall. Within hours, over 13 gigabytes of space was taken over by malicious code and files that I could not delete. The simple fact is that there are thousands of unscrupulous individuals out there who think it is fun to disable your computer just because they can.

These individuals strike randomly by searching the Internet for open, unprotected ports. As soon as they find one, they will delete files or download huge files that cannot be deleted,

shutting down your hard drive. They can also use your computer as a zombie for storing pirated software or sending spam, which will cause your ISP to shut YOU down and prevent you from accessing the Internet or sending and receiving e-mail.

If the malicious programs cannot be deleted, you will have to re-format the entire hard drive causing you to lose every piece of information you have ever owned UNLESS you were backing up your files properly (see 1 to 3 above).

Step #6: Update Your System With Critical Security Patches As They Become Available

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computer through a simple banner ad or through an e-mail attachment.

Most hackers do not discover these security loopholes on their own. Instead, they learn about them when Microsoft (or any other software vendor for that matter) announces the vulnerability and issues an update. That is their cue to spring into action and they immediately go to work to analyze the update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch.

Clearly, ***someone*** needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible. That is why we highly recommend small business owners without a full-time IT staff allow their consultant to monitor and maintain their network.

Announcing A Simple And Easy Way To Ensure These Disasters Don't Happen To Your Dealership:

If you are sitting there thinking, "This all sounds great, but I don't have the time or the staff to handle all of this work," I have got the solution.

Thanks to our Managed Services plans, we can completely take over the day-to-day management and maintenance of your computer network and **free you from expensive, frustrating computer problems, downtime, and security threats**. You will get all the benefits of a highly-trained, full-time IT department at only a fraction of the cost.

And here is the best part…

In most cases, we can cut your IT support costs by 30% to 50% WHILE improving the reliability and performance of your network and eliminating spyware, spam, downtime, and other computer frustrations!

The Benefits Are Obvious:

- **You will eliminate expensive repairs and recovery costs.** Our network monitoring and maintenance will save you money by preventing expensive network disasters from ever happening in the first place. As a matter of fact, we guarantee it.

- **You will avoid expensive trip fees while receiving faster support**. Our remote monitoring software will enable us to access and repair most network problems right from our offices. No more waiting around for an engineer to show up!

- **How does faster performance, fewer "glitches", and practically zero downtime sound to you?** Under this program, that is exactly what we will deliver. Some parts of your system will degrade in performance over time, causing them to slow down, hang up, and crash. Our preventative maintenance and network monitoring will make sure your computers stay in tip-top shape for maximum speed, performance, and reliability.

- **You will have ALL of the benefits of an in-house IT department WITHOUT all of the costs.** As a Managed Service Plan customer, you will have access to a knowledgeable support staff that can be reached immediately should you have any kind of problem or question.

- **You will receive substantial discounts** on IT services that you are already buying. Most IT firms will nickel and dime you over every little thing they do; under this program, you will pay one flat, affordable rate and get all of the technical support you need. No hidden charges, caveats, or disclaimers.

- **You will never have to fear a big, expensive network repair bill.** Instead, you can budget for network support just like rent or insurance.

- **You will sleep easier** knowing the "gremlins at the gate" are being watched and kept out of your network.

- **You will safeguard your data.** The data on the hard disk is always more important than the hardware that houses it. If you rely on your computer systems for daily operations, it is time to get serious about protecting your critical, irreplaceable electronic information.

- **You will finally put a stop to annoying spam, pop-ups, and spyware** taking over your computer and your network.

- **You will gain incredible peace of mind.** As a business owner, you already have enough to worry about. We will make sure everything pertaining to your network security and reliability is handled so you do not have to worry about it.

A Final Word and Free Assessment Offer to Review Your Current Network Security Proficiency

I hope you have found this guide helpful in shedding some light on what to look for when hiring a professional firm for outsourced IT security and/or support. As I stated in the opening of this report, my purpose in providing this information was to help you make an informed decision and avoid getting burned by incompetent or unethical firms luring you in with a cheap price.

If you are worried about whether or not your current backup and security processes are up to par, I'd like to offer you, for a limited time, a free Network Assessment and PEN Test (a value of $3,995-$19,995) as a means for introducing our services to you. Our test will inform you of your **vulnerability and risk of an attack.** The PEN Test simulates a cyberattack to identify your security weaknesses. Why do we do this? Simply because I know how confusing and difficult it can be to find a good IT support company that is responsive, easy to work with and actually knows what they're doing.

Just about anyone can say they are an "IT expert." And since most dealership owners and managers do not have the ability to evaluate whether or not their IT is secure as it needs to be and running as efficiently as possible, we find that offering this assessment is a no-risk way of demonstrating how we can help you. At the very least, you will get a free, qualified 3rd party evaluation of your network security, current backup, and voice communications profile and score which is extremely valuable even if you do not choose to hire us.

At no charge, one of our security specialists will …

- Audit your current data security and protection policy, including backup and restore procedures. Validate if ALL of your data is actually being backed up in a format that could quickly be restored. We often discover data on drives, laptops or PCs that is overlooked.

- Confirm if your current backup is working as expected, if you would be able to get your data and systems back up and running, and if so, would it be in a reasonable time frame (hours, days, weeks)? Many of the companies we have reviewed are shocked to learn the backup would NOT survive a ransomware attack.

- Assess if your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees. If you are not getting weekly security updates, your systems probably are not secure. You should also know that antivirus software and most firewalls are grossly inadequate against the sophisticated attacks happening in 2021.

- Evaluate your VoIP system. If you utilize VoIP, it is important to know that with today's technology, VoIP needs to be configured correctly to work seamlessly with your computer network. If not, it will not work right (static, dropped calls etc.) and is an open invitation for cybercriminals to hack your healthcare practice.

- Run a Dark Web Assessment– **9 out of 10 times** we find compromised company credentials/passwords are available on the Dark Web**.**

Depending on what we discover, we will either give you a clean bill of health or reveal gaps in your network that could prove disastrous. If it is appropriate, we will provide you with an actionplan for further securing your data.

How To Request Your Data Security Assessment and PEN Test?

To request your assessment, simply do one of the following:

1. Call our office at 810-629-0131
2. Send us an e-mail to: info@tdaniels.com
3. Go online to: https://www.tdaniels.com/assessment/

As soon as we receive your request, we will call to schedule a convenient time for us to meet with you and to conduct the assessment. Again, you are under no obligation to do or buy anything. Even if you choose not to hire us for any additional work, you will at least get a free, 3rd party evaluation of your company's data backup and security.