

Auto & Ag Dealership IT & Cybersecurity CHECKLIST

A practical checklist to uncover technology risks that could disrupt your sales, service, parts, and business operations.



REDUCE
RISK



KEEP YOUR
TEAM PRODUCTIVE



KEEP YOUR
DEALERSHIP MOVING

HOW CONFIDENT ARE YOU THAT YOUR DEALERSHIP IS PROTECTED AND PREPARED?

Your dealership depends on technology across sales, service, parts, accounting, communications, and customer service. When systems go down or an IT provider is slow to respond, the problem can quickly affect your employees and customers.

Use this checklist to identify areas that may deserve a closer look. You don't need to be an IT expert. You just need confidence that someone is taking ownership of your technology, security, and support.

How to use this checklist

Check Yes, No, or Not Sure for each statement. Pay particular attention to every statement where your answer is No or Not Sure.

DEALERSHIP: _____

COMPLETED BY: _____

1. Cybersecurity

CHECKLIST STATEMENT	YES	NO	NOT SURE
Multi-factor authentication (MFA) protects email and other critical accounts.	☐	☐	☐
Employees receive regular cybersecurity and phishing awareness training.	☐	☐	☐
Computers and devices are protected with centrally managed security tools.	☐	☐	☐
Security updates and patches are installed consistently.	☐	☐	☐
We monitor our environment for suspicious activity and potential threats.	☐	☐	☐
We have a documented plan for responding to a cybersecurity incident.	☐	☐	☐
We know who to call immediately if we suspect our dealership has been compromised.	☐	☐	☐

ASK YOURSELF

If an employee clicked a malicious link today, how quickly would someone know?

2. Backups & Disaster Recovery

CHECKLIST STATEMENT	YES	NO	NOT SURE
Critical dealership data is backed up automatically.	☐	☐	☐
Our backups are protected from ransomware and unauthorized access.	☐	☐	☐
At least one backup copy is stored separately from our primary systems.	☐	☐	☐
Backups are regularly tested to confirm that data can be restored.	☐	☐	☐
We know which systems need to be restored first after a major outage.	☐	☐	☐
We know approximately how long it would take to restore critical operations.	☐	☐	☐
We have a documented disaster recovery plan.	☐	☐	☐

ASK YOURSELF

Do you know that your backups work, or are you assuming they work?

3. Dealership Operations & Downtime

CHECKLIST STATEMENT	YES	NO	NOT SURE
We know which technology systems are critical to sales, service, parts, and accounting.	☐	☐	☐
We have plans for keeping critical departments operating when a system or internet connection is unavailable.	☐	☐	☐
Our internet connectivity is dependable enough for daily dealership operations.	☐	☐	☐
Critical network equipment is monitored for problems.	☐	☐	☐
We have appropriate backup power protection for important technology.	☐	☐	☐
Recurring technology problems are investigated and permanently addressed rather than repeatedly patched.	☐	☐	☐
Leadership knows what happens operationally if a critical system goes down.	☐	☐	☐

ASK YOURSELF

If your primary systems went down during your busiest day, which departments would stop working?

4. User Access & Employee Security

CHECKLIST STATEMENT	YES	NO	NOT SURE
Employees have access only to the systems and information required for their jobs.	☐	☐	☐
Administrator accounts are limited and separately protected.	☐	☐	☐
Former employees have their access removed promptly.	☐	☐	☐
New employees follow a consistent technology onboarding process.	☐	☐	☐
Departing employees follow a documented technology offboarding process.	☐	☐	☐
Password and authentication policies are consistently enforced.	☐	☐	☐
Shared accounts are minimized or eliminated where possible.	☐	☐	☐

ASK YOURSELF

Are you confident that former employees and vendors no longer have access to your systems?

5. Email, Microsoft 365 & Cloud Services

CHECKLIST STATEMENT	YES	NO	NOT SURE
Microsoft 365 or our primary email platform is protected with MFA.	☐	☐	☐
Email has appropriate phishing, spam, and malicious attachment protection.	☐	☐	☐
Administrative cloud accounts receive additional protection.	☐	☐	☐
User and administrator permissions are reviewed periodically.	☐	☐	☐
Important cloud data is appropriately protected and backed up.	☐	☐	☐
Employees know how to report suspicious emails.	☐	☐	☐
We have visibility into suspicious account logins and activity.	☐	☐	☐

6. Dealership Systems & Third-Party Vendors

CHECKLIST STATEMENT	YES	NO	NOT SURE
We maintain an up-to-date list of our critical technology vendors and systems.	☐	☐	☐
We know who is responsible for supporting each major system.	☐	☐	☐
Our IT provider understands how our dealership's major systems fit together.	☐	☐	☐
When a technology problem involves multiple vendors, our IT provider helps coordinate the resolution.	☐	☐	☐
Our leadership does not have to referee disagreements between technology vendors.	☐	☐	☐
Someone takes ownership of an IT problem until it is resolved, even when another vendor is involved.	☐	☐	☐
Important vendor contacts, account information, and escalation procedures are documented.	☐	☐	☐
ASK YOURSELF			
When vendors start pointing fingers at each other, who owns the problem until it's solved?			

7. Network, Wi-Fi & Physical Locations

CHECKLIST STATEMENT	YES	NO	NOT SURE
Business and guest Wi-Fi are appropriately separated.	☐	☐	☐
Network equipment is professionally managed and monitored.	☐	☐	☐
Remote access to dealership systems is secured.	☐	☐	☐
Security cameras, phones, printers, and other connected devices are appropriately separated or protected.	☐	☐	☐
We know which devices are connected to our network.	☐	☐	☐
Network documentation is current.	☐	☐	☐
FOR MULTI-LOCATION DEALERSHIPS			
Technology standards are consistent across locations.	☐	☐	☐

Leadership has centralized visibility into technology across all locations. ☐ ☐ ☐

Adding a location does not require rebuilding our IT strategy from scratch. ☐ ☐ ☐

8. IT Support & Accountability

CHECKLIST STATEMENT	YES	NO	NOT SURE
Employees know exactly who to contact when they need IT help.	☐	☐	☐
Our IT provider responds quickly when an issue affects dealership operations.	☐	☐	☐
We receive clear communication about the status of important problems.	☐	☐	☐
Problems do not repeatedly disappear into a ticket queue without explanation.	☐	☐	☐
Our IT provider communicates in business language rather than unnecessary technical jargon.	☐	☐	☐
Recurring problems are investigated instead of simply fixed temporarily.	☐	☐	☐
Our IT provider proactively identifies risks rather than waiting for something to break.	☐	☐	☐
Someone takes ownership of problems from beginning to end.	☐	☐	☐
Leadership does not have to personally manage the IT provider to get results.	☐	☐	☐
YOUR IT PROVIDER SHOULD BE ONE LESS THING YOU HAVE TO MANAGE.			

HOW DID YOUR DEALERSHIP DO?

- **MOSTLY YES**

Your dealership appears to have many important IT fundamentals in place. Continue reviewing and testing them regularly.

- **SEVERAL “NOT SURE” ANSWERS**

Uncertainty can be a risk by itself. Identify who owns these areas and verify that appropriate protections and processes are actually in place.

- **SEVERAL “NO” ANSWERS**

You may have technology, security, or support gaps worth addressing before they cause downtime or disruption.

This checklist is intended as a conversation starter and general planning resource. It is not a comprehensive cybersecurity, regulatory, or compliance assessment.

YOU SHOULDN'T HAVE TO MANAGE YOUR IT PROVIDER JUST TO KEEP YOUR COMPANY RUNNING.

When technology problems keep coming back, vendors point fingers, or you're left wondering whether your dealership is truly protected, IT becomes another responsibility on your plate.

EK Computer helps Northwest Ohio businesses take IT off their plate.

We've been helping businesses with their technology since 1998, providing local support and straightforward guidance without unnecessary geek-speak.

READY TO GET IT OFF YOUR PLATE?

Schedule a conversation with our team.

We'll learn about your dealership, review your technology and support concerns, and help you understand where your biggest opportunities and risks may be.

SCHEDULE A CONVERSATION • WWW.EKCOMP.COM

IT should help your dealership move forward — not become one more thing you must manage.

EK Computer Inc. | Business Technology Specialists

Office: 419-592-2600 | Email: team@ekcomp.com | Web: www.ekcomp.com