EMPLOYEE ACCESS CONTROL CHECKLIST

With the amount of information moving through your dealership, it's important to implement the correct access controls to ensure your employees have access to only what they need. If an employee has too much access, it increases risk for a wide-spread cyber incident.

Fill out this checklist to see your current risk level. Give yourself one point for each item your dealership currently has set up.

YOUR DEALERSHIP ACCESS CONTROL

Do you have multi-factor authentication (MFA) set up for your employees to log in?	
Is MFA regularly enforced for all associates accessing cloud resources?	
Do you have controls set up to limit the location from which employees can access their cloud applications? (For example, they can't log in from a foreign country.)	
Do you have controls in place to limit the frequency of MFA challenges or log-in attempts?	
Are you able to block any unexpected attempts to access email or cloud resources?	
For tools that contain sensitive information, do you have more verification requirements in place for employees to sign in?	
Do you restrict employees from downloading or installing software on their own devices?	
Do you have a process to approve what applications are installed on devices?	
Are employees limited to only accessing the necessary tools to complete their jobs? For example, your accounting personnel don't need full access to your CRM.	
Do you have anti-spam, anti-phish, and anti-malware controls in place to protect employee emails?	
Do you have a managed security incident and event management (SIEM) tool in place?	
Do you keep logs of cloud and email sign-in activities?	
Do you send the logs to an SIEM tool to analyze the logs for abnormal activities, like a compromised account?	
Do you have processes set up to contain, eradicate, and recover what information is needed when an compromise or breach is detected?	
Do you train employees how to identify and avoid phishing emails?	
Do you train employees how to handle sensitive information when using your solutions?	
Do you test your employees with fake phishing emails to see if they correctly handle them?	

Total 0

DEALERSHIP RISK LEVEL

SCORE	RANKING
0-7	**High Risk** Your dealership is missing critical checkpoints to help prevent cyberattacks. It can seem like a lot to implement all these processes and procedures, but they are designed to safeguard your systems and your data from malicious threats. If you don't have someone at your dealership with the knowledge to set up these controls, an automotive-specific cybersecurity firm, like Proton, can help. We'll work with your team to ensure proper controls are in place and working.
8-14	**Moderate Risk** Your dealership has a good foundation of controls set up, but take a look at some of the items you didn't check off to see if there are opportunities for you to improve your cybersecurity posture. Continuing to introduce new controls and technologies will help build a more secure business.
15-17	**Low Risk** You've done a great job at monitoring what your employees have access to and putting the proper processes in place to protect your dealership. Make sure you stay up to date on the latest threats and trends to adapt your processes and controls as needed.

No matter your risk level, it's important to stay vigilant. Attackers are evolving and continue to find new ways to get access to sensitive information. While your focus is selling and servicing vehicles, it can be challenging to stay up with the latest cyber news and threats. Partnering with an automotive-specific cybersecurity firm can help reduce your risk through networking monitor, endpoint detection and response, incident response, cybersecurity training, and so much more.

866.605.1027 | INFO@PROTONTECHS.COM | PROTONTECHS.COM

PROTON DEALERSHIP IT CYBERSECURITY