FACTSHEET

Common Areas of Risk in the Auto Industry

DID YOU KNOW?
In 2017, more than 24,000 records were compromised in an average data breach.[1]

With so many records at risk, businesses across North America must be aware of their areas of vulnerability.

Lack of Policy

Car dealerships have been slower to keep up with the state of information technology, as well as its dangers.[2] Organizations need to have formal cyber security policies, incident response plans, back-up, and restoration procedures in place.

Employees

Employees can be one of its biggest risk factors. Often an attack is triggered when an unsuspecting employee opens an email that contains a malicious virus. In a recent study, 54% of small and medium-sized businesses (SMB) said careless employees were the root cause of cyber security incidents.[3]

Online scams

Phishing scams try to trick the end user into logging into a fraudulent system or downloading malware. In a recent security warning, one automotive technology company warned that hackers were planting malware inside social media posts designed to lure employees to click on the post.

Bring Your Own Device (BYOD)

Employees often store personally-identifiable information on their own mobile devices or laptops. Personal devices are one of the most frequently-used tools by malicious employees and hackers where theft of data is involved.

Limited IT security staff

A recent survey[5] showed that SMBs generally have a low number of dedicated IT security staff members available to deal with security issues. About 80% of companies with 100 to 500 employees have two or fewer security staff members.

Dated equipment

Technology today dates quickly, and legacy equipment can make a car dealership vulnerable to attack.

Interconnectivity

Dealerships are interconnected with car makers, suppliers and vendors. Research has shown that many breaches are being linked to third parties.[4]

COMMON AREAS OF RISK IN THE AUTO INDUSTRY

3 Tips to Keep Your Business Secure

Identify All Potential Areas of Risk

Conduct a walk-through of your office. Point out and mitigate any risks that you see. This will allow you to discover your pain points and solidify an information security strategy to keep data secure.

Implement Secure Workplace Policies

By establishing comprehensive policies such as a *Shred-it All* Policy and Clean Desk Policy, you encourage people to think twice about their actions in the workplace. This will push them to comply and help protect your data.

Build a Total Security Culture

Using a top down approach and integrating information security throughout the workplace, you will be able to embed it into people's everyday behavior. This will encourage them to re-consider how to securely destroy any and all confidential information.

Sources:

1. 2017 Cost of Data Breach Study, Ponemon Institute, 2017
2. 6 Steps to Prevent Hacking at Your Dealership, Dealer Marketing Magazine, August 2017
3. 2017 State of SMB Cybersecurity Report, Keeper Security and Ponemon Institute, 2017
4. The Third Party Data Breach Problem, Digital Guardian, July 2017
5. IT Security at SMBs: 2017 Benchmarking Survey, Cyren, 2017

Learn more about information security in the automotive industry:

888-979-4048 | shredit.com/auto

Shred-it®