onestep
Secure IT Services

Cybersecurity and the Auto Industry: Costly Attacks on the Rise

By One Step Secure IT Team

In an interconnected world driven by technology, the battle against cyber threats is intensifying. With our increasing reliance on technology, dealerships must adopt robust cybersecurity practices to protect sensitive data and ensure the continuity of their operations.

The Ransomware Saga

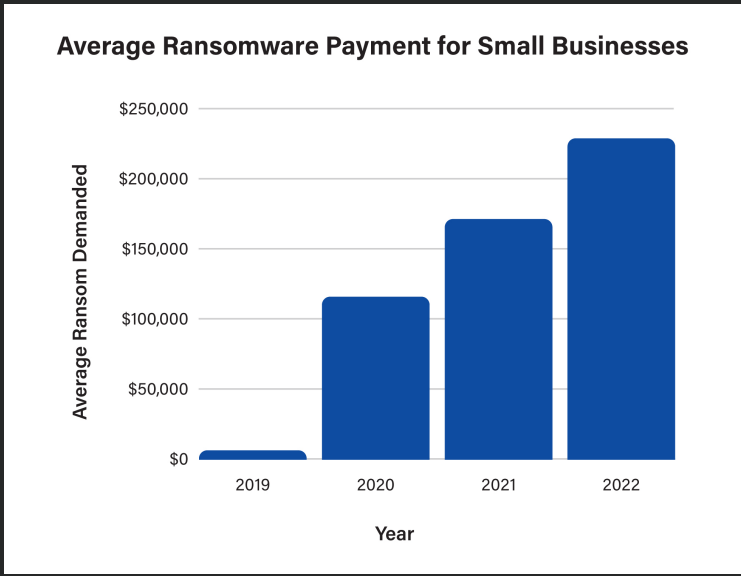
Ransomware attacks, in particular, have emerged as a significant threat to the automotive industry. In the pre-pandemic era of the first quarter of 2019, the average ransomware payment was a mere $6,000. As the COVID-19 pandemic took hold and necessitated a shift to remote work across the United States, cyber criminals swiftly exploited the heightened security vulnerabilities resulting from businesses' inadequate cybersecurity protocols. By 2020, the demanded ransom payment skyrocketed to an average of $115,000.

This situation was like a perfect storm of technological mishaps, including employees connecting to company servers through unsecured Wi-Fi connections, the hasty introduction of new applications without appropriate safeguards, and the limited implementation of multifactor authentication measures, among others.

It was a recipe for disaster created by a mix of clueless employees, hasty IT decisions, and a sprinkle of security negligence. It's like watching a train wreck in slow motion, except this time, the passengers are the company's sensitive data and reputation.

In 2021, the average demanded ransom rose even further to $170,404, and in 2022, the average demanded ransom was up to $228,000. It’s important to keep in mind that the financial impacts for businesses stretch far beyond just the ransomware payment itself.

In addition to the cost of the ransom, the cost of downtime, employee pay, remediation, and other expenses could add up to about $1 million. It's no longer a world where auto dealerships can turn a blind eye to these threats; it's just too costly to i gnore.



The average cost of a ransomware attack is only expected to increase in the coming years — painting a bleak financial picture for auto dealerships.

Unfortunately, the likelihood of a ransomware attack isn’t slim. According to AAG, a staggering 64% of businesses have fallen victim to at least one ransomware attack, with a concerning 79% opting to pay the ransom. Even more alarming is the fact that among those previously attacked, a staggering 88% stated they would repeat the payment if targeted again.

However, it's not all doom and gloom. If you have been fortunate enough to avoid a cyber attack thus far, you have the ability to protect your business and build your defenses. If you have already experienced a cyber attack but are still in business, you have a golden opportunity to enhance your cybersecurity strategy.

In the past, antivirus software and firewalls provided a certain level of protection by detecting and blocking known malware and unauthorized access attempts. However, the evolving nature of cyber threats demands a proactive approach beyond traditional defense mechanisms.

Here are a few cybersecurity practices for businesses to adopt in a world of increasing cyber threats.

Cybersecurity Strategies for Auto Dealerships

Implement Endpoint Protection and Response (EDR): Auto dealerships must fortify their remote access solutions and deploy comprehensive endpoint protection systems. Implementing robust endpoint protection involves deploying comprehensive security solutions on individual devices such as computers, laptops, and mobile devices to safeguard against a wide range of cyber threats, including malware, phishing, and unauthorized access attempts.

Administer Regular Employee Training: Employee awareness plays a crucial role in preventing cyber attacks. By educating staff members about the risks associated with phishing emails, social engineering tactics, and the importance of strong passwords, dealerships can significantly reduce the likelihood of successful attacks.

Regularly Update and Patch Software: Promptly applying software updates and patches is vital for closing security vulnerabilities. Auto dealerships should have a robust patch management process in place to minimize the risk of exploitation by cybercriminals.

Conduct Network and Security Scans: By conducting regular network and security scans, businesses can proactively identify vulnerabilities, allowing them to address and fortify their defenses before cyber criminals have a chance to exploit them, ensuring enhanced protection for their sensitive data and operations.

Align Network with the Zero Trust Security Model: Under a Zero Trust model, every access request is fully authenticated, authorized, and encrypted before granting access, regardless of where the request originates from or what resource it accesses. Many businesses still operate under the assumption that everything within their internal network can be trusted.

The High Stakes

The consequences of cyber attacks on the automotive industry are profound. If left unaddressed, it is estimated that the industry stands to lose a staggering $505 billion by 2024. The financial impact, reputational damage, and potential legal consequences underscore the urgent need for proactive cybersecurity measures.

In a world increasingly dependent on technology, businesses must prioritize cybersecurity to protect sensitive data and maintain operational resilience. By implementing strong access controls, keeping software and systems up to date, educating employees, regularly backing up data, deploying robust endpoint protection, conducting security audits, and fostering a culture of vigilance, businesses can fortify their defenses against cyber threats.

Cybersecurity is a continuous journey that requires ongoing attention and adaptation to stay ahead of evolving threats. By adopting these essential cybersecurity practices, businesses can safeguard their valuable assets.