Cyber

Acting with urgency against the cyber threats to auto dealers

And why car dealers are attractive targets for cyber criminals

With the increasing reliance on technology and the growing threat of cyber attacks, it's more important than ever that you have the right strategy, technology and resources in place to survive a data breach and its potential multimillion-dollar impact.

Cyber attacks on dealerships are becoming more and more prevalent and are costing hundreds of thousands of dollars, lost customers, and reputational damage. You probably already know of a dealership that has been victimized of this growing crime.

What is the risk and why the urgency?

Cyber Security

84%
of car buyers said they would not return to a dealership whose data had been breached [1]

On an average day,
153 viruses
and 84 malicious spam emails are blocked by technology on a dealership's network [2]

70%
of dealers are not up to date on their anti-virus software leaving consumer data at risk of being exposed during a cyber attack [3]

A data breach can hit businesses with less than 1,000 employees with disproportionately higher costs when compared to organizations with 25,000 or more employees

Smaller organizations average $2.65 Million
or $3,533 **per employee** [4]

Cyber Risk a very real threat for auto dealers

A dealership was hit by **Ransomware.** Hackers reportedly messaged that they had infiltrated the dealership's network and downloaded sensitive information.

(April 2021)

Dealer group hacked when 2 employees fell victim to a phishing scam, exposing 1000's of customers' personal information and bank details.

(December 2020)

Personal details of 3.000.000 customers of a US car company leaked after hack of a car dealership service provider

(February 2021)

Why car dealerships are attractive targets for cyber criminals

Dealerships have become very attractive targets for cyber criminals because they have several key vulnerabilities that the threat actors can exploit:

- The data dealers possess represents a treasure of information to hackers. Dealerships store large amounts of confidential, personal data, including financing and credit applications, customer financial information and home addresses.
- Many dealerships lack basic cyber security protections. A large percentage of auto dealers use outdated systems and/or have outdated software. Unsecure networks can act as gateways to stealing information or creating digital mayhem.
- In addition, dealership systems are often interconnected to external interfaces and portals, such as external service providers.
- Finally, dealership employees may lack training in the most frequent of cyber attacks, phishing scams. Phishing campaigns and ransomware attacks have seen big increases, with email and other communications aimed at tricking users to open malicious attachments or, in some cases, make wire transfers on behalf of their company.

More than 90%
of cyber breaches start with phishing or social engineering campaigns

Assessing your exposure and managing the risk

Dealers must be diligent in cyber protection and response capabilities. Building resilient systems is the best preparation for the next cyber attack. Beating back the assault takes a multi-department approach that includes strengthening protections. This strategy, combined with training employees can thwart efforts to break into dealership networks and educating employees on the scope of the threat.

The National Institute of Standards and Technology (NIST) established its Cybersecurity Framework in 2014 in response to a 2013 executive order. The framework is aimed at reducing risk to critical infrastructure and is a great resource you can use to identify risk and protect your operation prior to a cyber incident, and to detect, respond and recover should an incident occur. (nist.gov)

Pre-Cyber Incident

Prepare
Understand the steps you'd take in the event of a breach - develop an Incident Response Plan. Conduct an Asset Inventory and understand what you need to protect.

Back-up
Ensure you have a strong back-up and recovery strategy in place, and test regularly.

Train
Ensure your employees and other end-users are "Cyber risk aware" through consistent security and awareness training, phishing campaigns, etc.

Recover
Consider cyber insurance coverage if it meets the strategic objectives of your dealership. Also, conduct risk assessments to understand where you need to invest in protection

Identify	Protect	Cyber Incident	Detect	Respond	Recover
Asset Management	Identity Management & Access Controls		Anomalies and Events	Response Planning	Recovery Planning
Business Management	Awareness and Training		Security Continuous Monitoring	Communications	Improvements
Governance	Data Security		Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures			Mitigation	
Risk Management	Maintenance			Improvements	
Strategy	Protective Technology				
Supply Chain Risk Management					

Cyber *Continued*

Zurich cyber risk engineering services for automotive businesses

Zurich delivers a variety of services that can provide you with an objective and rapid assessment of your security posture, along with specific recommendations for addressing any control deficiencies that are discovered.

The challenge

Cyber security is the top concern for senior management and boards, as companies are exposed to a wide variety of vulnerabilities. Prioritizing investment in cyber security can be a daunting task with the risk evolving daily. The hardest part is knowing where to start.

How Zurich delivers

Zurich helps you understand your cyber risk by assessing your unique threat environment and the effectiveness of your cyber defenses. An experienced and qualified Zurich Cyber Risk Engineer will provide a holistic view of your controls and their adequacy with respect to your exposure. The results will be presented in the context of business risk, so that they are easily understood by various stakeholders, but with adequate technical depth. From there, we can deliver additional services targeting specific risk areas and bring industry-leading partners to perform technical work at a Zurich preferred rate.

Benefits you can expect

Your organization will benefit from Zurich's expertise and pragmatic approach. Specifically, you'll be better positioned to:

- Advance your cyber security maturity and mitigate risks you may have not known existed
- Know how you compare to your industry peers through our benchmarking capabilities
- Make informed decisions from a cost benefit perspective through our strategic advice
- Prepare for emerging cyber risks through forward-looking insights

For help, reach out to us @ CyberRE@zurichna.com

1. Crane, Casey. "15 Auto Dealership Cybersecurity Statistics That Will Drive You To Action," Cyber Crime Magazine, 14 February 2020,
2. www.cybersecurityventures.com/15-auto-dealership-cybersecurity-statistics-that-will-drive-you-to-action/
3. Burden, Melissa. "Retailers prime targets for data theft," Auto News Magazine, 09 December 2019,
4. www.autonews.com/finance-insurance/retailers-prime-targets-data-theft
5. Nachbahr, Erik. "Why do Cybercriminals Target Auto Dealerships?" F&I Showroom & Magazine, 12 August 2020,
6. https://www.fi-magazine.com/361606/why-do-cybercriminals-target-auto-dealerships
7. Cost of a Data Breach Report 2019, Ponemon Institute/IBM Security

Zurich

7045 College Boulevard,
Overland Park, Kansas 66211-1523
800 840 8842 ext. 7449
www.zurichna.com/automotive

Zurich Resilience Solutions has basic services as a great starting point on your cybersecurity journey

Cyber Risk Snapshot

- Work with a **Zurich Cyber Risk Engineer** to develop a basic overview of your cyber exposures and vulnerabilities
- Receive tailored advice that you can immediately act upon to improve your Cybersecurity posture

Free Trial of SecurityAdvisor

- Deploy the Platinum version of **SecurityAdvisor** for Security & Awareness Coaching of your employees and other users for a period of 45 days-free to Zurich customers
- Includes unlimited phishing exercises, awareness campaigns, and proprietary teachable moment intervention. Set up and start using in under an hour!

Zurich Risk Advisor (free)

- Download the free **Zurich Risk Advisor iOS/Andriod app** to take a 23-question Cyber Self Assessment
- Receive practical advice based on your responses

BitSight Security Rating

- As a Zurich customer, your customized Security Rating from **BitSight Technologies** - the most widely adopted Security Ratings Platform in the world
- This is an external scan providing data-driven and dynamic measurement of your organization's cybersecurity performance