Everything you wanted to know about retail but were afraid to ask

Lisa Plaggemier
**What Are We Protecting?**

<table>
<thead>
<tr>
<th><strong>Business</strong></th>
<th><strong>Technology</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>$2 billion in revenue FY 2018</td>
<td>85 facilities in 34 countries</td>
</tr>
<tr>
<td>$350+ billion in revenue in hosting centers</td>
<td>4000+ mobile devices</td>
</tr>
<tr>
<td>7 of 10 top auto groups</td>
<td>6500+ laptops</td>
</tr>
<tr>
<td>500+ million consumer credit records (PII)</td>
<td>12 global hosting facilities: 4 NA, 8 International</td>
</tr>
<tr>
<td>~35 million consumer credit applications &amp; scores</td>
<td>7,000 dealer sites &amp; 225,000 connections world-wide</td>
</tr>
<tr>
<td>5,800 servers, 18,000 virtual Servers, 6.3 petabytes of storage</td>
<td>65 products comprised of 500+ applications</td>
</tr>
<tr>
<td>Web Hosting with 100 million page hits per month</td>
<td>Digital Advertising with 25 million ad impression per day</td>
</tr>
<tr>
<td>Hosted telephony: &gt; 4,000 dealer sites, 146k phones, 40 million minutes per month</td>
<td></td>
</tr>
</tbody>
</table>
Dealer Data Ecosystem

- OEM
- Inventory Management Systems
- Insurers
- Website Providers
- Reputation Management
- DCS
- Telematics
- Vehicle Marketing
- Advertising
- Vehicle History Providers
- Lead Generators
- Desking Providers
- CRM
- Desking Providers
- Banks
overall employee turnover: 43%
sales: 67%

Source: NADA DATA
Two former Wolf Auto Center (Sterling, CO) employees “used their user names, passwords, and email accounts to obtain data, confidential information and trade secrets.”
FTC, in a first, says Georgia dealership failed to safeguard consumer data. “Franklin Toyota-Scion of Statesboro, Ga., failed to adopt reasonable security measures to protect consumers' personal information…. 95,000 consumer records impacted.”
The New York Times

“No Business Too Small to Be Hacked”

“Cyber Attacks on Small Businesses on the Rise”

“Four Years after Target, the Little Guy is the Target”
Stores swindled by hacker battle over blame

Judge orders 1 to pay again for vehicles
$2M
70% out-of-date anti-virus
A day in the life of a car dealership

**153** Viruses blocked

**84** malicious spam emails blocked

**3,000** failed login attempts to their network

**10%+** of those from automated credential guessing

**≥56%** year over year

Gateway is port scanned **7** times each day

1 in **20** dealers were infected with a botnet utilizing up to **60%** of their bandwidth

Source: Nuspire Networks
Trust

Who do you trust with your data?

- Large Companies: 32%
- Google: 44%
- Apple: 46%
- Auto OEMs: 10%
- I don’t trust any entity with my private data: 68%

Q: If the car you own has Android Auto or CarPlay (Apple’s infotainment system), who do you trust most with your data?

In-vehicle technology survey, August 2015 (N=2076)
A Day in the Life

7 am – Arrive at work be sure everything is working

7:30 am – Verify owner’s access to NASCAR web site is working for the race that day

9 am - Help Desk Call – How do I use spell checker in Excel?

10 am – Service is complaining about slow systems – issue, find parts watching videos

10:15 am – DMS is running slow, check network, enter a ticket with DMS provider

10:30 am – Travel across town to Ford store to install new PCs for 4 associates. Pick up cables at Best Buy. Take help desk calls while on the road.

1:00 pm – Pick up lunch and drive back to main office, pick up parts from another dealer while on the way for Service.

1:40 pm – Meet network installer who is installing a new wireless network in the service bay for new electronic service tools being deployed by GM.

1:45 pm – Clean back office PC that had a virus

2:15 pm – Install new application on CFO’s PC

2:30 pm – Call DMS vendor – follow up on morning issue

3:00 pm – Upgrade Sales PC

4:00 pm – Call ISP about security system connection problems, report bad camera

5:00 pm – Head home but stop by Nissan store to check on an issue

10:00 pm – Resolve remote access issue dealer is experiencing
INDUSTRY BEST PRACTICES AND RECOMMENDATIONS FOR AUTOMOTIVE RETAIL DATA SECURITY

1. STAR Dealer Data Security Guidelines
   1.1 Overview
   1.2 Disclaimer

2. STAGE 1: Security Policies, Procedures, and Compliance
   2.1 Security Policies
      2.1.1 Acceptable Use Policy
      2.1.2 Asset Management Policy
      2.1.3 Business Applications Policy
      2.1.4 Electronic Communication Policy
      2.1.5 Identity and Access Management Policy
      2.1.6 Security Incident Management Policy
      2.1.7 Network Policy
      2.1.8 Risk Management and Audit Policy
      2.1.9 Threat and Vulnerability Management Policy
      2.1.10 Dealer Guidance on Security Policies
   2.2 Identity and Access Management
      2.2.1 Introduction
      2.2.2 Basic Concepts and Definitions
      2.2.3 Identity Management
      2.2.4 Authentication
      2.2.5 Authorizations and Access Management Policies
      2.2.6 End users and Physical Consideration
      2.2.7 Protection Levels
      2.2.8 Dealer Guidance on Identity and Access Management (IAM)
   2.3 Patch Management
      2.3.1 Guidance with Patch Management
   2.4 Disaster Recovery
      2.4.1 Guidance with Disaster Recovery
   2.5 Security Awareness Training
      2.5.1 Guidance on Security Awareness Training
   2.6 Compliance with Federal Regulations
      2.6.1 Gramm-Leach-Bliley Act and Safeguards Rule
      2.6.2 Payment Card Industry Data Security Standard (PCI DSS)
      2.6.3 Dealer Guidance on Compliance with Federal Regulations
   2.7 Additional Resources

CDKGlobal
Evolving the Automotive Retail Experience
Dealership Security Workshop

CyberSecure My Business™ for car and light truck dealers
5-Step Approach

1. Identify
   assets you need to protect

2. Protect
   assets and limit impact

3. Detect
   security problems

4. Respond
   to an incident

5. Recover
   from an incident
Dave’s Downtown Dealership

Open office environment—no private offices, except for F&I and senior management

Customers complete a mix of online and paper-based forms and tablets

BDC, Sales, Service, Parts, and F&I all have access to CRM system incl. mobile app on personal devices
Third Party Security

Vendor Survey

Make a list of cloud services you use. Ask about how they handle:

- Maintenance
- Patching
- Firewall
- Encryption
- Backup/Restore
Goal of 5-step Approach is Resilience

- Know the threats and Identify and Protect your assets
- Detect problems and respond quickly and appropriately
- Know what recovery looks like and prepare
Questions?

lisa.plaggemier@cdk.com
(512)350-5403