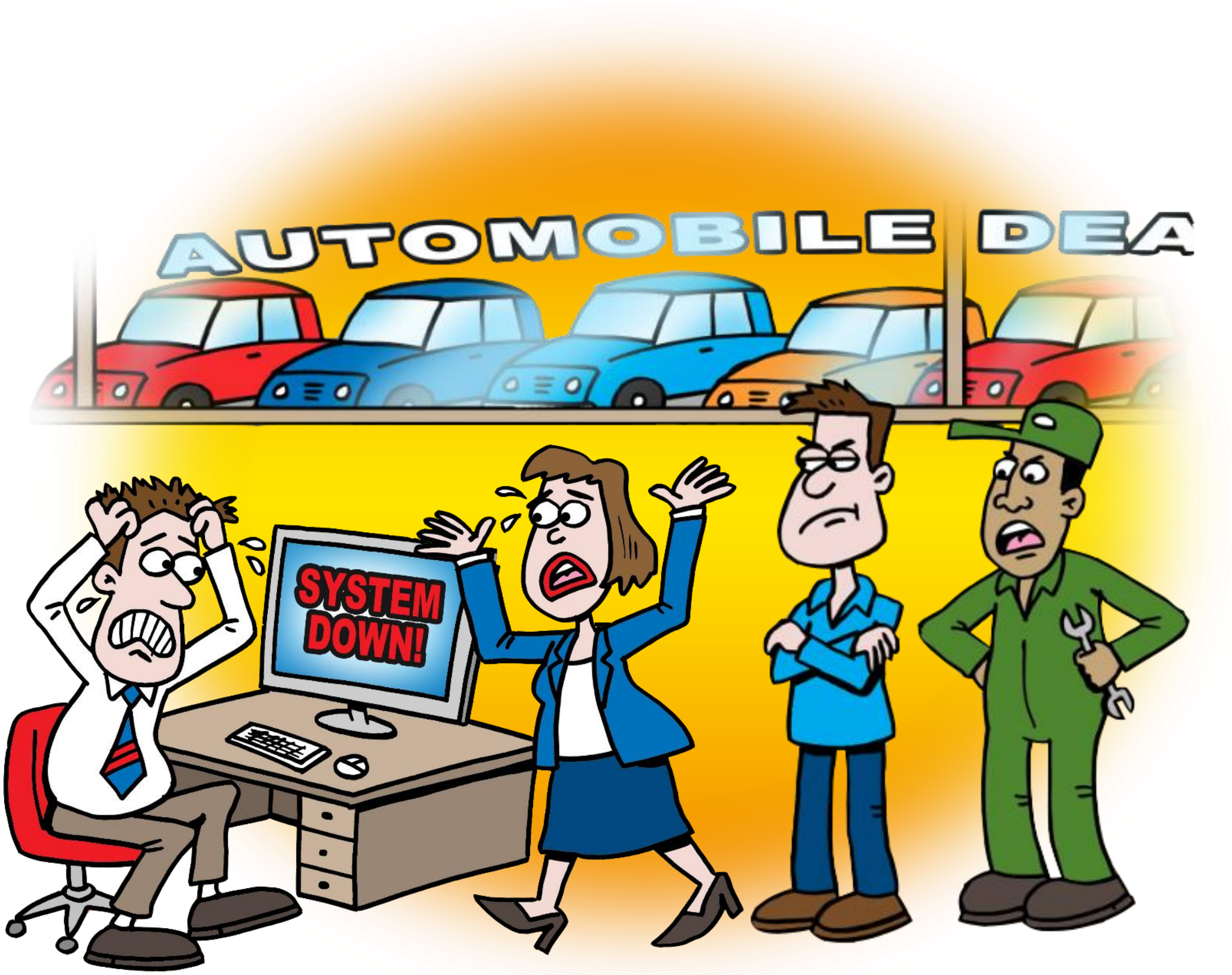
Don't Get Cyber-Clobbered

Cybercrimes happen to auto dealerships without warning.
Are you prepared?



HELION
AUTOMOTIVE TECHNOLOGIES

Putting Your Dealership in the *FAST LANE!*

Table of Contents

It’s a Dangerous World Out There, and It Wants Your Data!

As you read this, cybercriminals are probing your dealership networks from the outside – and perhaps more crushingly -- from within. They are waiting patiently to steal your customers' data and to pick-pocket their bank accounts--and yours.

These criminals look for weaknesses in data networks, often cobbled together from old technologies, outdated connections and weak access points: all of them poorly protected from hacking.

“It’s not a matter of *if* we’ll get hacked, but *when*,” says Chip Doetsch, President of Apple Ford-Lincoln in Columbia, Maryland.

“If that happens without something to stop the loss of my customers’ personal data, that’s a multimillion-dollar problem I can’t predict."

Which is why Doetsch has put in place the measures discussed in this whitepaper to secure his dealership’s data and protect its computers, website, Wi-Fi, and networks from cybercriminals.

Attacks in which sensitive and confidential information are stolen are increasing 6% year over year[1] according to the Ponemon Institute, an independent research firm. And, according to CNN Money, 47% of U.S. adults have had their personal information exposed by hackers.[2] Here's a small sampling:

- 70 million Target customers' personal information
- 4.6 million Snapchat users' account data
- Potentially all of eBay's 148 million customers' credentials
- 36 million members of the Ashley Madison web site

Auto dealers have also fallen prey to both malicious and unintentional network breaches, as evidenced in these recent headlines:

- **Employee downloads malicious code:** *Malware gets by anti-virus software, gains access to online credit app code and copies Social Security and credit card numbers from 200 customers before discovery, costing loss of credit-pull ability for weeks, for a $40,000 loss.*

- **Dealer admits internal breach:** *A former employee may have accessed customers' names, birthdates, addresses, phone numbers, Social Security numbers and driver's license information.*

- **Honda Canada e-commerce breach:** *Data breach accesses personal information from 283,000 Honda and Acura customers in Canada.*

- **Dealer falls victim to typosquatting:** *Accountant inadvertently visits bogus e-commerce site for dealership’s bank and sends a $450,000 wire transfer to phony website.*

For most dealerships, an in-house or outsourced IT "guy" isn't sufficiently equipped or prepared to provide the 24/7 data security protection that today's digital dealerships demand.

What Type of Data is Vulnerable to an Attack?

Can you define these terms? Brute Force, Command Injection, Backoff, KeyLogger, CryptoLogger and Typosquatting. No, they're not military maneuvers. These terms are just a few of the various types of spyware, malware, viruses and other malicious codes that threaten your dealership's enterprise.

Some threats intend to disrupt your e-commerce, frustrating every party that relies on secure and properly functioning networks, websites, email and Wi-Fi.

Other threats, driven by criminal gain and easy access to OPM – other people's money – scrape business networks for social security numbers, credit card numbers, bank account numbers, and driver's license data.

Specifically, the dealership data hackers are going after include:

- Information contained in deal jackets
- Service Repair Orders (ROs)
- Login codes for PCs and mobile devices that allow access to customer information such as credit reports, credit card numbers, copies of driver's licenses, vehicle insurance cards and social security numbers
- Customer bank account and routing numbers
- Dealership bank account and routing numbers
- Access to copiers and scanners that contain thousands of stored digital documents
- Physical access to accounting offices and computer/server rooms

THE DEVIL YOU KNOW

Experts say most privacy breaches are caused by insiders. Many of these are honest mistakes made by employees who are unaware of what they're doing.

However, 11% of security hacks are committed by malicious employees, notes a 2014 study by Identity Theft Resource Center (ITRC).

Protecting company data can be a difficult task, especially as the Bring Your Own Device (BYOD) movement grows. If you do not have the correct security tools in place employees who are looking to steal information can easily copy it onto a USB drive.

Thus, it's prudent to establish security protocols so all employees are aware of risks as well as possible penalties for violating those policies.

The Consequences and Costs of a Data Breach

The consequences of hacking can be especially costly for a dealership -- not only in money lost, but also in loss of consumer trust and confidence.

One of the biggest expenses dealers incur from a security breach is the cost to contact all customers and then manage and monitor their credit to ensure they are not adversely affected. If this happens to you, you can figure a cost of around $3 million per 100,000 customers.[3] According to the Ponemon Institute, the average cost per stolen record is approaching $200.[4]

Additional consequences include investigations, audits, lawsuits and possible FTC action for non-compliance with the Gramm-Leach-Bliley (GLB) Act and software copyright laws. Violations can add up to hundreds of thousands of dollars per incident.

Altogether, it's entirely feasible for a single data breach to cost $2 million or more.[5]

Dealers like Mossy Automotive Group recognize this risk. The group operates 14 stores in the San Diego market. Until a few years ago it managed its stores with an internal IT team that acquired its technical experience on the job. This is not an unusual scenario.

CFO John Epps says management recognized that its internal IT strategy was putting Mossy at risk.

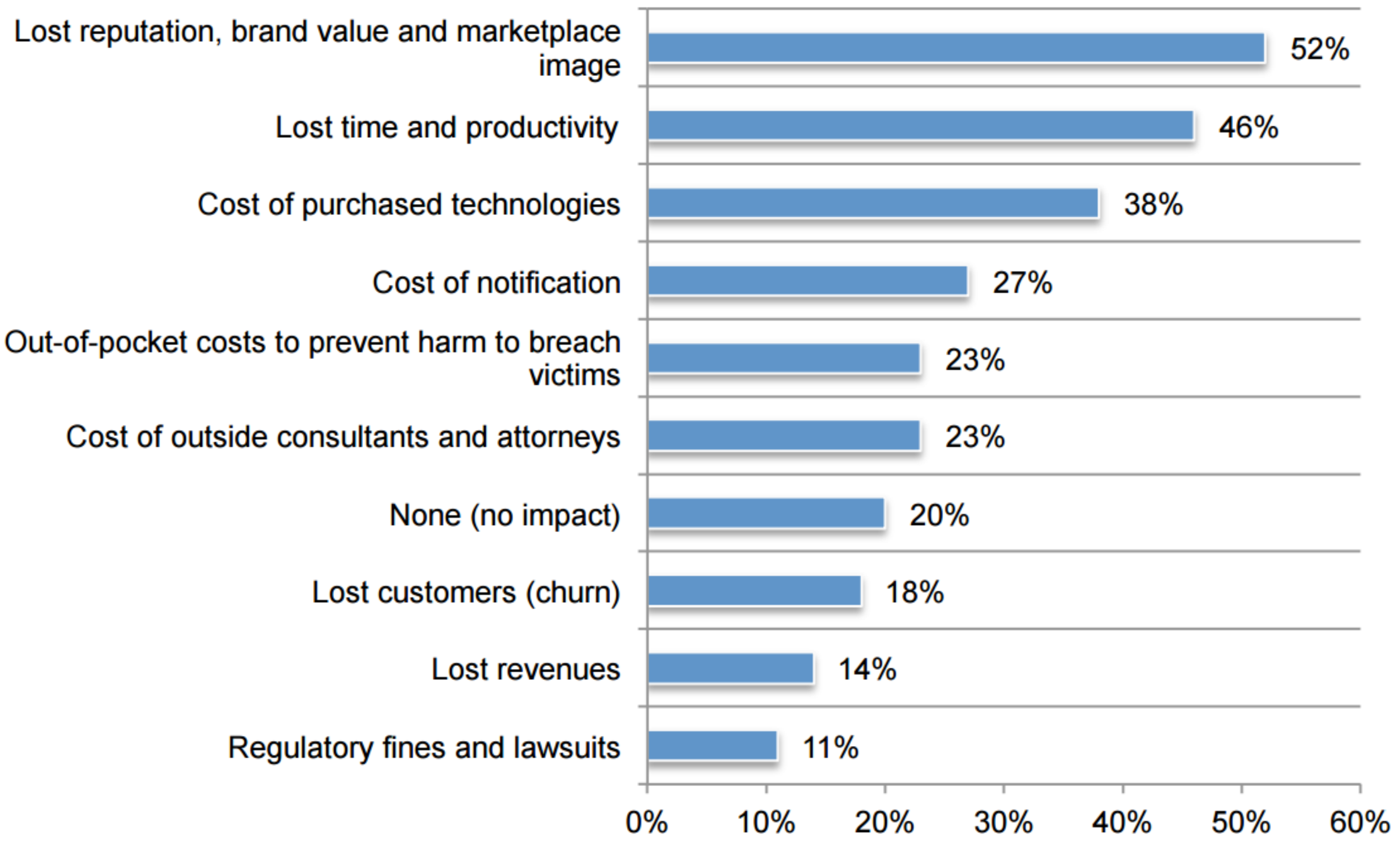
COSTS TO INVESTIGATE A BREACH AND RESTORE DATA INTEGRITY AND CONSUMER CONFIDENCE CAN REACH $2 MILLION OR MORE PER INCIDENT.

”We have grown to 1,200 employees using 1,000 or more PCs, who were often bringing their own devices like USB drives to work that could infect our network if we didn’t protect it,” Epps says

“We eventually turned IT and network security over to a managed services provider. They constantly analyze our networks, upgrade our systems and build in redundancies that give us a superior level of protection.

“We have lots of data - customer information, credit apps with all social security numbers, etc. - so we’re making sure no one can breach our systems and scoop thousands of records, which would cause damage to our customers and cost us a lot of money,” Epps says.

This chart from the Ponemon Institute illustrates the full list of consequences that victims of data breaches have reported:



You Need a Plan

Without a solid data security defense in place at your dealership, committed hackers (and even malicious employees) *will* get by your off-the-shelf firewalls, anti-malware and anti-virus software.

To fully protect your customers and your treasury, you'll want to have in place:

- Sufficient cyber liability insurance
- Excellent business practices
- Technology to prevent/deter hacking
- Plans/programs for recovery and remediation after a breach

Establishing a security plan is no easy task. The plan and its policies should be well documented, scrupulously implemented, and be:

- Approved by senior management
- Published and communicated to existing and new staff

- Readily available for reference and use
- Assigned to an owner responsible for updates
- Complete with provisions for disciplinary actions for noncompliance
- Reviewed annually
- Agreed to by all employees

HACKED COMPANIES WERE "HOPEFUL" THEIR SECURITY MEASURES WERE SUFFICIENT, BUT 65% FOUND ATTACKS "EVADED EXISTING PREVENTIVE SECURITY CONTROLS."

An effective IT security plan also addresses:

- Log-in, password, and access authorizations – some dealers almost never change them - best practice is every 90 days!

- Multiple or redundant or outdated software licenses – costing money or putting you at potential risk of software piracy

- Older, no-longer supported PCs, such as Microsoft's popular but now outdated XP operating system – patches and updates are no longer available

- Employee Training – educate staff on data security risks and their responsibility to protect the business and its customers by utilizing safe and proper data-management practices.

On the following pages are three sample security plans, presented in a Good/Better/Best format.

Level 1: Confidential

At a minimum, dealers should protect their computer systems and Internet connections using security-protection software.

Off-the-shelf varieties provide a fundamental defense from such productivity and security troublemakers as Phishing, worms, malware, spyware and Trojans.

Data security protection should also address the usage of physical media, such as USB thumb drives, DVDs, backup tapes and other devices used to store or transfer computer files. Employees should not be allowed to copy data onto physical media.

Passwords and access codes require protection security as well. Both employee and vendor access to the dealership's network should be secure with unique login IDs for all users, and prohibition on sharing login IDs. Likewise, your dealership's password policy should prohibit the sharing of passwords, require passwords to be entered at every login, and require periodic password changes.

Additional considerations include:

- Establish policies for securing data-rich targets such as deal jackets, service department documents, F&I documents, accounting documents and more.

- Recognize that copiers and scanners present unique risks. Today's digital machines contain thousands of pieces of private customer information. Handle documents carefully and when replacing your machines, be sure to have a data forensic specialist eliminate all data files.

- Secure the accounting offices and computer rooms. Some dealerships are beginning to restrict physical access into sensitive facilities through the use of security guards, electronic and even biometric access devices.

- Deploy closed circuit TV to monitor access not only to the dealership's lots, but also to computer rooms and internal access areas. Store that video for 90 days or more.

Level 2: Secret

As good as your internal IT people may be, many security risks are too big and too problematic for almost any dealer or dealer group – a stronger defense is necessary.

Ponemon Institute studies point out that while many attacked companies were "hopeful" that their security measures were sufficient, 65% found that the attack evaded existing preventive security controls.[6]

A defense built upon excellent security should also include:

1. **Focused organization:** Organize, structure and manage your IT systems as you do your cash flows.

2. **Reviews**: Review and communicate privacy and system access policies. Control if not ban the use of plug-in devices, especially those (including customers) brought from home or elsewhere.

3. **Intentional attacks:** Bring in an outside party to "hack" your system infrastructure to identify system weaknesses – it's not uncommon for such testing to uncover thousands of vulnerabilities on a dealer's network.

4. **Secure Wi-Fi:** Be sure to configure wireless devices at their highest encryption levels; set up separate wireless accounts for internal and customer use.

5. **Update computers:** Update PCs and other devices with all manufacturers' security patches and updates. They are designed to close identified security loopholes. Within days of Microsoft's retirement of the XP platform in 2014, the first attacks began to grab data from these machines.

6. **Set alarms:** Install an intrusion prevention system (IPS), which will prevent intrusion by malware such as CryptoLocker, which encrypts computer files making them unreadable – and ransoms access to files for a large "payment"; or Keylogger, which hackers place into an F&I computer where it transmits to the hacker every 3-digit, 2-digit, 4-digit keystroke pattern for Social Security numbers.

7. **Get help:** Evaluate the merits of a managed service provider to secure and monitor your network 24/7 and respond promptly and correctly to threats.

Also deploy the following *off-the-shelf* products:

Hardware Firewalls: Provide different levels of protection and protect all PCs on the network from hackers getting into the dealership's internal network. Hardware firewalls can also "block" internal departments from each other – for example; keeping human resources information away from other employees.

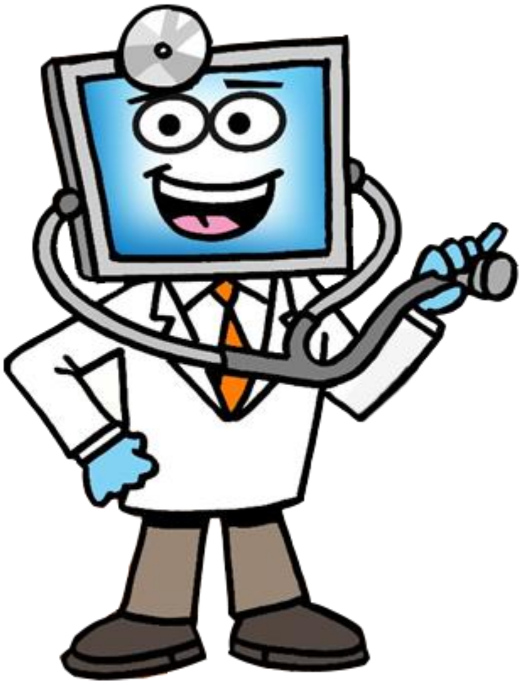
Software Firewalls: Provide security to all PCs at the dealership and protect employees while working offsite or from home.

Antivirus Software: Along with antispyware programs, this software should be running on every PC to look for malware, viruses, worms, Trojans and other malicious threats.

"IT'S NOT A MATTER OF IF WE'LL GET HACKED, BUT WHEN. IF THAT HAPPENS WITHOUT SOMETHING TO STOP THE LOSS OF MY CUSTOMERS' PERSONAL DATA THAT'S A MULTIMILLION DOLLAR PROBLEM I CAN'T PREDICT." –
CHIP DOETSCH, APPLE FORD-LINCOLN

Data Back Up: Prevention is key when planning how to protect your dealership data. If you are not regularly backing up, you could permanently lose financial records, customer records, employee files, leads – everything. Many dealers prefer to use outsourced back up services to handle this important security need.

Level 3: Top Secret



The best way to ensure that hackers can't get at your dealership data is to implement Professional-Grade security measures.

Apple Ford-Lincoln dealer Doetsch has in place the basic and best practice security practices already discussed, but also enforces:

- Wi-Fi and mobile device security, including separating public and private access
- Employee usage policies for business computers; prohibiting social media activities and disallowing public chat rooms and viewing of questionable and pornographic websites.
- Protection of consumer data contained on paper documents, such as customers' drivers license copies or deal jackets, that may be left in copy machines or in public view.

Professional-Grade Security measures also include:

Professional-Grade Web Filtering: Prevents access to sites that can be malicious. In many cases, hackers try to trick users into taking action in order to gain access to their PC. They create enticing messages encouraging users to click on a link that will trigger another action, such as downloading a file that contains a virus. Web filters improve dealership productivity by blocking sites that are distractions to employees such as social network sites, gaming sites and online shopping. Additionally, it also can block streaming services like YouTube, Netflix and Hulu to prevent employees from wasting time and to ensure that Internet bandwidth is not overwhelmed.

Professional-Grade Anti-Virus/Anti-Malware: Along with antispyware programs, this software runs all the time to look for malware, viruses, worms, Trojans and other malicious threats. Running antivirus software helps to protect a dealership's investment in equipment. Attacks can damage computers, software or infect a network and interrupt Internet service – slowing down, or even stopping, a dealership from running, costing time and money.

Professional-Grade Monitored Firewall: This device offers an additional layer of security, sitting between the dealership's Internet connection and the computers plugged into it. It ensures that outside machines are never able to connect directly to the dealership computers.

Firewalls are monitored continuously so security can be increased as needed.

- Statistically, most hacks could have been avoided if logs were monitored, as most hackers will probe a computer before they hack it.

- Firewall logs are constantly monitored to see what ports and services hackers attempt to exploit. This information is then applied to all computers to ensure they are secure from these exploits.

- The logs also provide forensic evidence for authorities should a data breach ever occur.

It is because of the ever-increasing security risk today that an increasing number of dealer principals and operating managers are engaging outsourced IT managed network services.

The Devil Gets In; Now What?

You always want the best protection you can find and afford.

Even so, creative hackers seem to run faster than counter-measure teams, so occasionally even “Fort Knox” gets hacked.

“You can be proactive, do everything right, use the best protocols, and monitor your network. But unfortunately, something can still happen,” says Brian Dunphy, Senior Managing Director at Crystal & Company, a New York-based insurance brokerage firm.

When you’re attacked, and if it’s discovered your data is compromised, call the police!

Next, notify your network and data security professionals and your cyber liability insurance team. They’ll investigate the crime.

Companies are now required to have a centralized logging system that is separate from all network systems. It must capture logs and keep a month’s worth of replay logs so that investigators can learn the following:

- Which IP address was used to gain access to the network
- The type of viruses installed and which computers they've infected
- Whether hackers cleared the logs to eliminate traces of their fingerprints

The cost to defend a breach can pillage a dealership’s treasury. Dunphy says typical recovery costs are $2 million, which a dealer can mitigate by having an **Information Security and Privacy Liability** policy.

“Information Security and Privacy Liability Insurance policies go a long way to respond appropriately to a data incident, by utilizing qualified counsel to provide proper resources needed to investigate the cause of a breach, prevent further damage, and notify individuals whose personally identifiable information may have been compromised," said Dunphy.

Data breaches and losses are not covered by traditional property insurance policies, Directors and Officers Liability policies, or business umbrella policies. Losses for damaged equipment, such as PCs, laptops and other “hardware” *are* covered by most property policies, but again, the data stored in them are not.

The alternative to insuring for data breach losses and related costs is to pay out of pocket and wrestle with the fallout for months.

The Solution That Lets You Sleep At Night

To thwart the ever-present threat of hackers, Mossy Automotive Group, Apple Ford-Lincoln and hundreds of other dealerships have chosen to outsource their IT security needs to a Managed Service Provider (MSP). These vendors remotely manage their customers' IT infrastructure, typically on a proactive basis and under a subscription model.

MSPs provide 24/7 monitoring of a dealership's network and computers, and offer a fast and thorough response to cyber threats and attacks. If you're considering an MSP, ensure they utilize security software designed for the finance industry, the most stringent and effective protection software and services.

"A provider like Helion Automotive Technologies, with as many dealers it services, is exposed to all the different issues and attacks dealers face, and they bring that experience to the table. We feel more comfortable with that breadth of knowledge to keep us protected," Mossy Automotive Group CFO Epps says.

"THIS SECURITY LEADS TO A MORE PREDICTABLE BUSINESS MODEL FOR WHICH I DON'T HAVE TO WONDER WHEN A $5 MILLION SHOE IS GOING TO DROP"
– CHIP DOETSCH, APPLE FORD-LINCOLN

For the Mossy Automotive Group, there is a concrete ROI from outsourcing its 14-store IT needs to Helion.

"Helion saved us more than $300,000 by advising us to switch data network and phone providers, and saved us another $100,000 by helping to streamline licensing and upgrade our PCs," said Epps. "It's difficult to put an ROI on the security as one data breach could potentially cost us hundreds of thousands of dollars. We believe the fact we have not had a data breach is worth a lot; not just in dollars but in peace of mind."

"IF SYSTEMS GO DOWN WE CAN'T WRITE SERVICE OR SELL CARS. HELION MAKES SURE OUR NETWORK IS SECURE SO THAT DOESN'T HAPPEN." – JOHN EPPS, THE MOSSY AUTOMOTIVE GROUP

"Our network is now monitored constantly, and our downtime has been virtually eliminated, which is absolutely essential for any dealership. If systems go down a dealer can't write repair orders or sell vehicles. It's critical that we have this real-time protection."

Dealers who recognize that data attacks can happen at any time say handing off prevention responsibility to an MSP is prudent management oversight. "It makes managing risk a more predictable business model so I don't have to wonder when a $5 million shoe is going to drop," says Apple Ford-Lincoln's Doetsch.

For more information or a complimentary assessment, visit Helion Automotive Technologies at www.heliontechnologies.com or call 443-541-1500 today.

Bibliography

[1]“Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels,” Company Press Release, May 27, 2015; http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html

[2]Jose Pagliery, “Half of American adults hacked this year,” CNN Money, May 24, 2014

[3]Erik Nachbahr, President, Helion Automotive Technologies, interview, July 2015

[4]“Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels,” Company Press Release, May 27, 2015; http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html

[5]Brian Dunphy, Senior Managing Director at Crystal & Company, interview, August 2015

[6]“Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels," Company Press Release, May 27, 2015; http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html