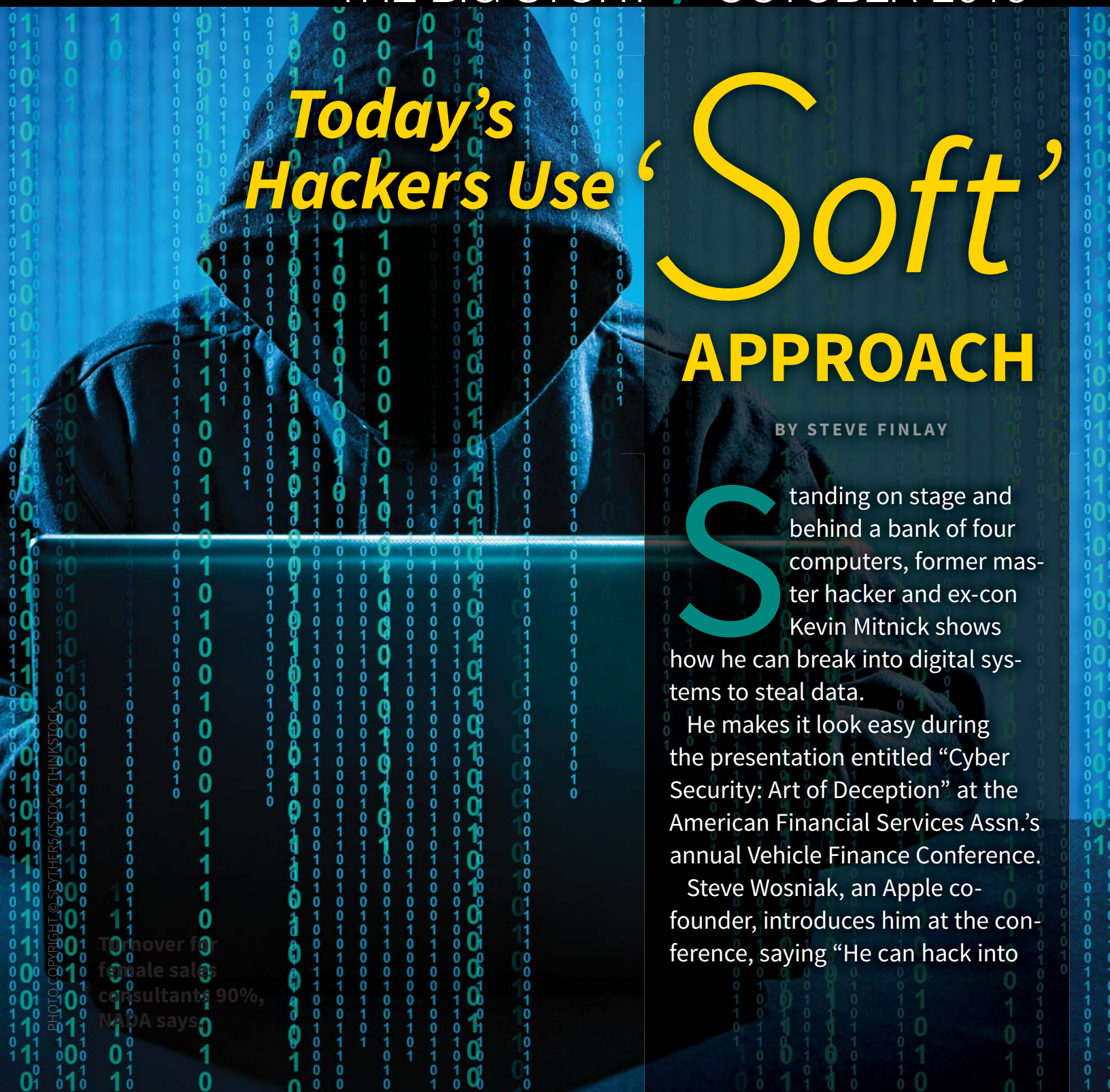
WARDSAUTO™

THE BIG STORY / OCTOBER 2016



Today's Hackers Use 'Soft' APPROACH

BY STEVE FINLAY

Standing on stage and behind a bank of four computers, former master hacker and ex-con Kevin Mitnick shows how he can break into digital systems to steal data.

He makes it look easy during the presentation entitled "Cyber Security: Art of Deception" at the American Financial Services Assn.'s annual Vehicle Finance Conference.

Steve Wosniak, an Apple co-founder, introduces him at the conference, saying "He can hack into

Turnover for female sales consultants 90%, NADA says

any system." For the next hour, Mitnick, who now runs a cybersecurity consulting firm, shows and tells how.

But few of his means of entry involve a blunt-force frontal assault. Typically today, with systems as secure as they are, hackers need help to get the job done. And often, the helpers are employees at a place of business who innocently become aiders and abettors.

It's enough for dealerships to take notice of who's doing what on the store's computer system.

"Ninety-nine percent of the time the hacking is done through an innocent human being who becomes a victim through things like phishing and malware," says Lisa Plaggemier, security director for CDK Global, a major dealership information technology provider.

HUMAN ERRORS THAT LET HACKERS IN

- Losing a laptop
- Plugging in a flash drive
- Opening a legitimate-looking email attachment
- Duped by a cybercriminal impersonating a colleague or vendor

"People think it happens to them, rather than them unknowingly doing something that allows it to happen," she says.

The better-than-bad news is that if most cybercrime threats to dealerships involve human error at the stores "I stress to dealers that's the easiest thing to fix through training and processes," Plaggemier says.

The unwitting human goof-ups include a dealership employee losing a laptop; plugging in a flash drive that allows a hacker to monitor every click and key stroke; opening a legitimate-looking email attachment that ends up spreading a malicious infection; and getting duped into giving sensitive security and financial information to a cybercriminal impersonating a colleague or

vendor on the telephone.

Studies indicate that those "soft attacks" by far represent the biggest cybersecurity threats, says Brad Miller, the National Automobile Dealers Assn.'s director-legal and regulatory affairs.

"Every expert in this field will tell you there is no impervious system," Miller says.

"I've had conversations with the FBI (cyber task force) on this," says Miller, NADA's point man on the matter. "These are the biggest security problems and most profitable area for the criminals across all industries: the efforts to gain information through what looks like legitimate means."

He adds, "It is not a blunt-force hacker who is breaching your system without you knowing about it. It is trying to get in through another door."

FRONTAL ATTACKS RARE THESE DAYS

The risk of an unaided frontal attack on a system is real, say cybercrime fighters.

But digital criminals use that battering-ram tactic less often, in part because system fortifications have become so strong.

"The automated systems have gotten so good," Miller says. "You may get in, but you won't be able to mess around in there for a long time.

"However if you get in through a soft method, you may be able to do damage for quite a while before people realize what's happening. A bad guy can do more damage that way."

Still, no one has yet to build absolutely hack-proof protection.

"Every expert in this field will tell you there is no impervious system," Miller says. He cites a financial institution that spent $200 million a year on cybersecurity, and still sustained a data breach last year.

A failsafe security system is something of a digital unicorn, say members of the defense team.

"We're doing as much as possible to prevent (a breach)," says Peter Ord, national sales director for DealerSocket, a firm that provides dealers with customer-relationship- and dealership-management soft-

ware. “We’ve mitigated it to the highest possible extent, but nothing is 100%. Hackers are hackers.”

Brian Allan agrees. He is director of business development for Galpin Motors, a dealership group in California. Of cybersecurity,

> SOMETIMES IT IS A QUESTION OF **AN ENEMY WITHIN,** OR A LARCENOUS EMPLOYEE.

he says: “Here’s what we know: Nothing is fool-proof.”

Sometimes it is a question of an enemy within, or a larcenous employee.

“A big scare is that the leak occurs on the dealership side,” says David Brotherton, a consultant for the National Independent Automobile Dealers Assn. “Employees have access to dealership computer equipment. Even if they can’t download something, they can write it down.”

But even the best of employees can cause problems. For example, diligent staffers using company laptops and mobile devices to do after-hours work can pose an unwitting threat. The threat of a hack attack increases if an employee puts sensitive information on a mobile device and logs onto a public Wi-Fi hotspot.

“Obviously, you want to make sure your system is password-protected, encrypted and secure,” says Miller. “But the biggest problems are things like lost laptops or folks sending information they shouldn’t over insecure emails. Those represent an ongoing effort dealers need to focus on in training and processes.”

Some major information technology companies such as Reynolds and Reynolds that provide dealership-management system software to dealers have expressed security concerns over dealers contracting with a third-party digital-service providers who, in turn, plug into the main system.

The fear is that the risk of a breach is increased when various third-party providers piggyback on

the DMS. One concern is of a potential domino effect that could occur if a provider gets hacked and the infection spreads to the DMS.

That said, dealers can feel reasonably assured their information is safe with an IT provider, certainly safer than if they were to keep it themselves.

"The risk is greater if data resides in the server at a dealership and the dealer has to provide both the physical and connectivity security for that data," says Sharon Kitzman, Dealertrack's vice president and DMS general manager.

"Because we are cloud-based, security compliant and have people monitoring our network and server against an attack or breach and defending ourselves 24/7, we take the fear away from the dealer."

DealerVault bills itself as the first cloud-based system designed to empower dealerships with control over the syndication and distribution of their DMS data.

DealerVault CEO Steve Cottrell says the 3-year-old company has put a lot of money into data security and "making sure our platform is secure."

Dealer Trevor Gile, a partner at Motorcars Honda in Cleveland Heights, OH, says, "I'd rather have a cloud-based major company protecting my data than me trying to do that. I feel way more comfortable having them do it."

> **THE RISK IS GREATER** IF DATA RESIDES IN THE SERVER AT A DEALERSHIP.

The cloud heightens security, but it's not infallible, Ord says. "Cloud is preferable but that is not to say there aren't risks with cloud. But it is much better than dealers storing the information themselves."

It would be bad enough if hackers break into a dealership's computer system and start helping themselves to proprietary information.

But the real jackpot would be the customer information that dealers keep. That often takes the form of confidential financial information, collected for credit-

application purposes. Armed with that, an identity thief would be off to the races.

"Dealerships become the meeting point for a lot of stuff," says one industry insider.

NADA's Miller says dealers do a pretty good job there. "They have had consumer transactional and relationship data for 100 years. Because of what they do, dealers get very sensitive and valuable information. Privacy is something dealers handle well, especially given the regulatory framework they work under."

GOING AROUND THE FIREWALLS

Still, cybercrime experts say auto retailing needs to focus on those soft attacks through the likes of so-called spear phishing (personalized emails with infectious attachments) and social engineering (collecting information about someone from social-media websites and the like).

Mitnick says if firewalls are too formidable, he'll simply opt to go around them.

"Why bother bypassing a firewall when I can persuade someone to give me their username and password?"

He tells how he does that. "Go to a company website and get contact names, phone numbers and titles. You don't even have to go to the website, just go to LinkedIn. I look for marketing and sales people, not tech types because they're too aware."

He then calls them, posing as a colleague, vendor or someone otherwise legitimate and talks them into giving him the digital keys to the kingdom.

Social-networking websites also contain information a hacker can put to ill-use, Miller says, offering this scenario.

"Your Facebook update shows you were in Las Vegas last week. Then you get an email saying 'Nice to see you in Vegas. Check out this attachment.'"

An unsuspecting recipient opens it. The computer is infected. The cybercriminal can track everything that person does, from keying in a password to entering a bank-account number.

"They are able to tie these

pieces together for spear phishing or to otherwise make their approaches more realistic-looking," Miller says. It is the social engineer, the spear phisher who is able to gain the trust of an employee to get information.

"What they want is money, whether it is by getting into your bank account to take it or tricking you into paying them," he says.

There are variations on that. A common one is they'll pose as a vendor, saying they have a new bank-routing number. They may even include a legitimate-looking phone number.

It's not like the old days when an illicit email from an alleged Nigerian prince wanting to share millions of dollars was rife with misspellings and other glaring signs of fraud.

Today's phishing emails look much more legitimate, even though their infectious attachments are as toxic as ever. Some are particularly alluring. "If the attachment says 'payroll 2016,' at least one employee will open it up to take a look," Mitnick says. "That's all I need, one employee."

Laptops have microphones and cameras, he notes. Hacked into a laptop, he can turn on the webcam. "I can see who I hacked."

Dealership employees in the front office are particularly vulnerable to a spear phishing attempt, Plaggemier says.

"Spear phishing emails are sent with a specific goal," she says. "A cybercriminal goes on a dealer website and finds out who the office manager is.

"That person is sent an email that looks like an order confirmation for something she didn't order. She clicks the attachment to cancel it, and the hacker ends up getting into a bank account."

Dealers are vulnerable to cybercrimes because of the nature of their business. They are technically considered small businesses but they're big-small.

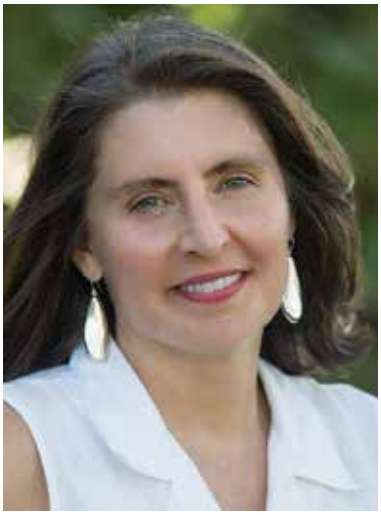
"Sixty percent of all attacks are on small businesses," Plaggemier says. "If someone is going to target a small business, it probably won't be the local clothing store. Dealers are the more likely targets because they employ a lot of people, have a high staff turnover and

have a lot of operating money."

WHAT'S A DEALER TO DO

What can a dealer do?

"You just have to raise the level of awareness," Miller says. "It's a cat-and-mouse game. It is doing the reasonable things, getting technical pieces in place – such as firewalls and intrusion-detection software that stops the virtual attacks – and then just being smart.



"People think it happens to them, rather than them unknowingly doing something that allows it to happen," says CDK's Plaggemier.

"There are technical fixes to implement, but it is also being aware of this stuff, spotting the red flags and knowing what to do."

Plaggemier's CDK duties include serving as a "client advocate" to help dealers understand cybercrime risks and know what precautions to take.

She periodically speaks to groups of dealers on how they can protect their computer systems.

Her advice ranges from training employees how to spot malicious material to having a process to make sure staffers who leave the organization cannot continue to access the system. Amazingly, many of them are.

"It's people, processes and technology," she says in describing the best way to thwart the hackers of the world.

Do dealers she meets show a healthy concern or a disturbing apathy towards cybercrime?

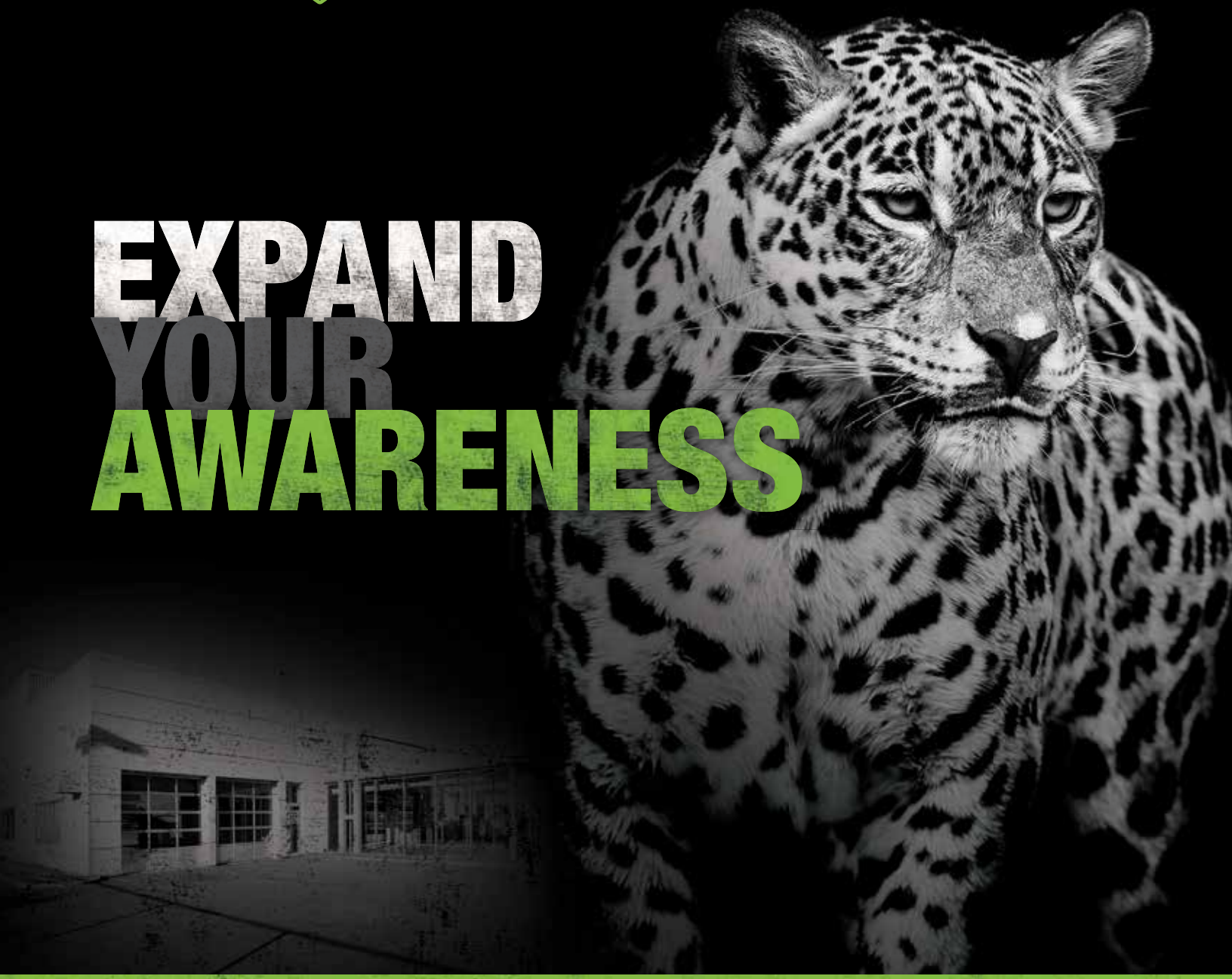
"They definitely are concerned," Plaggemier says. "A dealer told me a vast majority of them have experienced some sort of security issue. But it is not something they like to talk about a lot."

She grabs their attention when she gives real-world examples during her group presentations. "If I have six or seven dealers afterwards come up and talk to me about it, that's a good sign."

Mitnick says his hacking was just for fun. The tomfoolery ended after the FBI sent him to prison. "Being a fugitive? I've been there, done that. It's no fun."

Most hackers are in it for more than just a lark, whether they are from the U.S., China, Russia or sub-Sahara Africa. "They want your money," Miller says. **WA**

CDK SECURITY 1ST



EXPAND YOUR AWARENESS

$5.9M IS THE AVERAGE COST OF A DATA BREACH*

WHEN IT COMES TO CYBERSECURITY, IT'S A JUNGLE OUT THERE.

In this jungle, your reputation is everything. When you partner with CDK Global, we'll help you protect your data, financials and reputation by providing the expertise, partnership and industry-specific support your business needs.

PUT SECURITYFIRST WITH CDK GLOBAL AT WWW.CDKGLOBAL.COM/SECURITYFIRST

CDK Global®

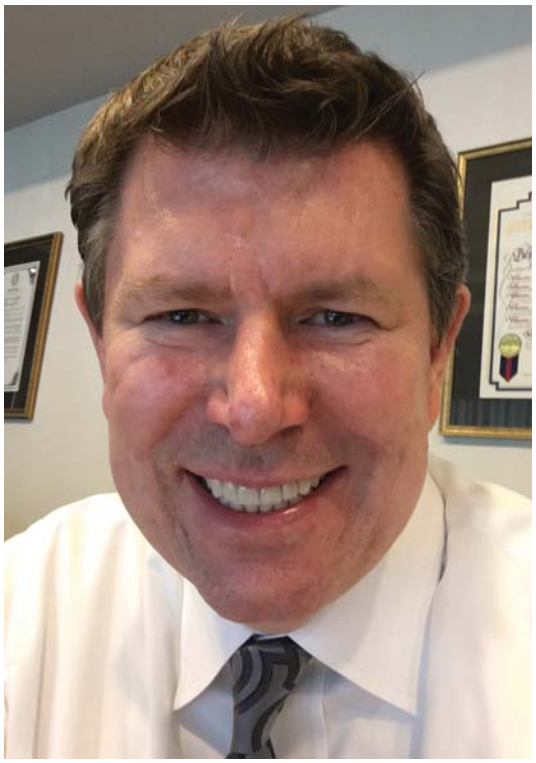
Evolving the Automotive Retail *Experience*

 *Source: "Security Risk," *F&I and Showroom,* February 2015

Show You're Trying, Says Dealership Executive

Part of an effective dealership cybersecurity plan is showing you care, says Brian Allan, business development director at Galpin Motors, a Southern California automotive group that includes the world's top-volume Ford store.

He talks with *WardsAuto* about how the company systematically defends itself against system hackers and their ilk.



> HERE'S WHAT WE KNOW
> **NOTHING IS FOOL-PROOF.**

GALPIN'S
BRIAN ALLAN

WardsAuto: Cybersecurity for dealers involves protecting their information and their customers' information. Your dealership is one of the biggest in the world. How do you do it?

Allan: Galpin has a full compliance department. That includes part of our legal team and compliance coordinators. We've set up what we call a safe-harbor system where you take all the guidelines and instill a process to check those. We have monthly reviews, looking for areas of concern.

The biggest advantage a dealer can have today is to have a compliance system that is a documented process that shows you are trying to do the right thing.

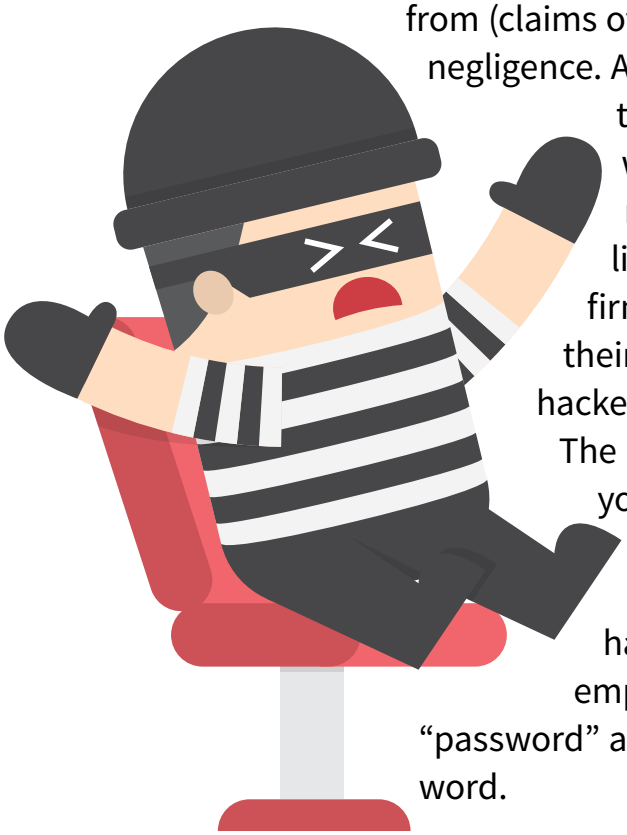
WardsAuto: What would be a couple examples?

Allan: In the cyber end, it involves password issues. We do password audits. Now, the passwords are more difficult, but also where different machines are utilized, they are turned off with no activity. It's having those

check-the-box compliance elements that help insulate you from potential fines or even criminal action.

WardsAuto: Worse case, a hacker breaks into your system and gets all sorts of information on customers.

Allan: Here's what we know: Nothing is fool-proof. But if you at least show the due diligence, that you made every reasonable attempt to protect that data, you are pretty much protected from (claims of) gross negligence. And that's the key. As we know, multi-billion-dollar firms can get their accounts hacked.



The key is that you didn't do something stupid, like having every employee use "password" as their password.

WardsAuto: Galpin seems like it is run like a corporation.

Allan: Absolutely.

WardsAuto: So presumably you really have a defensive strategy.

Allan: We do. Of course, every system will have weaknesses that are just part of the human link. Oddly, humans are the problems when it comes to cybersecurity. You have to have faith in your employees, but it's like the old adage, "Trust but verify."

Again, a documented process will give you the best possible protection, recognizing that nothing is 100%.

WardsAuto: Is this method of defense something you set up as a response to a hack attempt or breach or was it more proactive?

Allan: It's more learning from others' mistakes. That's the cheapest way to learn. It's keeping up to date on bulletins, what's happening, where are areas of weaknesses that others have experienced and then mapping out a protection plan to insulate yourself. **WA**

– Steve Finlay

10 WAYS DEALERS Can Live in a Safer Cyber World

Cybersecurity experts recommend dealership personnel take these precautions, among others, to fight hack attacks and protect data:

1 **Do not allow employees to take home sensitive customer information** that's contained on laptops, memory sticks or the like. Despite the best intentions of devoted staffers working after hours, that practice runs risks. Increased use of mobile devices can infect a dealership network if they are taken off site and connected to insecure public Wi-Fi hotspots.

2 **Dealership Wi-Fi networks should be segmented** into in-store hotspots from the main network to thwart such cross infection.

3 **Understand applicable regulations**, in particular the Gramm-Leach-Bliley Act and the Federal Trade Commission's Safeguards Rule that require dealers to protect collected customer information.

4 **Understand security risks**. Consider having a network assessment done to probe for weaknesses so you can remediate.

5 **Educate employees** not to share passwords or other confidential system information with anyone. Monitor employee computer use.

6 **Put in place policies and procedures**. That will reduce potential threats. If everyone knows it's inappropriate to take home customer information, it turns everyone into human firewalls.

7 **Change passwords regularly** and have stronger passwords then, say, dealer1234.

8 **Click on anti-virus protection** for PCs, including updates. "Those updates typically are to fix security vulnerabilities, although they don't say that," says Lisa Plaggemier, CDK Global's director-business security.

9 **Scrub systems** of user names and passwords of former employees. Don't just get the front-door keys from them, get them out of the system.

10 **Be on the lookout** for phishing emails in which cyber crooks pose as legitimate companies. Opening an attachment that claims to be a payment or invoice can infect your system.