Protecting Your Dealership
Tools to build your cyber defense
Understand Cybercrime Risks

The threat from cybercrime today should put us all on alert. Cybercriminals have one goal: breaking into businesses like your dealership to prey on your employees, compromise your data, and ultimately tap into your accounts.

Cybercrimes are multiplying at an alarming rate. Yet, in a February 2017 study by IBM Resilient, 71% of businesses said their organizations were not prepared for a cyber event.

At Bank of America, we want to help you understand the risks and take important steps to prevent cybercrime.

The most effective approach to protecting your dealership starts with you. Too many executives view cyber fraud prevention as the job of the IT department alone. Addressing the cybercrime threat demands a change in overall strategy and business practices, and this requires executive leadership. The stakes are too important: your money, your reputation and your employees’ well-being are at risk.

We know that a dealership is only as secure as its weakest link, and that you must educate your entire staff — from the F&I team to the fixed ops crew — to be alert to possible threats.

In this article, the Bank of America team offers a big-picture look at fraud today, and a glimpse of the specific dangers to dealerships. Because we know the issue can seem overwhelming, we have also gathered ideas for some pragmatic, step-by-step ways to begin tackling the problem.

Cybercrime isn’t a topic that will go away. But in an uncertain world, the Bank of America team is here to help you harness the power and the resources needed to effectively address cyber threats and secure your business.
Outlaws in Your Inbox

Email fraud costs businesses billions... and all it takes is one click

The stories are in the news every week, with ominous words in their headlines: Cybercrime. Phishing. Hackers. Spoofing. Ransomware.

In 2017 alone, $5 billion was lost to criminals holding corporate systems hostage with ransomware — a tactic that’s grown exponentially, according to Cybersecurity Ventures estimates. And hackers were busy in 2017, perpetrating data breaches that exposed more than 3 billion personal information records, 6 billion email accounts and more than 2 billion Facebook accounts.

*Cybersecurity Ventures
Cybercrime attempts against businesses are surging, whether it’s criminals trying to penetrate your dealership’s payment systems or ransomware covertly installed that locks up your data, crippling operations. Auto dealerships — with large transaction amounts, expensive inventory and a network of third-party vendors — are a prime target.

The bottom line is that your business success and profits depend on your ability to protect yourself from cyber attacks. Many of these bad actors are not always just lone hackers but can be organizations, says Mary Rosendahl, director of Global Employee and system compromise. Cybercriminals will try to gain access to a company’s employees and information. Then they will either work to get into the payment system to send a wire or automated-clearinghouse payment for a fraudulent transaction, or they will try to trick an employee into wiring a payment to a fraudulent bank account.

Two key types of cybercrime

1. Employee and system compromise
   Cybercriminals will try to gain access to a company’s employees and information. Then they will either work to get into the payment system to send a wire or automated-clearinghouse payment for a fraudulent transaction, or they will try to trick an employee into wiring a payment to a fraudulent bank account.

2. Ransomware attacks
   Cybercriminals often will try to look for a way to install ransomware onto a company’s computer system. The software encrypts a user’s important files and documents, making them unreadable, until a ransom is paid. In 2016, victims of this type of fraud collectively paid criminals $1 billion, according to the FBI’s Internet Crime Complaint Center.

90% of these attempts come through phishing emails directed at a company’s weakest link: its users, who often are unaware and unprepared, says Rosendahl.

"There are illegitimate companies located all around the world — with research departments, writing departments — who use the dark web," Rosendahl says. "Committing fraud is their business model." Two key types of cybercrime are typically being attempted, she says.
“The most dramatic increase has been in the area of business email compromise,” she says. “If I’m a bad actor and send out a horde of phishing emails to companies and trick just one employee at one company to change a payment account number or wire money to a fraudulent account, I’ve succeeded.2

At an auto dealership, this type of fraud often arrives as a fake email that appears to be from a senior executive of the dealership — asking for urgent help, including wire transfers. Or it might be a message in which an outside vendor’s email address is being spoofed. Typically, the cybercriminal is trying to get someone in the company to click on the email, respond to the request and either alter information to redirect payments to the cybercriminal’s bank account or outright wire money to the perpetrator.

Cybercriminals may also use email messages containing ransomware. Unless monitoring technologies are in place, when a user clicks on the message, a link in the message, or an attachment to it, the software is installed on the computer system. Files throughout the network may be encrypted, making them inaccessible. The term “ransomware” was created because criminals increasingly are demanding a ransom from business owners to remove the restrictions or provide a key to decrypt the files and return to normal.

“If you don’t educate your users, just one person — any user on your network — can click on a link or an attachment and can freeze the computer code of the entire company,” Rosendahl says.

Besides malicious emails and malware, many experts who follow trends in cybercrime worry about a third, emerging threat to a company’s systems: the “Internet of Things” — the connections of everyday devices such as cars and appliances to the Internet. For instance, a thermostat, security camera or printer connected to the Internet might be a vulnerable spot from which a criminal could attack the entire computer network of a business.

“Seventy percent of the devices in the marketplace are prone to attack because they don’t have good security protocols,” Rosendahl says, citing industry data from Inverse.com. “These types of Internet-connected devices are becoming more commonplace in businesses. Until consumers and businesses demand security on these devices, we are going to continue to see Internet-connected items with no ability to upgrade the software or with ineffective administrative controls.”3

The good news in all this, she says, is that most cybercrime problems occur because of simple employee carelessness or unawareness, both of which can be addressed with ongoing education.

Our primary goal is simply to raise awareness to the critical issue about cybercrime and other cyber threats. “These criminals’ actions are premeditated,” Rosendahl says. Cybercriminals might target emails at employees at the beginning of the day before the first cup of coffee or the end of the week, for instance, when people are rushing around, they may be less focused and become complacent to cyber threats.

“Dealerships should have good, strong educational awareness to let employees know the risks in email fraud — to not click on links or attachments, not to respond to a suspicious message and to verify information. In addition, every dealership should have its important information regularly backed up, install security patches and run security scans to see where the computer system is vulnerable.”

But even setting up employee awareness training is not necessarily enough, Rosendahl warns. Even when businesses commit to an education program, she says, training is not conducted often enough to keep up with new threats — and ineffective or boring videos may discourage employees from completing the training.

3https://www.inverse.com/article/22815-iot-dyn-hack
Rosendahl’s first suggestion is that business owners work with partners including their financial institutions, using the most advanced awareness and training opportunities to keep abreast of emerging threats. In addition, they should consider conducting periodic security audits of their information networks. The time to start, Rosendahl says, is now.

Lack of cybercrime preparation can expose you to financial loss, operational shutdowns and reputational risk.

Why are email-based attacks successful?

In an estimated one in four attempts, according to the FBI, email-based attacks are successful—for two reasons: the targeted company is unaware or employees have been inadequately trained. Businesses and employees need to be alert to these types of requests, and unexpected or non-standard requests for changes need to be verified via an out-of-band method—that is, a secondary verification through a separate communication channel in addition to the typical ID and password.

1
Messages appear to be authentic
- Information is well-researched, using the Internet and social media sites.
- Messages use the right names, correct titles and other corroborating information.
- The fraudulent domain names are similar enough to escape notice.
- The messages are custom-written to avoid spam filters.

2
Messages appear to come from a senior executive in need of immediate action
- The messages exploit the natural human tendency to be helpful, especially to a boss or supervisor.
- The messages sometimes are sent when the executive is on vacation, making it more plausible that the executive would use a different email or unknown domain name or have an unusual request.
- Messages might be sent during a transitional time for the company, taking advantage of uncertainty in leadership, policies or organization.

3
The company lacks policies and controls to prevent fraud
- The company does not use a dual-signature or sign-off procedure for payment instruction changes or payments that deviate from normal processing procedures.
- Despite the policies, an employee is duped into ignoring the procedures in the interest of time and efficiency or does not want to make a boss or superior angry.

4
The company’s technology setup lacks security safeguards
- The company does not use data encryption.
- The company’s email gateway does not use technology to identify and filter suspicious messages and users.
- The company does not use controls such as endpoint security, which protects a corporate network when accessed using remote devices such as laptops.
How Vendors Can Supply Crooks

Barring entry into your dealership

Auto dealerships work with a variety of vendors, which can create new avenues for cybercriminals to attack the business.

First, someone posing as one of your vendors might try to trick your financial department into sending funds. Typically, the perpetrator will send a message asking you to change the vendor’s account profile or payment instructions. **The message can be delivered via email — with a slightly modified email address to mislead the recipient — or by postal mail, with contact information for the cybercriminal instead of the vendor’s company.**

Usually, the requests are inconsistent with established protocols. For instance, the “vendor” will ask the dealership employee to change his company’s profile, address or bank information in the dealership’s database. Or the email might ask the dealership to change the name of the contact person for the vendor. Typically, the message or letter will include a request for a confirmation email when the changes are completed.
Second, if one of your vendors’ technology or payment systems is compromised by a cyber attack, it also could affect your business if you haven’t put in place the proper controls, security and liability agreements.

The best way to protect your business is to institute procedures to check and verify vendor information, to keep that information up to date and to limit the ways that vendors can access your company’s data.

“Every vendor you do business with is an extension of your business to some degree,” says Mary Rosendahl, director of Global Digital Channels Security, Fraud Education & Risk Management for Bank of America Global Transaction Services.

“Cybercriminals look for backdoors to attack businesses. As you think about fraud protection, you need to install a strong vendor management program.”

A dealership should deem creating a cyber security plan as important as installing an on-site security system on the lot.

---

Security best practices when working with vendors

Establish a written procedure for adding a vendor to your system.

Create a vendor profile form that verifies the vendor company’s proof of existence by checking product catalogs, federal tax returns, sales tax certificates, recently audited annual reports, city or county business licenses, and 1099 or W-9 tax forms.

Organize vendors into folders based on their specialty or business.

Categorize past and future payments on a month-to-month basis.

Apply standard rules for names and addresses.

Ask for a W-9 form from each vendor in advance of any payments being issued.

Create a schedule and make sure to perform regularly scheduled maintenance of vendor records and files. Keep the files up to date.

Allow vendors access only to data required for their business with you.

Verify any requested changes to vendor names, contacts, addresses or payment information via a separate communications channel — make a phone call, send a letter or have a colleague create a new email message from a different computer to validate any changes.

Ask the sender for confirmation in the form of old payment instructions and accounts or by printing the new payment instructions on company letterhead.

Verify the letterhead when it arrives.
Something Smells Phishy
Steering clear of email cybercrime

Picture this scenario: While your dealership’s owner is on vacation, the assistant treasurer receives an urgent email. It looks as if it’s from the dealer/principal; the message uses his name and what appears to be his email address. It contains details that make it sound authentic: it refers to his vacation plans and addresses the employee by name.

The message looks legitimate. And of course the employee wants to help — it’s the boss! Before consulting with anyone else, the assistant treasurer wires the money to the account listed in the message.

And just like that, the money is gone. The dealership has just become the victim of an email spoofing cybercrime.

Dealerships face a variety of cybercrime risks, and because of the nature of the auto business, the treasurer’s office is a prime target, says Sue Caras, Treasury Sales Executive for Bank of America Dealer Financial Services.

“Dealerships are vulnerable and often targeted because, despite relatively high dollar sales, many dealerships operate like small businesses,” says Caras. “Dealerships move a lot of money with relatively few transactions. But because a lot of dealerships feel like a family business, often they don’t necessarily have the controls of a larger company.

“They have, as you might expect, a lot of trust in their employees. And they also don’t necessarily have the controls of authentication that a big corporation might have.”
While there are many common cyber risks across industries, Caras says, “What’s unique to dealerships is that family-business feel and also the titled nature of the vehicles — which leads dealerships to use the wire system more for payments.”

“Dealerships can also be vulnerable because there’s a lot of money moving in and out. A lot of money can build up on the weekend; if you sell five Mercedes on a weekend, you might have $500,000 in the system.”

Cybercrime attempts aimed at dealerships usually take three common forms: payment fraud via email spoofing, forged treasurer’s checks and fraud resulting from the use of the automated-clearinghouse system. Because you can’t transfer the ownership of a vehicle without a title, most vehicle transactions are conducted using either a wire payment or treasurer’s check — both regular targets for cybercriminals. Caras says business email compromise is the most common fraud tactic in the industry today. The criminals typically use bogus email messages — such as the one at the start of this story — to persuade an employee to wire money to a cybercriminal’s bank account. But in the past year, Bank of America also has seen several instances of dealerships losing expensive vehicles because they accepted forged treasurer’s checks. “Once the car leaves the lot,” Caras says, “it’s very difficult to get it back.”

The third way that cybercriminals target dealership money is through the national automated-clearinghouse system. ACH is used to transfer funds electronically between companies and individuals, usually for routine payments in established business relationships. “What we are seeing is that the speed of ACH transfers has accelerated over the past year because of same-day ACH transactions,” Caras says. “It’s a really good thing; it’s what customers have asked for. But what it also means is that a business has less time to reconcile accounts and identify fraudulent transactions.”

One type of ACH fraud involves convincing a business to redirect funds meant for a third party, like a vendor, into a cybercriminal’s bank account instead. The perpetrator will email the dealership asking to change the information in a vendor’s payment profile — the street address or bank account information, for example. That small change can mean that a vendor’s printed check is mailed to a cybercriminal or that a vendor’s electronic payment ends up in someone else’s bank account.

A second type of ACH manipulation occurs when a cybercriminal gains access to a business’s bank account information and initiates a debit from the business to a new account. Bank account numbers are surprisingly easy to acquire — they are included on every printed check.

The ACH debit might come through with a vendor name or the name of a made-up government agency that looks legitimate. It’s often a small amount of money at first, in hopes of not attracting attention. “It might be a payment to something you’ve never heard of, but it’s a small amount of money,” Caras says. “That’s a test. If you don’t catch it, the amount might be larger the next time. And then often if you’ve seen the name a couple of times, you might not think anything of it.”

Most often, dealerships are going to block these fraud attempts, she says. “But if a $10 payment goes through, the cybercriminal realizes people aren’t paying attention — and he or she is going to try again,” Caras says. And before long, the payment amount can be significant. “The common denominator in all of this is that cybercriminals are always looking for weakness,” Caras says. “They try to manipulate employees and steal information. That is how it always starts.”

Once a cybercriminal has breached the system or gained an employee’s trust, the information can be used against the dealership, almost inevitably to get money. First and foremost, Caras says, “The best thing you can do for your dealership is to start having a conversation about possible fraud and how to prevent it. Prioritize your risks, get your staff educated and take it one step at a time. Remember that it’s not a one-size-fits-all solution, either.”

Many dealers say they are frustrated and overwhelmed by the issue, Caras says. “They say: ‘I don’t know what to do, so I’m not going to start. I can’t take the time anyway.’ That’s a mistake,” Caras says. “It’s almost impossible to go from being unprotected to being fully protected overnight, but it is critical to keep making your systems better, because cybercriminals keep getting better at stealing money.”
You Protect Your Car Lot. Why Not Your Computers?

The first step in preventing a cyber attack through the computer network of your dealership is to make a plan. Many businesses wait to address cybercrime until after their systems have been compromised or they lose money to a cybercriminal. “Often businesses are more reactive than proactive,” says Caras. “They wait to do something until they have a problem or hear about fraud at another dealership.” Given the increase in fraudulent activities, Caras recommends that a dealership deem creating a cyber security plan as important as installing an on-site security system on the lot. “It helps to have a conversation with someone who has experience with the sorts of problems your company might encounter — who can ask the right questions and help prioritize the risks,” Caras says. No one plan is right for every dealership; specific advice might come from a financial services company or a security advisory firm. Here are some starting points to consider.

Cybercrime prevention checklist
Cybercrime is a growing threat to dealerships. Follow these suggestions to protect your business, employees and assets.

✔ Protect your data
  • Develop a data storage plan and policies for data retention, privacy and disposal that extend across your entire organization
  • Be wary of any requests for information about customers or employees
  • Regularly back up digital information and data, and check to see that departments with their own databases and information collections are similarly performing backups

✔ Keep your systems safe and up to date
  • Install security solutions (e.g., firewalls, anti-virus, data loss prevention (DLP)) and control employee access to the Internet from your business network
  • Create a software management plan including checking for software updates, updating anti-virus software, and installing software patches on a regular or as-needed basis

✔ Arm your employees to recognize and handle potential cybercrime
  • Conduct employee training for potential cyber risks and attacks, including how to recognize a phishing email and understanding the potential consequences of opening and clicking on malicious links or attachments
  • Teach employees how to protect the organization with smart password management
  • Test your staff on a regular basis by sending out fake phishing emails
  • Raise awareness to the latest trends of cyber risks and threats

✔ Create policies to support cybersecurity
  • Establish data protection policies for employees working off site or at home — policies for using data and also for disposing of any information
  • Institute a clear policy for professionals bringing their own devices — tablets, phones, laptops — into your dealership, and especially when they use those devices to access customer data
  • Make two approvals a requirement for any significant financial transaction, including initiating payments, changing vendor information and creating user accounts

✔ Keep your vendors on the same page
  • Review your vendors’ own cyber security policies. Require notification if your system or data is impacted by a breach of their systems
  • Carefully evaluate the potential security risks when new systems and apps are introduced
  • Do not allow vendors to dictate how data is used, backed up or protected

✔ Be prepared for a fraud event
  • Construct a plan to deal with cyber fraud events, ransomware and other attacks that may impact the network and make your systems or data inaccessible
  • Conduct tabletop exercises that simulate a cyber attack, and evaluate the results

✔ Stay informed
  • Keep updated on the newest types of cyber threats and criminal activity by reading trade publications and business news
  • Keep in touch with partners, like Bank of America, who have a global view of fraud across markets and industries
  • Attend webinars and roundtables
  • Share information with your peers
THE POWER TO

turn corners

Navigate changing conditions to move your dealership forward. That’s how we’ve been helping businesses like yours succeed for more than 90 years.
Dealer Financial Services from Bank of America.

What would you like the power to do?®

bofaml.com/dealer