CDK GLOBAL

Cyber Liability Insurance

WHAT YOU NEED TO KNOW

cisco SECURE

This e-book was created in partnership with Cisco and CDK Global.

CONNECTIONS THAT MOVE YOU

IT Solutions / Digital Sales / CRM / F&I / DMS / Fixed Operations / Intelligence

Table of Contents

Cyber Liability Insurance: The Basics

Cyber liability insurance can be a lifeline in the event of a major incident or breach. Cyber incidents rose 35% in 2020 alone with data breaches costing $4.24 million per year, resulting in cyber insurance premiums jumping up by 50-100%.* Modern challenges like phishing, ransomware, remote workforces, stolen credentials and personal devices demand increasingly sophisticated cybersecurity practices. Dealerships must secure themselves against unknown, advancing threats while striking a balance between proactive and reactive measures. No doubt, cyber insurance is a hot topic right now. Do you need it? How do you qualify for it? How much will it cost?

Cyber insurance is a necessity for dealerships big and small to mitigate losses from data breaches and other attacks. It's no longer a question of should you buy cyber insurance and what does it cover — it's how much of this insurance should you buy. And what security practices do you need to put in place to qualify?

*SearchSecurity 2021

Cyber Liability Insurance Overview

Loss or destruction of data

Damage to software/hardware

Extortion demands from bad actors

Breach incident response and crisis management

Legal claims for defamation, fraud and privacy violations (third-party coverage)

How Cyber Insurance Helps

Software exploits* continue to be the leading cause of data loss. Some of the things cyber insurance can do for you in the event of an incident are:

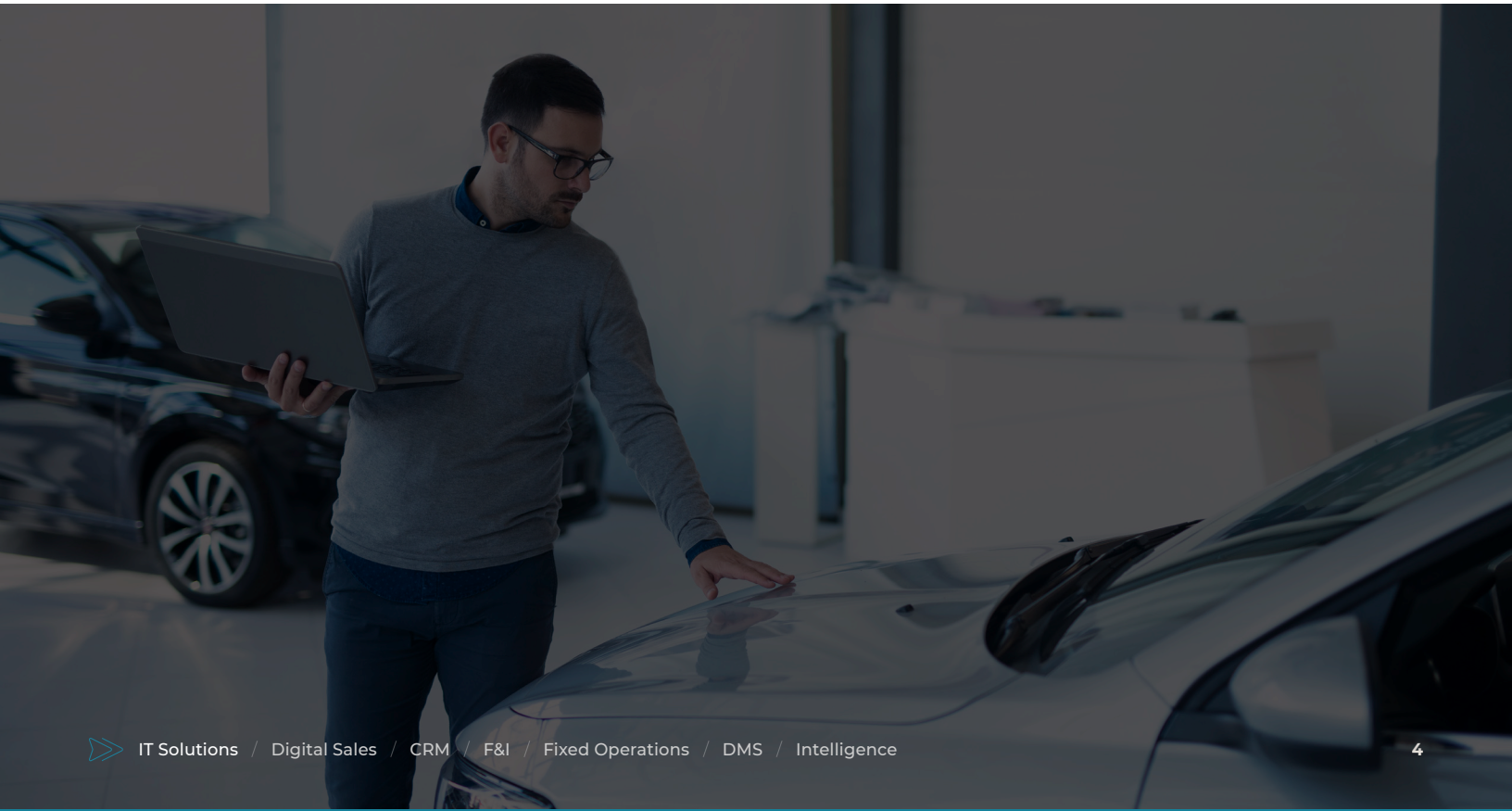
Notify impacted parties and monitor their credit.

Evaluate and fix any security flaws, replace income from system downtime.

Hire a PR agency to manage reputational damage and coach you on the best way to handle and communicate the situation to your customers and the public.

Recover expenses to continue business operations so you can get back up and running.

*ZDNET, 2020



The Playing Field Has Changed

Insurance companies today are focused on a dealership's ability to prevent, mitigate and respond to ransomware attacks. It's all driven by losses.

The spread of cybercrime had a significantly negative impact on insurance companies over the last two years. Some of the top leaders in the cyber insurance space wrote coverage at a loss. Insurance companies' loss ratios for cyber insurance (how much is paid in premiums versus how much is paid out in claims) worsened by nearly a third in 2020 compared to the previous year, according to a report by the National Association of Insurance Commissioners (NAIC).

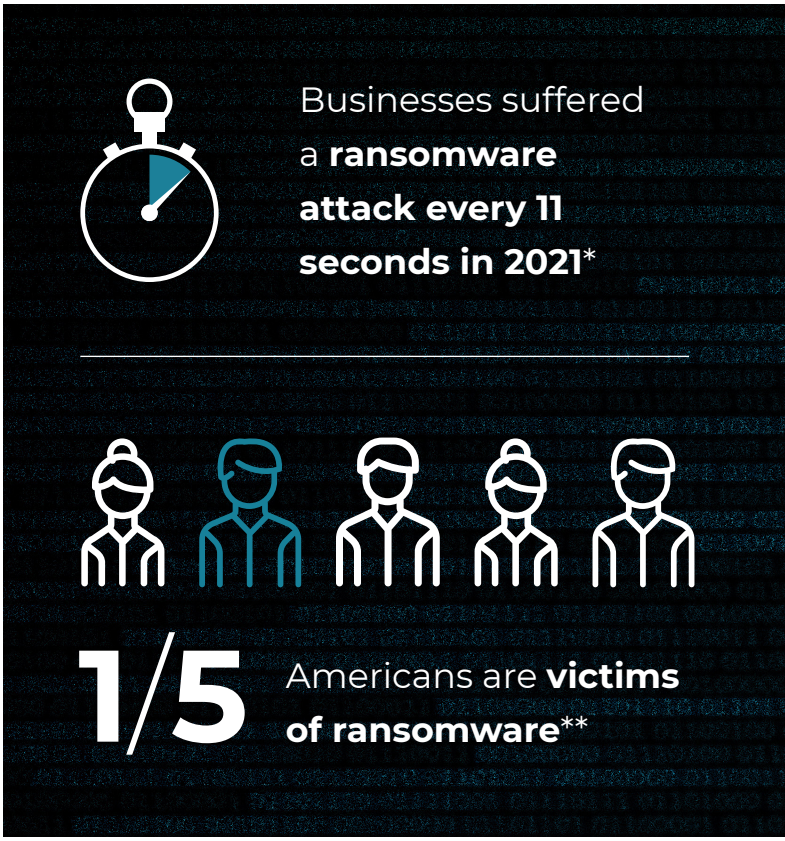
This forced insurance companies to significantly raise their rates. Previous actuarial modeling did not account for ransomware losses. Even with ransomware factored into pricing, attacks kept growing in frequency and severity to the point where insurance companies had a hard time keeping up with it. There was a ransomware victim every 10 seconds in 2020, and according to **a recent survey in Sensors Tech Forum*** one in five Americans are victims of ransomware.

Why Premiums Are Increasing

Ransomware attacks are growing, with the negative impact hitting companies of all sizes, forcing insurance companies to make huge changes in how they approve coverage.
Data breaches take years to play out — there's liability, class action lawsuits, regulatory fines, penalties, and investigations — things that take a long time to resolve. Insurance companies continually analyze these situations and adjust their pricing.

Premiums have sharply risen due to ransomware's ability to quickly cripple the data and IT systems of insured parties. "With a ransomware claim, an insurance company could be out of full limit loss (the maximum amount offered) in a week." said Cole Haney, vice president and team lead, cyber practice at Marsh, a global leader in the areas of insurance brokerage and risk management solutions.

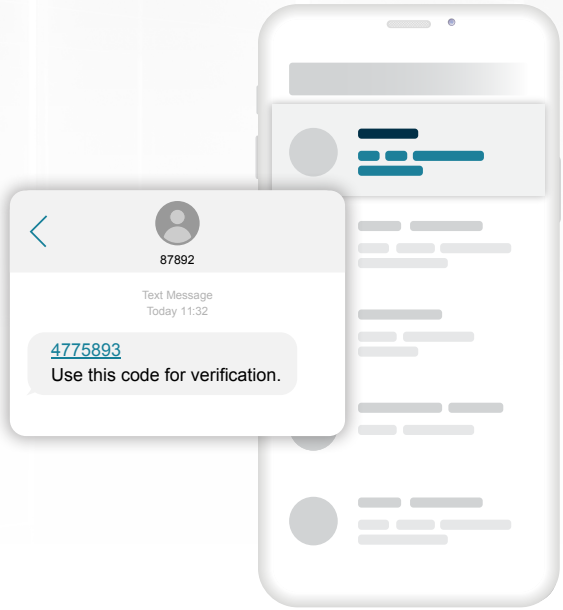
When things move fast, insurance companies can have a hard time keeping up, and are forced to constantly adjust pricing. Those increased insurer's costs are drastically raising the price of coverage for nearly everyone.



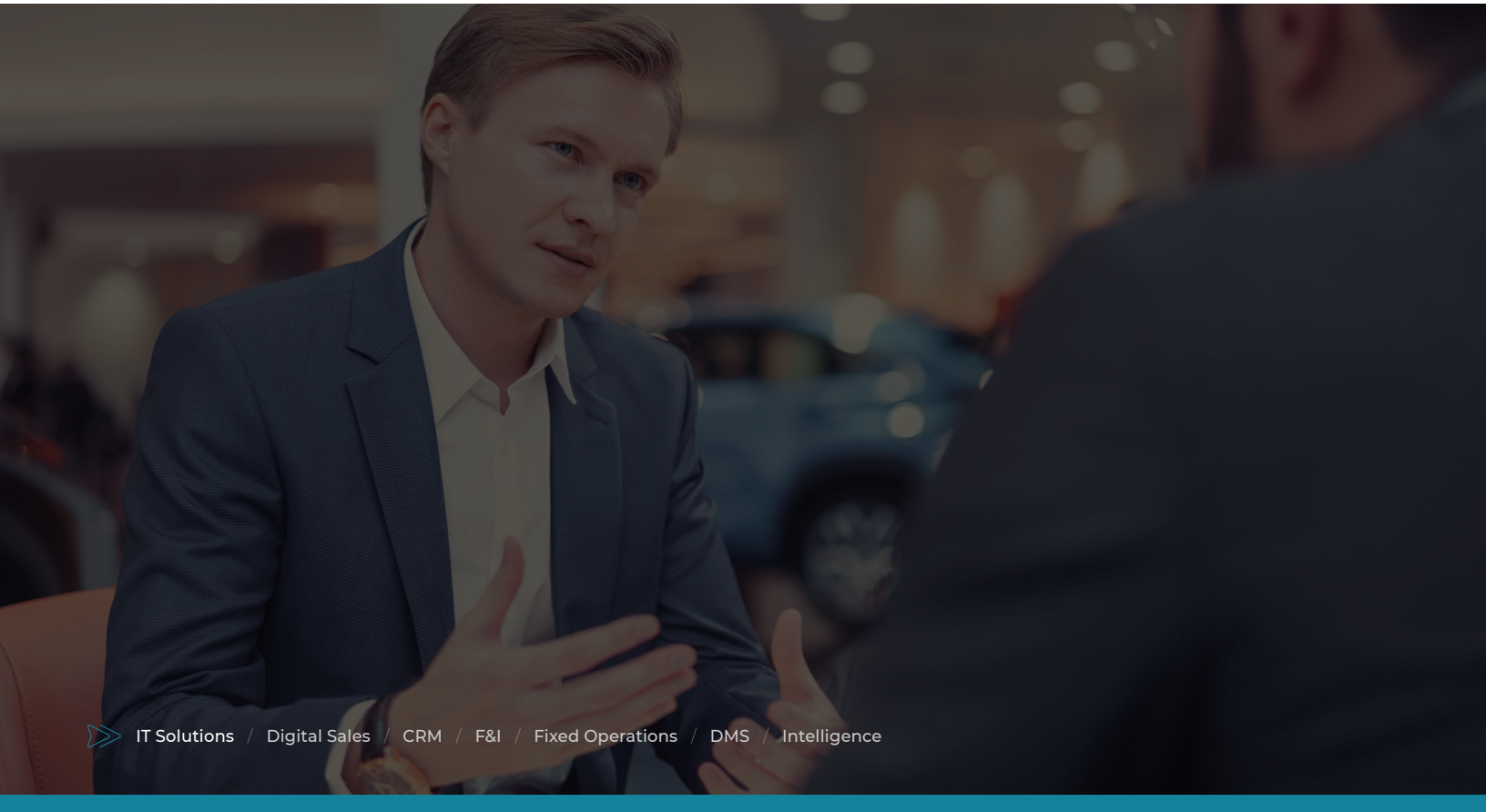
*CyberCrime Magazine, 2022
**Sensors Tech Forum, 2019

Insurers' Risk Evaluation

Many dealerships have been affected by how rapidly the insurance companies change the cyber evaluation process. Cyber insurance companies are taking a closer look at risk and evaluating it prior to issuing coverage. Today, cybersecurity and particularly ransomware protection are now top of mind. Security practices like **multifactor authentication (MFA)*** typically meant a discount on premiums but now it is often a baseline requirement.



*Cisco, 2022



Key Security Measures For Coverage

Multifactor Authentication

- Remote access to network
- Remote access to email
- Privileged user access
- Device trust

Data Backup and Recovery

- Regularly scheduled
- Test restoration
- Incident response and disaster recovery planning
- Encrypted and separate from network (offline/air-gapped)
- Encrypted backups

Additional Controls of Concern

- Patching cadence
- Endpoint Detection and Response tool implemented
- Employee training
- Email filtering and validation process
- Privilege Account Management (PAM) software

Insurance companies are looking at whether or not dealerships have the practices outlined above in place. A variety of risk factors are analyzed to calculate the cost of coverage. Among them are type of industry, amount and type of data to be covered, and most importantly, the security measures already in place. These providers want to ensure their clients are taking fundamental safety measures to protect its systems and users.

One common basic requirement is multifactor authentication. MFA defends the account against compromise through more than one method of validation of the user's identity. Creating a proactive security strategy means finding and implementing the right MFA solution for the modern hybrid or cloud environment.

What You Can Do To Prepare for Policy Renewal

- Get ahead of your cyber liability insurance renewal by working closely with your IT team to implement the controls previously discussed.
- Review by mapping the risk surface and shoring up your security strategy. Strong practices will not only lower your premium, they'll also give you the strongest security stance possible.
- Have conversations about what is feasible with key stakeholders and decision-makers.
- Before purchasing a new security product, understand your particular risks, what it would take for your team to implement a new security protocol, as well as coverage options available.
- Discuss with your team what new controls and procedures the insurance companies are going to ask for this year.
- Create an accurate inventory of your IT applications, users and devices. Make an up-to-date list of all current users, their location and the devices and applications they use.
- Document resilience processes to review your security posture. Be prepared to review them against the list of items needed to shop liability insurance.

Summary

Whether you are getting cybersecurity liability insurance for the first time or renewing an existing policy, tightened security requirements are the rule in obtaining coverage approval at favorable rates. The prevalence of ransomware and the cost of remediation has driven up costs across the board. To stay ahead of threats, there are some key interventions every insurer expects to see in place. Multifactor authentication is the most important step to implement.

Help your dealership get the best rates for a new policy or a renewal — it's time for enhanced security hygiene and protocols.

Discover how CDK Global's enterprise-level MFA can strengthen your security posture. Contact your local CDK Sales Representative, call 888.424.6342 or visit cdkglobal.com/mfa

Cisco Partner

Gold Certified
Security Advance Certification

CDK Global is a Cisco Gold Certified partner in the U.S., allowing us to incorporate the deepest level of Cisco Lifecycle Services expertise into our offerings and demonstrate a measurably high level of customer satisfaction.

Why CDK IT Solutions?

Our IT Solutions help you stay competitive with a secure, enterprise-grade network designed to meet your needs and budget. Our team enables dealers to focus on selling vehicles and servicing their customers by providing reliable, trusted and secure IT solutions that help reduce expenses, protect against cyberthreats and increase productivity.

- **Largest IT Solutions provider in the industry**
- **20+ years of proven experience**
- **Over 8,500 networks built and monitored**
- **More than 10,000 sites supported with IT services**
- **Over 4,000 dealers use our Managed IT Services**