ESSENTIAL CYBERSECURITY BUSINESS PRACTICES
HOW TO PREVENT RANSOMWARE

IMAGINE THIS...

It's a normal day. You arrive at your rental business to start meeting with customers. As you turn on your computers, you instantly realize something is WRONG. You can't access ANYTHING.

- Where are all the orders for the day?
- Where are all the dispatch routes?

Everything is gone. All of your operating systems have been locked by hackers who are now demanding more than $100,000 in RANSOMWARE to get your data back.

WHAT WOULD YOU DO...?

WHAT YOU SHOULD DO:

Take preemptive steps so this never happens to you! Now is the time to take action.

- Work with your internal IT department or an outsourced cybersecurity service provider to create and implement a plan.
- Using cybersecurity measures will ultimately save you time, money, and heartache.
- This document provides essential cybersecurity practices to avoid ransomware and other cyber attacks in your business.

WHY CYBERSECURITY MATTERS:

According to NETWORK COVERAGE, a national cybersecurity service provider, the average downtime due to a ransomware attack is **19 days.**

- **19 days** without being able to conduct payroll.
- **19 days** without being able to deposit receivables.
- **19 days** where you cannot service existing customers OR take on new business.
- **19 days** where competitors take over your market share while you sit in paralysis.

Finally, on **day 20**, you get to explain to your customers what happened and how their data may have been compromised in the attack.

NOTE: Important cybersecurity definitions can be found on page 5.

ARA
American Rental Association

ESSENTIAL CYBERSECURITY BUSINESS PRACTICES
HOW TO PREVENT RANSOMWARE

At a minimum, your company should employ tactics in each of the following categories:

CYBERDEFENSE
How do you protect yourself from cyberattacks, such as ransomware and phishing?

INCIDENT RESPONSE PLAN
What will you do if something happens at your company?

DATA & SYSTEM BACKUPS
How will you recover your data? Do we have weekly backups?

CYBERSECURITY COVERAGE
What cyber insurance do you have in the event of an attack?

NOTE: Each category will be covered in more detail on the following pages.

Remember, cybersecurity is the cost of doing business in the cyber age and an investment in your future!

Watch this video to learn more about cyber threats.

ARA
American Rental Association

This page outlines tactics you can employ in each cybersecurity category.

CYBERDEFENSE

- Do we regularly update systems with the appropriate security patches?
- Do we filter web searches for dangerous sites and content?
- Do we require multi-factor authentication to verify the identity of employees logging into internal and external systems/accounts?
- Do we have a password policy to enforce password age and complexity?
- Do we use advanced endpoint protection tools and anti-virus software on all devices and servers to detect advanced cyberattack behavior?
- Do we have a secure way of allowing remote desktop access, including a VPN connection and firewall?
- Do we implement permissions and security levels so our employees have access to only the systems they need to perform their jobs?
- Do we use unique accounts and passwords that can be protected when an employee leaves the company?
- Do we require cybersecurity training so our staff can identify phishing emails and suspicious cyber behavior?
- Do we receive timely updates that identify emerging threats and help us improve our security plan?

Use this video as a tool to educate staff on cyber threats.

ARA
American Rental Association

INCIDENT RESPONSE PLAN

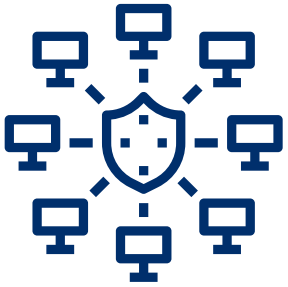
- Does our plan illustrate how security events will be escalated?
- Does our plan name the key decision makers within the organization and their respective roles?
- Does our plan provide a roadmap for how to handle different cybersecurity incidents?
- Do we review these scenarios regularly to rehearse how to handle a cyberattack?

DATA SYSTEMS BACKUPS

- Do we retain redundant backup copies of systems and critical data in an offsite location?
- Are our various backups protected by robust encryption while in transit and at rest?
- Do we have hourly backups for at least four weeks, weekly backups for at least six months, and monthly backups for at least a year?
- Do we physically and digitally separate critical data and networks?
- Do we have regular testing (at least annually) to validate usable backup data and timely recovery?

CYBERSECURITY COVERAGE

- Does our company have cybersecurity coverage that includes legal advocates and a forensics team to deal with cybercriminals and cover monetary losses?


ARA
American Rental Association

ESSENTIAL CYBERSECURITY BUSINESS PRACTICES
DEFINITIONS

Ransomware:
Malware that locks up your system so you cannot access your data. Hackers demand a ransom for getting a key to unlock your data, but sometimes paying does not work.

Phishing:
A reputable-looking email that entices you to share personal information. Example: Request to change your password since your computer got corrupted.

Redundancy:
Storing the same data in multiple places so that you have a real-time, fail-safe backup.

Virtual Private Network (VPN):
Encrypts your internet connection on any network, including public networks. It keeps your online work private and minimizes attacks by hackers. The VPN you use should be approved by your company.

Multi-Factor Authentication:
A way to verify that users are who they say they are by requiring at least two pieces of evidence to prove their identity.

Advanced Endpoint Protection:
Software that identifies and blocks the suspicious behavior of viruses.

ARA
American Rental Association