

Proof to Profit: How Trucking Leaders Protect Revenue in the Age of Ransomware and AI



Melanie Padron
Vice President of Strategic Growth
IT ArchiTeks

ABOUT ME

- Dallas, Tx
- 30 Years in Risk Management
- VP of Strategic Growth
- Host Mission Secure Podcast
- Founder, She Leads Securely, Women's Conference



Ninety-five years

Thousands of loads. Decades of relationships.



"Hello. Your files have been
stolen and encrypted.

All you need to do is **PAY.**"



**Trucking doesn't just support the American economy.
It IS the American economy.**

“

The ransom note
is not the attack.

It's the bill.

The question is **not** whether you have cybersecurity.

**The question is *can*
*you prove it works.***

THE GAP

Between what you believe about
your security and what you can
actually prove.



1

The Email Your Team Couldn't Tell Was Fake





The question is no longer whether
someone on your team will be fooled.

The question is whether your systems
are built to catch it when they are.

2

The Vendor You Trust With Your Technology

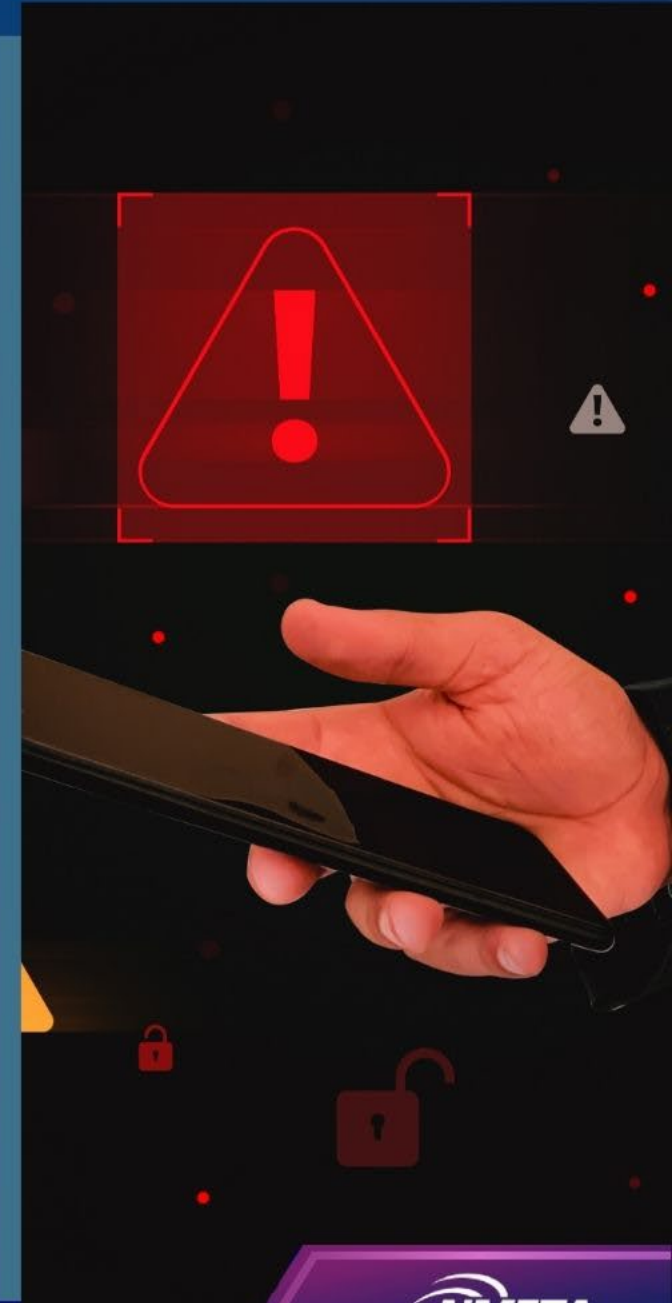


“

Having someone manage
your technology is not the same
as having someone defend it.

3

The Security Alerts That Nobody Owned



That's not an IT failure.

**THAT'S A
LEADERSHIP
FAILURE.**





Who owns security monitoring at your company right now?

4

The Backup That Was Never Tested





A backup never tested
under real conditions
is not a safety net.

**Raise your hand if your company
has an Incident Response Plan.**

“

An Incident Response Plan is not a door.

It's the key to closing one
that's already been compromised.

NOW YOU KNOW



FUEL HAULER RANSOMWARE ATTACK





Zero encryption.

Zero data loss.

Zero ransom paid.

Five disciplines.

Five words.

01 **PREPARE**

Discipline before disaster.



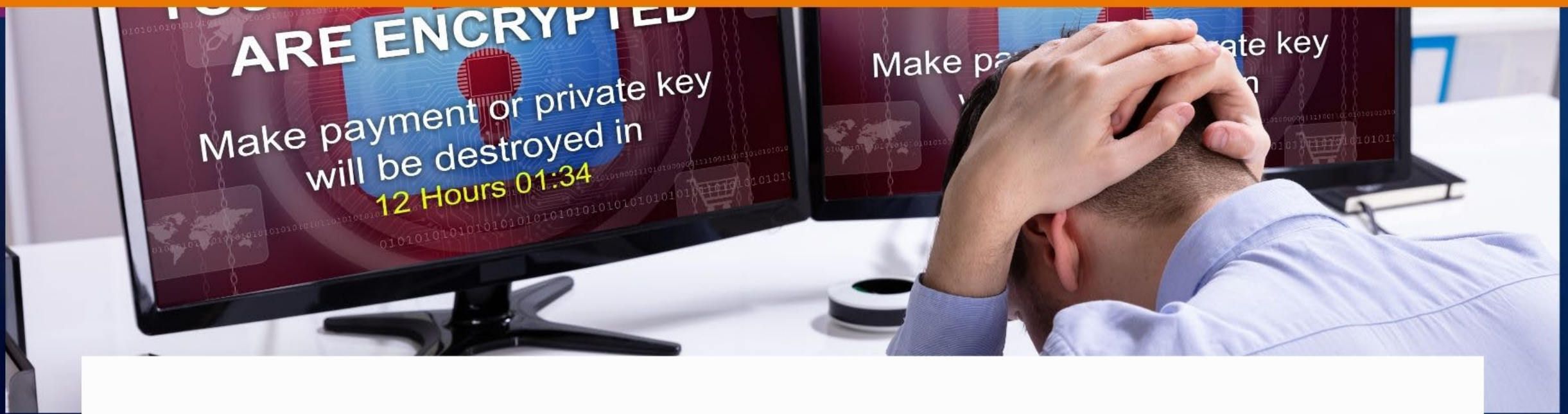
What isn't owned isn't prioritized.

**And what isn't prioritized becomes
exposed.**

02 PROVE

*Stop assuming.
Start validating.*





**Criminals are counting on
the fact that nobody else is
grading your security either.**

03 PRACTICE

Execute. Don't improvise.





**Pressure reveals
what preparation conceals.**

**That's the difference between
disruption and disaster.**

04 PROTECT

Position for the best possible outcome.





Protection is **not installed.**
It's validated and measurable.

05 **PROFIT**

Resilience is revenue.



Cybersecurity is no longer an IT discussion.

It's a BUSINESS CONTINUITY decision.

It's a MARGIN PROTECTION strategy.

It's a LEADERSHIP responsibility.



THE PROOF TO PROFIT FRAMEWORK

01 PREPARE

Discipline before disaster.

02 PROVE

Stop assuming. Validate.

03 PRACTICE

Execute. Don't improvise.

04 PROTECT

Protection is measurable.

05 PROFIT

Resilience is revenue.

THE 5 POINT CYBER BATTLE PLAN



**POINT
1**

ASSIGN OWNERSHIP

Discipline before disaster.

**Who is responsible for making sure the
gaps get closed at the executive level?**

FILL IN THE BLANK

"The person who owns cybersecurity at my company is _____

Within 30 days I will confirm they have the authority, the resources, and the mandate to act.



**POINT
2**

SCHEDULE AN INDEPENDENT AUDIT

Stop assuming. Start validating.

An independent, comprehensive audit that looks at your team, your applications, your network, and your data with zero conflict of interest.

FILL IN THE BLANK

Our last independent cyber risk assessment
was _____

I will have one scheduled by



POINT
3

RUN A TABLETOP EXERCISE

Execute. Don't improvise.

Gather your key people. Give them a scenario.

Walk through it together.



SCENARIO:

Ransomware hits at 2 a.m.

Dispatch is down. Drivers can't pull logs.

Payroll is frozen.

Who calls who?

Who has decision-making authority?

Who communicates with customers and drivers?

Who contacts legal, insurance, forensics?

Who handles media if it gets out?

FILL IN THE BLANK

We last practiced our Incident Response
Plan on _____

I will schedule our next tabletop exercise by
_____.



POINT
4

AUDIT YOUR VENDOR ACCESS

Position for the best possible outcome.

Pull your vendor access list and ask three questions:

Who has active credentials?

When were they last reviewed?

Who shouldn't still have access?

FILL IN THE BLANK

I will request a full vendor access audit by

_____.

The person responsible for reviewing
credentials is _____.



POINT
5

TEST YOUR BACKUPS

Resilience is revenue.

**Prove your safety net actually
holds before you need it.**

The 3-2-1 Rule

3

Copies of your data

2

Different types of
storage media

1

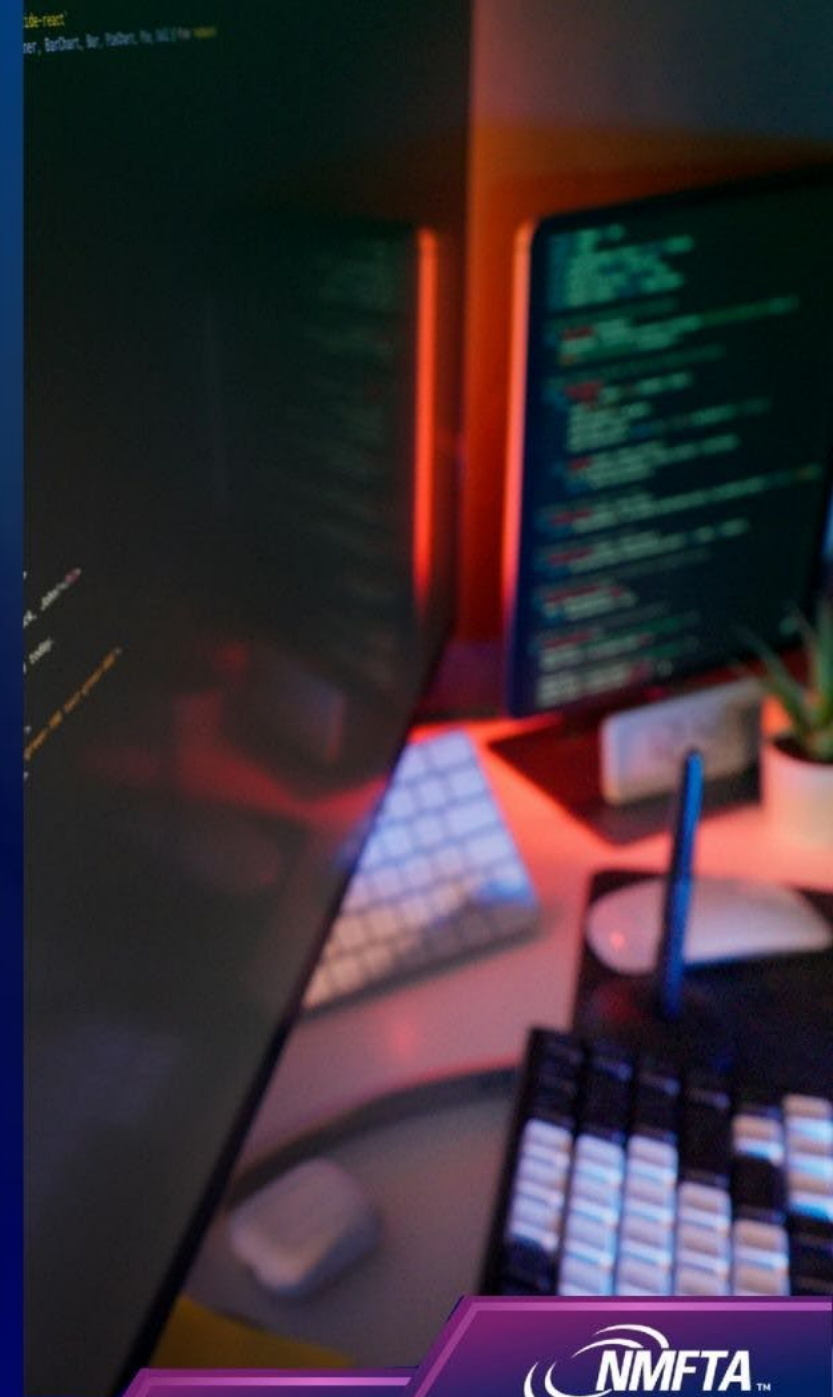
Copy kept offsite
(cloud or separate location)

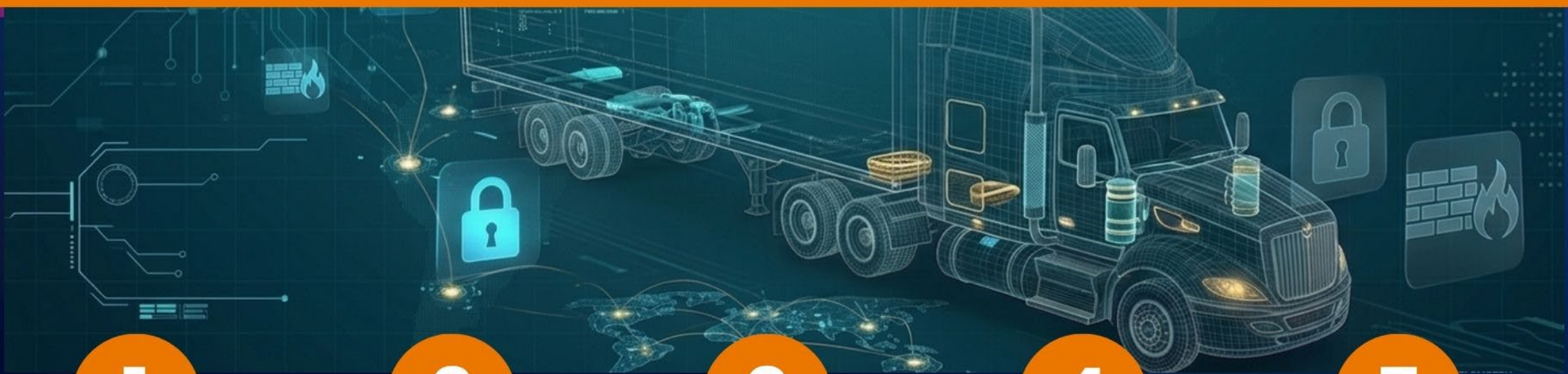
FILL IN THE BLANK

Our last full backup restoration test was

_____.

We will schedule our next timed restoration
test by _____.





1

Who owns
your risk?

2

When was
your last
independent
audit?

3

When did
you last
rehearse
your
response?

4

Who has
the keys to
your
network?

5

Can you
prove your
backups
work?



The most **expensive** cyber
mistake isn't the attack.

It's believing you're protected without proof.

**WHEN THIS INDUSTRY
STOPS MOVING,
OUR COUNTRY STOPS MOVING.**

**CRIMINALS
KNOW THIS.**

AND THEY ARE COUNTING ON THE
GAP BETWEEN WHAT YOU BELIEVE
ABOUT YOUR SECURITY AND
WHAT YOU CAN ACTUALLY PROVE.



95 Year *Legacy* Lost



Let's Move Forward Together.

STRONGER SECURITY.
STRONGER FLEETS.
STRONGER FUTURE.



Book a time to connect

Scan the QR code to schedule a meeting with me.



Email

melanie@itarchitekts.com



Connect on LinkedIn

Melanie Padron



Speaking Inquiries

Looking for a speaker who delivers real-world insight that moves audiences to action?



Fleet Security Audit

Let's uncover the gaps you can't afford to ignore.



MELANIE PADRON

PUBLIC SPEAKER, CYBERSECURITY STRATEGIST