Why Nobody Trusts Us

Robert Wagner

CornCon 2026

A story about a printer.



~~governance gap~~

A customer who chose a competitor.

The competitor: a decision made in a meeting we weren’t in.

80%+

office workers

~90%

security pros

use unapproved AI tools

Source: UpGuard.

Nobody sends you a note.

WHEN IT GOES SIDEWAYS

Will they call before they have the whole picture?

Will they tell you what they know while it’s incomplete?

Will somebody admit the mistake?

Mean time to detect

Mean time to remediate

Patch cadence

Phishing click rate

Coverage

Findings closed

Disclosure Lead Time™

all about us

Your last five decisions.

	BEFORE	AFTER
A vendor selection	☐	☐
An architecture	☐	☐
A product launch	☐	☐
A data move	☐	☐
	☐	☐

Nobody tells you they stopped trusting security.

They just stop telling you things.

And nobody tells you when it comes back, either.

You just start hearing about things earlier.

We blame ourselves.

We blame them.

?

Nobody returned our calls

Regulatory backing, a board mandate

They stopped telling us why

We won the argument and we lost the conversation.

1

They didn’t see it.

2

Their math said don’t do it.

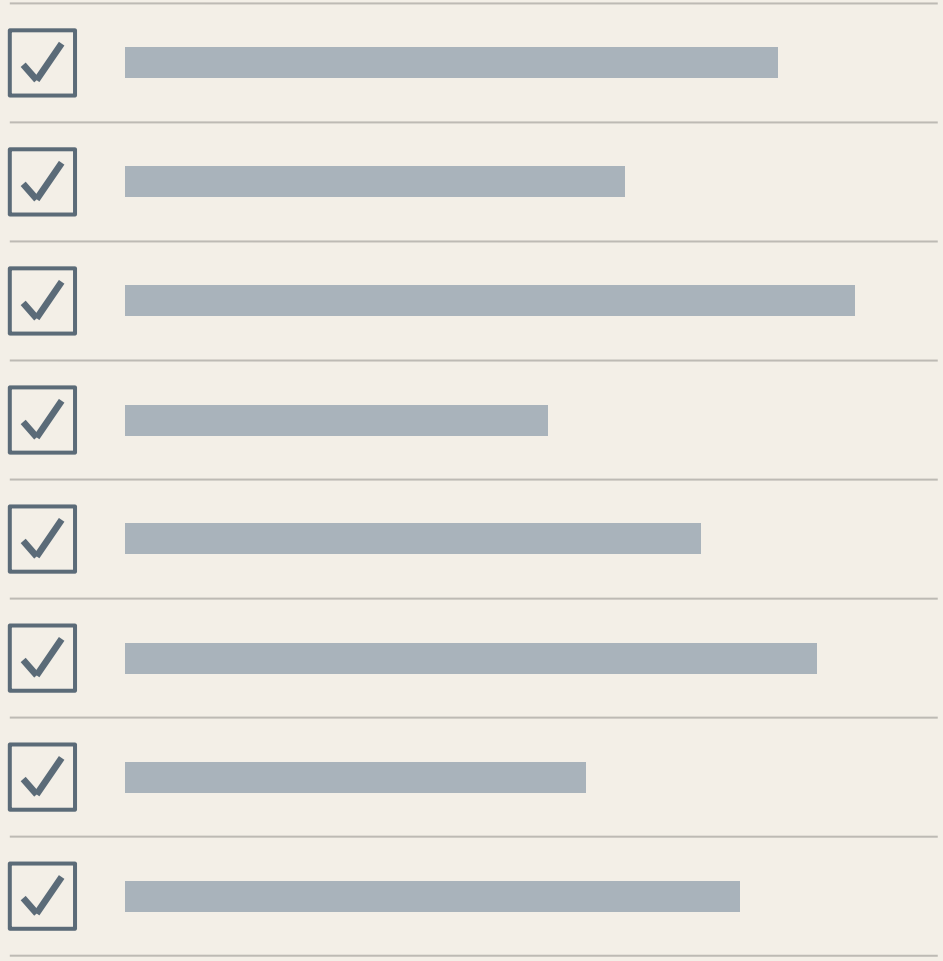
The request sat for two months.



They didn’t see it.	→	Move the security implications to where the work is.
The math said don’t.	→	Make the secure path the fast path.

Our reflex: more policy, more training, more gates.

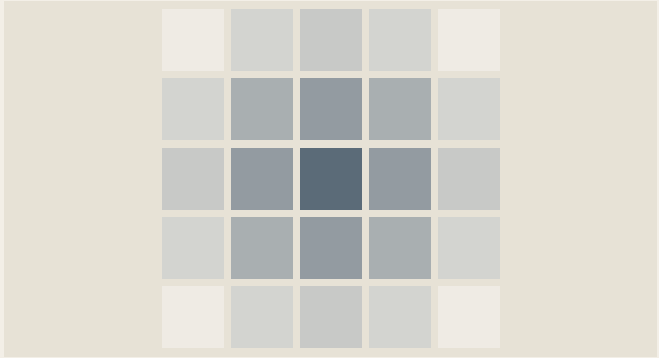
Your audit doesn’t measure either one.



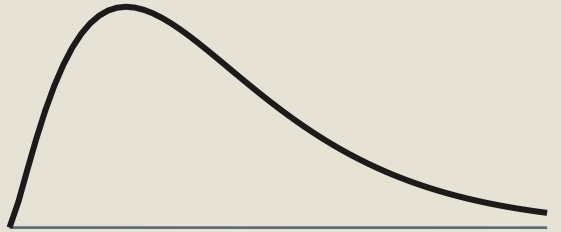
example

Critical	14
High	87
Medium	412

Vulnerabilities



Risk



Dollars

“Where did you get that number?”

Give me the evidence.

WHAT HAPPENS TO THE MESSENGER

Shot. | Neglected. | Trained.

Ron Westrum.

Westrum's culture model: six statements from DORA, adapted for security

ASK THE BUSINESS, NOT YOUR OWN TEAM **SCORE EACH 0 TO 5**

1. When someone tells security about a problem, security actively seeks more information.
2. When someone discloses a mistake to security, it is treated as a learning opportunity rather than held against them.
3. Security shares responsibility for outcomes rather than assigning it.
4. Working across the line between security and my team is encouraged and rewarded.
5. When something fails, security asks what happened rather than who did it.
6. New ideas are welcomed by security.

Want a copy? Find me on LinkedIn.

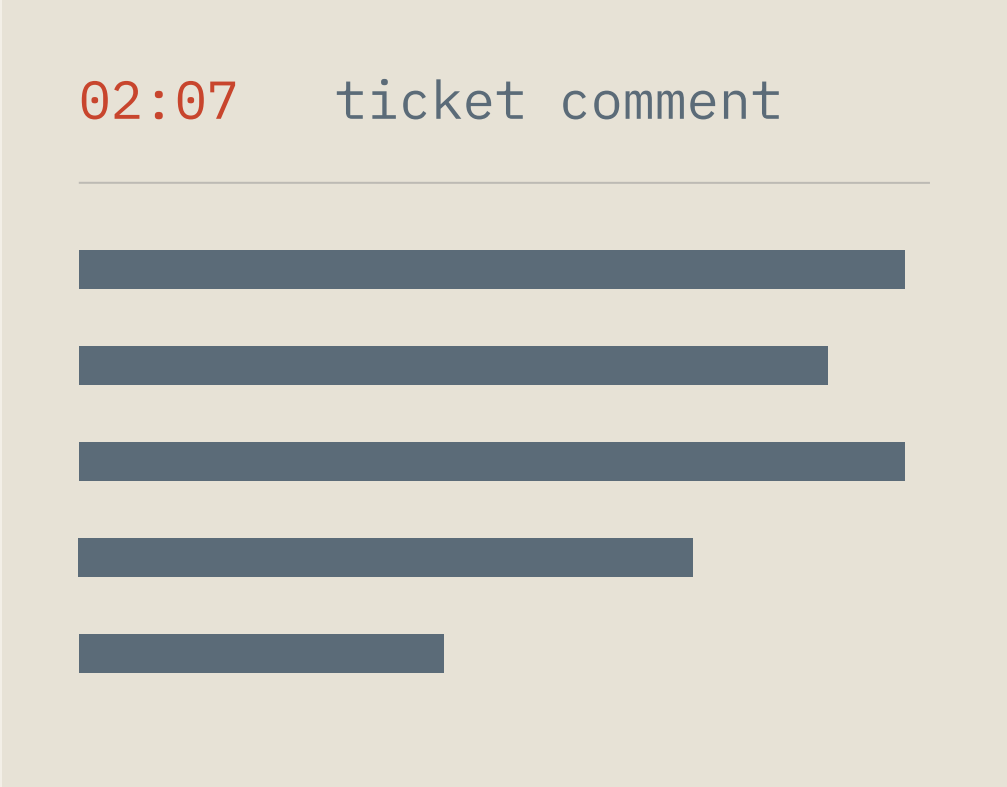
Give them a no they can predict.

Compliance is necessary. It isn’t sufficient.

Every outage started
with the same phone call.



Trust is a forecast.



EXECUTIVE	sets the terms.
MANAGERS	set the temperature.
PRACTITIONERS	set the truth.

None of it needs a budget.



2 things to do

Executive

Sets the terms.

Disclosure Lead Time™

Your last 11 decisions, two dates each.

Decided minus security in equals lead time.

EXAMPLE

POSITIVE: YOU HAD WARNING

+22 days

```
decided     2026-03-14
security in 2026-02-20
```

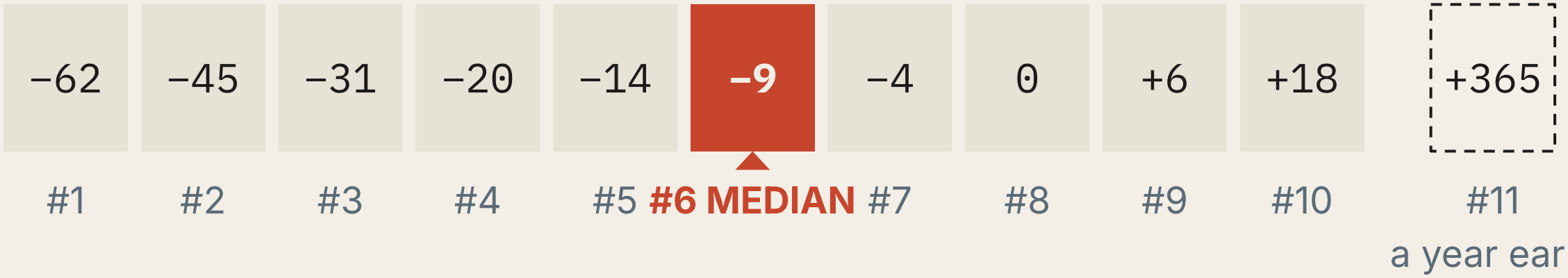
NEGATIVE: YOU FOUND OUT AFTER

−40 days

```
decided     2026-05-02
security in 2026-06-11
```

DISCLOSURE LEAD TIME™

EXAMPLE DATA



Median: −9 days

Average: +19 days

GRC tool | Change tickets | Incident timelines

It’s a baseline.

If security was never invited, don't invent a date. .

“Where did you get that number?”



From your own change log.

Edmondson: the best hospital teams reported the most errors.

We cost you

$_____ this quarter



2 things to do

Manager

Sets the temperature.

“If you already did something without us, come tell me anyway. We’ll deal with it together.”

“Thank you for telling me. Let’s work out what we need to do.”

WE MEASURE ONE OF THESE.

```
response time, alert:    4 min

response time, person:
```

?



3 things to do

Practitioner

Sets the truth.

“This isn’t secure.”

> “This isn’t secure. Here are two ways out of it. Here’s the one I’d pick, and here’s why.”

About 45 extra seconds.

Written for the person who has to fix it.

THE POLICY VERSION

Finding 4471: TLS 1.0 enabled. Remediate per policy 7.2. Due in 30 days.

THE HUMAN VERSION

TLS 1.0 is still on for the payments API. An attacker can push a connection down to it. The fix is two lines in the load balancer config, linked below. I'm around until 7 if you want to talk it through.

“I don’t know. Let me find out, and I’ll come back to you.”

EXECUTIVE	MANAGER	PRACTITIONER
Disclosure Lead Time™	Come tell me anyway	Two ways out
Report your own cost	Response time to a person	Tickets for humans
		“I don’t know”

Relationships are resilience infrastructure.

Every control carries an opinion about people.

Somebody has to go first.

MFA, unexplained: one more hoop. MFA, explained: protection.

MONDAY

What would have had to be true for you to call us first?

Then stop talking.

Disclosure Lead Time™

The Monday conversation

Both are free, and you can start without asking anybody’s permission.

Trusted in 20 minutes.



THE BOARDROOM

“Where did you get that number?”

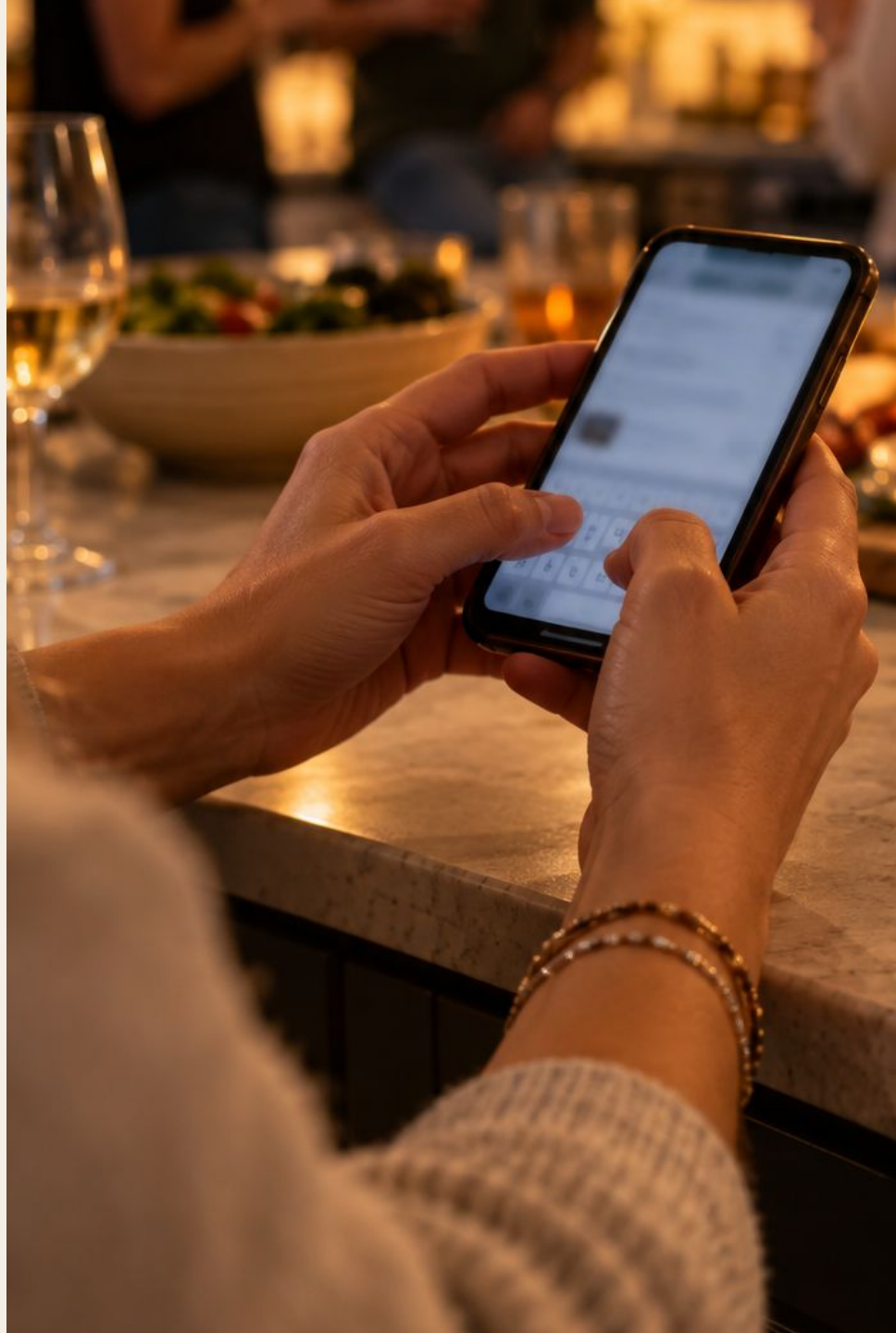
THE KITCHEN

“That’s all I needed.”

We want to be believed.



Now it’s our turn.



Nobody tells you they stopped trusting security.

They just stop telling you things.

And nobody tells you when it comes back, either.

But you'll know it's back when
you start hearing about things earlier.

Thank you.

Robert Wagner



linktr.ee/rwagner1

linkedin.com/in/robertwagner2