



Culture is a Control

Overseeing the Human Side of Cybersecurity at Your Credit Union

Culture is a Control | NACUSAC 2026

- "I want to start with a pattern."
- Every IR engagement I've been part of had a person at the center. Every single one.
- Somebody clicked, reused a password, plugged in a found USB — or saw something off and *said nothing*.
- **Scenario:** Accounting employee gets CEO email asking for a wire → then a video call, CEO's face and voice, new project, funds needed now → employee wires it.
 - Reconciliation later flags it: CEO never sent the email, never made the call. Email spoofed, video call an AI fake. **More than a million dollars gone.**
 - No firewall, no network tool would've caught it — nothing was technically breached; controls worked as designed.
 - The only thing that stops it: a person free to pause and verify in person, even against a "CEO" request. **That pause is a cultural artifact. You either have a culture that produces it or you don't.**
- (Theoretical/composite — not attributable to a specific credit union)



Barry Lewis

CCISO, CISSP, ECSA
blewis@optiri.com



2 Culture Is a Control | NACUSAC 2020

27+ years in/around credit unions; computer operator → VP of IT → MSP side → today lead a team of vCISOs (couple hundred million to \$6B+ in assets).

It Always Comes Back to a Person

Your strongest control isn't a firewall.

~60%

In every incident response, there's a human at the center: the click, the reused password, the USB drive, the thing no one reported.

It's your culture. The one control a SOC report and a pen test can't fully see, which is exactly why it's your job.

Majority of all breaches involve a human element. Reported as roughly 60%-68% in recent Verizon DBIR reports.

1,072 cyber incidents in reporting rule's first year; 7 in 10 involved a third-party according to NCUA Letter 24-CU-02.

3 Culture Is a Control | NACUSAC 2026



- Uncomfortable truth: strongest control isn't the firewall, endpoint, SIEM, or last year's tool spend. It's your culture — how people behave when no one's watching.
- Human element = majority of breaches yearly (~60–68%, recent Verizon DBIR).
- NCUA rule, first full year: 1,072 incidents reported; 7 in 10 involved a third party. Trend line isn't our friend.
- Why this room? Firewall shows up in an audit; culture doesn't. SOC report can't see it, pen test can't fully measure it. **The one control that never appears on paper — which is exactly why it belongs to you.**
- Next 50 min: not how to *build* a culture, but how you *evaluate* one.

Why This Lands on Your Desk

Culture is risk management, your discipline.



The Oversight Gap

Technical controls get audited every year. Culture almost never is; yet it's the variable that most often decides the outcome.



A Business Decision

Understand it, measure it, weigh it against the credit union's risk tolerance - the same lens you already apply to everything else.



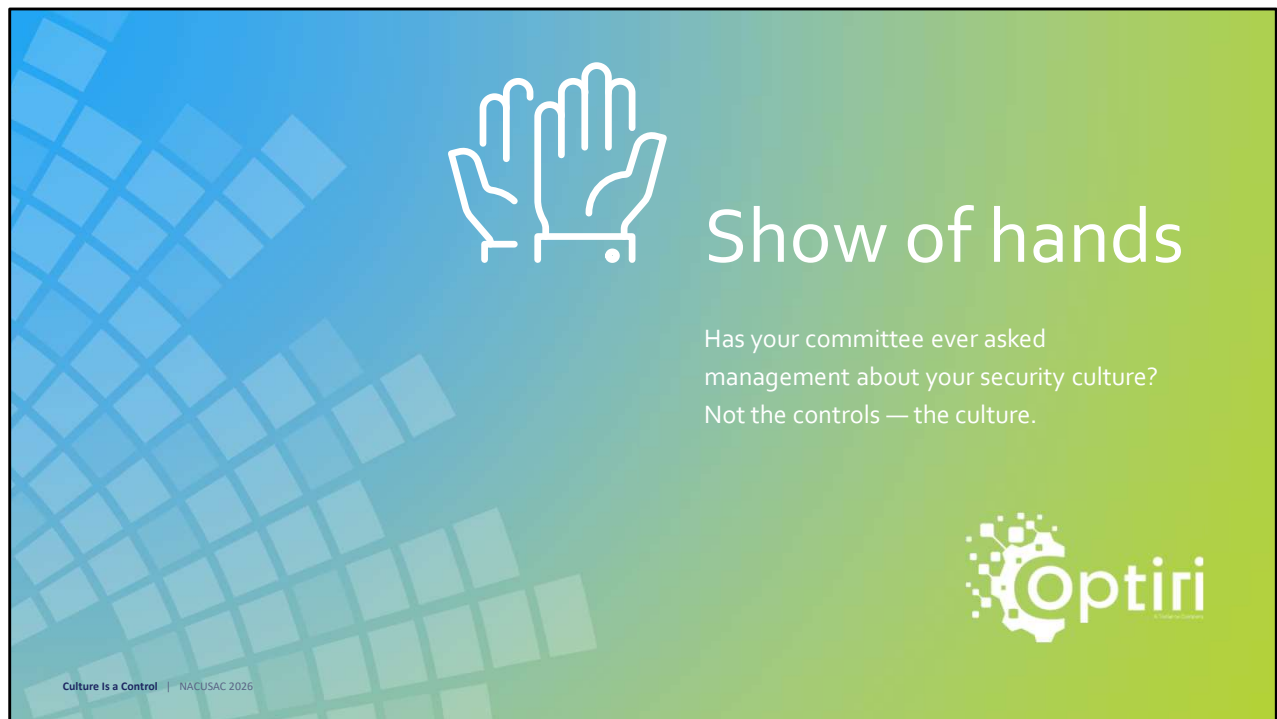
The Stakes

\$6.08M average breach at a financial institution, 22% above the global average. Member trust is the thing on the line.



4 Culture Is a Control | NACUSAC 2026

- The gap: technical controls get audited yearly; culture almost never does — yet culture decides footnote vs. headline.
- Authority (be precise — differs by seat):
 - **Board:** NCUA Letter 24-CU-02 (Oct 2024) — treat cyber as top governance duty; "embed cybersecurity into the organizational culture" (regulator's words). Part 748 = board approves/oversees the infosec program.
 - **Supervisory/audit committee:** Reg 715.3 — ensure management safeguards member assets and board controls are administered. Member info is a member asset.
 - **Internal audit:** same letter calls for independent audit of the program. That's you.
- Core belief: **security decisions are business decisions.** Culture is a risk to be measured against tolerance — the same muscle you already use for credit, liquidity, etc.
- Stakes: ~\$6M average breach at a financial institution (22% above global avg). 90% of members say identity theft is a serious worry. Member trust is what's on the line.



★ INTERACTION

- Ask for real hands: "Who on your committee has ever asked management about your security *culture*?" — not controls, not backups. Culture. Whether people feel safe reporting. Whether tone at the top is real.
- Look around; if small, count aloud ("four... five hands"), smile.
- "That gap is what we're closing this morning."

What 'Good' Looks Like

Six hallmarks of a strong culture, in evidence you can observe.



Visible leadership commitment

Adequate budget, the CISO has real standing, and security is tied to executive performance.



Shared responsibility

Security isn't "IT's job." It lives in job descriptions, onboarding, and how staff talk.



Psychological safety to report

When someone clicks, the first question is "how did that get through?" not "who's to blame?"



Continuous learning

Strong cultures spend more than twice as much of the budget on people and training (43% vs. 19%).



Security as enabler

The team asks "how can we do this securely?" instead of simply saying no.



Integrated into daily work

The secure path is the easy, default path — not an extra step people route around.

6 Culture Is a Control | NACUSAC 2026



You can't spot a problem until you know healthy.

Six hallmarks, each with *observable evidence*.

Top row (1–3):

- **Visible leadership commitment** — strategic priority, not checkbox. Evidence: real budget, a security leader with standing/access to you, security in exec performance expectations. Twice-a-year mentions = theater.
- **Shared responsibility** — not "IT's problem." Evidence: job descriptions, onboarding, how a teller/loan officer talks about it. Only IT badges can discuss it = problem hiding behind a good org chart.
- **Psychological safety to report** (the one I care most about) — after a click, first question is "how did it get past our filters?" not "who do we blame?" Afraid to report = you go blind. Best detection is a person who feels safe speaking up.

Bottom row (4–6) — no advance:

- **Continuous learning** — not one annual training. Ask the budget split: strong cultures spend 43% on people/training vs. 19%. Tools vs. people?
- **Security as enabler** — "how can we do this securely?" vs. "no." Roadblocks create workarounds = shadow IT.
- **Integration into daily work** — secure way = easy, default way. Fight the system to be secure, security loses.

Red Flags — Warning Signs of a Weak Culture

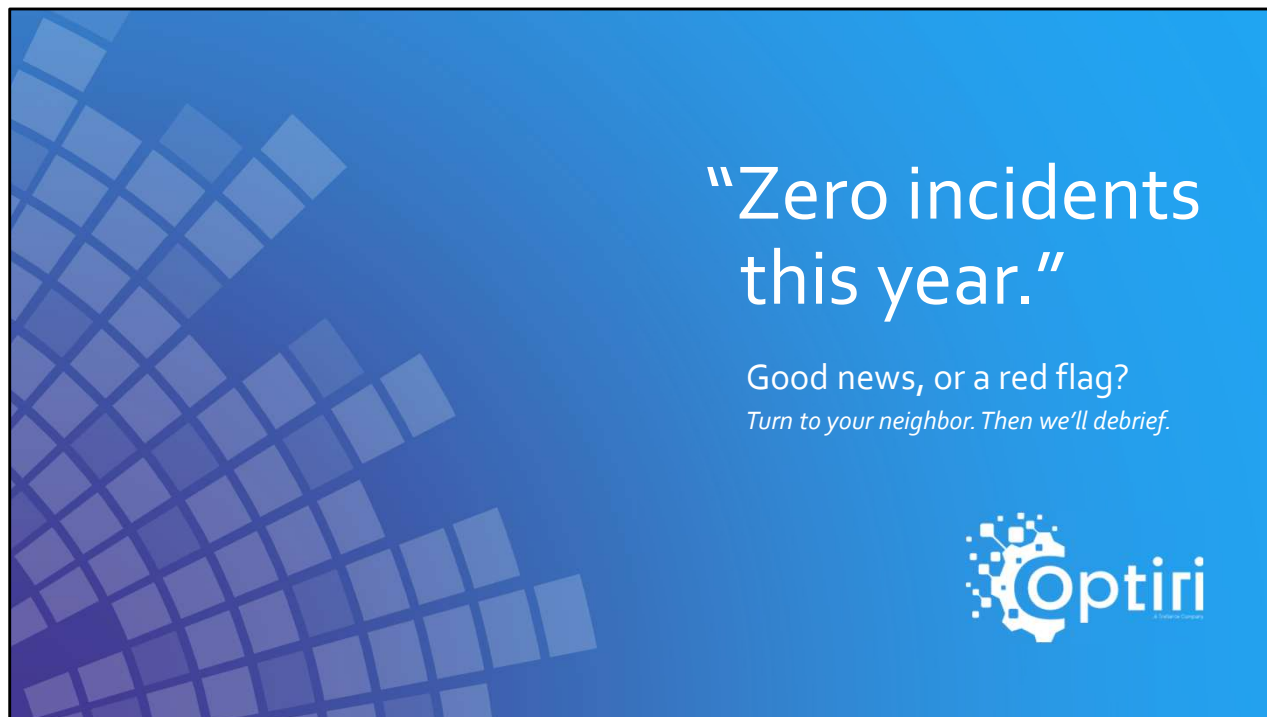
What should worry any overseer — in reports, interviews, and walk-throughs.



7 Culture Is a Control | NACISAC 2020



- Watch for these in reports, interviews, and walking the building.
- Left to right:
 - **Blame-focused IR** — "zero-intrusions-allowed" mindset; team blamed even when they stopped the attack. Poison. Punishing finders teaches everyone to stay quiet.
 - **High security-team turnover** — burnout, no support, ignored warnings. Revolving door → ask why.
 - **Compliance theater** — thick binder, boxes checked, nothing practiced. Dangerous for a committee because it's built to look good on paper. Look past the paper.
 - **Tools over people** — buys every appliance, under-resources the people running them. "A six-figure tool nobody has time to monitor is a receipt, not a control."



★ INTERACTION · TABLE TALK (90 SEC)

- Turn to your neighbor, ~90 seconds: "Your CU reports *zero* security incidents this year. Good news, or red flag?"
- "Who says good news? Who says red flag?"
- My answer: usually a **red flag**. Zero almost never means nothing happened — it means people aren't reporting (afraid, or don't know how). Healthy cultures generate a steady stream of reports. **When the stream runs dry, the silence is the finding.**

Measure The Right Things

100% Trained $\neq$ a Secure Culture

COMPLIANCE

Did people complete the training?

- Training completion %
- Quiz / assessment scores
- Policy acknowledgments
- Event attendance

CULTURE

Did behavior actually change?

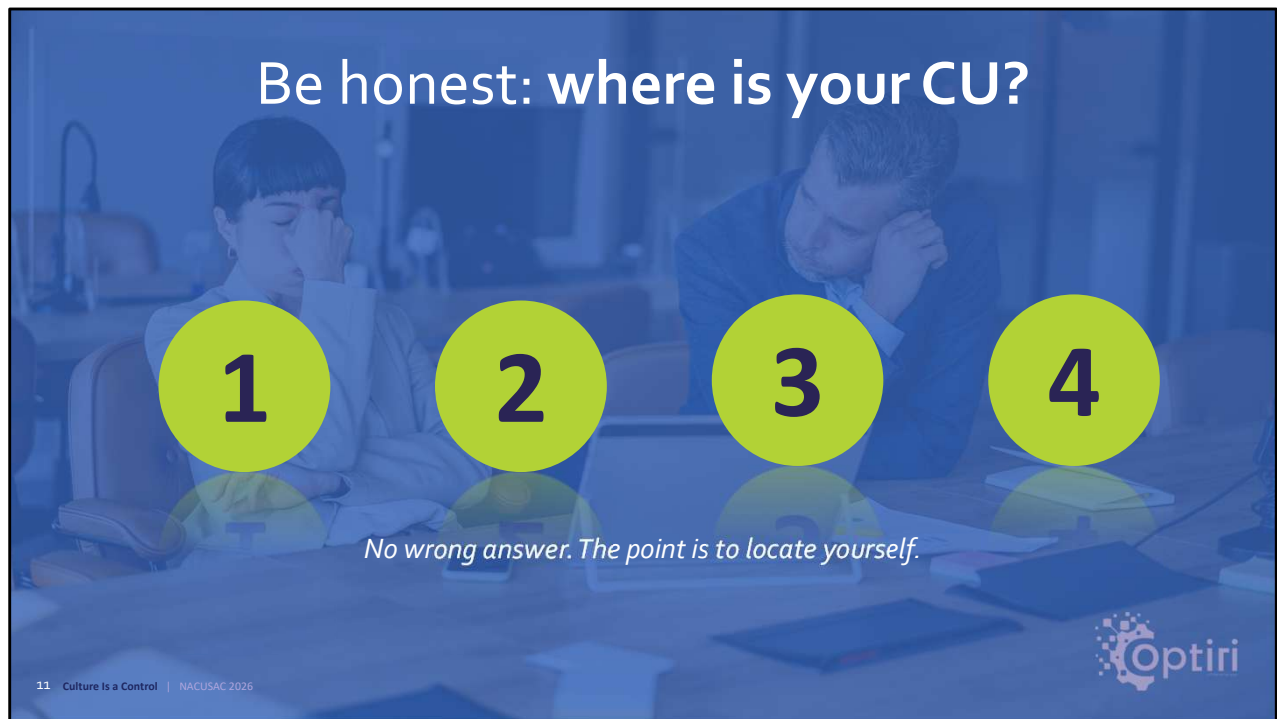
- **Phishing reporting rate (the #1 metric)**
- Time to report a suspicious email
- Voluntary incident reporting
- Policy-violation trend over time

© Cybersecurity Research | NACISAC 2026

- The distinction most leaders (and oversight bodies) miss: measuring compliance vs. measuring culture.
- Training completion = compliance. Says people did the training; says nothing about behavior change.
- Seen 100% completion CUs still clicking phishing, reusing passwords, sticky notes on monitors. Compliance solved, culture untouched.
- **Left (compliance):** completion, quiz scores, policy sign-offs, attendance — the floor, not the goal.
- **Right (culture):** phishing reporting rate, time-to-report, self-surfaced incidents, violation trend.
- **The one metric to remember: the reporting rate beats the click rate.** Clicks will happen — the question is the next 60 seconds: does someone speak up, or does it sit in silence while the attacker moves?



- Four levels:
 - **L1 Compliance** — "We train because we have to." Only completion measured.
 - **L2 Awareness** — people understand why it matters to their role.
 - **L3 Behavior Change** — doing things differently; "careful what I click, and I report." Reporting climbs, violations fall.
 - **L4 Culture** — security is just how work gets done; "we help each other"; little supervision.
- Honest field read: most CUs are L1–L2. **L3 is realistic and should be your target.** L4 takes years; few get there — that's fine.
- Point isn't to pretend you're a 4. It's to know where you stand and move up *intentionally*.



★ INTERACTION · SILENT SELF-ASSESSMENT

- Quietly, just for yourself, no hands: where is your CU right now — 1, 2, 3, or 4?
- "No wrong answer. The only wrong move is not knowing."

 LEADERSHIP	01 "How much of the security budget goes to people and training vs. tools?"
 REPORTING	02 "When an employee reports a mistake, what actually happens to them?"
 MEASUREMENT	03 "Beyond completion rates, do we track the phishing reporting rate?"
 BOARD ENGAGEMENT	04 "Has everyone completed cyber training, with documented proof of what & when?"

12 Culture Is a Control | NACUSAC 2026



- Oversight ≠ running the program. It's asking the questions that push leadership to build a real one. Full set on the one-pager; here's the top question in each category:
 - **Leadership:** how much of the security budget goes to people/training vs. tools? That ratio tells you if leadership thinks culture is real.
 - **Reporting / psychological safety (my favorite):** when an employee reports a mistake, what actually happens to them? Discipline = problem; thank + fix the system = good shape. Companion: how many concerns did staff report last quarter? (Low number = warning.)
 - **Callback:** the wire transfer — the question that saves the million dollars is whether someone who pauses a CEO request gets *thanked* or treated as slowing things down. **That safe pause is worth more than any tool.**
 - **Measurement:** beyond completion, what do we track? Push for reporting rate, time-to-report, repeat clickers, violation trends. Only a completion % = your gap.
 - **Board engagement** (carries weight with examiners): has every board/committee member done cyber training this year — with documented what/when/who? Examiners want proof, not "we got a briefing once."
- None of this needs a technologist — just a good overseer pointed at a control most committees never examine.

Culture As Competitive Advantage

Credit unions serve roughly

139 million

Americans, and trust is the differentiator.

A mature

security culture

protects member data, reputation, and that trust.

You're not here to run the program.

You're here to ask the questions

that push leadership to build a real one.



- Credit unions serve about 139M Americans. What sets us apart, the reason the movement exists, is **trust**.
- A mature security culture protects that trust — member data, reputation, the relationship. **Culture isn't a cost center; it's what lets you keep the promise you made to members.** Your role is specific: not to run the program, but to ask the questions that encourages CU leadership to build a real program.
- Start with the handout, at your very next meeting.

Thank you.



| NACUSAC 2026