

The **Human Layer:** Why Cybersecurity Is Still a People Problem

A human-centered framework for building resilient organizations



The One System You Cannot Patch

Every organization runs one production system with no patch schedule, no vendor support, and no two instances configured the same way — its people.

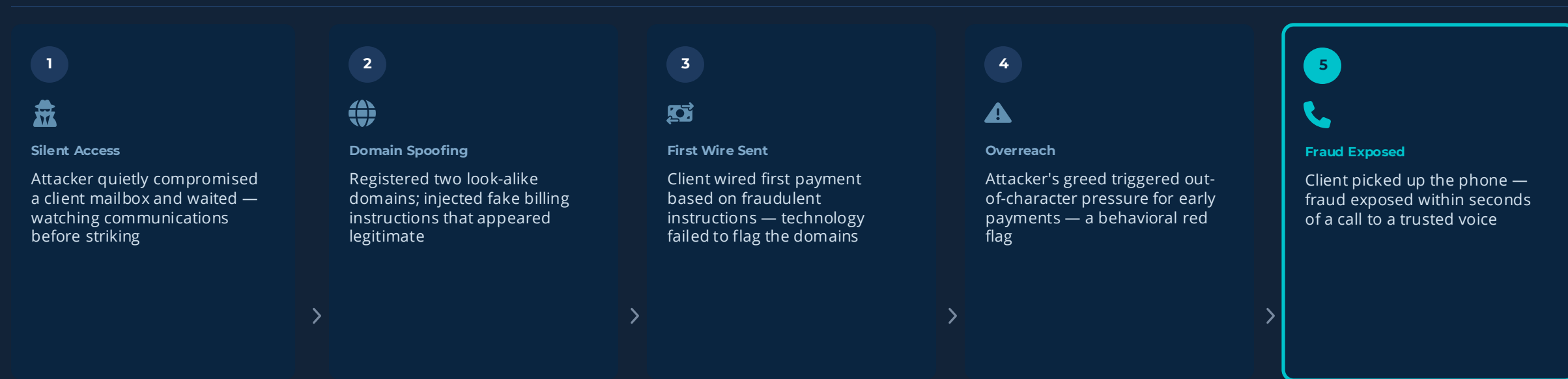
- Most cyberattacks do not start by targeting software or firewalls
- They target human trust and routine business workflows
- The most common and most costly attacks exploit people first, technology second

📌 Today's focus: **Culture** · **Human Factors** · **Crisis Decision-Making**



A Story About a Phone Call

A Business Email Compromise at a law firm shows how attackers exploit trust — and how a single human instinct stopped the fraud.



Technology failed to flag the look-alike domains — human eyes missed the slight variations.



What saved the day: out-of-band verification — a simple call to a trusted voice. Not a tool. Not a policy. A person.

Today's focus: **Culture** · **Human Factors** · **Crisis Decision-Making**

Culture Is the Bedrock

Culture is built by leadership example — what we reward and what we punish.



Practice 01

Blameless Postmortem

Ask what signals our culture sent — not who to blame. Turn every incident into a mirror for the organization, not a tribunal.



Practice 02

Psychological Safety

Do our people feel safe questioning a strange request — or too polite to push back? Safety to speak up is priceless and non-negotiable.



Practice 03

Celebrate Good Catches

Reward vigilance in the moment — not only after an incident. Recognition of near-misses reinforces the behavior we want repeated.



Practice 04

De-Shame Mistakes

When leadership admits errors openly, it normalizes learning over blame. A culture of honesty scales security awareness across the entire org.

“ Psychological safety is priceless — it is the foundation every other control is built on. ”

Culture in Action

Making Security Part of Daily Life

If security only comes up in October or after an incident, it is not in the company's DNA.

- **Security is often associated with mandatory training, warnings, or restrictions**
- **Reward good behavior:** thank-you notes, shout-outs, and small rewards for smart security choices
- **Keep it fresh:** slip security stories and tips into regular communications — not to preach, just to stay top of mind
- Over time, security stops being "that thing the infosec team does" — it becomes **"how we do business"**
- **Payoff:** a strong culture amplifies every control we put in place

“ “This doesn't feel right — I'm going to make a call.” That was culture.



Why Well-Intentioned People Take Risky Actions

Even in a strong culture, people make risky decisions — and the reasons are predictable.



Cognitive Overload

100+ emails a day makes it impossible to give every message perfect attention. After a point, the inbox becomes noise — and threats slip through.



Overconfidence

The most tech-savvy people sometimes take the biggest risks — because they believe they can handle it. Expertise breeds a false sense of immunity.



Workflow Pressure

When deadlines loom and a process feels too slow, people improvise. That is precisely when risk creeps in — urgency overrides caution.



Security Fatigue

Too many warnings, restrictions, and mandatory trainings without positive reinforcement desensitizes people — turning vigilance into exhaustion.

Three Approaches to Reduce Human Risk

Make the secure way the easiest way.

1



Reduce Friction

Bake security into the environment. **Automate and remove decision points** from end-user workflows — so the secure path is the path of least resistance.



2



Targeted Support

A small percentage of employees account for a **disproportionate share of incidents**. Provide additional coaching to those who consistently encounter difficulties.



3



Lead with Empathy

When someone circumvents a control, ask: **"Was there something we made too difficult?"** Shift from blaming individuals to designing for real-world behavior.



Section 3

Human Decision-Making During Incidents

Organizations come apart during crises not because of technical failures, but because people froze or squabbled over authority.

- In a true crisis, **runbooks go out the window** if people aren't ready to improvise
- ☎ If a critical system needs to be shut down at 2 AM — **do we know exactly who can make that call?**
- Remedy: establish clarity ahead of time and practice — **bring teams into your response process early and often**
- Prepare for the real thing and build trust

A Mental Model for Crisis Decisions

Give people a simple question: "Is this decision reversible?"

❓ Before acting under pressure, ask: **Can we undo this?**

↻ Reversible

⚡ Act fast — then adjust

Examples

- ✓ Isolating a device or subnet from the network
- ✓ Freezing an account suspected of being compromised

⚠ Not Reversible

⏸ Get a second opinion first

Examples

- ✗ Paying a ransom
- ✗ Shutting down a machine before forensics

🛡 Foster a culture where people can **make judgment calls with confidence** — the question gives them a framework, not just instinct

Enlist Your Employees as Sensors

Every organization has hundreds or thousands of potential sensors on the network — that is our employees.

Your Human Sensor Network



Appoint Security Champions

Embed champions across departments — people not on the security team who serve as eyes and ears inside their functions.



Leverage Peer-to-Peer Influence

When a respected colleague pushes for a secure practice, it lands far better than any top-down mandate from the security team.



Make Security a Team Sport

Everyone knows their position and plays it — the entire workforce becomes an active layer of defense, not a passive risk.



The Entire Human Layer in a Single Act

One person, feeling like something was off, picked up the phone instead of hitting reply. That is the human layer working.

- Cybersecurity will continue to evolve but the Human layer remains central
- As automation handles routine tasks, the decisions left for people **only become more important** — judgment, ethics, context, accountability
- The future of cybersecurity isn't just about building smarter tools — **it is about building better human systems**
- **If we invest in people as deliberately as we invest in technology, we turn the weakest link into one of our greatest strength.**