PURE EXPERTZ

SERVICES THAT YOU CAN TRUST

A WHITE PAPER FOR HR AND PEOPLE LEADERS

Smart Systems, Strong Humans

Safe AI adoption, workplace safety and a security culture people trust: what HR and people leaders can put in place now, before the next tool arrives and before the next incident.

SAFE AI ADOPTION
Owners, written rules and training before tools

THE BOARDROOM
Workforce, physical and cyber risk are one conversation

SECURITY CULTURE
Prevention that starts earlier than the incident

TRAIN THE TRAINER
Knowledge that stays inside your organization

THE ALLIANCE
Block by Block: education first, free to join

AI IMPACT FORUM
Nov 12–14, online. Day 2 is built for HR leaders

Andy Babala, CPP · Pure Expertz

Edition 10 · Current as of November 1, 2026

SMART SYSTEMS · STRONG HUMANS · BLOCK BY BLOCK

THE SHORT VERSION

One question on every people leader's desk

Every week, HR and people leaders are asked to answer for two things at once: the AI tools arriving in every department, and the safety of the people who use them. Who approved this tool? What data went into it? Who reads the concern an employee filed last night? Who confirmed that the candidate on the video call was who they said they were?

For most organizations those questions land on HR by default. HR writes the policies, runs the training, receives the concern that arrives sideways, and manages the hardest moments of employment: hiring, discipline and separation. That makes HR the natural owner of the question boards are now asking: **what do we owe our people, and have we decided who owns it?**

This paper looks at that question the way a security professional looks at everything: as a system. People who are trained, routines that are written down, tools that surface what matters, and a named owner for every decision. AI puts weight on all four at once. Handled well, it makes an organization safer and stronger. Handled carelessly, it multiplies the weak spots.

The first half explains why AI, workplace safety and trust now meet on HR's desk, and lays out a practical playbook: three tiers of responsibility for AI, a one-page policy, a security culture people can see, and training that sticks because people inside the organization learn to teach it.

The second half describes what Pure Expertz does about it: train-the-trainer programs, cohorts, consulting and builds, the **Block by Block AI Safety and Security Alliance**, which puts education first, and the **AI Impact Forum**, November 12–14, 2026, whose second afternoon is built for HR and people leaders. The idea underneath it all fits in four words: **Smart Systems, Strong Humans.**

FIVE COMMITMENTS FOR HR AND PEOPLE LEADERS

1. **Name an owner for every AI decision**, and write down who approves which tool, which use and which data.
2. **Keep employment decisions with people.** Use AI to draft and suggest, tell people when AI plays a part, and let a person decide.
3. **Build one reporting path people trust**, with a named person who reads it the next morning and closes the loop.
4. **Train everyone, starting with the people who notice first**, then train trainers inside so the knowledge stays.
5. **Practice together.** One short tabletop a quarter with HR, security, IT and a leader in the same room.

INSIDE

1 Why now: AI, safety and trust meet in HR
2 The author: a security professional
3 Safe AI adoption: owners and rules first
4 The boardroom: three risks, one conversation
5 Workplace safety and security culture
6 Training that sticks: train the trainer
7 Cohorts, consulting and builds
8 The Block by Block Alliance: education first
9 The AI Impact Forum, November 12–14
+ Start this week, contact, sources, disclosures

PART 1 · WHY NOW

AI, safety and trust now meet in HR

Adopted, not adapted

Most organizations have already adopted AI. Far fewer have adapted to it. In the 2024 Work Trend Index, a survey of 31,000 people in 31 countries by Microsoft and LinkedIn, 75 percent of knowledge workers said they use generative AI at work, and 78 percent of those users said they bring their own AI tools to work. Only 39 percent of people who use AI at work said they had received AI training from their company, and 60 percent of leaders said they worry their organization's leadership lacks a plan and vision to implement AI (Source 1).

75% of knowledge workers use generative AI at work

78% of AI users bring their own AI tools to work

39% of AI users have received AI training from their company

60% of leaders worry leadership lacks a plan and vision for AI

Microsoft and LinkedIn, 2024 Work Trend Index Annual Report (May 2024), a global survey. Your own workforce may differ; an anonymous inventory (Part 3) tells you where you stand.

That gap is where the risk lives, and it is a people problem before it is a technology problem. Tools nobody approved, data nobody decided to share and output nobody checked are what turn a productivity tool into an exposure. Closing the gap takes owners, written rules and training, which is the everyday work of HR.

AI-era fraud now reaches the hiring desk and the payroll desk

In its 2025 Internet Crime Report, the FBI's Internet Crime Complaint Center (IC3) recorded 1,008,597 complaints and $20.877 billion in reported losses, a 26 percent increase from 2024. Business email compromise alone accounted for about $3.05 billion in reported losses. For the first time, the report counted complaints with AI-related information: more than 22,000 of them, with adjusted losses above $893 million (Source 2).

Two details in that report belong in every HR team's next meeting. The FBI describes chat generators producing "official-sounding emails mimicking a company's CEO," and voice cloning used to request payments. It also describes voice spoofing, and potentially deepfakes, during online job interviews, where the goal "generally appears to be gaining access to private computer networks." **A hiring process is now a security control.** So is the habit of calling back on a known number before anyone changes a payment or a direct-deposit detail.

The rules are moving, and they differ by place

Employment rules for AI and for workplace violence are changing quickly and unevenly. A few examples, checked on November 1, 2026:

WHERE	WHAT APPLIES
Illinois	Since January 1, 2026, amendments to the Illinois Human Rights Act (Public Act 103-0804) make it a civil rights violation for an employer to use AI that has the effect of subjecting employees to discrimination on the basis of protected classes in covered decisions, such as recruitment, hiring, promotion, discipline and discharge, and they require employers to give notice when AI is used for those decisions. The Illinois Department of Human Rights has proposed rules on how notice is given (Source 3).
Illinois	Since 2020, the Artificial Intelligence Video Interview Act has required employers that use AI to analyze recorded video interviews for Illinois-based positions to notify applicants, explain how the AI works and obtain their consent before the interview (Source 4).

California	Since July 1, 2024, Labor Code section 6401.9 has required covered employers to establish, implement and maintain a written Workplace Violence Prevention Plan, train employees and keep a violent incident log (Source 5).
Federal (OSHA)	OSHA states that there are currently no specific OSHA standards for workplace violence; it enforces through the General Duty Clause. A rule for health care and social assistance remains a long-term item on the federal regulatory agenda, with no date set for a proposed rule (Sources 6–8).

This is not legal advice and not a complete list. The point is practical: an HR team that already knows which AI tools touch employment decisions, has written its rules down and has trained its people is ready for whatever its own jurisdiction requires. Your counsel decides how each rule applies to you.

The front line now runs through ordinary workplaces

Outside the office, public safety is being reorganized too. Many police departments and emergency communications centers describe staffing strain. Cities collect more camera, sensor and records data than they have trained people to review. More early behavioral-health work is moving to clinicians and community partners. And AI is arriving in public safety through features added to systems agencies already own. Put together, the first person to notice a problem is more and more often a receptionist, a nurse, a store manager, a supervisor or an IT administrator. Many of them report to HR.

> The front line of public safety now runs through ordinary workplaces. Most of them have not been told.

Trend descriptions without a numbered source come from public reporting and professional experience. Conditions vary by city and by organization; every reader should check their own.

PART 2 · THE AUTHOR

A security professional who sees systems



Ask a security professional what went wrong after an incident and you rarely hear about one bad moment. You hear about a trail: the warning sign nobody was trained to notice, the report that had nowhere to go, the decision that belonged to no one.

Andy Babala has spent his working life on that trail. He is a Certified Protection Professional (CPP), board certified in security management. He has more than ten years in security, including security management roles, where the job is as much about training people and writing down routines as it is about posts and patrols. The CPP is the credential that career earned him, and it is the only credential this paper claims.

He did not start in security. He began his career in direct patient care. He holds a four-year degree earned in Poland and worked in Illinois outpatient rehabilitation and workers' compensation settings, including clinic operations. That is where he learned how a team's day actually runs, and how much of anyone's safety depends on the person who notices first.

Today he leads Pure Expertz, a marketing and automation agency with an education practice, building practical AI systems for organizations: the intake that answers for a team, the follow-up that goes out without being chased, the report that stops eating a Friday, and the written rules that say who approves each tool. Pure Expertz runs its own operation the same way, so the hours go to conversations and decisions, the part a person actually has to do.

He writes for HR and people leaders because they own the moments where systems meet people: the policy, the training, the concern and the hard conversation.

> A response plan tells you who to call after something has gone wrong. A prevention plan decides, in advance, what a trained team watches for, who notices, and what happens next.
>
> **ANDY BABALA, CPP**

Most organizations have the first plan. Far fewer have the second. The same technology that changes what someone acting in bad faith can do also changes what a trained team can see early.

Why a security professional is writing about AI

AI is usually sold as a productivity story. Seen from security, it is also a story about exposure and about early warning. The same tool that drafts a letter can imitate a voice, and the same software that schedules a shift can surface a pattern a supervisor would have missed. Somebody has to decide, in advance, which of those uses an organization wants, who watches them, and what happens when they go wrong. That has always been a security manager's question. It now sits on every people leader's desk.

Train the whole company, not just the C-suite

Pure Expertz trains the whole organization, not one team and not only the executives, because leadership without operator literacy is theater, and operator literacy without leadership is chaos. Leadership sessions, department sessions and function-specific problem solving all point at one goal: your people can run the systems, and teach them, after we leave.

PART 3 · SAFE AI ADOPTION

Safe AI adoption: owners, rules and training before tools

Safe AI adoption is not a software purchase. It is a set of decisions made in advance: which tools are allowed, what may go into them, who checks what comes out, and who can switch them off. HR does not have to make every one of those decisions, but it is usually the department that makes sure they are written down, taught and followed.

Three tiers of responsibility

TIER 1 **AI drafts, a person approves**	**Everyday work.** First drafts of job posts, policies and announcements; meeting summaries; schedules; training refreshers; reminders. Nothing leaves the building until a person has read it.
TIER 2 **AI suggests, a person decides**	**Judgment calls.** Which training a team needs first; themes in anonymous survey comments; which open items to review first; what to say in a hard conversation. The suggestion is an input, never the decision.
TIER 3 **People only**	**Decisions about a person.** Hiring, discipline, discharge and pay decisions; any decision to intervene with an individual; reports to authorities; anything involving health information; money movements and changes to payment details.

Pure Expertz's recommendation, written for people-facing work. Where a law allows AI to play a part in a decision, the tiers still ask the same question: who signs?

AI IN EMPLOYMENT DECISIONS

Employment decisions deserve the strictest tier. Pure Expertz recommends that final hiring, discipline, discharge and pay decisions stay with people; that anyone affected is told when AI played a part; and that every AI tool used in those decisions is reviewed for fairness before it is switched on and on a schedule after. In some places, including Illinois, notice is a legal duty and not only a good practice (Part 1). Your counsel decides what your obligations are; the habit of writing down who decided, and why, serves you everywhere.

What "without losing control" means

- You know which AI tools are in use, including the ones nobody formally approved.
- A named person approves each tool and each use.
- Sensitive data stays out unless someone with authority decided it may go in, and the reason is written down. Employee personal data and health information never go into an unapproved tool.
- A person reviews what matters before it leaves the building.
- Your team can run, change or switch off every system without outside help, on accounts you own.

Start with an amnesty, not a crackdown

People bring their own tools because the tools help them. An anonymous, no-blame inventory of what people already use tells you more in a week than a ban will in a year. Approve what is safe, replace what is not, and publish a short list everyone can find. A rule people understand beats a rule people work around.

THE ONE-PAGE AI USE POLICY, AND A CHARTER FOR EVERY AGENT

Agents are systems that are given a goal and work across connected apps, sometimes for hours, without being asked again. With a chatbot, the risk was a bad answer. With an agent, the risk is a bad action, taken quickly and repeated. Before any agent works for your organization, write one page:

Goal: one sentence, with a clear "done."

Allowed alone: reversible, low-risk actions such as drafting, organizing, reminding and researching.

Never: payments and payment-detail changes, employment decisions, health or legal decisions, personal data leaving approved systems.

Log and review: where its actions are recorded, and who reads the log each week.

Owner: the person accountable for the agent's work.

Needs approval: anything sent to a candidate, employee or client; anything published; anything that commits time or money.

Limits: which apps and data it may touch, and how much it may spend.

Off switch: who can stop it, and how fast.

People decide. Agents do the work. A person signs off.

A framework you can check your work against

The tiers and the charter line up with the four functions of the National Institute of Standards and Technology's voluntary AI Risk Management Framework (AI RMF 1.0, released January 2023): **Govern** (who owns and who signs), **Map** (where AI touches candidates, employees and customers), **Measure** (errors caught, concerns raised, time saved) and **Manage** (a short quarterly review that changes something). NIST's Generative AI Profile (NIST AI 600-1, July 2024) applies the same framework to generative tools. Both are free to download. NIST does not endorse Pure Expertz (Sources 9–10).

A 30-day start for an HR team

WEEK 1

See it

Run the anonymous AI-tool inventory, and time three recurring HR tasks as they are done today.

WEEK 2

Teach it

One hour for managers with your own examples: the call-back rule, pausing on urgency, and where a concern goes.

WEEK 3

Write it

The one-page AI use policy, "who approves what," and a charter for any agent you plan to use.

WEEK 4

Practice it

A 30-minute tabletop with HR, security, IT and a leader. Adjust what broke, and choose your first internal trainers.

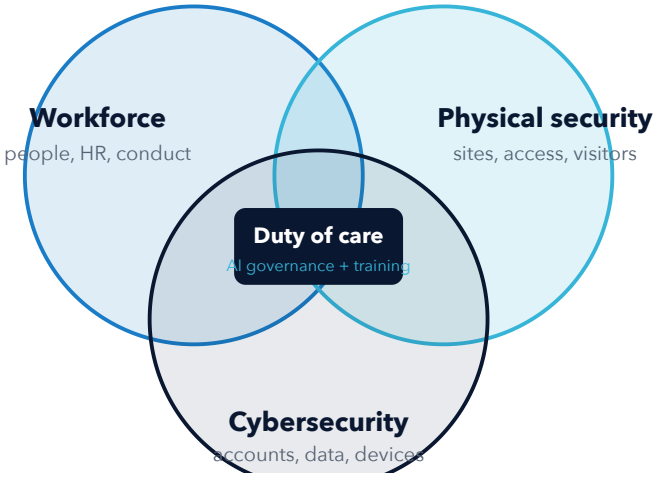
PART 4 · THE BOARDROOM

Three risks, one conversation

Not long ago, workforce issues, physical security and cybersecurity belonged to three different departments, with three different owners and three different budgets. Boards are finding that the same incident now runs through all three.

Consider how incidents actually unfold now. A finance manager gets a call in the chief executive's voice asking for an urgent transfer, and the voice was generated by AI. A former employee who left on bad terms still has a badge that works and a login nobody disabled. A threat against a facility is posted online on a Sunday night and seen by an employee on Monday morning, who is not sure whom to tell. A candidate on a video interview is not who they claim to be. A remote employee's home network becomes the way into the company. Each of these is a people problem, a physical problem and a cyber problem at once.

AI speeds all of it up. It lowers the cost of impersonation and phishing, it lets one bad actor do the work of many, and it puts powerful tools into every department, often before anyone has approved them. In May 2025 the FBI warned that malicious actors were using text messages and AI-generated voice messages to impersonate senior U.S. officials (public service announcement I-051525-PSA). Its advice is the habit every front desk and every payroll team now needs: find the person's number independently and call back to verify (Source 11).



Where all three overlap, the question is the same: what do we owe our people, and have we decided who owns it?

Where AI, safety and trust meet in the employee lifecycle

MOMENT	WHAT CAN GO WRONG NOW	WHAT A STRONG SYSTEM DOES
Hiring	A candidate on video is not who they claim to be; an AI screening tool filters people unfairly and nobody notices.	Confirms identity in live steps; knows every AI tool in the process; gives notice where required; a person makes the decision.
Onboarding	New hires learn the tools before they learn the rules.	Day one includes the AI use policy, the reporting path and a short lesson on greeting visitors and calling back to verify.
Everyday work	Unapproved tools; sensitive data pasted into them; a cloned voice asks for a transfer or a direct-deposit change.	A published list of approved tools; written data rules; a call back on a known number before any payment or payment-detail change.
Concerns and conflict	A worrying comment goes nowhere, so people stop reporting.	One reporting path people trust; a named person who reads it; early support first; the person who reported hears what happened next.

Discipline and separation	Access outlives employment; a hard conversation escalates.	People-only decisions; badges and logins removed on time; a plan for a respectful exit; the organization's own trained team involved when there is a concern.
Remote, traveling and solo work	The workplace reaches homes, cars and job sites with nobody nearby.	Check-in routines; home-network basics; training that also protects employees' families at home.

FIVE QUESTIONS FOR HR LEADERS THIS QUARTER

1. Which AI tools are our people actually using, including the ones nobody approved, and who decides what is allowed?
2. Where does AI touch an employment decision here, who reviews it, and how do we tell the people affected?
3. If an employee sees a warning sign tonight, where does the report go, and who reads it tomorrow morning?
4. Could a cloned voice, a fake candidate or a convincing email move money, data or access out of this organization? What stops it?
5. When someone leaves on bad terms, who removes their badge and logins, and how fast?

None of this asks a company to become a police department. It asks leadership to decide, in advance and in writing, what the organization will do, who owns each piece, and how it will work with the public agencies that keep their own authority. An employer's people live in the communities around its sites, so the protection it provides, or fails to provide, is felt well beyond its payroll.

PART 5 · WORKPLACE SAFETY AND SECURITY CULTURE

Prevention starts earlier than the incident

Picture a front desk on a Tuesday afternoon, a nurse at the start of a shift, a supervisor on the floor, a recruiter on a video call. Long before anyone calls for help, someone in that spot usually saw something. The question is whether they were trained to recognize it, and whether their report had somewhere to go.



Most programs start too late

Most safety programs are built around the response: the investigation, the discipline, the call for help, the after-action report. Those matter. But a program that begins at the incident has already missed its best chance. By the time something is serious enough to set off a formal response, the people nearby have often been uneasy for a while, and nobody gave them a way to say so.

Where real prevention starts

Observable behavior. What a person does and says, and how that changes over time. Never who someone is, and nothing based on race, religion, national origin, disability, age, sex or any other protected characteristic.

Early support. A conversation, a check-in, a schedule change, a referral to help the organization already offers, such as an employee assistance program. Most concerns are best met with support long before they need anything else.

Practical systems. A named person who receives concerns, a simple way to report, a record kept with care, and a regular review of what came in and what happened next.

> Faster, cheaper, more capable tools don't make a place safer on their own. People who've decided what they're looking for do.
>
> ANDY BABALA, CPP

What the public research says

Pure Expertz builds its prevention education on free, public sources rather than on any proprietary method. The research base is the U.S. Secret Service's National Threat Assessment Center (NTAC), which publishes its research for anyone to read. Its January 2023 study, *Mass Attacks in Public Spaces: 2016–2020*, examined 173 attacks in businesses and workplaces, schools, houses of worship and other public places. Two of its key findings speak directly to people leaders (Source 12):

NTAC KEY FINDING

"Most of the attackers had exhibited behavior that elicited concern in family members, friends, neighbors, classmates, co-workers, and others, and in many cases, those individuals feared for the safety of themselves or others."

NTAC KEY FINDING

"Half of the attackers were motivated by grievances, and were retaliating for perceived wrongs related to personal, domestic, or workplace issues."

The same report is careful about what this means. Behavioral threat assessment programs, it says, "are not designed to predict who will become violent," but to identify, assess and intervene with people whose behavior raises concern. That assessment work belongs to an organization's own trained team, and to law enforcement where needed. **Pure Expertz does not conduct threat assessments.** What it teaches is the step before: noticing, and making sure a concern reaches someone who can act. The Director's message that opens the report names who shares that work, including workplace managers, school personnel and faith-based leaders alongside law enforcement and mental health professionals. That is the audience of this paper.

The four steps, in CISA's order

Pure Expertz teaches this as education, using the four steps in CISA's free De-escalation Series (cisa.gov/resources-tools/resources/de-escalation-series; Source 13):

STEP 1	STEP 2	STEP 3	STEP 4
Recognize	**Assess**	**De-escalate**	**Report**
Notice when someone's behavior shifts away from their usual, before it turns into a crisis.	Decide how serious it is, and whether anyone is at risk right now.	Lower the temperature: a calm voice, some space, more time.	Bring it to the person your organization has named, the same day.

The four steps and their order are CISA's. CISA publishes the series for critical-infrastructure owners and operators, and anyone can download and use it at no cost. The descriptions above, and the audiences in this paper, are Pure Expertz's own. CISA does not endorse Pure Expertz.

The Power of Hello: vigilance without confrontation

For front-line staff, CISA's free Power of Hello materials teach a simple, non-confrontational habit in four steps: **Observe, Initiate a Hello, Navigate the Risk, and Obtain Help**. A friendly greeting, offered to everyone, often tells a lost visitor from a real concern, and it gives an employee a way to act without becoming a guard. The steps are CISA's; CISA does not endorse Pure Expertz (Source 14).

Insider risk: HR has a seat at the table

Many concerns start inside: a grievance, a separation that went badly, access that was never removed. CISA's free *Insider Threat Mitigation Guide*, now in a 2026 edition, and its guidance on assembling a multi-disciplinary insider threat management team describe programs that bring HR, security, IT, legal and leadership together, balancing protection for the organization with care for the individual. Pure Expertz teaches the step before any assessment; the team belongs to the organization (Source 15).

WHAT A SECURITY CULTURE LOOKS LIKE

A security culture is what people do when no one is checking. You can see it in small habits:

- People verify before they pay, share or change access, and nobody is embarrassed to call back.
- Visitors get a hello, every time, from whoever is nearest.
- A worrying comment is reported the same day, and the person who reported it hears what happened next.
- Near-misses are discussed openly, without blame.
- Leaders follow the same AI rules as everyone else.
- The reporting path works for remote, traveling and night-shift staff too.

Safety culture, security culture and AI-era culture are one culture. HR shapes all three through who gets hired, what gets taught, what gets recognized and how concerns are handled.

Where prevention education belongs

WORKPLACES

A duty-of-care conversation

Prevention at work is a duty-of-care conversation, not a compliance checkbox. Pure Expertz explains which tools and duties exist; the employer's own counsel decides how they apply. The work draws on HR, security and IT together, the same convergence boards see in Part 4.

HEALTH SYSTEMS

Inside the existing program

In 2018, health care workers accounted for 73 percent of all nonfatal workplace injuries and illnesses due to violence, according to the U.S. Bureau of Labor Statistics (Source 16). Education fits inside the organization's own workplace violence prevention program and never replaces security training, HR process or clinical judgment.

SCHOOLS

Inside the school's own process

Many schools and districts already have a threat assessment team, often because the law requires one. Pure Expertz does not replace or sell into that team; education for staff and families fits inside the school's own process, and any paid program for a public district follows the district's procurement rules.

Health-system programs run discovery, a leadership briefing, one pilot unit, then unit-by-unit scale with train-the-trainer. Programs are designed to avoid collecting protected health information or student records.

FEDERAL RULES, AS CHECKED ON NOVEMBER 1, 2026

OSHA states that there are currently no specific OSHA standards for workplace violence; it enforces through the General Duty Clause of the Occupational Safety and Health Act. A rule for health care and social assistance has been in rulemaking since a 2016 request for information, and the federal regulatory agenda lists it as a long-term action, with its small-business review completed in 2023 and no date set for a proposed rule (Sources 6–8). Some states, such as California, already require written plans (Part 1).

CITIES, DISTRICTS, POLICE AND FIRE

Public bodies get public terms. The offer is public education the body hosts, open to residents, on identical terms for every community, with nothing of value to any official: no meals, gifts, tickets or thank-you items. A paid program is bought only through the body's own purchasing process. For police and fire departments it is education only: no assessments, patrols, investigations, threat assessments, security surveys, or alarm or monitoring design. It is not accredited for any mandated law-enforcement training credit.

GROUND RULES FOR PREVENTION EDUCATION

- Pure Expertz provides training, not security services. No guards, patrols, investigations, threat assessments or security surveys, and no alarm or monitoring design. Education only; no result is promised.
- Not officer training, and not accredited for any mandated law-enforcement training credit.
- Programs are designed to avoid collecting protected health or student records. If patient information were ever needed, a business associate agreement would be signed first. Compensation is fixed for the work described and is never tied to patient referrals, admissions, census, revenue, or the volume or value of any business between the parties.
- Public buyers (cities, districts, police and fire): each body's own ethics and purchasing rules apply, and nothing of value goes to any official.
- Nonpartisan, always. No nation or group is named as the threat; the subject is behavior, speed and method.

PART 6 · TRAINING THAT STICKS

Train the whole company, then train the trainers

Training fades when it is an annual video. It sticks when the people who notice first practice with their own examples, and when someone inside the organization keeps teaching after the consultant leaves.

Three levels, one calendar

LEADERSHIP

Set the rules

Who owns AI decisions, what the organization owes its people, and how leaders model the same habits they ask of everyone else.

DEPARTMENTS

Apply the rules

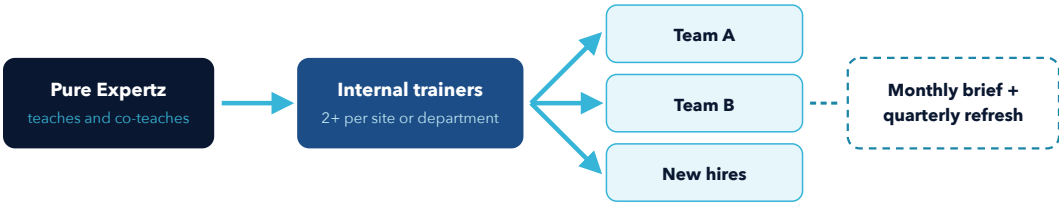
HR, finance, operations and IT turn the policy into routines: approved tools, data rules, call-back verification, the reporting path.

FRONT LINE

Build the habits

The people at the front desk, on the floor and in the inbox practice the four steps, the Power of Hello and the pause on urgency. Nobody learns a tool without its rules.

Train the trainer: leaders learn it, then teach their own people



1. **Choose.** Each site or department names at least two internal trainers, people others already trust and go to with questions.
2. **Learn.** Trainers complete the AI Impact Academy train-the-trainer path: the AI use rules, the four steps, the Power of Hello habits, the call-back rule and how to run a tabletop.
3. **Co-teach.** Their first sessions are taught alongside Pure Expertz, using their own examples and their own language.
4. **Lead.** They teach on their own with a ready kit, and bring hard questions back to the trainer group.
5. **Refresh.** The monthly prevention brief and a quarterly trainer session keep the material current as the tools change.

WHY TRAIN THE TRAINER

- Leaders learn it first, then teach their own people, so the message comes from someone the team knows.
- Knowledge stays when staff turn over, and new hires learn it in week one.
- Internal trainers know the culture, the shifts and the language of their teams.
- The organization stops depending on an outside instructor for every new group.

The AI Impact Academy is private professional education. Completing it is not a credential, and it awards no title, designation or academic credit.

What gets measured

Participation; competency on self-checks before and after; concerns routed through the reporting path; AI tools inventoried and approved. Findings only, with the host's own data. No outcome or saving is promised.

A monthly prevention brief

A short read a leader can forward to the front line: one behavior pattern worth recognizing, one AI-era scam to brief the front desk on, one free public resource and one ten-minute tabletop question. Ask for it at community.pureexpertz.ai.

PART 7 · COHORTS, CONSULTING AND BUILDS

Leaders learn faster together

Why cohorts

Masterminds and cohorts put leaders at a table instead of in an audience. Cohorts run for three months with at least two people from one organization, because one person goes home and nothing changes; two go home and the organization changes.

Cohorts are grouped by role or industry, such as HR and people leaders, or healthcare and home-care operators, so everyone at the table is working on the same kind of problem. Each participant works on their own operation: the AI use policy, the reporting path, the first group of internal trainers. New cohorts form after the AI Impact Forum.

The order of work

Consultancy comes first. A team needs to see how a deployment actually happens, week by week and day by day, in its own operation. Implementation comes after a cohort, once the people who will use the system understand it. The other order is how organizations end up with expensive tools nobody opens.

Consulting: AI implementation without losing control

For organizations ready to build, the advisory engagement is month to month: a written scope, a weekly working session with Andy, and advisory and deployment hours applied to the organization's AI adoption, from systems selection and workflow design to staff enablement and rollout support. The services are consultative. Your team makes and owns the implementation decisions, and no result or saving is promised.

The connector's role

No single firm has every answer. An organization that takes duty of care seriously may need a cybersecurity firm, employment counsel, a physical security integrator, behavioral health and employee assistance resources and technology vendors, all working from one plan. Andy's role is to be the connector: to see the problem as a system and bring the right partners and providers to one table. Each organization chooses and contracts with its providers directly; an introduction is not an endorsement, a ranking or a guarantee.

An AI campus inside your organization or community

The most durable thing Pure Expertz builds is a small campus where people learn the tools, practice on real work and teach the next group. Pure Expertz installs it and leaves it behind.

THE TEACHING LAYER

AI Impact Academy

The train-the-trainer path in Part 6, so the knowledge stays after Pure Expertz leaves. Private professional education; completing it is not a credential.

THE GATHERING LAYER

Community in a Box

A community program built for your organization, under your name: the rooms, the rhythm, the content calendar, the onboarding and the systems that run it, on your accounts, with your data and your members.

THE WORKING LAYER

30-Day AI Build

We configure your AI toolkit (intake, a content engine and workflow automations) on accounts you own, under your brand, and train your team to run it. You own your accounts, data and configurations.

GROUND RULES FOR EVERY BUILD

- The buyer is an organization that will use what is built, never an individual buying a business. A written scope comes before any work. You buy any equipment and third-party subscriptions yourself, in your name.
- Your brand, not ours: no Pure Expertz brand, marketing plan or revenue share comes with any build, and Pure Expertz takes nothing from your revenue. Pure Expertz keeps its own templates and methods, which you may use inside your organization. No income, member-count or payback claims; no result or saving is promised.

PART 8 · THE COALITION

The Block by Block AI Safety and Security Alliance: education first

The Block by Block AI Safety and Security Alliance is Pure Expertz's voluntary principles for using AI responsibly in safety and security work, and the coalition of people and organizations who hold themselves to them. It costs nothing to join. Members acknowledge three laws and hold themselves to them, block by block.

LAW 1

Legal

Members commit to following the law where they operate. Where the law is settled, we follow it. Where it is unsettled, as much of AI law is in 2026, we take the more conservative path and document our reasoning.

LAW 2

Ethical

All activity respects the professional ethics of each participant's profession and the ethical norms of the markets we serve. Compliance with the law is necessary but not sufficient.

LAW 3

Moral

All activity considers its impact on the people, families, communities, and institutions affected. We reject results achieved at the cost of human harm.

Education comes first

The Alliance's first job is education. Before networking and before introductions, members learn a shared vocabulary and the same free public tools, so that when two organizations on the same block need each other, they already speak the same language.

- **A shared vocabulary:** observable behavior, the four steps, the Power of Hello, the call-back rule and the three tiers of responsibility for AI.
- **A free-resources map:** CISA's De-escalation Series, Power of Hello materials, tabletop exercise packages and Insider Threat Mitigation Guide; NTAC's published research; NIST's AI Risk Management Framework. Nobody pays for what is free (Sources 9, 12–15, 17).
- **The monthly prevention brief**, written for leaders to forward.
- **Free Clubs:** virtual-first communities of practice where trainers and leaders compare notes with peers.



Why an alliance exists

The gaps in Parts 1 to 5 are bigger than any one organization. Police cannot staff every early warning. Employers cannot run public safety. A consultant cannot be the cybersecurity firm, the employment lawyer, the facilities team and the trainer at once. What closes the gap is a coalition: organizations and providers who share a vocabulary, work by the same ground rules, and know whom to call.

What people in it get. Trusted service providers and members get access to networking events, workshops and education, and to complementary tools and solutions from one another. Everyone who comes in contact with Pure Expertz, at any layer, learns what the Alliance is and what it asks. "Trusted" means a provider has acknowledged the three laws and holds itself to them. The Alliance grades, ranks and approves no one, and nobody is promised referrals, clients or revenue.

For HR and people leaders

Join free as an organization. Bring your HR, security and IT leads into the same room. Send your internal trainers to the Clubs to compare notes with peers. And ask the providers you already use whether they hold themselves to the same three laws.

What it asks, and what it doesn't

The Alliance asks an organization to decide its AI guardrails in advance, name who owns them, and train the people who would notice first. It asks every member to make factual claims only: if you don't know, say "I don't know, let's verify." It does not grade, rank or approve anyone. Joining is a commitment a member makes, not a status Pure Expertz awards, and nobody pays dues.

It is honest about its stage. The first written Rules and Regulations took effect May 1, 2026; the full name was locked in July 2026; a full rewrite of the charter was prepared in September 2026. The principles exist; an independent body around them does not yet. The Alliance is in development and currently administered by Pure Expertz.

JOIN FREE

Join through the community at **community.pureexpertz.ai** by acknowledging the three laws. Everything the Alliance teaches is educational. It is not legal, financial, tax or medical advice.

PART 9 · THE AI IMPACT FORUM

Three afternoons, November 12–14, 2026

The AI Impact Forum is the flagship gathering: three afternoons, 1 to 4 PM Central, online. Each afternoon runs keynotes from 1 to 3 PM, then a 3 to 4 PM panel discussion about what works now, not predictions. **Day 2 is built for HR and people leaders.**

DAY 2 · FRIDAY, NOVEMBER 13 · PEOPLE, BEHAVIORS AND PREVENTION

1:00 PM CT	**Andy Babala, CPP:** the people who notice first. Then the Day 2 keynote by **Michael Van Chau**.
2:00–3:00 PM CT	**Keynote: Dr. John D. Byrnes**, Founder, Center for Aggression Management. One hour on prevention through education.
3:00–4:00 PM CT	**Panel:** HR leaders and working professionals on prevention that works now.



KEYNOTE · 2-3 PM CT

Dr. John D. Byrnes
Founder, Center for Aggression Management



DAY 2 KEYNOTE · 1 PM HOUR

Michael Van Chau
Entrepreneur and human-trafficking prevention consultant

For HR leaders, managers and supervisors, and for the security, safety and executive teams who work beside them. Bring a colleague: the cohort rule applies here too.

DAY 1 · THURSDAY, NOVEMBER 12

Business and real estate

Running the business: Andy opens with how Pure Expertz serves organizations of every size, followed by questions submitted in advance, keynotes and a panel on what works now.

DAY 3 · SATURDAY, NOVEMBER 14

Systems

The systems that keep a business running: Andy on how a cohort is created, then keynotes and a closing panel on what works now.

JOIN

pureexpertz.com/forum

Send your question for the Day 2 speakers and panel ahead of time at **pureexpertz.com/forum/ask**.

GOOD TO KNOW

Online, from anywhere: 1–4 PM Central is 2–5 PM Eastern. Sessions are recorded with notice before anyone speaks. Speakers speak for themselves; see the disclosures.

HOW TO ENGAGE

Start this week

Start wherever you are. You do not have to buy anything to belong in the room. Three doors are open now.

FREE · TUESDAYS AND THURSDAYS

Open office hours

zoom.pureexpertz.ai

1 PM Central on Zoom. Bring one real problem and get a straight answer. No camera required, and nobody chases you afterward.

FREE · JOIN ANYTIME

The community

community.pureexpertz.ai

Meet the network, find the rooms, and join the Block by Block AI Safety and Security Alliance by acknowledging the three laws.

NOVEMBER 12-14, 2026

The AI Impact Forum

pureexpertz.com/forum

Three afternoons, 1 to 4 PM Central, online. Day 2 is for HR and people leaders.

GOING FURTHER

4 **Take a workshop or bring training in.** A four-week live workshop on one topic, or leadership, department and front-line training inside your organization.

5 **Start train-the-trainer.** Name two internal trainers per site or department and begin the AI Impact Academy path.

6 **Join a cohort.** Bring at least two people from your organization and work on your own operation for three months.

7 **Bring prevention education in.** For a workplace, health system, private school or community group: one briefing, then one pilot group. Public bodies follow their own procurement rules.

8 **Build an AI campus.** The AI Impact Academy, Community in a Box or a 30-Day AI Build under your own name, or the month-to-month advisory engagement. Every build starts with a written scope.

9 **Partner, sponsor or join as a provider.** Underwrite free briefings, contribute space, or join the trusted provider network. Written, disclosed, no say over content, no exclusivity, and nobody is promised referrals or clients.

None of these shifts will wait for a perfect plan. Name an owner. Write down the rules. Train the people who notice first. Get to know the neighbors, public and private, who share the work. That is how communities get safer: not all at once, but block by block.

CONTACT

Come meet us

Andy Babala, CPP

Pure Expertz, a marketing and automation agency

EMAIL	andy.babala@pureexpertz.com
OFFICE HOURS	zoom.pureexpertz.ai · Tuesdays and Thursdays, 1 PM CT
COMMUNITY	community.pureexpertz.ai · the Alliance joins here
AI IMPACT FORUM	pureexpertz.com/forum · questions: pureexpertz.com/forum/ask
WHATSAPP	chat.whatsapp.com/DWK4frxd24B3grpPK0lAVE

About Pure Expertz

Pure Expertz, LLC is a marketing and automation agency with an education practice. It helps leaders put AI to work safely, in their organizations and their communities, with prevention built in from the start. Founded by Andy Babala, CPP, it runs free open office hours, live workshops and training, train-the-trainer programs, masterminds and cohorts, consulting and AI implementation, the AI Impact Academy, Community in a Box and the 30-Day AI Build, prevention education, the AI Impact Forum and Pure Expertz Media. It administers the Block by Block AI Safety and Security Alliance, a free and voluntary set of principles for using AI responsibly in safety and security work.

Sources and notes

Public facts in this paper were checked against these sources on November 1, 2026. Public rules and programs change; check the source before relying on any of them.

1. Microsoft and LinkedIn, "AI at Work Is Here. Now Comes the Hard Part," 2024 Work Trend Index Annual Report, May 8, 2024. microsoft.com/en-us/worklab/work-trend-index. Survey of 31,000 people in 31 countries.
2. Federal Bureau of Investigation, Internet Crime Complaint Center, *2025 Internet Crime Report* (released April 2026). ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf. Totals: 1,008,597 complaints and $20.877 billion in reported losses; business email compromise $3,046,598,558; "Artificial Intelligence (AI) Used in Cybercrime" section: 22,364 complaints, adjusted losses above $893 million, including the employment-interview example quoted in Part 1.
3. Illinois Public Act 103-0804 (House Bill 3773), amending the Illinois Human Rights Act, effective January 1, 2026. ilga.gov. The Illinois Department of Human Rights is responsible for rules on notice; check its current rules.
4. Illinois Artificial Intelligence Video Interview Act, 820 ILCS 42, effective January 1, 2020. ilga.gov.
5. California Department of Industrial Relations, Cal/OSHA, "Workplace Violence Prevention in General Industry" (Labor Code section 6401.9, enforceable July 1, 2024). dir.ca.gov/dosh/Workplace-Violence/General-Industry.html.
6. Occupational Safety and Health Administration (OSHA), "Workplace Violence: Enforcement." osha.gov/workplace-violence/enforcement. States that "there are currently no specific OSHA standards for workplace violence" and describes the General Duty Clause, Section 5(a)(1) of the Occupational Safety and Health Act of 1970.
7. OSHA, "Healthcare: Workplace Violence." osha.gov/healthcare/workplace-violence. Request for Information published in the Federal Register on December 7, 2016.
8. Unified Agenda of Federal Regulatory and Deregulatory Actions, RIN 1218-AD08, "Workplace Violence in Health Care and Social Assistance," reginfo.gov. Latest listed entry: Long-Term Actions; small-business review (SBREFA) initiated December 29, 2022 and completed May 1, 2023; proposed rule "To Be Determined."
9. National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, released January 26, 2023; voluntary. nist.gov/itl/ai-risk-management-framework.
10. NIST, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, NIST AI 600-1, July 26, 2024.
11. FBI Internet Crime Complaint Center, "Senior US Officials Impersonated in Malicious Messaging Campaign," public service announcement I-051525-PSA, May 15, 2025. ic3.gov/PSA/2025/PSA250515.

12. National Threat Assessment Center (2023). *Mass Attacks in Public Spaces: 2016–2020.* U.S. Secret Service, Department of Homeland Security, January 2023. secretservice.gov/protection/ntac. Quotations in Part 5 are from its executive summary; the list of who shares the work is from the Director's message that opens it. The report states that it is in the public domain.
13. Cybersecurity and Infrastructure Security Agency (CISA), "De-escalation Series" (De-Escalation Series for Critical Infrastructure Owners and Operators), published September 21, 2021. cisa.gov/resources-tools/resources/de-escalation-series. Four steps: Recognize, Assess, De-escalate, Report.
14. CISA, "Power of Hello" (Employee Vigilance through the Power of Hello). cisa.gov/power-hello. Four steps: Observe, Initiate a Hello, Navigate the Risk, Obtain Help.
15. CISA, *Insider Threat Mitigation Guide* (2026 edition), and "Assembling a Multi-Disciplinary Insider Threat Management Team." cisa.gov/resources-tools/resources/insider-threat-mitigation-guide.
16. U.S. Bureau of Labor Statistics, "Workplace Violence in Healthcare, 2018," fact sheet, April 2020. bls.gov/iif/factsheets/workplace-violence-healthcare-2018.htm. Counts cases with days away from work.
17. CISA, "CISA Tabletop Exercise Packages." cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.
18. Pure Expertz, AI Impact Forum, pureexpertz.com/forum: November 12–14, 2026, 1 to 4 PM Central, online.

Disclosures

About this paper. This paper is written by Andy Babala, CPP, and reflects his views and the programs of Pure Expertz. Statistics appear only where a public source is named; trend descriptions without a source come from public reporting and professional experience, and conditions vary by city and by organization. Public agencies, companies and laws are named only to cite their public reports, resources and rules. Pure Expertz is nonpartisan and endorses no candidate or party.

Education, not advice. This is educational content. Pure Expertz provides education, consulting, marketing, automation and media services. Nothing here is legal, tax, financial, investment, medical, clinical, employment-law or security advice, and nothing replaces your own professionals. Laws are summarized as examples, not interpreted; your own counsel decides how they apply to you. No result, saving or income is promised.

Training, not security services. Pure Expertz provides training, not security services. It does not provide guards, investigations, threat assessments, security surveys, or alarm or monitoring design or installation. Its prevention programs are not accredited for any mandated law-enforcement training credit.

Programs. Pure Expertz programs, including the AI Impact Academy, are private professional education. They award no title, designation or academic credit. The only credential referenced for Pure Expertz in this paper is Andy Babala's own CPP; ASIS International, which awards it, does not endorse Pure Expertz.

Speakers. Dr. John D. Byrnes and Michael Van Chau are named, and pictured, with their permission, and each speaks for himself. Naming a speaker or the Center for Aggression Management does not mean that either endorses Pure Expertz's programs, and Pure Expertz claims no rights in the Center's materials.

Privacy and health. Programs are designed to avoid collecting protected health or student records, and Pure Expertz accesses no patient information without a business associate agreement signed first. Pure Expertz makes no claim that any program satisfies any law on an organization's behalf; each organization's own counsel decides how a program fits its obligations.

Public resources. The four prevention steps are the four steps in CISA's free De-escalation Series, and the Power of Hello steps are CISA's. The research findings quoted in Part 5 are from the U.S. Secret Service National Threat Assessment Center's public-domain reports. The FBI, NIST, OSHA, the Bureau of Labor Statistics, Cal/OSHA, Microsoft and LinkedIn are named only to cite their public statements and reports. None of them endorses Pure Expertz. Pure Expertz points people to free materials and does not resell them, and no agency seal or logo appears in this paper.

Introductions. Introductions to partners and service providers are not endorsements, rankings or guarantees. Organizations choose and contract with providers directly.

Recording. Sessions are recorded with notice before anyone speaks. Attendees' faces, voices, names and chat are never streamed, sold or published.

Prices. No prices appear in this paper. Terms for any engagement are set out in a written scope.

⬡ SMART SYSTEMS · STRONG HUMANS · BLOCK BY BLOCK ⬡