

Guided Speaker Notes – Securing the Human Element: Culture, Policy, and Trust

Prepared for ARMA Presentation by Roy Bene' II
Bene-Ficial IT Services

Slide 1 – Title: Setting the Stage

Say: 'Technology is predictable. People aren't. That's where true cybersecurity leadership begins.'

Remind them why they're here: 'Today isn't about more tools, frameworks, or compliance checklists. It's about people — and how we lead them.'

Transition: 'Let's start by talking about what happens when culture doesn't meet commitment.'

Slide 2 – The Problem with Check-the-Box Security

Say: 'Too often, we see organizations where compliance has replaced culture.'

Add: 'Policies get written, signed, and stored — but they never make it off the page.'

Personal example: 'At the City of Irving, I saw this early. People followed the policy because they had to — not because they believed in it. That had to change.'

Transition: 'So, why does this happen? Because cybersecurity isn't a technology issue — it's a human one.'

Slide 3 – Why the Human Element Matters

Say: '82% of breaches involve the human element. Not bad tech — human choices.'

Reframe: 'People aren't the weakest link. They're the least supported asset in the organization.'

Ask ARMA group: 'What if instead of calling them the weakest link, we called them our first line of defense?'

Transition: 'Culture defines how people act when no one's watching — and that's where leadership comes in.'

Slide 4 – Culture Eats Policy for Breakfast

Say: 'Culture defines behavior when no one's watching. Policy simply defines what you hope they'll do. But in governance, hope isn't a strategy.'

Add: 'Leaders can't enforce what they don't embody. People don't follow policy — they follow example. If leadership wants to bypass retention reviews, skip cybersecurity training, or make exceptions for convenience, they're teaching everyone that policies are optional.'

Transition: 'So how do we build trust — not fear — into our programs? How do we make policy something people believe in, not just comply with?'

Slide 5 – Building Trust: The Forgotten Security Control

Say: 'Fear-based security creates compliance, but trust-based security builds ownership.'

Add: 'When people understand the why, they'll protect the what.'

Personal xample: 'At Irving, I saw this first-hand. By forming the Cyber Governance Committee — and later the AI Review Committee — I stopped making the decisions alone. I gave the departments a voice. Though I was the final decision maker, it was never just my decision. That's trust.'

Transition: 'Trust transforms policy into partnership — and that's where the magic starts.'

Slide 6 – From Policy to Practice

Say: "Policies don't change behavior. People do. A great policy doesn't live in a binder — it lives in the choices people make every day."

Add: "Our goal is to make those policies real and relatable. That means translating technical or legal language into something people actually understand and connect with."

Make it actionable: "Work with HR, Legal, and Communications so your policies aren't isolated documents. Let HR weave them into onboarding. Let Legal shape them for compliance. And let Comms bring them to life through stories, visuals, and short refreshers."

Give a relatable example: "If you want staff to understand why retention rules matter, don't show them policy citations — show them what it looks like when information goes missing. When they see the human consequence, the policy suddenly has purpose."

Transition: "Once you've turned policy into practice, the next challenge is keeping that understanding consistent — and that starts with how we communicate."

Slide 7 – Communicating Security Beyond IT

Say: “The best security or records program in the world fails if no one understands it. Communication isn’t about broadcasting rules — it’s about connecting purpose.”

Add: “If we want people outside IT or Records to care, we have to speak their language. Skip the acronyms and explain outcomes. Don’t say ‘data classification tiers’; say ‘here’s how we protect what the public trusts us with.’”

Make it relatable: “Think about your own departments — HR, Finance, Legal, Public Information. Each of them handles information differently, but all of them play a part in the same story: keeping data accurate, accessible, and accountable.”

Example: “When we rolled out multi-factor authentication, we didn’t lead with tech jargon. We said, ‘It’s that double-check that keeps your paycheck safe.’ That small language shift earned more buy-in than any policy memo ever could.”

Encourage reflection: “Ask yourself — does your policy language sound like it was written *for* people, or *at* them?”

Transition: “Leadership isn’t about how loudly we communicate — it’s about how clearly we do. And clarity starts before the message is ever spoken.”

Slide 8 – Lessons from Leadership

Say: ‘In the Navy, mission readiness wasn’t optional — it was the difference between order and confusion. Before any mission, we’d run drills over and over until every step was second nature.’

Parallel: ‘That same principle applies here. Whether it’s handling sensitive records, responding to an open-records request, or preparing for an audit — consistency and clarity are what keep chaos at bay. When people know the process and trust it, they perform with confidence.’

Add: ‘Clarity prevents chaos and sharpens readiness. The clearer your procedures, the fewer mistakes you’ll see under pressure — and the stronger your organization becomes when something unexpected happens.’

Transition: ‘That’s why culture matters. When your people understand not just what to do but why it matters, you don’t need constant reminders — accountability becomes instinctive.’

Slide 9 – Turning Culture Into Measurable Impact

Say: 'a big mistake I notice In cybersecurity, we tend to count incidents — how many breaches or errors occurred. But in records and information management, that's like only measuring when something went wrong — a lost file, a missed retention deadline, or a FOIA request gone sideways.'

Add: 'Real maturity shows up when we start measuring engagement instead — how many people are doing the right thing before they're told, how often procedures are followed without reminders, how confidently your team responds when an open records request comes in.'

Examples of meaningful metrics I can use:

- Training Engagement Rate: % of staff completing records or data governance training on time and scoring above target.
- Records Review Completion Rate: % of departments completing retention schedule reviews each cycle.
- Records Correction / Self-Reporting Rate: # of times employees proactively correct or flag record issues.
- Open Records Request Response Time: Average and % on-time responses.
- Audit Findings Reduction: Fewer repeated or preventable audit issues year over year.
- Employee Engagement in Governance Activities: # of departments nominating 'records champions' or attending governance meetings.

Add: 'These aren't compliance metrics — they're culture metrics. They tell you whether people believe in the program, not just whether they're checking the boxes. Because when you start measuring belief, not just behavior, you'll know your culture is shifting.'

Encourage: 'Celebrate your "records champions" — the admin who catches a misfiled record, or the clerk who asks before deleting something questionable. Recognize them publicly — that's culture reinforcement.' We call these people our "human firewalls".

Transition: What does that look like in action?

Slide 10 – Turning Trust Into Action

Say: "When I founded the Cybersecurity Governance Committee at the City of Irving, the goal was simple — to foster enterprise-wide accountability for IT and cybersecurity decisions. I was tired of IT being the only one making the calls — getting none of the credit, but all of the blame when something went wrong."

Add: “By creating that committee, everyone — all the way up to the City Manager’s office — now had a stake in the decisions being made. It wasn’t just IT’s problem anymore; it became a shared mission.”

Continue: “Then came the AI Review Committee. That one was built out of necessity. We had a wave of AI program requests coming in, and we needed to hit pause — to create guardrails. So, we brought HR, Legal, Process Improvement, Employee Communications, and IT to the same table. That shift changed everything.”

Bridge: “The same principle applies in records and governance. When you bring multiple departments together, you move from enforcement to collaboration. People stop seeing compliance as a rulebook and start seeing it as responsibility.”

Transition: “That’s what turning trust into action looks like — not more control, but shared ownership.”

Slide 11 – Call to Action

Say: “ If you take one thing away from today, let it be this — governance isn’t about control. It’s leadership through clarity.”

Add: “ Lead with empathy. People protect what they feel part of. Teach the ‘why’ behind the policies, and they’ll carry that understanding into every decision they make.”

Continue: “Build a culture where people see themselves not as policy followers, but as *stewards* of transparency and accountability. When that happens, you don’t just build compliant teams — you build trustworthy ones.”

Close the slide: “Because In the end, this isn’t about securing systems — it’s about safeguarding integrity.”

Transition: 'Let me close with this thought...'

Slide 12 – Closing and Gratitude

Say: 'In every field — whether it’s cybersecurity, records management, or governance — the one constant is people. The systems change. The rules change. But people are the heartbeat of every decision, every safeguard, and every record we protect.'

Add: 'When you trust people, teach them, and include them — they don’t just follow policy. They own it. They see themselves as part of something bigger — a shared responsibility to protect truth, transparency, and trust.'

Go deeper: 'Because at the end of the day, records aren’t just data. They’re the story of who we are, the proof of how we lead, and the evidence that we did it right. And that story — that legacy — depends on every one of us showing up with clarity, consistency, and care.'

Close with warmth: 'Thank you for the work you do to protect that legacy — not just for your organizations, but for the people who will depend on your integrity long after we're gone.'