LEADERSHIP FOR CYBER AND TECH PROFESSIONALS

Based on "How to Win Friends and Influence People" by Dale Carnegie
and "The Leadership Challenge" by James Kouzes and Barry Posner

---

1. INFLUENCE WITHOUT AUTHORITY

Most cyber professionals can't force anyone to patch, can't make a developer fix their code, can't stop a project from shipping, and still get blamed when something breaks.

- Get an engineer to prioritize your vulnerability when they have 40 other tickets
- Convince a team to change a config without escalating to their manager
- Make security feel like part of their job, not extra work you're dumping on them
- Ask "what would make this easier for you" instead of "this is due Friday"
- The moment you rely on authority or escalation, you've already lost ground

2. MODEL THE WAY

People follow what you do, not what you say. Hypocrisy is fatal. Inconsistency kills trust fast. "Rules for thee but not for me" is remembered forever.

- Follow the same controls you enforce
- Admit mistakes publicly
- Protect your team when things go wrong
- Never throw engineers under the bus to look clean

3. MAKE PEOPLE FEEL IMPORTANT

This feels soft. It is not. Engineers are tired of being blamed. Ops teams feel punished by security.

- Give credit publicly, even if it's quick
- Correct privately, always
- Acknowledge constraints before asking for change
- Treat non security people as intelligent partners

4. INSPIRE A SHARED VISION

Leading with controls, fear, or compliance language fails. Tying security to mission and meaning succeeds.

- "Being diligent with audit prep means we're not revisiting this when we should be with family"
- "This helps the product team ship faster and shows our value"
- "Doing this right prevents after hours on call incidents"
- People rally around purpose, not CVEs

5. SEEK FIRST TO UNDERSTAND

Security solutions fail when context is ignored. Resistance often hides legitimate risk or workload issues.

- Ask what pain points the team sees
- Ask what has broken in the past

- Ask what they've already tried
- One question before proposing can save you from pushing something that will never land

6. CHALLENGE THE PROCESS

Cyber leaders must challenge bad architectures, unsafe defaults, and "we've always done it this way." But challenge systems, not people.

- Question assumptions
- Propose experiments
- Offer alternatives, not just objections
- The goal is progress, not purity

7. AVOID CRITICISM, CONDEMNATION, AND BLAME

Post incident behavior defines your reputation permanently.

- No finger pointing
- No "why wasn't this caught"
- No public shaming in reviews
- Blameless analysis, systemic fixes, learning over punishment
- Teams who feel safe reporting issues catch problems earlier

8. ENCOURAGE THE HEART

Cyber teams live in constant urgency, invisible success, and thankless prevention work. Recognition is fuel.

- Acknowledge effort, not just outcomes
- Celebrate avoided incidents
- Thank people for boring, correct work
- Burnout kills more security programs than attackers do

LEADERSHIP ACCORDING TO ME: FAILURES AND FREEBIES

- Be gracious when able. Crushing someone's spirit who had good intent is a trust killer.
- You still have to produce. Showing you do work matters.
- Toxic environments need different leadership. Sometimes your whole year is boundary setting or trust rebuilding.
- Look at your processes, people, and projects from a birds eye view.
- Be the enabler, the tactful honest professional, the one who listens first, protects their team, and remembers that people rally around purpose, not policies.