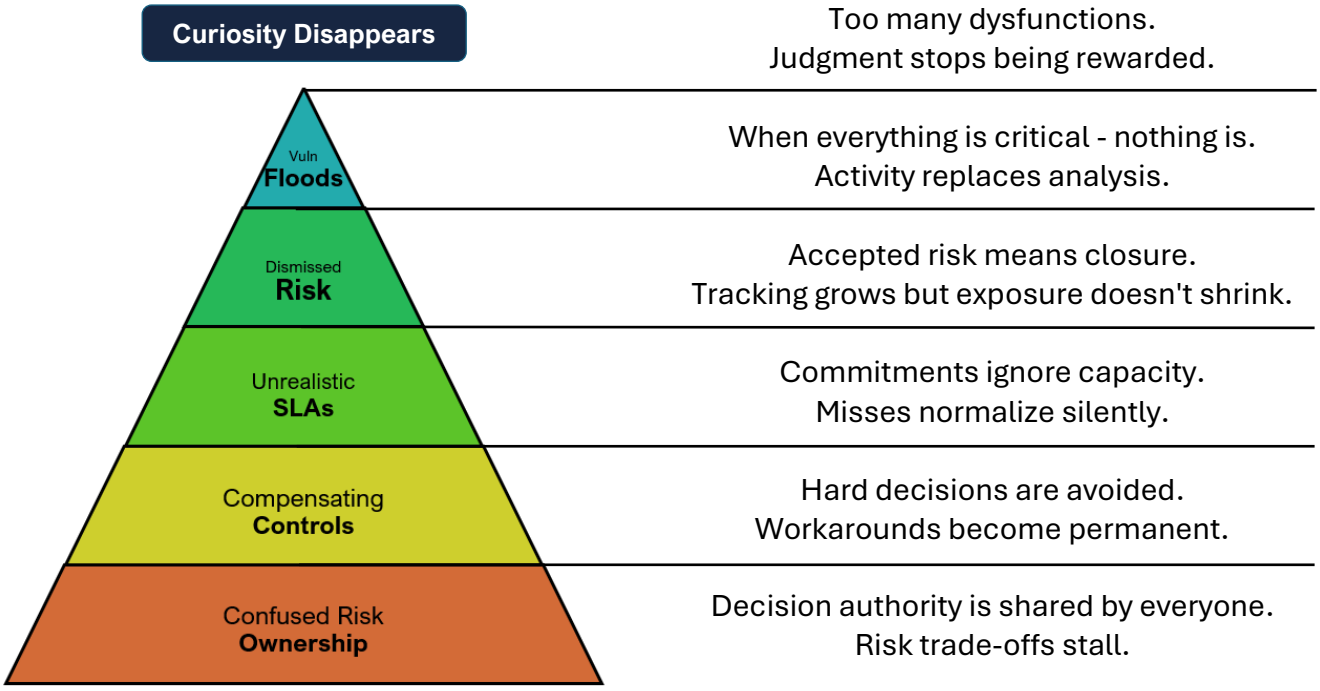
Five Dysfunctions of a Security Team

Failure analysis of mature security programs — and how to fix the decision system that underlies them

Security doesn't fail because we lack information. It fails because we avoid decisions

Five Security Dysfunctions + One Terrible Result



Questions to Ask Monday

Ownership	**Who's holding the bag for the top 3 risk scenarios?**
Conflict	**Which risks are we actively trading off right now?**
Commitment	**Which SLAs do we routinely miss — and what decision do they force?**
Accountability	**Which approved risks are we still tracking?**
Results	**How do we know risk is going down?**
Curiosity	**Pick a control you trust most — why does it reduce risk here?**

Security Team Assessment

Use the scale below to indicate how each statement applies to your security team. Evaluate the statements honestly and without over-thinking your answers.

3 = Usually · **2** = Sometimes · **1** = Rarely

#	Statement	Score
1	Think of your highest risk scenarios (e.g., shutdown, IR, 3rd party access). Do you have explicitly named decision owners?	
2	When a security risk is identified, the team knows who can accept it without requiring committee approval.	
3	During incidents or emergencies, risk trade-off decisions are made without delay because ownership is clear.	
4	When a control can't be implemented as designed, the team debates whether to delay, accept risk, or truly compensate — rather than defaulting to "add a compensating control."	
5	When a security risk is "accepted with compensating controls," the team can describe what specific exposure remains and who monitors it.	
6	Temporary security workarounds are documented, approved, tested, owned and a date is set for risk renewal.	
7	Security SLAs (e.g., "critical vulnerabilities patched within 48 hours") are met, or when missed, trigger an explicit decision (delay, compensate, or accept risk).	
8	Team members believe that stated SLAs (policies, remediation timelines) reflect what's actually achievable.	
9	Items labeled "Critical" receive a critical-level response, not just critical-level labeling.	
10	When security risks are formally accepted, someone verifies whether exposure has actually decreased — not just that the risk remains on a register.	
11	The security team can quickly identify which previously accepted risks are still active and what their current exposure status is.	
12	Every accepted risk has a named owner and a mandatory review date.	
13	When leadership discusses security posture, they describe trend direction (improving/stable/declining) rather than citing total vulnerability counts.	
14	Vulnerability reports show aging distribution (how old are open findings?) rather than just counts.	
15	Security dashboards highlight what changed (new risks, closed risks, aging items) rather than current totals.	
16	Security team members regularly question assumptions about controls ("Does this work in our world?") rather than accepting certifications or vendor claims.	
17	When security tools or frameworks report "compliant" or "pass," the team validates findings through recent manual inspection or testing.	
18	Security team members can explain why specific controls reduce your organization's risk profile, not just that they are "required" or "certified."	

Scoring & Interpretation

Transfer scores from the assessment into the table below. Each dysfunction is measured by three questions. **Your lowest-scoring dysfunction is your starting point.**

Dysfunction	Questions	Score	Total
1. Confused Risk Ownership	Q1 ___ + Q2 ___ + Q3 ___		/ 9
2. Compensating Controls	Q4 ___ + Q5 ___ + Q6 ___		/ 9
3. Unrealistic SLAs	Q7 ___ + Q8 ___ + Q9 ___		/ 9
4. Dismissed Risk	Q10 ___ + Q11 ___ + Q12 ___		/ 9
5. Vulnerability Floods	Q13 ___ + Q14 ___ + Q15 ___		/ 9
6. Loss of Curiosity	Q16 ___ + Q17 ___ + Q18 ___		/ 9

Scoring 8–9 suggests the dysfunction is largely absent from your team. **Scoring 6–7** is a warning sign — the dysfunction may be quietly taking hold. **Scoring 3–5** signals an active problem that demands attention.

Whatever the numbers say, no team stays healthy on autopilot. Even high-performing teams drift toward dysfunction without deliberate, ongoing effort.

Next Steps After Assessment

If Scores Indicate Problems (3-6 range):

1. **Pick ONE dysfunction** to address first (typically start with Confused Risk Ownership)
2. **Implement one operational mechanism** (Decision Rights, Exception Tracker, SLA/SLO separation)
3. **Measure improvement** over 90 days using same assessment

If Multiple Dysfunctions Are Critical:

It's OK. Just don't try to fix everything at once.

The dysfunctions cascade: 1. Fix ownership clarity first (enables conflict) 2. Fix commitment mechanisms second (enables accountability) 3. Address results and curiosity third (requires foundation)

Strategies for Overcoming Each Dysfunction

Confused Risk Ownership

- Create Decision Rights document mapping 8-10 high-impact scenarios to named owners
- Establish single escalation path for each scenario
- Practice decision authority in tabletop exercises

Compensating Controls

- Implement Exception Governance Tracker with mandatory expiry dates
- Create Decision Board with 4 outputs: Accept | Fund | Delay | Compensate (all time-bounded)
- Conduct quarterly review of all active compensations with sunset requirement

Unrealistic SLAs

- Separate SLAs (intent/policy) from SLOs (operational reality)
- Make commitments capacity-aware (state available capacity, negotiate timeline)
- Treat missed SLAs as signals that trigger decisions, not failures that require excuses

Dismissed Risk

- Track accepted risks on the same board as delivery work
- Implement mandatory 90-day review cycle for all risk acceptances
- Measure and report “Reopened Risks” metric to force accountability

Vulnerability Floods

- Replace vulnerability totals with trends (direction of change)
- Implement Vulnerability Aging metric (age distribution, not counts)
- Remove low-signal findings from dashboards to reduce noise

Loss of Curiosity

- Use tabletops as diagnostics to test control assumptions
- Require “why this control works in our environment” explanations, not just “it’s certified”
- Create safe space for “what else might we be missing?” questions
- Track and reward examples of controls that were tested and found wanting

Author: John Duffy, Head of ID/Payment Security, CBN Secure Technologies
Based on: Patrick Lencioni’s *The Five Dysfunctions of a Team*
Version: 1.1 - 18 questions (3 per dysfunction), blind questionnaire format