BENEFICIAL TENSION | WHY YOUR SECURITY TEAM NEEDS CONSTRUCTIVE CONFLICT

In my years of observing high-performing security teams, I've noticed a counterintuitive pattern: the most effective ones aren't always the most harmonious. In fact, teams with built-in tension often produce more innovative and robust security solutions. Here's why embracing productive conflict might be the key to strengthening your security posture.

The Problem with GroupThink

NASA's investigation into the 1986 Challenger disaster provides one of the most well-documented cases of how organizational harmony can lead to catastrophic outcomes. The Rogers Commission Report revealed that engineers who had concerns about the O-rings' performance in cold weather were present, but felt unable to effectively challenge the prevailing group consensus. This tragic example, while not from cybersecurity, demonstrates how even highly skilled technical teams can fall victim to groupthink.

In the same way, the U.S. Intelligence Community made significant reforms post-9/11, documented in the 9/11 Commission Report, specifically targeting organizational groupthink. Those reforms created structures for intentional disagreement and alternative analysis. They also led to the creation of "red team" units and formal devil's advocate roles - practices now common in modern security operations.

Cognitive Diversity as a Security Asset

The most resilient security teams deliberately maintain cognitive diversity. Here's what this looks like in practice:

- The U.S. Army Cyber Command intentionally combines personnel with different backgrounds - from traditional military training to civilian "white hat" hackers
- MITRE's ATT&CK framework development team deliberately includes both offensive security researchers and defensive practitioners
- The National Security Agency's red teams are structured to include both technical and behavioral science expertise

These intentional tensions create "requisite variety" - the idea that a system's internal complexity should match the complexity of its threats.

The Psychology of Productive Conflict

Research from Harvard Business School suggests that teams with managed conflict outperform their harmonious counterparts by up to 40% in complex problem-solving tasks. The key lies in understanding the difference between cognitive conflict (disagreement about ideas) and affective conflict (personal friction).

There are three common types of beneficial team conflict:

1. Task conflict (disagreement on how to solve problems)
2. Process conflict (disagreement on how to approach tasks)
3. Relationship dynamics (disagreement on how to interact)

The most successful security teams actively manage all three (3) types while preventing them from becoming personal.

Building Productive Conflict into Your Team

So, how do you foster beneficial tension without descending into dysfunction? Research from the MIT Sloan School of Management suggests three key principles:

1. Structure the Conflict | Create formal roles for opposing viewpoints. Assign "devil's advocates" in security planning meetings. Have dedicated red teams challenge blue team assumptions. These structured oppositions prevent personal conflicts while maintaining intellectual tension.
2. Establish Psychological Safety | Google's Project Aristotle found that psychological safety was the most important factor in team effectiveness. Team members need to know they can voice dissenting opinions without fear of reprisal. Make it clear that respectful disagreement is not just tolerated but expected.
3. Focus on Learning Outcomes | Frame conflicts as learning opportunities. When your threat hunters and compliance officers disagree, they're not fighting - they're expanding the team's perspective. Data from McKinsey shows that teams who view conflict this way are much more likely to make better decisions.

The Real-World Impact

Here's a recent example: A major retailer's security team was divided over implementing a new zero-trust architecture. The tension between those advocating for innovation and those who preferred stability led to a hybrid approach that proved more effective than either original proposal. The key was channeling the conflict into productive discussion rather than suppressing it.

Another case study comes from a multinational bank where deliberate conflict between risk-focused and customer-experience teams led to the development of a novel two-factor authentication system. The solution balanced security with usability in ways that neither team would have achieved independently.

Making It Work: Practical Implementation

1. Start with Team Design
    - Deliberately hire for diverse thinking styles
    - Create balanced teams with complementary perspectives
    - Establish and document clear channels for dissent
2. Develop Conflict Management Skills
    - Train leaders in conflict management and facilitation
    - Teach team members how to disagree productively
    - Hold regular workshops on constructive debate
3. Measure and Adjust
    - Track team decisions and outcomes
    - Survey team satisfaction and psychological safety
    - Monitor for signs of unhealthy conflict

Your Next Steps

1. Audit your team's cognitive diversity. Do you have enough different perspectives?
2. Create structured opportunities for disagreement in your security planning
3. Reward team members who thoughtfully challenge prevailing assumptions
4. Establish clear ground rules for productive conflict
5. Implement regular "challenge sessions" where team members are expected to critique current practices

Remember: The goal isn't to create discord, but to harness the creative energy that comes from different perspectives colliding in a constructive way. What's your experience with team conflict in security settings? Have you seen cases where disagreement led to better outcomes? Share your thoughts in the comments below.

Assisting your organization in creating a strong cybersecurity culture is something that IntraSystems Advisory Division can help with. Reach out today and let's talk!

MEET MERVYN CHAPMAN, Ph.D. | Advisory, Cybersecurity/GRC

Mervyn brings over 20 years of experience in Cybersecurity and Information Technology. Currently a Doctoral Candidate in Cybersecurity Innovation Management, he brings a people and process centric perspective to security operations and management. He has served as a Chief Information Security Officer in the Healthcare and non-profit space and as a Principal Consultant within a large nationwide consultancy. He is passionate about user involvement and education as well as crafting business-relevant security policies and processes.

.

MERVYN CHAPMAN, Ph.D.

mchapman@intrasystems.com

706.594.1081