Name: Emma Humphreys
Date: August 3rd, 2025
Class: CYSE 495- Human Factors and Policy in Cybersecurity
Professor: Saltuk B. Karahan, PhD
Assignment: Final Paper
Topic: Cybersecurity and Organizational Culture

Introduction

In recent years, cybersecurity failures have increasingly been traced not to technological flaws, but to mistakes in human behavior. As such, human factors have emerged as essential to the development and enforcement of cybersecurity strategies. Beyond technical controls, organizational culture- the shared values, beliefs, and norms within a component- dictates how employees perceive and act on security policies. When employees feel engaged in shaping security decisions, they are more likely to internalize and comply with those policies. This essay investigates the hypothesis that employee engagement in security decision-making leads to better adherence to cybersecurity policies. By exploring organizational culture frameworks, empirical research, and real-world examples, it argues that participatory approaches transform compliance from a top-down requirement into an internalized norm that strengthens an organization's overall security posture, transforming compliance from a checkbox into a cultural norm.

Organizational Culture and Cybersecurity

Organizational culture refers to the underlying values, beliefs, and practices that shape behavior in an organization. Within that framework, information security culture is the subset of attitudes and practices aligned with cybersecurity goals. Research has consistently demonstrated that organizational culture significantly affects adherence to security policies. A security-first culture ensures employees at all levels view cybersecurity as a shared responsibility rather than solely a technical concern. Karlsson et al. (2021) found that internally focused cultures, particularly bureaucratic and clan-orientated environments, are strongly associated with higher compliance among Swedish white-collar workers. These findings suggest that both structured rules and people-centered values can foster secure behavior when integrated into organizational culture. In other words, employees in structured, rule-orientated (bureaucratic) or people-orientated (clan) cultures reported higher self-compliance rates.

Frameworks like the Organizational Cybersecurity Culture Model (OCCM), reinforce this connection, highlighting the role of leadership, shared vision, communication, and employee involvement as key dimensions of a mature security culture (Solomon & Brown, 2021). Studies by Da Veiga and Eloff (2010) further emphasize that a well-developed information security culture correlates with stronger adherence to policies and fewer incidents. These finding underscore a critical point: while technical defenses are essential, an organization's cultural environment largely determines whether security policies are embraced or ignored.

Building a resilient security posture therefore requires actively cultivating a culture where cybersecurity is embedded into everyday operations and decision-making.

Embedding a security- orientated culture is a foundational step—but culture alone is not sufficient unless employees are actively engaged in shaping it.

Beyond technical controls and policy frameworks, the human elements remain the most dynamic and unpredictable aspect of cybersecurity. Employees are not just potential vulnerabilities; they are also the first line of defense when equipped with the right knowledge, mindset, and cultural support. A positive organizational culture reframes security from being perceived as an external imposition to an intrinsic part of daily operations. Studies on high-reliability organizations show that when staff internalize collective responsibility, incident prevention and rapid response become embedded behaviors rather than reactive tasks. In this sense, cybersecurity is not only a technological challenge but also a social one, where attitudes and shared norms determine the effectiveness of policies. Bridging this cultural and technical divide is what turns written policies into living practices that actively defend an organization.

Employee Engagement in Decision-Making

Employee engagement is a crucial mechanism for translating culture into secure behavior. Engagement involves including staff in policy development, incident analysis, and awareness initiatives, shifting employees from passive recipients of rules to active co-creators of the security environment. When employees are invited to participate in shaping policies, they are more likely to view those policies as relevant and legitimate.

A strong example of this dynamic is Liberty Mutual's "culture of data protection" initiative. Faced with rising phishing threats and recognizing that traditional compliance training was not translating into secure daily behavior, the company launched the "Responsible Defender" program to embed cybersecurity into its organizational fabric. Employees were engaged not only through mandatory training but also via ongoing micro-campaigns, branded messaging, and recognition programs that rewarded secure behavior. Importantly, staff were encouraged to provide feedback on policies and participate in shaping awareness campaigns, creating a sense of shared responsibility and ownership for security outcomes (Huang & Pearlson, 2019).

Research by Solomon and Brown (2021) supports what Liberty Mutual's experience demonstrated in practice: that active employee participation enhances the development of a strong information security subculture, which in turn increases compliance. By shifting from a top-down model to one that emphasizes employee engagement, organizations can transform policy adherence from an obligation into a shared organizational norm.

Engagement and Policy Adherence

Engagement leads to policy adherence through a combination of psychological and organization mechanisms. When policies are developed collaboratively, employees are perceiving the process as fair, which establishes procedural legitimacy and encourages

voluntary compliance rather than reluctant obedience (Tyler, 2006). Participation also fosters a sense of ownership, as employees who contribute to shaping policies often feel personally responsible for upholding and advocating for them, increasing intrinsic motivation to comply (Deci & Ryan, 2000). In addition, team-based involvement and security champion networks create positive peer pressure, making secure behavior a social norm rather than a rule enforced from above (Cialdini & Goldenstein, 2004).

Empirical research supports these dynamics, showing that control orientated cultures, such as bureaucratic environments, paired with engagement strategies produce significantly higher compliance rates among white-collar works (Karlsson et al., 2021). Similarly, Solomon and Brown (2021) demonstrated that participation helps translate broader organizational values into a robust security subculture, reinforcing secure behavior across the workforce. Together, these findings- and Liberty Mutual's case- support the hypothesis that meaningful engagement is a driving factor in policy adherence and organizational resilience.

In contrast, strictly top-down, punitive or compliance-only models create disengagement, fatigue, and under-reporting of incidents. A survey of workplace cyber-hierarchies found that many employees attempt to resolve incidents privately or avoid reporting them entirely due to fear—an indicator of negative culture and lack of engagement.

Practical Strategies for Implementation

To translate employee engagement into tangible improvements in cybersecurity culture, organization can adopt several interconnected strategies. One effective approach is the creation of initiatives similar to Liberty Mutual's Responsible Defender program. By appointing cybersecurity champions, using branded campaigns, and embedding awareness into daily operations, Liberty Mutual demonstrated how leadership-driven engagement strategies can integrate cybersecurity into the organizational fabric. Complementing this, participatory workshops and policy co-creation sessions empower staff to contribute to rulemaking, fostering a sense of ownership that increases adherence.

A real-world example of these strategies can be seen in Liberty Mutual's "culture of data protection" imitative. The company launched the 'Responsible Defender' program after recognizing that traditional compliance training was not translating into secure daily behavior amid increasing regulatory demands and phishing threats. Executive leadership supported a company-wide cultural shift using internal branding, micro-campaigns, and recognition for positive security behaviors, framing data protection as part of the company's core values. This engagement-driven approach significantly increased employee participation and created a shared sense of responsibility for cybersecurity (Huang & Pearlson, 2019). Liberty Mutual's experience highlights how leadership-driven engagement initiative can successfully embed cybersecurity into the organizational fabric.

Other effective strategies include involving employees in non-punitive incident post-mortem reviews to foster a learning-based culture, conducting regular culture surveys to adapt

training programs to employee perceptions, and ensuring executives consistently model secure behavior. Together, these initiatives show that engagement is not a one-time training event but an ongoing partnership between leadership and employees that transforms cybersecurity into a share organizational value.

Challenges and Counterarguments

While engagement brings benefits, organization need to manage potential downsides. One concern is that involving too many voices in policy creation can slow down decision-making or lead to conflicting perspectives, particularly in large organizations. This risk can be mitigated by structuring engagement through representative forums or champion networks that balance inclusivity with efficiency. Another challenge is the potential for security fatigue, where constant messaging or repeated training leads to disengagement. Research on cybersecurity fatigue highlights the risk of cognitive burnout, underscoring the need to pace initiatives and ensure content remains meaningful and relevant to employees' roles.

In addition, diverse employee contributions can sometimes create inconsistencies in policy interpretation, making oversight and clear frameworks essential to maintain uniform standards. Finally, cultural and industry contexts influence how engagement strategies work; findings from specific regional or sector-based studies may not universally apply, requiring organizations to adapt their approach to their workforce. These challenges do not undermine the value of engagement but underscore the need for thoughtful implementation.

Conclusion

The evidence shows that organizational culture significantly influences cybersecurity behavior—and that employee engagement in security decision- making amplifies that influence. Organizational culture provides the foundation for secure behavior, but engagement transforms that culture from a top-down directive into a shared, internalized practice. Case studies like Liberty Mutual's initiative and empirical research on engagement mechanisms demonstrate that when employees are active participants in shaping security policies, they are more likely to comply, advocate, and integrate those practices into daily work.

By adopting strategies such as champion networks, participatory policy design, and leadership-led communication, organizations can cultivate a culture of shared responsibility and reduce human-factor vulnerabilities. While challenges such as security fatigue and policy consistency must be managed carefully, the long-term benefits of engagement outweigh these risks. In an era where cyber threats evolve rapidly, embedding cybersecurity into organizational culture though employee participation is not just a best practice-- it is essential for building resilient, adaptive defenses.

References:

Cialdini, R. B., & Goldstein, N. J. (2004). Social Influence: Compliance and conformity. *Annual Review of Psychology*, *55*(1), 591–621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and Assessment Instrument for Information Security Culture. *Computers & Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*(1), 68–78. https://doi.org/10.1037/0003-066x.55.1.68

McWilliams, L. (2024, May 5). *EY Research: Cybersecurity fears on the rise among US workers, with a vast majority concerned about AI in cybersecurity*. EY. https://www.ey.com/en_us/newsroom/2024/05/ey-2024-human-risk-in-cybersecurity-survey

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2021). The effect of perceived organizational culture on employees' information security compliance. *Information and Computer Security*, *30*(3), 382–401. https://doi.org/10.1108/ics-06-2021-0073

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 6398–6407. https://doi.org/10.24251/hicss.2019.769

Solomon, G., & Brown, I. (2021). The influence of Organizational Culture and Information Security Culture on employee compliance behavior. *Journal of Enterprise Information Management*, *34*(4), 1203–1228. https://doi.org/10.1108/jeim-08-2019-0217

Tyler, T. R. (2006). *Why people obey the law*. Princeton University Press.