- **Cybersecurity Ethical Decision Making Framework (Sadeghi et al., 2023) (Formosa, Wilson, & Richards, 2021)**
    - **5 Ethical Principals:**
        - **Beneficence**
            - Cybersecurity technologies should enhance human lives
        - **Non-maleficence**
            - Cybersecurity technologies should not be used to harm individuals' lives
        - **Justice**
            - Cybersecurity technologies should improve fairness and provide impartial access for all
        - **Autonomy**
            - Cybersecurity technologies should not limit users' choices of applications
        - **Explicability**
            - Cybersecurity technologies should be both understandable and accountable clearly for their functioning

- **Ethical Fading (Sadeghi et al., 2023) (Bazerman, 2011)**
    - Vulnerability gap that occurs when someone grows unaware of the ethical implications that come with a solution when trying to solve a cybersecurity problem
    - *"For example, a system administrator who pushes the deployment of two-factor authentication (2FA) on a software application can cause harm (non-maleficence issue) or loss of service (beneficence issue) to vulnerable end users (justice issue) who either have no access to a smartphone or suffer a disability or lack the digital competence needed to use smartphones for 2FA (assuming 2FA is only available via a smartphone's app)."* (Sadeghi et al., 2023)

- **Schwartz's Theory of Basic Human Values (Sadeghi et al., 2023) (Schwartz, 1994)**
    - The theory proposes that a small set of universal values guide human behavior and decision-making across cultures, functioning as "guiding principles in people's lives" (Schwartz, 1994, p. 21), which Sadeghi et al. (2023) apply to ethical decision-making in cybersecurity contexts.
    - **Human values drive cybersecurity ethics**
        - Ethical conflicts in cybersecurity stem from universal human values that act as "guiding principles in people's lives" (Schwartz, 1994, p. 21) (Sadeghi et al., 2023).
    - **Ethical principles translate values into practice**
        - The five ethical principles provide "a structured way of identifying and reasoning about ethical issues in cybersecurity" (Formosa, Wilson, & Richards, 2021, p. 3).
    - **Ethical fading explains harm despite good intent**
        - Ethical considerations can disappear when decisions are framed as technical, causing "the ethical dimensions of a decision [to] fade from view" (Bazerman, 2011, p. 38) (Sadeghi et al., 2023).

- **Where power appears in daily practice**
    - The ethical decision-making framework explains how discretionary power manifests in routine cybersecurity tasks by showing how practitioners prioritize beneficence, security, and efficiency under uncertainty, aligning with our focus on everyday authority rather than rare edge cases (Sadeghi et al., 2023) (Formosa et al., 2021)
- **Why ethical failures occur despite codes**
    - Ethical fading provides a direct explanation for the identified failure modes, such as over-collection, silent fixes, and excessive access, by showing how moral considerations disappear when decisions are framed as technical or urgent (Bazerman, 2011) (Sadeghi et al., 2023)
- **What effective ethical control requires**
    - Schwartz's values theory and the five ethical principles support our argument that ethical codes alone are insufficient, reinforcing the need for enforceable routines like logging, separation of duties, and escalation mechanisms to keep human values visible under operational pressure (Schwartz, 1994) (Formosa et al., 2021) (Sadeghi et al., 2023)

- **Malicious Insider Threats in Cybersecurity: A Fraud Triangle and Machiavellian Perspective**
    - Analyzes data from 768 full-time U.S.-based professionals using PLS-SEM.

CyBOK as the Structural Framework (Flechais & Chalhoub)

- **Human & Organizational**
    - Locates discretionary power in daily practice, including access control, monitoring, incident response, and reporting behavior, where ethical fading and abuse of authority are most likely to occur.
- **Attacks & Defenses**
    - Surfaces ethical tensions around proportionality, disclosure, and collateral harm when defensive actions prioritize security over beneficence and justice.
- **Systems, Software & Infrastructure**
    - Captures how ethical issues become embedded in design and deployment decisions, where choices are often framed as technical and ethical implications fade from view.

Citations

Bazerman, M. H. (2011). Blind spots: Why we fail to do what's right and what to do about it (Unabridged ed.). Brilliance Audio.

Flechais, I., & Chalhoub, G. (2019). Human factors. In The Cyber Security Body of Knowledge (CyBOK), version 1.0. University of Bristol and University of Oxford. https://www.cybok.org

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. Computers and Security, 109, 1-15. https://doi.org/10.1016/j.cose.2021.102382

Idensohn, C., Flowerday, S., van der Schyff, K., & Chua, Y. T. (2026). Malicious insider threats in cybersecurity: A fraud triangle and Machiavellian perspective. Computers in Human Behavior, 174, Article 108809. https://doi.org/10.1016/j.chb.2025.108809

Sadeghi, B., Richards, D., Formosa, P., McEwan, M., Bajwa, M. H. A., Hitchens, M., & Ryan, M. (2023). Modelling the ethical priorities influencing decision-making in cybersecurity contexts. Organizational Cybersecurity Journal: Practice, Process and People. https://doi.org/10.1108/OCJ-09-2022-0015

Schwartz, S. H. (1994). Are there universal aspects in the structure and contents of human values? Journal of Social Issues, 50(4), 19–45.