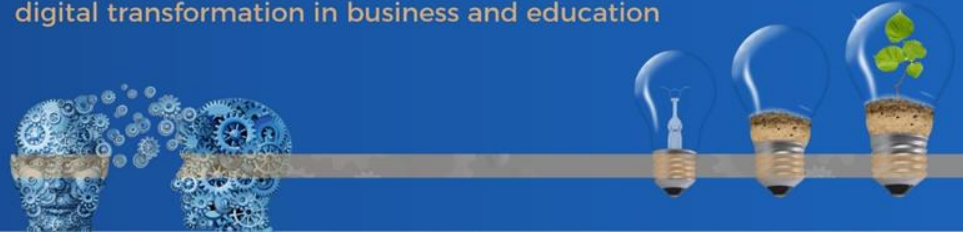


SID 2024

Sibiu Innovation Days

24 - 25 October, Sibiu - RO



Explore the intersection of Self-Determination Theory and Cybersecurity Education - a literature review -

Iulia Feraru
Visma Software SRL

Table of contents

- 03 **The real challenge in security**
- 07 **What helps people learn the right behavior?**
- 08 **The Fogg Behavior Model**
- 10 **Intrinsic motivation - Self Determination Theory**
- 13 **Literature review**
- 15 **Findings**

The real challenge in cybersecurity



- Cybersecurity often focuses on technology—firewalls, encryption, multi-factor authentication.
- But there's a key challenge that's often overlooked: the **human factor**.
- 68% of breaches involved a non-malicious human element. (source: 2024 Verizon DBIR report)

Humans perform

1

Process Management

Humans prioritize and manage multiple tasks, much like an OS manages running processes, ensuring critical activities are completed efficiently.

2

Memory management

Humans store and retrieve information as needed, optimizing their cognitive resources, similar to how an OS handles memory allocation.

3

Device management

Humans interact with and control various tools and devices, similar to an OS managing peripheral devices to enhance productivity.

4

File system

Humans organize and manage data in a structured manner, just as an OS organizes files and directories for easy access.

5

User interface

Humans use communication and sensory inputs to interact with their environment, much like an OS provides a user interface for interaction.

6

Security

Humans adopt security practices to protect themselves and their information, similar to an OS implementing security measures to guard against threats.



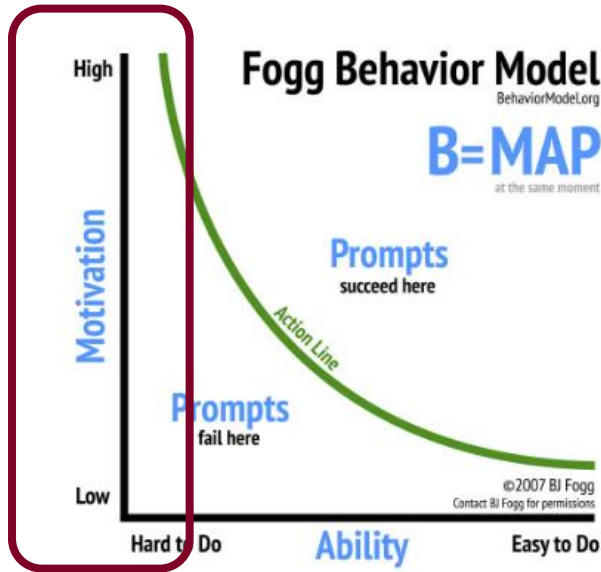
**Humans are yet
another
Operating
System.**

**Vulnerability =
Inadequate Behavior**



**What helps
people learn
the right
behavior?**

The Fogg Behavior Model



“Behavior happens when **Motivation**, Ability, and a Prompt come together at the same time. When a behavior does not occur, at least one of those three elements is missing.”

Motivation

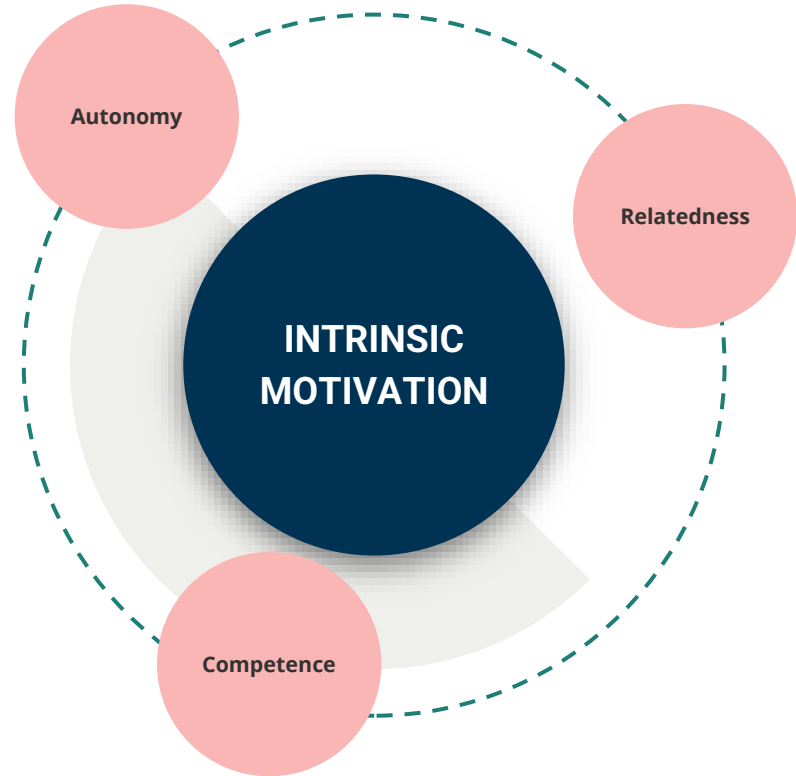


Extrinsic

Intrinsic

Intrinsic motivation - Self Determination Theory

- The Self-Determination Theory (SDT) was developed by Edward L Deci and Richard M Ryan in the 1980s;
- The theory posits that humans are driven by three (3) psychological needs:
 - Autonomy
 - Competence
 - Relatedness.



Information Security is a Shared Responsibility



Relatedness

- the importance of feeling connected, supported, and valued in a group or organization;
- cultivate a sense of shared responsibility and foster a security-first culture.

How can organisations create a security-first culture that increases employees' intrinsic motivation and sense of shared responsibility towards Information Security, thereby promoting compliance with security policies?

This research question was part of a larger systematic literature review that is addressing the interplay between organisational and national culture, leadership, and motivation in the context of information security.

All Research Questions (RQs)

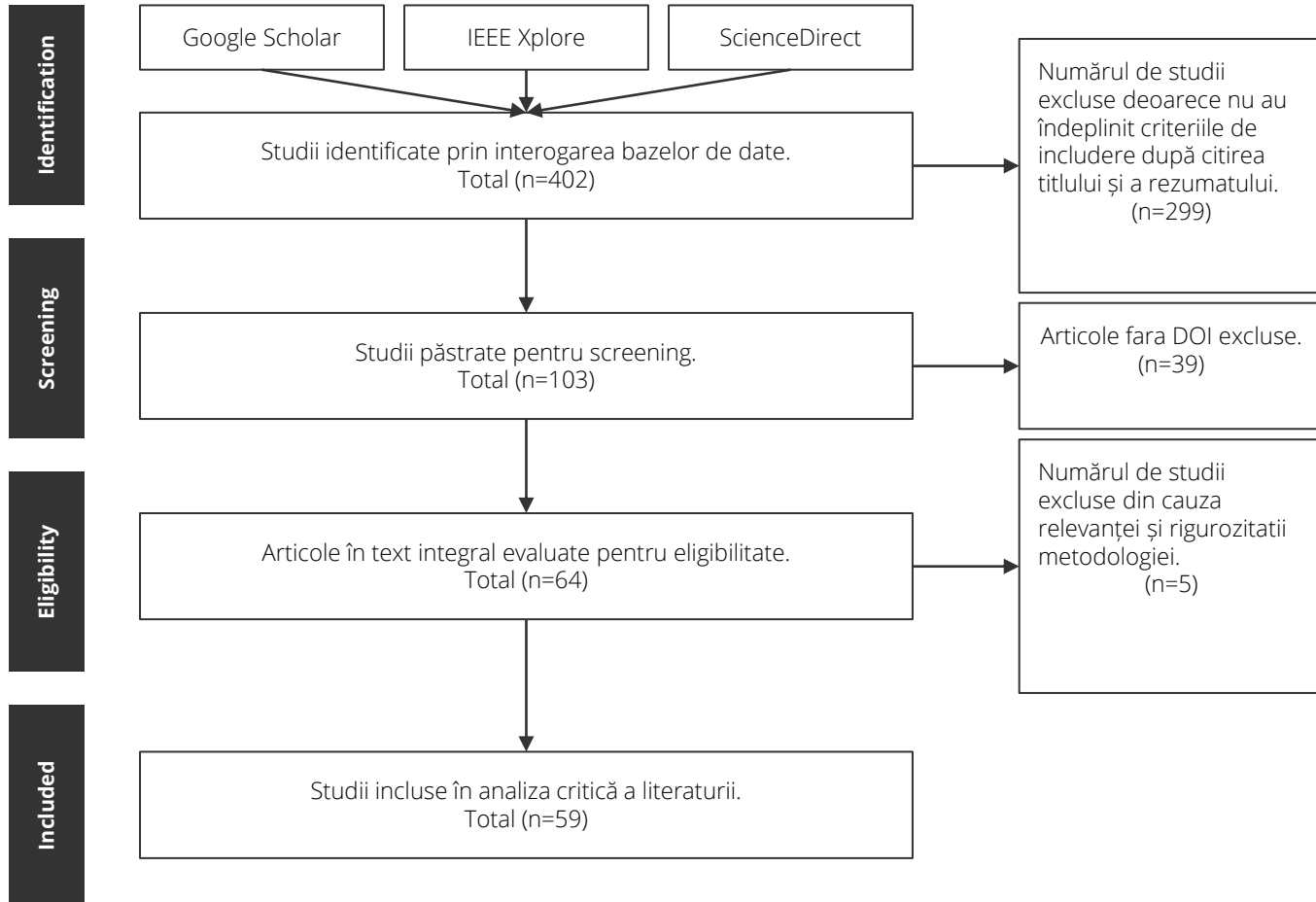
RQ1. How do specific aspects of organisational culture (e.g., communication, trust, norms) influence employees' motivation to adhere to Information Security policies?

RQ2. In what ways does leadership style impact the motivation of employees to engage in secure behaviour and comply with Information Security best practices?

RQ3. How do national cultural dimensions, such as Hofstede's dimensions (e.g., individualism vs. collectivism, uncertainty avoidance), affect employees' attitudes and behaviours towards Information Security practices?

RQ4. How can organisations create a security-first culture that increases employees' intrinsic motivation and sense of shared responsibility towards Information Security, thereby promoting compliance with security policies?

Articles selection flow diagram



Intrinsic motivation as a key driver

- 26 out of 59 papers highlighted the importance of intrinsic motivation in promoting long-term compliance with security policies;
- Studies emphasized that intrinsic motivation, driven by employees' sense of personal responsibility and engagement with security, is more effective than extrinsic motivators like rewards or sanctions.
- Fostering intrinsic motivation requires aligning security objectives with personal values and ensuring employees feel their contributions are meaningful.
- Security awareness and training programs were seen as critical in cultivating intrinsic motivation, as continuous engagement enhances employees' security-conscious behavior.

Shared responsibility increases compliance

- 19 papers out of 59 discussed the concept of shared responsibility, where security becomes a collective effort, not just the responsibility of IT departments or leadership.
- Studies emphasized that creating a culture where all employees feel accountable for security significantly increases compliance, as employees are more likely to act when they perceive themselves as part of the security process.
- Leadership involvement in security initiatives, where leaders actively participate and encourage employees to take responsibility, promotes a shared security culture.
- Establishing a shared responsibility model reduces the risk of human error as employees are more aware of the impact of their actions on overall security.

Security-first culture as foundation

- 25 papers out of 59 specifically addressed the concept of building a security-first culture, where security is embedded in the daily activities of employees and is treated as a core organizational value.
- Transformational leadership significantly contributes to creating a security-first culture by promoting open communication, fostering trust, and encouraging employee engagement in security practices.
- Other studies suggested that to build a security-first culture, organizations must align their security policies with employees' intrinsic values, making compliance a natural part of their workday rather than an additional burden.

Role of the Security Awareness Programs (SAP)

- 18 papers out of 59 emphasized the role of security awareness programs in fostering both intrinsic motivation and a sense of shared responsibility.
- Continuous, relevant, and engaging security training is necessary to maintain employees' interest and motivation toward secure behavior.
- Interactive training that allows employees to see the real-world consequences of security breaches is more effective in fostering a security-first culture than traditional, compliance-driven approaches.

Key Takeaways



Intrinsic motivation is key to sustainable security behaviour (and therefore learning)



Shared responsibility boosts collective accountability

Empowering employees to take ownership of their actions in relation to security creates a stronger, more resilient security-first environment.



Leadership and continuous awareness training cement a security-first culture

A woman with long blonde hair, wearing a leopard print top, is shown in profile, looking towards the right. She is in a social setting with other people in the background, some of whom are smiling. The lighting is warm and indoor.

**Entrepreneurial
Responsible
Dedicated
Inclusive**

Champions of business software

