Cybersecurity Policies in the Workplace: Expectations and Challenges

Presented by Prof. Maeve Dion

October 26, 2022

As part of the USNH Cybersecurity Events recognizing National Cybersecurity Awareness Month

CC-BY 4.0
• Policy: what it is and why we have it

• Intentions and perceptions related to policy

• Policy compliance and motivations to obey (or not)
What do we mean by policy?

Definition

• “a set of ideas or a plan for action ...” *
• “... used as a basis for making decisions” **

Based on an organization’s missions, priorities, and mandates.

* Cambridge English dictionary
** Collins English dictionary

Policy Levels

• Strategic (board of directors)
• Operational (management)
• Tactical (in the weeds, technical)

Policy Types (terminology varies)

• Strategy
• Policy
• Procedure
Examples of Cybersecurity-related Policy

- Security Policy Framework/Strategy (e.g., UK)
- Risk Management Policy
- Information Security Policy
- Identity & Access Management Policy
- Password Policy
- Acceptable Use Policy
- Bring Your Own Device (BYOD) Policy
- Social Media Policy
- Remote Work Policy
- Technology Procurement Policy
- Incident Management & Response Policy

- Information Security Risk Acceptance, Exception, and Waiver Procedure
- Endpoint Management Procedure
- Organizational Email Procedure
- Security Categorization Procedure
- Security Configuration Management Procedure
- Privileged Access Management Procedure
- Security Logging and Monitoring Procedure
- Cloud Service Security Procedure
- Information Security Training & Awareness Procedure
Why have policy?

Policy is typically:

• Reactive to a need or problem (or anticipatory)
• Goal oriented (objectives)
• Part of an approach or strategy (not a one-off)
• Authoritative in nature (governing, fiscal)

In other words:

Policy is an organizationally-informed collection of ideas or instructions that is used to direct or change behavior (decision making).

To be effective, policy must be (a) in tangible form and (b) accessible.
Keep Off the Grass

Here, a sign is a statement of policy.

But there are inherent nuances that can affect compliance.

Imagine this is a college campus.

*Image* by Bart Everson.

*(CC BY 2.0)*
Moral Rule vs Ultimate Command

Bernard Suits
(game studies)


Article has a different focus, but this is an interesting example.

- Scenario 1: Keep off the Grass! sign on the campus lawn, but you see across the quad: deaf Prof. Snooze asleep and about to be eaten by a man-eating plant.

- Scenario 2: Keep off the Grass! sign on the campus lawn, but you see across the quad: deaf Prof. Snooze asleep and about to be shot by Prof. Threat ... and you also are strongly committed to a rule that forbids you from taking a human life.
Intention and Perception (employers)

Intent

• Is your policy intended as a moral rule? To exist in an environment with a mix of other moral rules and ultimate commands?

• Or is it intended as an ultimate command, to be prioritized over any moral rules in that same environment?

• Have you addressed potentially conflicting rules & commands within your policy set?

Perception

• Is your chosen intent & prioritization clear to your employees? How do you communicate such intent? Is prioritization clearly addressed and accessible?

• In the everyday work environment, do your employees perceive your intent the way you wish? How do you know?
Intention and Perception (employees)

• Do you understand whether this policy is a moral rule or an ultimate command?

• Do you understand the prioritization of other rules and commands that interact with this policy or related work activity?

• Have you confirmed these understandings with the security team and your superior?

• If this rule/command significantly interferes with your ability to accomplish your day-to-day activities, raise this matter with superiors and the security team. Openly discuss the issue and find solutions that align with the organization’s risk tolerances.
Since policy is about changing behaviors of human beings, we must consider people’s motivations to perform (to change their behavior appropriately).
Why might we obey?

What may motivate us to obey this?

Image by Bart Everson. (CC BY 2.0)
Motivations to Obey/Comply

Internal principles

• Respect for authority (legitimacy theory)

• Signaling of your own beliefs to others (coordination theory)

• Incorporate others’ beliefs into your own (coordination theory)

Consideration of consequences

• Fear of sanctions (deterrence theory)

• Avoidance of conflict or disapproval (coordination theory)

• Help/contribute toward some important goal or ideal that is larger than the rule/command (coordination theory)

Speak to ALL motivations (employer)

Clearly, mere command (legitimacy) or sanctions (deterrence) is not enough; that’s only one human motivation.

Be sure to incorporate coordination-related motivations to encourage behavior change in a variety of people (different strokes for different folks).

Also:

• Reference motivations within policy
• Include motivations in training and awareness activities
• Mention motivations in everyday meetings (i.e., not merely during security related meetings, but operational meetings, too)
• Inculcate motivations into culture (cybersecurity culture is a whole separate presentation ... or ten!)

Image by Bill Gracey.

(CC BY-NC-ND 2.0)
It can make a difference!


Alligator sign [image] by Hampton Lamoureux.
Consider the Breadth of Consequences (employee)

Possible organizational impacts from a security failure:
• Harm to operations, profit
• Harm to achievement of organizational mission
• Reputational harm, loss of customers or constituents’ confidence
• Legal sanctions, especially in highly regulated industries

Possible impacts to you:
• Loss of position
• Reputational harm, loss of future opportunity
• Legal sanctions (if your noncompliant activity was also unlawful)

Possible impacts to others:
• Loss of services
• Loss of money
• Increased risk of individual harm (e.g., data breach info to a stalker)
• Increased risk of harm to other organizations (e.g., data leak of partner organizations’ proprietary materials; or social engineering breach that enables access to critical infrastructure/national security assets)
Rationalizations that enable minimization of perceived impact:

• Denial of responsibility (it’s beyond my control)
• Denial of injury (the policy violation is only a minor issue)
• Defense of necessity / Appeal to higher loyalties (I’m under pressure for my team to meet a tight deadline, and using this non-accepted, external service/app is faster)
• Condemnation of the condemners (this policy is stupid; or: I don’t see our executives/leadership following it)
• Metaphor of the ledger (most of the time I obey policy, so this one time isn’t too bad)

Cybersecurity Policy & Risk Management (M.S.)
An interdisciplinary master’s degree offered 100% online.
Designed for full-time working professionals in a variety of fields.

https://online.unh.edu/cprm

Accelerated admission option for UNH undergraduates.

Presenter contact info:

Maeve Dion
Assistant Professor of Security Studies
University of New Hampshire

https://www.linkedin.com/in/maevedion/

maeve.dion@unh.edu