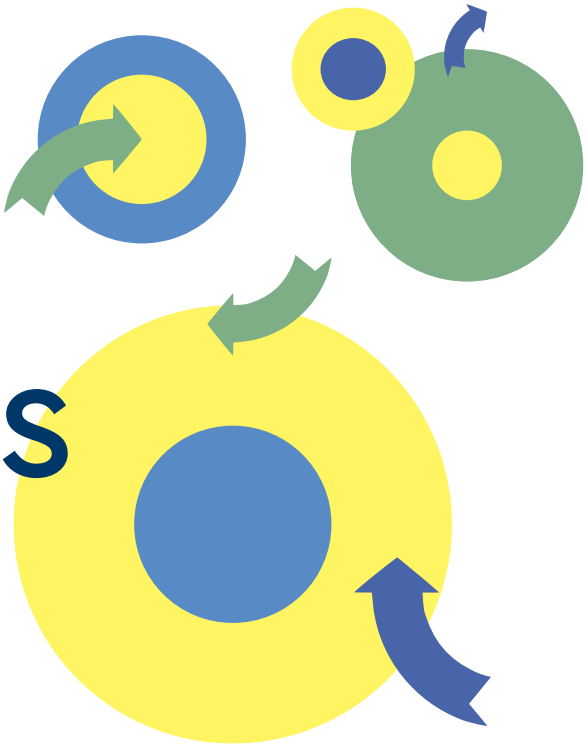
CERTs & Ethics: Guidelines



Four steps for a value-driven cybersecurity culture

Why these guidelines? These guidelines seek to create a value-driven cybersecurity culture that supports all relevant stakeholders of an organization that are confronted with difficult and time-sensitive cyber threats. Making well-informed decisions to safeguard information and systems can be challenging in situations that:

- involve ethical, legal, or organizational conflicts and /or respective tradeoffs;
- are hard to understand, because the interpretation of applicable law is not mastered or disputed;
- show a gap between the ideal and the actual practice within the organization; or
- do not allow much time to conduct a thorough analysis.

Target groups of those guidelines involve (but are not restricted to) supervisors and members of CERTs, CSIRTs, SOCs, cyber fusion centers, forensic IT teams, and similar units within critical infrastructures that are responsible for protecting the cyber-infrastructure of their organizations.

A value-driven cybersecurity culture

Cybersecurity professionals are skilled people, equipped with various guidelines and checklists for handling the technical aspects of cyber threats. However, these resources may be insufficient in situations that involve difficult decisions, where technical aspects conflict with ethical values, or are confronted with regulatory and social complexity.

This is why creating a value-driven cybersecurity culture is needed – a culture that does not only value technical and organizational skills but also encourages open discussions among peers about how their actions align with their personal value system or the collective or societal value system.

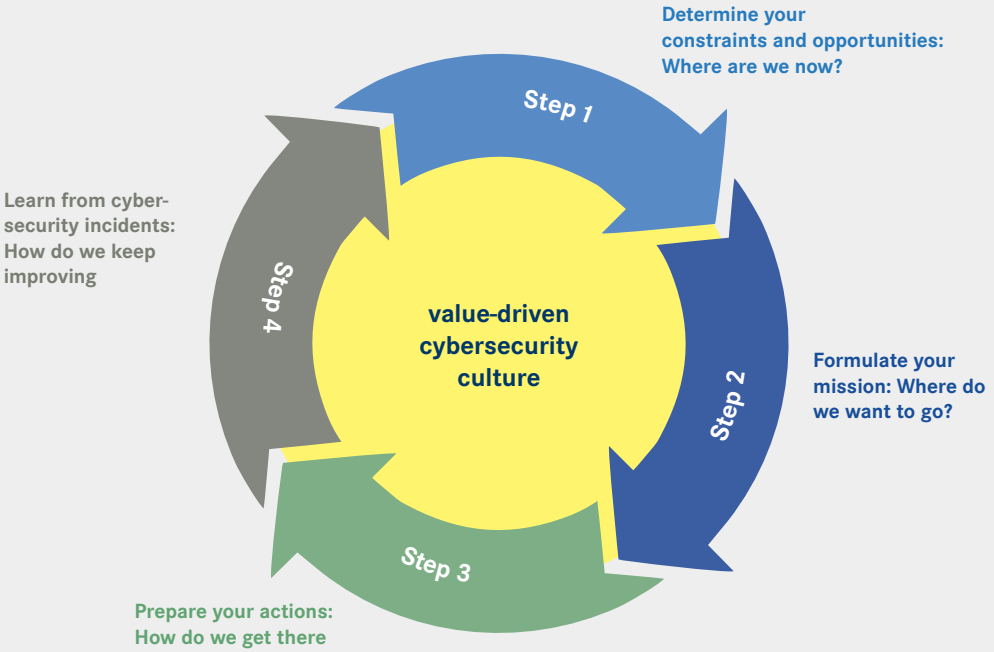
The guidelines result from a research project entitled "Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland" that has been executed within the National Research Programme 77 "Digital Transformation" by researchers from the University of Zurich and the University of Lausanne with support from the Swiss National Cyber Security Centre.

77 NRP Digital Transformation National Research Programme

Universität Zürich[UZH]

UNIL | Université de Lausanne

Create and maintain a value-driven cybersecurity culture in a nutshell



It is crucial that every member of a technical team understands the ramifications of their actions, not solely from a technical or organizational standpoint and from a local and short-term perspective, but also in connection with fundamental values, like respecting and advancing universal human rights, promoting transparency and honesty, practicing responsible use of technology, and maintaining personal and professional integrity.

The guidelines serve as a means to establish and uphold such a value-driven cybersecurity culture. They are structured into four steps, which outline processes, methods, and conditions for building such a culture. A concise four-page document provides the essence of the guidelines, while a longer document offers additional content and examples. The material can be used by team-leaders, supervisors and other persons responsible for upholding cybersecurity of an organization to initiate and maintain processes that enable and support such a culture.

Sustaining a value-driven cybersecurity culture is a never-ending process. New challenges, new team-members, or changes in circumstances will repeatedly affect this culture. Therefore, the four steps should not be understood as a linear, but a circular, process, driven by the successful handling of difficult decisions. The chart below shows a summary of the steps.

In the event of a cybersecurity incident, it is essential to act quickly, without having to engage in in-depth philosophical reflection or ethical analysis at the time.

Therefore, a value-driven cybersecurity culture becomes vital in increasing the likelihood of making sound decisions and responsible incident management – not least to protect the members of the team. Those guidelines seek to support technical teams to prepare for such situations by offering valuable assistance in this pursuit.

In short, technical teams are advised to go through the following four steps, which are briefly outlined here. Further details and resources can be found online in an accompanying document (see page 4).

→ Step 1 — Determine your constraints and opportunities: Where are we now?

The goal of this first step is to gain an overview about the components that shape difficult decisions in a given context. Technical teams like CERTs are embedded in organizations, institutions, and social structures that will shape what can and cannot be done. This step will help to understand why a decision "feels" difficult. It will also clarify the boundaries and opportunities in which the team can actually make decisions. Key insights to be gained in this step are:

- Get a sufficient understanding on the regulatory framework that applies to your context/industry. Do not use laws as an excuse not to act.
- Determine the organizational embedding of your unit within your institution. Make implicit communication channels explicit, clarify role expectations, and identify responsibility gaps.
- Map relevant contact points in your wider social environment such as peers from other teams, legal councilors, law enforcement, NCSC and others that may have a role in difficult decisions. Make sure that this knowledge is distributed in your team.
- List generic and likely cases of difficult decisions that may be relevant for your context. Such cases later can be used to shape the process of value prioritization in your organization.

→ Step 2 — Formulate your mission: Where do we want to go?

The purpose of the second step is to formulate your value priorities, guiding norms, responsibilities, and thresholds for rules of engagement within the team. Whereas the first step helps the team to get an idea about the current culture, the second step is to determine the desired direction more precisely. Key insights to gain in this step are:

- Obtain an outline of values that are relevant within your organization and that are directly involved in potential difficult decisions that you may face. Try to bring them in some priority order by considering that the order may change in new and unexpected situations.
- Discuss norms that could guide your behavior in such situations. The ethical guidelines of FIRST[1] are a good starting point.
- Rethink the responsibilities within the team as well as with other members of your organization based on your internal discussions regarding values and norms and their prioritization. Discuss potential adaptations with the respective persons (higher management, etc.). Distinguish between line, specialist and personal responsibility.
- Determine thresholds of engagement based on the previously obtained generic cases of difficult decisions. Enrich those examples as an instrument to guide future regular discussions within the team regarding ethical questions.

→ Step 3 — Prepare your actions: How do we get there?

The goal of this step is to turn the knowledge and reflection gained in the first two steps into preparatory measures and action plans so that in case of real cybersecurity incidents difficult decisions can be handled responsibly. The various sources of information gained in the first two steps can be turned into new solutions that takes the form of checklists that are developed by the team and for which the team feels some ownership. Key achievements in this step are:

- Determine an "ethics lead" within the team, probably a senior member of the team with experience.
- Establish regular meetings within the teams where you can discuss ethical and value-based issues — also those that may pop-up in the day-to-day business — in an informal manner.
- Create within the team short checklists for exemplary types of actions that you may have to take in incidents, e.g., access blocking or involvement of external partners.
- Put an emphasis on communication procedures, as this is known to be a critical component to be handled in real incidents. Clarify who in the team will talk to whom, who in the company will communicate to internal (e.g., employees) and external (e.g., customers or law enforcement) partners.
- Make sure that the key components of your team culture are known to the central decision-makers within your organization.

[1] www.first.org/global/sigs/ethics/ethics-first

→ **Step 4 — Learn from cybersecurity incidents: How do we keep improving?**

Real cybersecurity incidents that trigger difficult decisions will always be a reality check for a value-driven cybersecurity culture within an organization. You cannot expect that all the preparatory measures and checklists will survive this test. Therefore, it is central to enable structured and iterative learning from incidences with the intent to increase the knowledge base and experience of the organization with difficult cybersecurity decisions. Key achievements in this step are:

- Make sure that any recording/logging of what happened during an incident is not restricted to the current technical and organizational measures taken, but also includes a summary of the ethical components of the problem and the decisions taken.
- If an incident has been considered to be "disruptive" in ethical terms (e.g., it shattered your value priorities or it has been perceived to be a completely new problem), reserve some time after the incident for an open team discussion outside of the daily business.
- Bring your "ethics learning" to know also to the decision-makers of your organization.
- Re-iterate the "value-driven cybersecurity culture process": reconsider which boundary conditions may have changed, whether new priorities are needed, and reflect those findings into your updated team checklists.

Finally, be aware what those guidelines are not: They do not intend to cover all aspects to consider in a cyber-incident (there are already many guidelines for that) and they will not replace your risk management and legal advice. The guidelines are also not made to be used for general value-discussions within your whole organization; although they may support such a process.

Imprint:

Research team: Markus Christen, Melanie Knieps, *Digital Society Initiative, Universität Zürich.*
David-Olivier Jaquet-Chiffelle, Sylvain Métille, Pauline Meyer, Delphine Sarrasin, *Faculté de droit, des sciences criminelles, et d'administration publique, Université de Lausanne*.
Reto Inversini, *Nationales Zentrum für Cybersicherheit.*

Design: Rosa Guggenheim, guggenheim.li

Contact for questions: christen@ethik.uzh.ch

The brochure is available in English, French and German, the accompanying document is only available in English.