CERTs & Ethics: Guidelines

Four steps for a value-driven cybersecurity culture

Preliminary remark: This document complements a short version of CERT ethics guidelines with additional information. The document is conceptualized as a “living document” intending to collect experiences of CERTs related to ethical decision making. Suggestions for complementing the document can be sent to the editor contact.

Editor contact: Markus Christen, University of Zurich (christen@ethik.uzh.ch)

Version: Version 1.0 dated December 2023

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. Further information is available in the imprint at the end of this document.

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 dealing with difficult and time-sensitive cyber incidents. Making well-informed decisions to safeguard information and systems can be challenging in situations that:

- involve ethical, legal, or organizational conflicts and tradeoffs;
- are hard to understand due to a lack of mastery or disputes over the interpretation of applicable law;
- show a discrepancy between the ideal and the actual organizational practices; 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

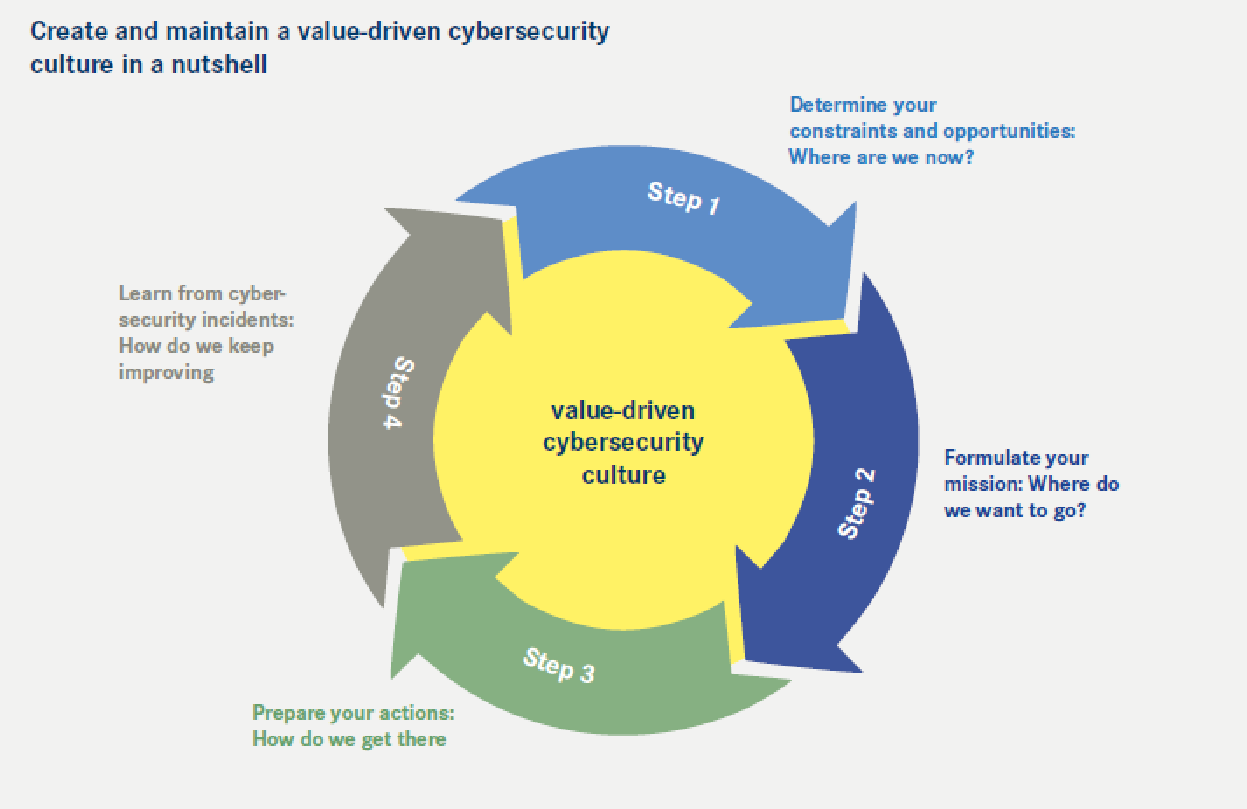
Values serve as a compass for decision-makers in complex and uncertain environments. While cybersecurity professionals are skilled in managing the technical facets of cyberthreats through guidelines and checklists, these resources may prove inadequate in situations that require the consideration of – at times conflicting – technical, ethical, regulatory, or social aspects. A value-driven cybersecurity culture encourages open discussions among peers about how their actions align with their personal value system or that of the collective/societal. Ultimately, the predefined and mutually agreed-upon values serve to alleviate the stress on security teams, thereby enabling them to make decisions that are both time-sensitive and less prone to error.

It is crucial that each 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. Linking these frameworks with the specific workplace demands the security experts personally encounter will offer additional guidance in difficult situations.

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.

Establishing your own value-driven cybersecurity 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 and informed by the successful handling of past difficult decisions. The chart below shows a summary of the steps. Further below, the text of the short version is color-coded for each step and complemented with in-depth information


Create and maintain a value-driven cybersecurity culture in a nutshell
Determine your constraints and opportunities: Where are we now?
Step 1
Step 2
Formulate your mission: Where do we want to go?
Step 3
Prepare your actions: How do we get there
Step 4
Learn from cyber-security incidents: How do we keep improving
value-driven cybersecurity culture

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.

Every organization acts within the boundaries of the law. Depending on the sector, different laws may be relevant. Knowing its rights and obligations in concrete circumstances is an important component of step 1. Below, most common examples of Swiss law (only national level; remind that also cantonal law may be relevant) are listed and briefly described.

- **Federal Act on Data Protection (FADP):** This law applies to any processing of personal data and includes obligations to protect personal data as to notify a security breach.
- **Information Security Act (ISA):** This law applies to government entities and critical infrastructures. A short description of content and shortcoming of the ISA is contained in a White Paper available on the website of the project team.
- **Labor law, civil code and code of obligations:** Employers have a general obligation to instruct their employees and are responsible for they work as employees, but also have an obligation to respect their personality rights.

CERTs and other cybersecurity technical teams may not have a coherent view on all applicable law relevant to their domains. Therefore, a good relation and regular exchange to the legal team of your organization should be maintained.

Difficult legal questions may arise when operating in an international context. Examples may be multinational companies that also operate in countries with a totalitarian regime. CERTs of organizations operating in such domains should be sensitive for potential issues that may arise here, e.g. when legal requirements demanded in such countries conflict with fundamental rights.

Determine the organizational embedding of your unit within your institution. Make implicit communication channels explicit, clarify role expectations, and identify responsibility gaps.

Organizations as well as the teams and people within them often vary greatly. Before being able to think about values, it is essential for cybersecurity experts to identify the organization's size, complexity, and functions, the security team's capacity, formal structure, and skills set. Once the status quo is uncovered, it is possible to pinpoint possible opportunities and constraints. As much as possible, this knowledge should be made available to the team through easily accessible fact sheets.

This analysis should also include an overview of the various roles – particularly within the technical team. These roles include, but are not limited to:

- **Decision-makers:** Who are the people who have the authority to decide on a certain course of action?
- **Decision executors:** Who are the people who will implement these decisions?

- **Communicators:** Who are the people who communicate decisions to the affected stakeholders and are also available to answer questions if necessary?
- **Analysts:** Who are the people who investigate cybersecurity-related incidents and create the respective fact base for decisions?
- **Tool developers:** Who are the people who develop and maintain the tools for analysis?

The clarification of such roles and associated responsibilities should be done in such a way that the people concerned are involved and develop a certain "ownership" of their role(s).

Staff turnover is a particular challenge in this process. In smaller teams, changes in personnel can significantly impact knowledge about roles and responsibilities. Job descriptions that are as precise as possible are then helpful so that new employees can quickly fit into the structure of the team.

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.

A third important factual component in step 1 is gaining knowledge regarding potentially involved stakeholders – both internal and external. These stakeholders can play a role in cybersecurity incidents in very different ways: Some of them should be mandatorily involved (e.g. for decision making, for criminal law reasons or for investigation), some are likely to have important additional information in the management of incidents, again others are directly affected by the incidents and should be adequately informed. The specific circumstances will dictate which stakeholders need involvement and in what capacity. Nevertheless, it is advisable to proactively compile a list of stakeholders in advance who will likely be impacted by an incident.

On the one hand, this list should consist of the organization's internal departments, such as:

- **Technical peers:** Other positions within the organization with sufficient technical knowledge of cybersecurity that can play a role in the implementation of measures (e.g. development teams). Depending on the size of the organization, there could also be more than one cybersecurity team or even defined leaders in this area (e.g. CISO).
- **Legal and compliance:** Persons with legal knowledge who can be consulted if necessary. A relevant point here is in particular the consideration of necessary "translation work" between a technical and a legal view of a problem.
- **Operational departments:** Persons whose activities are directly affected by cyber security incidents. The contact persons who can quickly disseminate information on incidents in the respective departments must be identified in advance.
- **Communications departments:** Individuals who play a role in both official internal and external communications; which may be particularly the case in major incidents. Here too, it is advisable to maintain a certain level of contact with the relevant responsible persons.
- **Management level:** In particular, those people should be identified who have sufficient technical knowledge of cyber security and who can be approached quickly in the event of incidents or who in turn have a fast line to the team when the management level discusses incidents and needs to access information quickly.
- **Shareholders:** Depending on the incident, shareholders may also be affected and it is important to clarify how relevant shareholders can be informed in the event of incidents.

On the other hand, external bodies that can play a role in managing cyber security incidents in various capacities should be listed. The following are particularly worth mentioning here:

- **Peers from organizations in the same sector:** Colleagues from other technical teams are a key source of practical knowledge in the event of incidents. Informal relationships often exist (e.g. due to shared training or previous joint work in the same organization). Such informal relationships can be very valuable; in specific cases, however, trade-offs must be made with other requirements (e.g., protection of trade secrets). Nevertheless, technical teams should definitely know from each other which peers have such relationships so that the team as a whole can access this resource if necessary.
- **National Cybersecurity Center (NCSC):** The NCSC is the federal government's most important competence center for cybersecurity and is also responsible for various implementation tasks within the framework of the Information Security Act. Due to the reporting obligation, contact with the NCSC is often indispensable, depending on the incident. It is therefore important to establish good informal contacts with GovCERT in advance in order to obtain an assessment and assistance in cases of doubt (is an incident reportable or not).
- **Police and public prosecutor's office:** Cybercrime prosecution is regulated at cantonal level and the cantonal police forces have varying degrees of expertise in this area. Informal contacts are also important here in order to obtain low-threshold assessments of the severity of incidents without having to start a formal process (e.g. criminal prosecution) straight away.
- **Customers:** Of course, attention must also be paid to individuals and organizations with whom the organization has entered into contractual relationships (e.g. regarding services) or who purchase the organization's products and who may be directly affected by cybersecurity incidents. In particular, it is important to assess which obligations may be violated by incidents and also which risks (e.g., recourse claims) exist as a result.
- **Cybersecurity community:** Insights into successes and failures in dealing with cybersecurity incidents can also be important for the community as a whole in order to better counter future threats. Accordingly, it should be determined which relevant organizations and exchange events (e.g., conferences) exist where such knowledge can be exchanged in an appropriately adapted form.
- **Public:** Finally, depending on the type of incident, the public as a whole may also be affected. Particularly in the case of large organizations, it can therefore be helpful to record which media people usually report on such incidents.

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.

Organizations can be affected by a variety of different cybersecurity risks, which are usually described by the "CIA triad": The compromise of the confidentiality, integrity or availability of data and systems. The spectrum of actors can also be very broad, from simple "script-kiddies" to hactivists and professional criminal groups or state actors (e.g. espionage). Numerous organizations have compiled comprehensive overviews in this regard.

These risks can lead to difficult decisions in the above-mentioned sense in various forms – for example, because they involve value conflicts or unclear legal standards. It therefore makes sense for technical teams to list generic scenarios of such difficult decisions that may be of particular relevance to the specific organization. Examples include:

- Sharing information during an incident (potentially violating privacy) vs. not sharing (potentially violating solidarity)
- Returning to business after an incident (potentially violating justice and law) vs. enabling forensic analysis (potentially violating profitability)

- Allowing an error culture when mistakes happened (potentially violating) vs. fighting carelessness of employees
- Being transparent and publicly communicating vs secret
- Interest in publishing toolsets and freedom of information/research vs. responsible use of dangerous tools that can cause harm in the hands of an attacker.

Such a list of generic scenarios then could be used for generating some kind of statistics of frequency of incidence types and for recording actions taken in concrete incidences, an important element of step 4.

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.

Values are fundamental orientation points of an organization that describe desirable goals with usually a high level of abstraction. Values can be in conflict, which is one characteristic of difficult decisions. Therefore, as a first step, it is important to understand which values at all may be relevant for an organization. Below, most common examples are listed (some values may be present in more than one category):

- **Economic-oriented values**
  - *Adaptability*
  - *Competitivity*
  - *Data availability*
  - *Efficiency*
  - *Flexibility*
  - *Profitability*
  - *Reactivity*
  - *Reputation*
  - *Resilience*
  - *Sustainability*
  - *Trustworthiness*
- **Privacy and legal-oriented values**
  - *Confidentiality*
  - *Data authentication*
  - *Data integrity*
- **Forensic-oriented values**
  - *Data authentication*
  - *Data integrity*
  - *Forensic preparedness*
  - *Reactivity*
  - *Traceability*
- **Interaction-oriented values**
  - *Adaptability*
  - *Autonomy*
  - *Collaboration*
  - *Cooperation*
  - *Flexibility*
  - *Harm avoidance*
  - *Honesty*
  - *Reputation*
  - *Solidarity*
  - *Trustworthiness*
- **Best practice-oriented values**
  - *Compliance*
  - *Reactivity*
  - *Resilience*
- **Other general ethical values**
  - *Exemplarity*
  - *Honesty*
  - *Human rights*
  - *Sustainability*

These short descriptions do not intent to capture the various facets value definitions may entail. They only serve as a starting point for the process of knowledge gaining.

When clarifying and prioritizing the content of values, it can be helpful to link them to the generic decision types (see step 1). As a rule, such decisions are accompanied by a certain conflict of values, i.e. you have to decide which value you will give preference to. However, such decisions are rarely final – changes in the situation can certainly lead to a previously prioritized value (e.g., confidentiality) being downgraded because important information can be obtained more quickly through openness.

It should also be noted that organizations as a whole often adopt a kind of "code of values"– usually a very general description of value orientations that are considered important for the company. Such a general code certainly also plays a role in clarifying values within the team, but is usually specified by the specific technical tasks of a cybersecurity team.

Discuss norms that could guide your behavior in such situations. The ethical guidelines of FIRST are a good starting point.

Many technical organizations in the field of cyber security have already dealt with ethical issues more intensively. One prominent example are the "Ethics for Incident Response and Security Teams" guidelines from the organization FIRST, the global Forum of Incident Response and Security Teams. These are specifically geared towards generic issues that arise in technical teams, such as the responsible disclosure of vulnerabilities. As a rule, it is highly recommended that technical teams spend some time studying and discussing these together.

Another helpful source for such standard discussions is the "Code of Ethics for Data-Based Value Creation" from the Data Innovation Alliance, a Swiss association of companies and universities dedicated to support innovations with data. This is particularly suitable for discussing data security issues in the broader context of value creation with data.

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.

The generation of an overview of possible responsibility holders within the organization is already an essential element of step 1. On this basis, a mapping between values and responsibilities can now be made in light of the identified values carried out in step 2. In concrete terms, this concerns examining which roles are responsible for protecting or strengthening the value identified as relevant in each case. A distinction must be made here between line responsibility, professional responsibility, and personal responsibility:

- **Line responsibility:** According to the organizational structure, these positions have a duty to protect certain values. For example, line managers must take responsibility for certain actions their teams because this is their function.
- **Professional responsibility:** This responsibility relates to standing up for values that are constitutive for the respective profession. For example, the data protection officer must stand up for the value of privacy.
- **Personal responsibility:** This role ultimately relates to the individual's values and conscience. In particular, a person should disclosed if he or she has strong commitments to individual values that could potentially lead to a conflict of values.

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.

In everyday working life, it will not be possible to subject every incident to a sophisticated ethical analysis. Often the situation is so clear that this is not even necessary. However, relying purely on a gut feeling as to when a situation is considered too serious for a single person to deal with is not a solution. This is why the discussion about "threshold values", i.e. when additional staff should be recruited to solve a problem, is part of creating a value-driven cybersecurity culture.

Below are some examples of questions that could require such a threshold value:

- At what point is an incident considered "sufficiently large" so that it is mandatory to involve the whole team?
- At what point is it necessary to involve members of higher management?
- When should the NCSC be informed?
- When should law enforcement authorities be involved?

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.

Special skills or even training in the field of ethics, are not usually part of the job profile of members of technical cybersecurity teams. However, this is not necessary, as everyone thinks about ethical issues and has more or less established views in this regard. Nevertheless, the creation of a conscious ethical culture in the area of cybersecurity can benefit from one person in the team taking a special interest in the topic and assuming an informal lead here. This is usually a more experienced member of the team who enjoys a certain level of respect within the team.

Such an "ethics lead" does not have to be accompanied by any formal obligations. An informal approach is often more effective, for example by suggesting "this evening we are drinking a beer together and talk about our values". Support from higher management could be that they pay the beer and the pizza and show up by themselves, but not in an active role.

In larger organizations, it may well be that ethics is also assigned an independent function – usually assigned to the topic of "data ethics", in which cybersecurity is one of several facets. This person is probably not directly assigned to the technical cyber security teams – but they can also take on this function within the team itself.

Finally, further training courses in ethics are increasingly being offered, for example at the Hochschule für Wirtschaft Zürich, the Institut für Kommunikation und Führung, or the Fernfachhochschule Schweiz. However, the focus of these courses is on data ethics in general and cyber security is often only a small part of the training.

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.

As explained in the previous paragraph, a low-threshold, informal approach is perfectly suitable for discussing ethical issues in the day-to-day work of cybersecurity teams. However, in order to implement all the recommendations formulated in these guidelines, a certain systematic approach is likely to be helpful.

There is a long tradition of institutionalizing ethical decision-making in certain industries – particularly in the healthcare sector in the medical and nursing professions. The information technology sector has only recently begun to benefit from this experience.

The Data Innovation Alliance was one of the first organizations in this area to provide concrete recommendations for the implementation of so-called "ethics structures". The term represents the various systems, positions and programs that an organization can use to implement ethical conduct. These ethics structures should fulfill the following basic functions:

- Recognize ethical issues that arise in the creation of new products and services or in day-to-day business.
- Deciding on how to proceed to resolve the ethical issue.
- Enforcing ethical behavior and facilitating learning from these issues

The range of possibilities is wide and also strongly dependent on the resources that an organization wants to devote to this topic overall. A comprehensive overview of this can be found in the "Implementation" document of the "Code of Ethics for Data-Based Value Creation".

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.

One result of using the ethics structures mentioned above are simple checklists for those difficult decisions that have been identified as likely in the respective organization (in steps 1 and 2). Such checklists are also a valuable tool for sharing lessons learned with peers. Such lists can also be used to easily document cases that can no longer be dealt with using the lists - for example, by indicating the points for which no solution could be found.

The following are examples of problem cases for which checklists could be created:

- Under what circumstances should you lock an employee's compromised account?
- When should you share what information about an incident with third parties?
- How should everyday, minor misconduct by employees of the organization be handled?
- MORE?

It is important that the respective teams perceive checklists as "their own result" – i.e. as a product for which one also has a certain obligation. It should be avoided that ethical issues are ultimately only understood as a "checking the box exercise".

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.

Communication issues in cybersecurity incidents are key, as this point can often be forgotten in the hustle and bustle of the incident itself, sometimes with serious consequences. Three levels in particular need to be considered:

- **Informal team communication:** Team members need to discuss how rapid, informal communication should take place during daily monitoring.
- **Internal organizational communication:** Based on the internal stakeholder analysis (step 1), it should be clarified within the team when which departments of the organization should be involved.
- **External communication:** Here too, the stakeholder analysis from step forms an important basis. Official communication is usually carried out by the responsible department of the organization; the technical team is then primarily a source of information. This must be distinguished from informal communication with external bodies that are important for dealing with the incident.

There are also temporal aspects to consider: Major cybersecurity incidents usually have a history; they form a sequence of many small events. The key question here is how to enable the team to recognize a pattern that indicates a serious incident. Once the incident is underway, communication focuses on transmitting information relevant to the decision to the departments involved. After the incident, communication focuses on damage limitation and enabling learning.

Make sure that the key components of your team culture are known to the central decision-makers within your organization.

This point is important – the organization's leadership should be made aware that the technical team has fully addressed ethical issues in their work.

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.

What is meant here in particular is that the conflicting values are named, the arguments for prioritizing the values are documented and the final decision is also recorded with reference to these values.

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.

Major incidents can also give rise to a team retreat in which members of other departments of the organization are also involved if necessary.

Introduce “ethics learning” to familiarize decision-makers within your organization with ethical principles.

The term “ethics learning” is intended to express the most important findings in ethical terms – i.e. with regard to value prioritization, responsibilities and adjustments to the checklists.

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.

For this point, reference can again be made to the ethical structures (step 3), which can form an institutional framework for such a system.

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.

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

Further material is available on the project web site.