Organizing cybersecurity in action: a Pragmatic Ethical Reasoning approach

Richard Baskerville[1], Paolo Depaoli[2], and Paolo Spagnoletti[3]

[1]Georgia State University, Atlanta, Georgia, USA and Curtin University, Perth, Western Australia
[2]Tuscia University, Viterbo, Italy and LUISS University, Rome, Italy
[3]LUISS University, Rome, Italy and Department of Information Systems, University of Agder, Norway
baskerville@acm.org
paolo.depaoli@unitus.it
paspagnoletti@luiss.it

Abstract. This paper contributes to the literature on cybersecurity governance by suggesting an approach based on pragmatism. As Jeffrey Sachs in his The Age of Sustainable Development, 2015, reminds us: "The essence of sustainable development in practice is *scientifically and morally based problem solving"*. Cybersecurity deals with problem solving in complex socio-technical settings where ethics and organizational learning are tightly related. The paper draws on pragmatism because from its earliest formulation, pragmatist thought was anchored to a dual interest in ethics and science. Under this lens, pragmatic ethics cannot exist as a set of rules or principles, but rather requires a cyclical, empirical process whereby ethical principles and context interact to promote justice among stakeholders in the search for reliable solutions during the unfolding of critical events. As a result, an Ethically oriented Cybersecurity Approach (ECA) based on Pragmatic Ethical Reasoning (PER) is proposed for managing unexpected critical events when organizations must learn on-the-fly and improve their security profiles.

Keywords: Cybersecurity, Pragmatism, Organizing, Action research, Design, Deming, ISO 27000

1 Introduction

A large number of cyberattacks are born on the Internet on a daily basis and even though most of them are harmless, some bear severe consequences: e. g. the stealing and manipulation of data, identity thefts, and taking over control systems with damages to the physical sphere (de Bruijn and Janssen 2017). Reflection and search for appropriate policies and security measures are being conducted by organizations to respond to these unexpected and often disruptive events. The effects of a cyberattack can be magnified, or even unwillingly supported by the lack of awareness of employees or by conflicting objectives of different organizational units (Ruighaver, Maynard, and Warren 2010).

Indeed, from the onset of the Internet to the expansion of broadband, a multitude of harmful incidents have taken place and a wide range of protection technologies and techniques have been developed and deployed. Yet, it is still difficult to have a clear understanding of how corporations and agencies are responding to threats by enhancing their security profiles, that is by nourishing their organizational and infrastructural characteristics towards cybersecurity (Baskerville, Rowe, and Wolff 2018). In this area of research this paper addresses one important support for organizational design and governance: cybersecurity in action, an approach and a process proposed to integrate organizational and ethical learning in a cybersecurity perspective.

Research on cybersecurity has shown that response and prevention strategies have to be balanced for developing effective security measures (Baskerville, Spagnoletti, and Kim 2014). The number and gravity of incidents concerning critical infrastructures - as for example healthcare, telecommunication, energy and transport systems - underscores the relevance of response strategies. The increasing diffusion of cyberattacks and the pervasive use of automated systems to control operation processes and physical systems (e.g. IoT) raise several interrelated issues: technical, organizational and ethical. In this paper, these three issues are approached from the perspective of normative ethics applied to cybersecurity by drawing on the works of the classic pragmatists (i.e. C.S. Peirce, J. Dewey, and W. James) and on recent commentaries on, and extensions of, their work (Ormerod 2006; Bernstein 2010).

A Pragmatic Ethical Reasoning (PER) process is proposed to support cybersecurity design and governance - that is to support organizations (management, CIOs, CISOs, employees) in understanding and then filling the gap between their pursued (or claimed) ethical behavior versus their actual ethical conduct. In the proposed approach, ethical reasoning is embedded in cybersecurity design and governance.

2 From ‘tool’ to ‘process’ in ethically oriented cybersecurity governance

The search for viable approaches to business ethics have led to the adoption of codes of ethics on the part of several companies worldwide (Adams, Tashchian, and Shore 2001; Long and Driscoll 2008). The research carried out on their efficacy shows that in most cases these formal statements of value are ineffective if they are not supported by other initiatives such as employee awareness programs and training to complement such tools (Velthouse and Kandogan 2007; Kaptein 2011; Garcia-Sanchez, Rodriguez-Dominguez, and Frias-Aceituno 2015). Hill and Rapp (2014) acknowledge the positive effect of involving the whole organization in the development of formal artifacts by adopting a bottom-up approach: both their literature review and the results of their study show that not only participation is important “in the development and operationalization of moral standards for healthy ethical climates in businesses” but that “formal statements of values are ignored unless they are the product of the company as a collective” (ibid p. 622). Similarly, specific codes of ethics for information systems have been found not to have significant effects on most employees (Siponen and Vance 2010; Harrington 1996) whereas security education, training and awareness (SETA) programs show better results (D’Arcy and Hovav 2009).

In some countries, as in Australia, research has shown evidence that ethical aspects have not been considered explicitly by organizations in their information security approaches (for example in developing acceptable use policies): the driver being lack of guidance in applying ethics in this field (Ruighaver, Maynard, and Warren 2010). Specific proposals have been developed: some belong to ethics applied to the information security literature as in the case of Ruighaver et al. (2010) who suggest the adoption of consequential ethics rather than deontological ethics to reinforce proactive behavior by employees since motivation should not be underestimated with respect to deterrence. Other contributions do not refer explicitly to the discipline of ethics but do consider conduct: it is the case of Siponen and Vance (2010) who explain information policy violations through neutralization theory (whereby people justify behaviors that violate norms by minimizing the perceived harm of their violations) rather than deterrence theory (whereby severity and certainty of formal sanctions are believed to dissuade people from infringements). Also Spears and Barki (2010) do not refer directly to ethical theories when they suggest user participation to leverage organizational aspects other than technology-focused ones in information security risk management. Further, "security training via user participation is specific to business processes, [it is] therefore likely to have greater meaning, and perhaps interest, for users, encouraging greater commitment in protecting sensitive organizational information" (ibid. p. 519). Some authors have even proposed to paradoxically extend the traditional Plan-Do-Check-Act (PDCA), Deming's cycle, by developing integrating bricolage, improvisation, and hacking in IS security practices (Baskerville 2005; Spagnoletti and Resca 2008) and prepare organizations to address unpredictable threats.

This concise literature review shows the need to approach conduct in cybersecurity from a 'process' perspective rather than from a 'tool' perspective. Indeed, in a pragmatist perspective, any theoretical or practical action is value-laden because it is performed only if it is considered to be worthwhile by the agent (Dewey 1897). This observation bears important consequences when trying to understand and change the ethical orientation of an organization: its overall ethical performance is the outcome of the actions and interactions of a large number of agents with probably heterogeneous interests. Furthermore, all studies mentioned above underscore user participation and involvement for an effective implementation of policies in security and ethics, while some researchers insist on participation across the board even in the design phase. We take these suggestions not only as a way to deal with the dissimilarity of interests and purposes of agents but also as an effective way to leverage their experience. As is well known, pragmatism highlights the role of experience in advancing, in an iterative process, both knowledge and practice (Ormerod 2006). The next section explains further reasons for drawing on pragmatism to answer the following research question: *how can cybersecurity be organized within an explicit ethical perspective? Specifically: what processes better support effective cybersecurity in organizations?*

The answer to the research question is developed in the following way. In the next section the theoretical underpinnings of this work are explained. The fourth section presents Deming's cycle because of both its recursive nature, similar to the approach proposed in this paper, and its being the foundation supporting the ISO 27001 standards.

Section five describes the Pragmatic Ethical Reasoning process (PER) and its connections with both Deming's cycle and the ISO standards to build the design and development of an Ethically oriented Cybersecurity in Action framework (ECA).

3 Theoretical underpinnings

Through an extensive examination of the works of its founders and of its critics, Richard Ormerod (2006) concluded that pragmatism is of interest to practitioners and academics alike because of the practical, commonsense and scientific approach embedded in it. From the perspective of an operational researcher and professional, he summarizes the main epistemological tenets of pragmatism arguing that knowledge is fallible and beliefs are theories developed through collective experience to support practice. "*Truths were held because they worked at that time in that context. Theories developed out of the need to shape, simplify and make memorable the multitude of contingent facts that action threw up".* Likewise, pragmatism attributes judgement-of-value to any action performed in a specific context. *"Morality lies in outcomes rather than principles. Therefore, it is the means that should be considered rather than ends. Whereas ends can be debated purely rationally, means always have a factual content." (ibid. p. 907-908)*

Ten years later Werner Ulrich (2016) argues that pragmatic reasoning makes possible to selectively deal with validity claims of both empirical (scientific) and normative (ethical) nature. *"For all practical purposes, the meaning and scope of valid application of a concept or proposition depend on our boundary judgments as to what "facts" (observations and forecasts) and "values" (worldviews, ideals, ends, and norms) are to count as relevant, and these judgments (as the word is meant to suggest) are not given to us by nature or dogma but are a matter of pragmatic selection in the concrete situation." (ibid. p. 9-10).* Thus, pragmatic reasoning is a suitable approach to address ethical issues in the design of complex sociotechnical systems when unobservable events, such as cyberattacks, raise the need of situational understanding.

Drawing on the cited works by Ormerod and Ulrich, complemented by another extensive analysis of pragmatist authors' work by Richard Bernstein (2010), and by referring directly to some works of classic pragmatists that will be cited when appropriate, we propose a Pragmatic Ethical Reasoning (PER) process applied to cybersecurity governance. The process is based on five principles of pragmatism: (i) inquiry and experience are intertwined; (ii) ethics permeate practice; (iii) in ethics context matters; (iv) principles are methods for action; (v) convergence on truth through critical reasoning.

First, for pragmatists, 'inquiry' and 'experience' are intertwined. Experience can prove present results of inquiry false through 'surprises': fallibilism is one of the pillars of their philosophy (Ormerod 2006; Bernstein 2010). Within a pragmatist perspective, cyberattacks can be considered as 'surprises' capable of questioning the results of previous 'inquiry' i.e. an occasion to revise both prevention and response measures thus revising also deterrence.

Second, for pragmatism ethics permeate practice. According to Dewey (1897), every act contains a judgment of value because it is performed only if it is considered to be

worthwhile by the agent ─for this reason the conduct of a person can be evaluated only from her acts. At the same time, "every judgment about conduct is itself an act" (ib. p. 2) because it affects conduct. Since information security relevant acts permeate the organization, it is crucial that responsibility and accountability are modulated across the organization together with the evaluation criteria to be adopted thereof (in the case at hand for example, through the process of information security audit).

Third, in pragmatic ethics context matters. Dewey (1897) underlines the role both of historic antecedents and of the physical and social environment in shaping conduct (ib. p. 8). The agent is affected (both consciously and unconsciously) by education into certain habits of thinking, feeling and acting. Furthermore, "our acts are controlled by the demands made upon us. These demands include not simply the express requirements of other persons, but the customary expectations of the family, social circle, trade or profession; the stimuli of surrounding objects, tools, books, etc.; the range and quality of opportunities afforded." (ib. p. 7). The consequence is that any idea or act or plan can become action but through the forces of the environment: in their respective roles both end users and cybersecurity operators set the scene for acts that affect information security.

Fourth, sets of ethical principles have been proposed in the information systems literature (e.g. Myers and Venable 2014). In pragmatism 'principle' is different from 'rule' or 'fixed precept': the former is "a method for action, [the] latter a prescription for it; former experimental, latter fixed; former orders in sense of setting in order, latter in sense of commanding" (Dewey 1897, p. 5). According to a pragmatist approach, ethical principles constitute experimental methods for action. For an organization this approach is vital because: (i) it supports critical discussions on the methods of action (principles) that better represent the different judgments of value of the people that make up the ethical profile of the organizational units; (ii) it allows for the convergence towards the identification of common principles (guides for action).

Fifth, for pragmatists (i.e. Peirce) there is a 'convergence' through critical reasoning on truth rather than a 'consensus' (Bernstein 2010, p. 228 and Ulrich 2016). This convergence is realistic because it rests on the experiences of the different organizational units which have to pursue both their business objectives and their information security objectives. It should be noted that this is not a 'relativistic' stance ("anything goes") but a 'pluralistic' one (different perspectives from which to consider a phenomenon); as Bernstein recalls (2010), pragmatism in ethics and society supports pluralism.

The development of the Pragmatic Ethical Reasoning (PER) process is built on these five basic concepts. Other supportive notions, drawn from pragmatist literature, will be introduced along the description of the process. Given the importance of practice in pragmatism, we describe PER from the perspective of an actor (e. g. CIO, CISO, hereinafter referred to as PER Promoter) who, drawing on her theoretical background and experience, is engaged in designing and implementing an ECA based on the ISO 27001 process. As in all ISO standards, the process is based on the Deming cycle which is introduced and explained in the following section.

4 Knowledge and improvement as an iterative process in management practice: the Deming cycle

Deming's cycle (Deming 2000) is known in the business literature on quality management as the PDCA cycle or as the PDSA (Plan, Do, Study, Act) cycle (Sokovic, Pavletic, and Pipan 2010). As Moen and Norman (2006) have noted, Deming considered the term 'check'(which became extensively used) to be originated from a wrong translation into Japanese of his term 'study'. Here we use his original acronym (PDSA) both because it is present in all of his work and because it better emphasizes the 'learning' aspect of the cycle. In his words, the PDSA cycle is "the flow diagram for learning, and for improvement of a product or of a process" (Deming 2000, p. 131).

The PDSA cycle starts with an idea for improving a product or a process. In this planning stage (Plan), a number of goals are suggested and compared on their feasibility and on the expected gains in terms of knowledge or profit. In the following step (Do), a test, comparison, or experiment is executed, preferably on a small scale. The results are analyzed (Study) to see if they correspond with hopes and expectations and possible causes of failure are identified. Finally, decisions are made on whether to adopt/abandon the change (Act), or run through the cycle again, possibly under different environmental conditions, different materials, different people, different rules (ibid., pp122-3).

According to some authors, Deming has a pragmatic vein through the influence of C.I. Lewis (Moen and Norman 2006; Canard 2011) whereas other authors underscore that "Deming's energies … have not been expended to espouse or to verify theories… The purpose of Deming management method has been and continues to be the transformation and improvement of the practice of management…" (Anderson, Rungtusanatham, and Schroeder 1994, p. 473) It is beyond the scope of this paper to establish a direct philosophical affiliation of Deming; however, because of his highlighting experimentation and experience, Deming's approach harmonizes with two of the basic propositions of pragmatism mentioned above: the first (inquiry and experience are intertwined) and the fourth (principles are methods for action). It is indeed the recursive character of his approach to be aligned with the pragmatist viewpoint.

5 Principles of pragmatic ethical reasoning (PER) to design and implement an Ethically oriented Cybersecurity Approach (ECA)

Since inquiry in pragmatism has an iterative nature (Singer 2010, p. 484) and Deming's cycle also has a recursive character, in this section our presentation of the PER process refers both to the four phases of the PDSA cycle and to the clauses of the ISO 27001 standard, namely: the PLAN phase includes clauses 4 (context of the organization), 5 (leadership), 6 (planning), and 7 (support); the DO phase is clause 8 on 'operations'; the STUDY phase (the original Deming term for 'check') is the clause on 'performance evaluation'; and the ACT phase is clause 10 on 'improvement' (Kosutic 2014).

Each of the following sub-sections has two aims: (i) to situate the PER Promoter in a pragmatist perspective, that is to describe how this perspective affects her approach to relevant issues; (ii) to highlight the add-ons of the PER process to the ISO 27001 standard together with their practical implications (methods and artifacts) for the design and implementation of the ECA.

5.1 PER, phase 1: 'Plan' the ECA

Three activities are important in an ISO 27001 process for building and maintaining an effective Information Security Management System (ISMS): planning, support and operations (clauses 6, 7, and 8 respectively of the ISO directive). This sub-section shows the web of relations that has to be understood by the ECA Promoter for her to undertake successfully the first two activities necessary to carry out the 'Do' phase (operations) described in the following sub-section. 'Requirements' in ISO and 'principles' in PER are different but not separated. The former are standards to comply with because they are built on factors considered relevant by the information security practice. The latter leave more room for interpretation and are the backbone of the guidelines for actions in the different contexts of the organization.

In designing and developing artifacts to implant an ECA in (and for) a socio-technical context, the Promoter brings her own individual experience to bear. Pragmatist ethics privileges the actor's engagement with her design context. This perspective follows from the preeminence pragmatism attributes to experience over universal conceptions: experience improves conceptions. For classic and contemporary pragmatists, the way to convergence on new truths is by reasoned agreement through critical confrontation in the process of inquiry (Bernstein 2010, p.118). This inquiry process recalls Deming's observation in planning: "Somebody has an idea for improvement of a product or of a process. This is the 0-th stage, embedded in Step 1. It leads to a plan for a test, comparison, experiment" (Deming 2000, p. 122). Indeed, pragmatism does not completely overturn previous experience: on the contrary, it builds on it, it revises it in the light of 'surprises' (e.g. incidents). New ideas are adopted as true while preserving "the older stock of truths with a minimum of modification, stretching them just enough to make them admit the novelty, but conceiving that in ways as *familiar* as the case leaves possible." (James 1907, p. 60 emphasis added). The value of pragmatist conceptions is instrumental. "Beliefs, in short, are rules for action; and the whole function of thinking is but one step in the production of active habits" (James 2002, p.430). But because action based on rules-for-action nets new experience, pragmatism is iterative: "since belief is a rule for action, the application of which involves further doubt and further thought, at the same time that it is a stopping-place, it is also a new starting place for thought" (Peirce 2001, p. 199). Furthermore, as mentioned above in the section on the theoretical underpinnings, pragmatism attributes judgment-of-value to every action because it is performed only if it is considered to be worthwhile by the agent.

In pragmatist planning settings, understanding is the reciprocal effect of actions taken in the context. In terms of pragmatism, the planner (our Promoter) gains a situated understanding of the ethical principles as part of her experience in making judgments about her actions in a socio-technical context. In other words, experience and agency

are shaped by the interaction of the agent (the Promoter) and the planning context. Her actions not only change the context, they change her understanding and the ethical principles in use. An hermeneutic circle is at work here: the PER Promoter goes back and forth from the specific context to the ethical frameworks arising from preceding experience (especially significant incidents). But in this situation, the hermeneutic circle is finalized to ethical action in revising the relevant security strategy and procedures, and not just to acquire a deeper and deeper understanding of them, as in an interpretivist approach (Goldkuhl 2012).

The ethical understanding is only one component of the Promoter's broad pragmatic understanding of the socio-technical context. The ethical conduct of a Promoter is not only affected by her inclinations and background but also by the contextualized conditions for her project. Pragmatic ethics involve both deciding what actions to perform in the context and estimating the consequences of these actions. Both decisions and estimates are products of the agent's beliefs *and* values. The Promoter in the inquiry (planning) phase gains an understanding of how the context can revise her ethical perspective on both the means and the ends of her actions. The ethical elements in this understanding may extend to such outcomes as the ethical situation created for other actors in the socio-technical context. In terms of the outcomes of the planning actions that operationalize the ECA, there are two aspects that a pragmatist promoter-planner should consider relative to the ethical behavior of others in the organizational context: the existence of competing ideas and the interplay of assignments.

Competing ideas for 'planning' in a socio-technical context. The Promoter-planner does not work in isolation but interacts with other actors in a socio-technical context. This context can include clients, users, suppliers, sponsors, and other individuals working in her same team. When she intervenes in such a context through action, three classes of practice can compete as ethical frameworks for ideas. First, there will be the class of practices relating to the information security discipline. Second, there will be the class of practices that are defined by the context or organizational setting, e.g., system developer practices around the present information security artifacts. Third, there will be the class of practices defined by the users of the information systems that have to ensure confidentiality, integrity and availability, e.g., in the case of a health care system, medical practices. Practices are: "a web of actions that are related and combined in a meaningful way" (Goldkuhl, 2004, p. 17). They are made up of human actions, shared practical understandings within a common language, material objects or artefacts and ethical principles. Because these classes of practices may differ even within a single organization, they illustrate how ideas within the socio-technical context may compete in shaping and reshaping the ethics of pragmatist design and planning. In an ethical process of pragmatist planning, the foundation in principles such as those present in the code of ethics will interact contextually with other frameworks of ethical principles within the community around the design context. Ultimately the soundest ethical principles "should correspond with the actual feelings and demands of the community, whether right or wrong." (Holmes, quoted in Hantzis 1989, p 584). When this does not happen, problems in the application of any institutional code of ethics emerge (they become a mere window dressing exercise) and security management will suffer because of the gap between the declared values and the real conduct of individuals and groups.

Further, incidents are managed with greater uncertainty because the ethical *humus* that feeds the conduct during unexpected events is unknown. Further still, the 'scapegoating syndrome' is more likely to take place in order to "protect" the structure from questioning present procedures or top managers from questioning their own conduct or the way they manage their staff. We are underlining that a PER development process to build an ISMS has to take into account both the identification *and* the application of principles in order to solve dilemmas and orient real conducts. To this end, the planning phase has to consider what are the key aspects to make the organization become an 'ethical learning' organization.

Implications for organizing. According to ISO 27001, when planning the ISMS, the organization shall determine: (i) the risks and opportunities that need to be addressed (clause 6.1, p. 3); (ii) the information security objectives and how to achieve them ─ including resources, responsibilities, and evaluation of results (clause 6.2, p. 5). The design and planning of the ECA supports these objectives and develops its specific activities and tools. The main actions and artifacts proposed are the following:

Identification of the PER Promoter who collates internal and external information on security theory and practice and guides the interaction (critical confrontation on ethical issues) among the Organizational Units (OUs) to build the ECA.

Organizing the ECA teams. Different from Ethical Committees which are permanent and cross-functional, they are temporary and made up of the representatives of the 'communities': one per each function and organizational unit. Parallel to the definition of the opportunities/threats, ECA teams have a purposeful interaction with the Promoter and the information security units/experts to identify the 'threshold' of accountability of individuals and of the OUs concerning security in both prevention and response. One of the aims of this critical reasoning and confrontation is to define an appropriate mix of deterrence and motivation-based leverages. Supported by diffused leadership, the spreading of awareness and responsibility (on emerging ethical dilemmas for example) would increase resilience after incidents and favor the emergence of bottom-up innovative security practices.

Definition of the structure of the ethical action plan that will be prepared by each ECA team. Basically, it should contain three areas that describe: (i) the interpretation of the general ethical guiding principles of the organization applied to the specific activities conducted by the OU with the relevant implications for information security; (ii) the business objectives that the OU is pursuing together with the relevant information needs, dilemmas, and critical issues; (iii) the possible competence gaps in addressing security issues.

Outline of the architecture of a 'Consolidated Ethical Action Plan'. It combines the ethical action plans prepared by the ECA teams. The name underscores the importance of identifying an ethical "bottom line" for organizations interested in going beyond formal statements: an ethical action plan is an operationalized code of ethics.

5.2 PER, phase 2 and 3: 'Do' in the ECA and purposeful interactions in operations during the 'Study' phase

The organizational set up of a company that intends to go from business-as-usual to an ethically sustainable form of business conduct includes the arrangements between the different agents in carrying out their respective tasks and activities. These different agents may have different purposes in mind that motivate the conduct of the PER Promoter and the other actors implementing an ECA. As a result, the evaluation of the adequacy of an action in the implementation phase is a form of purposeful interaction between the actors involved in the identification and application of the principles adopted by the organization. However, these agents also interact with regard to deciding ethical values in light of potentially conflicting purposes. This interaction, which may be regulated by formal arrangements (i.e. the ECA teams and the Ethical Action Plans), means that the ethical meaning of a pragmatic outcome evolves during the intervention. The various actors in the socio-technical context interact in their evaluation of the research process and outcome. Thus, the ethical aspects of the socio-technical context may seem unstable as the design and the action research unfolds, and the pragmatist Promoter may find the ethical outcome less a product of principles and more a moving target of conflicting justice. This instability is why a 'consolidated ethical action plan' is provisional, an open system related to a time horizon: the forces that move it both internally (intra-organizational conflicts) and externally (market, regulatory frameworks, digital innovation, and the upsurge of critical events such as the present Covid-19 pandemic) may induce changes both in the structure and in the aims of the ECA.

Interplay of assignments: implications in terms of 'support' in both 'Do' and 'Study' phases. Since an ECA is an evolving process, specific care should be taken to find out 'who' decides 'what' and 'how' in the organization. That is, it is important to evaluate the organizational setting from the perspective of the allocation of power among the different agents. Design (or re-design) interventions may intentionally or inadvertently shift power relationship in the context (Markus 1983). As with competing ideas, there may be at least three power groups involved: the staff in charge of cybersecurity operations, IT developers, and users (other stakeholders may be added to the analysis as needed). While each of these groups will exercise certain kinds of power, the actions of each group in the socio-technical context can reshape the power of each of the other groups. The PER Promoter (who acts also as a designer and a facilitator) should be aware of the ongoing interplay in the assignment of power that arises from the re-design interventions needed: (i) to implement the ethical turn of the organization; (ii) to keep information systems of the organization abreast with continuing digital innovation. ECA teams are an important support for the (re-)design and implementation of the ECA: power assignments in a specific context should be ethical for that context and, through specific reasoning and confrontation, should converge towards the general ethical principles pursued by the organization.

5.3 PER, phase 4: 'Act' in the open ECA

Because PER is an iterative process the Act phase is the synthesis of what has been planned, critically understood and enacted: it is action research applied to information security (ethically oriented). Consider Figure 1 which concisely illustrates such a process. "Ethical principles" (top bubble to the left) are only the opening context for a PER

Promoter starting to work at an ethical re-orientation of cybersecurity governance (Plan phase). These principles are a combination of her personal beliefs and judgments of value with the ones that, in her perception, are implicitly or explicitly implanted in the security policy and in the organizational context of the company (organizational behavior in operations). As mentioned above, in pragmatism, complications in handling ethical issues have to be scouted and resolved or, at least, mitigated. Difficulties include appraising the intensity and solving the conflicts among principles that might arise in practical security situations (e.g. during or right after incidents). For example, understanding and negotiating the meaning of phrases such as 'severity of potential risks' or 'minimize negative consequences' (phrases taken from Myers & Venable 2014, p. 2) in the different contexts of the organization. The Promoter moves along the path described in Figure 1 while interacting with different components of the organization and making sense of the different ethical, professional, and business aims and interests of the different stakeholders.

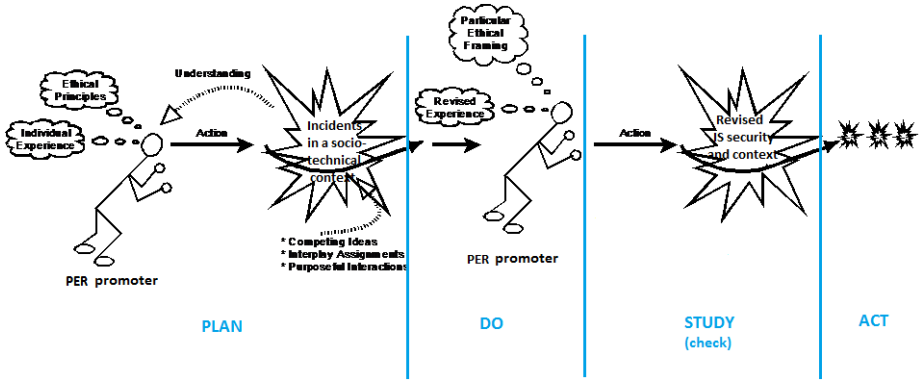

Fig. 1. The PER based ECA

6 Concluding remarks

Because of its anchors in Deming's quality cycles, ECA is quite a natural fit to cybersecurity actions oriented toward prevention of future incidents. In a preventative mode, it is an ethical learning cycle, oriented to cybersecurity, that revises IS security and its context. ECA has a relaxing fit with prevention because cycles span the time from incident-to-incident. However, ECA is a more important framework when applied within incident response, where the timeframe is much shorter. When an action is taken in response to an incident, another ECA cycle must revise experience and ethical framing (Do) in determining if the action resolved the incident ethically (Study). If not, further Act, Plan, and Do phases are to be undertaken to develop a better understanding of the interplay between the incident and the response action so that further actions can be planned to resolve the incident.

We can see that ECA as applied in incident response is a high speed PER cycle nested inside a slower-speed prevention PER cycle. Not dissimilar to Argyris and Schön's

double loop learning (1978), the rapid inner PER loop reflects learning about how to pragmatically respond to an incident, while the outer PER loop employs this learning in taking ethical actions to prevent a class of similar incidents from affecting the secured system in future. By applying PER to cybersecurity governance, we extend previous works on IS security theories for managing predictable and unpredictable threats (Baskerville, Spagnoletti, and Kim 2014). Moreover, PER can potentially contribute to the broader fields of High-Reliability Organizations and crisis management by providing a theoretical ground to develop theories on collective mindfulness (Fraher, Branicki, and Grint 2017), mindlessness (Salovaara, Lyytinen, and Penttinen 2019) and fragmented coordination (Wolbers, Boersma, and Groenewegen 2018)

Cybersecurity governance is a key priority of modern organizations. The paradoxical nature of cybersecurity limits the effectiveness of policymaking in this domain. Ethical dilemmas emerge at multiple levels when hierarchical structures of human and automated systems are implemented to control operational processes (Zuboff 2015). Effective cybersecurity governance and design cannot overlook the importance of ethical reasoning. An ethically oriented Cybersecurity Approach is proposed as a new way to design and manage cybersecurity operations. The philosophical underpinnings of pragmatism are discussed to present the model. Our conceptual analysis shows the applicability of the proposed model to cybersecurity design and governance.

Future research will explore how the PER based ECA approach can help address the several paradoxes and dilemmas that affect cybersecurity and that have been pointed out in the literature (de Bruijn and Janssen 2017). Empirical cases of ethical learning in cybersecurity practices will validate the ECA approach and offer guidance to cybersecurity professionals. For instance, with data breach notifications, companies can be damaged by making security problems visible; but such visibility is also necessary to create a greater sense of urgency and initiate action (Flak, Sæbø, and Spagnoletti 2019). Further, paradoxes trouble decision makers in organizations when deciding investments in cybersecurity: too little spending might indicate a lack of protection, while substantial spending might indicate a perceived high risk of attacks. Governments are to face privacy versus security adjustments as they decide to access data of individuals and organizations for prevention purposes. Further, the orientation of governments on these questions also depends on how experts, practitioners and advisors to governments conceive digital technologies (Depaoli, Sorrentino, and De Marco 2020): for some authors this technology is considered just a powerful tool to improve efficiency for the entire set of government interactions with citizens and relevant policies thereof (Hood and Margetts 2007); for others there is a transformative processing power of digitalization which is changing the very fabric of policy setting and making (Hildebrandt 2015). The purpose of successive explorations is therefore needed to further develop the potential of connecting ethical reasoning with organizational learning in the making of cybersecurity. Coping with paradoxes and dilemmas should thus become more explicit and manageable.

References

Adams, J. S., A. Tashchian, and T. H. Shore. 2001. “Codes of Ethics as Signals for Ethical Behavior.” *Journal of Business Ethics* 29 (3): 199–211.

Anderson, John C., Manus Rungtusanatham, and Roger G. Schroeder. 1994. “A Theory of Quality Management Underlying the Deming Management Method.” *Academy of Management Review* 19 (3): 472–509.

Argyris, C., and D. Schön. 1978. *Organizational Learning: A Theory of Action Perspective.* Reading: Addison-Wesley.

Baskerville, R. 2005. “Information Warfare: A Comparative Framework for Business Information Security.” *Journal of Information System Security* 1 (1): 23–50.

Baskerville, R., F. Rowe, and F. C. Wolff. 2018. “Integration of Information Systems and Cybersecurity Countermeasures.” *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 49 (1): 33–52.

Baskerville, R., P. Spagnoletti, and J. Kim. 2014. “Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response.” *Information and Management* 51 (1): 138–51.

Bernstein, Richard J. 2010. *The Pragmatic Turn*. Polity.

Bruijn, Hans de, and Marijn Janssen. 2017. “Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies.” *Government Information Quarterly* 34 (1): 1–7.

Canard, Frédéric. 2011. “W . E . DEMING, Pragmatism and Sustainability.” In *17th Annual International Deming Research Seminar*, 1–17. New York, USA: HAL archives-ouvertes.

D’Arcy, John, and Anat Hovav. 2009. “Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures.” *Journal of Business Ethics* 89 (SUPPL. 1): 59–71.

Deming, W. Edwards. 2000. “The New Economics.” *MIT Press*, 235.

Depaoli, P., M. Sorrentino, and M. De Marco. 2020. “Social and Ethical Shifts in the Digital Age: Digital Technologies for Governing or Digital Technologies That Govern?” In *Digital Transformation and Human Behavior - Innovation for People and Organizations*, edited by C. Metallo, M. Ferrara, A. Lazazzara, and S Za. Springer Berlin Heidelberg.

Dewey, John. 1897. *The Study of Ethics: A Syllabus.* Ann Arbor, Mich: Georg Wahr.

Flak, L. S., Ø. Sæbø, and P. Spagnoletti. 2019. “Privacy Violations in Light of Digital Transformation: Insights from Data Breaches in Norway.” In *Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy*, 1–7. Munich, Germany.

Fraher, A. L., L. J. Branicki, and K. Grint. 2017. “Mindfulness in Action: Discovering How US Navy Seals Build Capacity for Mindfulness in High-Reliability Organizations (HROs).” *Academy of Management Discoveries, , .* 3 (3): 239–61.

Garcia-Sanchez, Isabel -Maria, Luis Rodriguez-Dominguez, and José Valeriano Frias-Aceituno. 2015. “Board of Directors and Ethics Codes in Different Corporate Governance Systems.” *Journal of Business Ethics* 131 (3): 681–98.

Goldkuhl, Göran. 2012. “Pragmatism vs Interpretivism in Qualitative Information Systems Research.” *European Journal of Information Systems* 21 (2): 135–46.

Harrington, S.J. Susan J. 1996. “The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions.” *MISQ* 20 (3): 257–78.

Hildebrandt, Mireille. 2015. *Smart Technologies and the End (s) of Law: Novel Entanglements of Law and Technology.* Edward Elgar Publishing.

Hill, Ronald Paul, and Justine M. Rapp. 2014. “Codes of Ethical Conduct: A Bottom-Up Approach.” *Journal of Business Ethics* 123 (4): 621–30.

Hood, Christopher, and Helen Margetts. 2007. *The Tools of Government in the Digital Age.* Macmillan International Higher Education.

James, William. 1907. *Pragmatism: A New Name for Some Old Ways of Thinking*. London: Longmans Green and Co. http://catalog.hathitrust.org/Record/001382943.

———. 2002. *The Varieties of Religious Experience - A Study in Human Nature*. Edited by Jim Manis. Hazelton, PA: The Electronic Classics Series.

Kaptein, Muel. 2011. “Toward Effective Codes: Testing the Relationship with Unethical Behavior.” *Journal of Business Ethics* 99 (2): 233–51.

Kosutic, Dejan. 2014. “Has the PDCA Cycle Been Removed from the New ISO Standards?” 27001 Academy, The ISO 27001 & ISO 22301 Blog. 2014. https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/.

Long, Brad S, and Cathy Driscoll. 2008. “Codes of Ethics and the Pursuit of Organizational Legitimacy: Theoretical and Empirical Contributions.” *Journal of Business Ethics* 77 (2): 173–89.

Markus, M. Lynne. 1983. “Power, Politics, and MIS Implementation.” *Communications of the ACM* 26 (6): 430–44.

Moen, Ronald, and Clifford Norman. 2006. “Evolution of the PDCA Cycle.” Available from https://rauterberg.employee.id.tue.nl/lecturenotes/DG000%20DRP-R/references/Moen-Norman-2009.pdf.

Myers, Michael D., and John R. Venable. 2014. “A Set of Ethical Principles for Design Science Research in Information Systems.” *Information Management* 51 (6): 801–9.

Ormerod, R. 2006. “The History and Ideas of Pragmatism.” *Journal of the Operational Research Society* 57 (8): 892–909.

Peirce, C.S. 2001. “How to Make Our Ideas Clear.” In *The Nature of Truth: Classic and Contemporary Perspectives*, edited by M.P. Lynch, 193–209. Cambridge, Mass: The MIT Press.

Ruighaver, A. B., S. B. Maynard, and M. Warren. 2010. “Ethical Decision Making: Improving the Quality of Acceptable Use Policies.” *Computers and Security* 29 (7): 731–36.

Salovaara, A., K. Lyytinen, and E. Penttinen. 2019. “High Reliability in Digital Organizing: Mindlessness, the Frame Problem, and Digital Operations.” *MIS Quarterly: Management Information Systems* 43 (2): 555–78.

Singer, Alan E. 2010. “Integrating Ethics and Strategy: A Pragmatic Approach.” *Journal of Business Ethics* 92 (4): 479–91.

Siponen, Micco, and Anthony Vance. 2010. “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations.” *MIS Quarterly* 34 (3): 487–502.

Sokovic, M, D Pavletic, and Kk Pipan. 2010. “Quality Improvement Methodologies–PDCA Cycle, RADAR Matrix, DMAIC and DFSS.” *Journal of Achievements in Journal of Achievements in Materials and Manufacturing Engineering* 43 (1): 476–83.

Spagnoletti, P., and A. Resca. 2008. “The Duality of Information Security Management: Fighting against Predictable and Unpredictable Threats.” *Journal of Information System Security* 4 (3): 46–62.

Spears, Janine L., and Henri Barki. 2010. “User Participation in Information Systems Security Risk Management.” *MIS Quarterly* 34 (3): 503–22.

Ulrich, W. 2016. “Philosophy for Professionals: Towards Critical Pragmatism. Rev. Version of 20 March 2016. Reflections on Critical Pragmatism, Part 7. (Orig. Version in: Journal of the Operational Research Society, 58, No. 8, 2007, Pp. 1109-1113).” Ulrich’s Bimonthly. 2016.

Velthouse, Betty, and Yener Kandogan. 2007. “Ethics in Practice : What Are Really Doing ?” 70 (2): 151–63.

Wolbers, J., K. Boersma, and P. Groenewegen. 2018. “Introducing a Fragmentation Perspective on Coordination in Crisis Management.” *Organization Studies* 39 (11): 1521–1546.

Zuboff, Shoshana. 2015. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30 (1): 75–89.